Tecnológico de Costa Rica
Escuela de Ingeniería en Computación
Maestría en Computación con énfasis en Ciencias de la Computación

Especificación, diseño y simulación de un sistema de Criptodivisa con incentivos para la promoción de la Economía Circular

Tesis sometida a consideración del Departamento de Computación
para optar por el grado de *Magíster Scientiae* en Computación
con énfasis en Ciencias de la Computación

Wilberth Castro Fuentes

José Castro Mora
Profesor asesor

Cartago, Costa Rica
5 de noviembre de 2021

Instituto Tecnológico de Costa Rica
Escuela de Computación
Unidad de Posgrado

ACTA DE APROBACION DE TESIS

ESPECIFICACIÓN, DISEÑO Y SIMULACIÓN DE UN SISTEMA DE CRIPTODIVISA CON INCENTIVOS PARA LA PROMOCIÓN DE LA ECONOMÍA CIRCULAR

Por: Wilberth Castro Fuentes

TRIBUNAL EXAMINADOR

Dr. José Castro Mora
Profesor Asesor

Ing. Ignacio Trejos Zelaya, MSc.
Profesor Lector

Ing. Alberto Villalobos Sánchez, MAE
Lector Externo

Dra. Ing. Lilliana Sancho Chavarría
Coordinadora
Unidad de Posgrado, Escuela de Computación

26 de noviembre, 2021

Dedicatoria

A mi familia y a mis amigos, por la paciencia que me han tenido durante este tiempo.

Agradecimientos

A mi profesor tutor, José Castro Mora, y a mis lectores, Ignacio Trejos Zelaya y Alberto Villalobos Sánchez, a cada uno, por su invaluable guía en el desarrollo de esta investigación.

Prólogo

Si bien la tendencia a una progresiva asimilación de una consciencia ecológica se ha hecho patentemente manifiesta en los últimos años (ya sea por una implantación ideológica o por una auténtica preocupación medioambiental), es posible observar que quizá no se presta una real disposición política o los esfuerzos no son suficientes, aun cuando parece incluir disciplinas tan diversas —y en apariencia tan dispares— como la computación, la psicología o la economía. Es por ello que no ha de sorprendernos que más temprano que tarde se emprendieran investigaciones académicas que plasmaran propuestas de intervención multidisciplinaria cuya pretensión fuera la de tomar lo mejor de cada una de ellas y así contribuir con un método de investigación que permita abordar formal y científicamente la problemática medioambiental. De esta forma, aun cuando pertenecen a categorías particulares, conceptos abstractos como la conducta o el mercado pueden articularse formalmente a través de lenguajes informáticos sofisticados y orientarse a una meta específica como, en este caso, la reducción o eliminación del desperdicio de los recursos en una cadena de suministros a partir de una logística circular por medio de la utilización de mecanismos de incentivos no tan diferentes a las técnicas de modificación de conducta, como lo serían el condicionamiento de recompensa o el reforzamiento positivo, utilizados en intervención clínica por especialistas en psicológica conductual o cognitiva, disciplinas que se engloban dentro de un conjunto de enfoques teóricos con características estandarizadas bajo una misma denominación, en la que el punto de partida es la conducta como objeto de intervención, donde se enfatiza su relación con la cognición y el entorno y en donde la meta es la modificación o eliminación de comportamientos desadaptativos, reemplazándolos por adaptativos, de tal forma que se repiten si son premiados o se extinguen si no, siempre que esta intervención vaya produciendo cambios conductuales observables y medibles, procurando una evaluación objetiva y cuantificable, de forma tal que el criterio de su eficacia esté en la posibilidad de registro de los cambios producidos en las conductas. Todo lo anterior permite responder anticipadamente a cualquier posible refutación pretendidamente ética que ponga en cuestionamiento una hipotética manipulación de las decisiones de los participantes, especialmente considerando que si bien la pertinencia de la hipótesis se calcula con base en el resultado de simulaciones del comportamiento de agentes racionales, los experimentos de modificación de conducta con individuos humanos para entornos sociales también son comunes en la implementación de intervenciones psicológicas en ambientes clínicos, sociales, laborales o industriales.

—Fabián Alpízar Arce

Índice general

1

Introducción

Sinopsis. Este libro documenta una tesis desarrollada para obtener el grado de Maestría en Computación con Énfasis en Ciencias de la Computación, y su definición como proyecto de investigación. El objetivo general de este trabajo es diseñar un mecanismo de incentivos, de alcance global, que acelere la transición hacia una economía circular. El mecanismo que hemos diseñado está construido sobre un modelo de juego en forma normal, y debe ser soportado por el protocolo de consenso de un sistema de criptodivisa. La implementación del mecanismo de incentivos requiere de la definición de al menos un modelo de negocio circular, por lo que, como parte de este trabajo, hemos definido un modelo de negocio con configuración circular y, para este, hemos propuesto un criterio de circularidad que, mediante el lenguaje de un autómata finito, facilita el reconocimiento de las transacciones producidas por la actividad económica de las cadenas de suministro afines al modelo de negocio. Este trabajo también incluye un análisis estadístico del efecto del mecanismo de incentivos, que parte de los resultados de dos series de experimentos, y una descripción de un sistema de simulación, que permite recopilar los datos necesarios para el análisis estadístico.

Palabras clave. Economía Circular, Cadena de Bloques, Economía de Tokens, Bitcoin, Teoría de Juegos, Sistemas Dinámicos, Teoría de Autómatas, Métodos Formales, Cadena de Suministro.

Abstract. This book documents a thesis developed to obtain a Master's degree in Computing with an Emphasis in Computer Science, and its definition as a research project. The general objective of this work is to design an incentive mechanism, with global scope, that accelerates the transition towards a circular economy. The mechanism we have designed is built on a game model in normal form, and must be supported by the consensus protocol of a cryptocurrency system. The incentive mechanism implementation requires the definition of at least one circular business model, therefore, as part of this work, we have defined a business model with circular configuration and, for this, we have proposed a circularity criteria that, by the language of a finite automaton, makes it easy the recognition of transactions produced by the economic activity of the supply chains related to the business model. This work also includes a statistical analysis of the effect of the incentive mechanism, based on the results of two series of experiments, and a description of a simulation system, which allows to collect the data necessary for statistical analysis.

Keywords. Circular Economy, Blockchain, Token Economics, Bitcoin, Game Theory, Dynamical Systems, Automata Theory, Formal Methods, Supply Chain.

1.1. Antecedentes

En Costa Rica, a pesar de los avances en materia ambiental, el consumo de recursos es insostenible. Esta situación se evidencia en la creciente brecha que presenta el país entre el consumo de recursos naturales y la capacidad del territorio para proveerlos, una brecha del 57,9 %, según la más reciente medición de la huella ecológica, con datos de 2 016 [1].

En la década de 1 970 aparece el término "Economía Circular" (*Circular Economy*, CE) [2]. En esa década, el término fue utilizado para describir a cualquier mercado en el que la dinámica de la economía tendiera a ser "cíclica", en el que la dinámica promoviera el reciclaje, la reutilización de recursos, y la reducción del desperdicio [2]. El término se refiere a un paradigma que propone que el sistema económico funcione como un ecosistema, un sistema en el que los residuos de un proceso sean los insumos de otro [2]. Claramente, este no es el funcionamiento de nuestra economía, una economía "lineal", en la que tradicionalmente cada uno "adquiere, consume y desecha" [2]. En contraste, una economía circular sería una economía de alto rendimiento, con énfasis en la oferta de servicios [2]. El paradigma de la Economía Circular retoma viejas iniciativas, como la de *Cradle to Cradle*, la de "Reducir, Reutilizar y Reciclar" —3R—, la de la ecología industrial, y también retoma prácticas como las de la producción biomimética [2].

El sistema monetario actual promueve cualquier tipo de actividad económica, independientemente del impacto ecológico de la actividad, por lo que para transicionar hacia una economía regenerativa, en términos ambientales, puede ser conveniente utilizar otra forma de dinero, una forma de dinero que capture e incorpore el valor del capital natural [3]. Según Mike Goldin, "con la tecnología Blockchain hemos conseguido dinero programable, al programar dinero podemos programar incentivos, y al programar incentivos podemos programar personas" [4], esto nos invita a considerar que el dinero podría ser utilizado como una herramienta de organización social.

La proliferación de *pooles* de minería, i.e., granjas de servidores que se dedican al mantenimiento de una criptodivisa[1], evidencia que es posible modificar la dinámica de un sistema económico mediante la oferta de una criptodivisa que implemente un mecanismo de incentivos. Uno de los objetivos de este trabajo es acelerar la transición hacia una economía circular, para alcanzarlo, este trabajo incluye el diseño de un mecanismo de incentivos que puede ser implementado como parte del protocolo de consenso de un sistema de criptodivisa.

En Costa Rica, en abril del 2 018, fue liberada una plataforma tecnológica, una plataforma que permite disponer de "ecomonedas" virtuales, ecomonedas denominadas *ecoins* [5], para esto la plataforma permite implementar un sistema centralizado parecido a un sistema de puntos. Un *ecoin* puede ser interpretado como un tiquete de descuento, y es posible obtenerlos en "centros de valorización", a cambio de materiales reciclables. Hasta el año 2 021, el sistema ha sido implementado en Costa Rica, en Panamá, y en Perú [5].

La administración exitosa de cualquier sistema centralizado requiere de confianza, por parte de la comunidad de usuarios, en la organización que administra el sistema. La centralización facilita la concentración de la riqueza, y la violación de la privacidad, entre otras formas de violación de la seguridad, en términos generales, facilita el desalineamiento de incentivos. La tecnología de cadena de bloques, por el contrario, es descentralizada, y además es transparente[2], por esto hemos decidido considerar a esta tecnología el punto de partida en el diseño de nuestra propuesta.

Nuestro mecanismo de incentivos debe reconocer, y remunerar, la contribución de cada

[1] En el diccionario de Cambridge, el término "Criptodivisa" se refiere a cualquier moneda digital mantenida por el público en lugar de un gobierno, y que, mediante herramientas criptográficas, garantiza la seguridad de cada transacción.

[2] Paradójicamente, en el 2 018, más del 50 % de la potencia de cómputo en la comunidad de Bitcoin fue controlada por ocho granjas de minería, y más del 50 % de la potencia de cómputo en la comunidad de Ethereum fue controlada por cinco granjas de minería [6].

transacción a la "circularización" de la economía, esto para promover el alineamiento, tanto como sea posible, del comportamiento de cada consumidor con lo que sería su comportamiento en una economía circular, y así ofrecer una alternativa que pueda contrarrestar el crecimiento de la brecha entre el consumo de los recursos naturales y su disponibilidad.

Con lo anterior, intentamos introducir al lector en el tema, así como compartir nuestras ideas y nuestra percepción sobre la importancia de este trabajo. La sección 1.2, del marco teórico contiene un extracto de la literatura académica relacionada, y la sección 1.3, explora la problemática y establece la hipótesis de la investigación.

1.2. Marco teórico

Esta sección incluye contenidos que hemos extraído de artículos y revisiones de literatura[3]. Estos contenidos constituyen nuestra visión del estado del arte, de aquí partimos en el desarrollo de los siguientes capítulos.

1.2.1. Economía Circular

Llamamos "Economía Circular" a un nuevo paradigma económico, en el que, por diseño, la producción industrial es restaurativa y regenerativa. El paradigma exige que la vida útil de los recursos sea cíclica, que se descarte el uso de energías no renovables y de productos de difícil retorno a la biosfera, y que se elimine el desperdicio, todo esto a través del diseño estratégico de materiales, productos, sistemas y modelos de negocio.

La figura 1.1 ilustra la dinámica que propone el paradigma. En primer lugar, los productos deben ser diseñados y optimizados para ser desensamblados y reutilizados al final del ciclo de vida, sin generar residuos, mediante procesos que requieran un consumo energético mínimo, y una mano de obra también mínima, en esto difiere del reciclaje tradicional. En segundo lugar, los recursos pueden ser perecederos o no perecederos. Los perecederos deben ser de constitución biológica, o al menos no tóxica, para que puedan ser reabsorbidos por la biosfera de manera segura. Los no perecederos, como los metales y la mayoría de los plásticos, claramente no pueden ser reabsorbidos por la biosfera, por lo que estos deben ser diseñados para ser reutilizados, o actualizados, como en el caso de los dispositivos tecnológicos. En tercer lugar, la energía consumida debe ser renovable, para facilitar la recuperación de los sistemas naturales.

1.2.2. Configuraciones circulares de cadena de suministro

En general, en las cadenas de suministro que operan en mercados circulares, los componentes o materiales que son invertidos en la producción, son recuperados al final del ciclo de vida, esto permite no solo contrarrestar el crecimiento de la brecha entre el consumo de los recursos naturales y su disponibilidad, también permite reducir la inversión en materia prima. En la revisión de literatura de Masi *et al.* sobre configuraciones de cadenas de suministro circulares, los autores identifican tres distintas configuraciones: parques ecoindustriales, cadenas de suministro sostenibles y cadenas de suministro cíclicas [11].

[3]La sección 1.2.1, sobre Economía Circular, está basada en el artículo "Hacia la Economía Circular, Acelerando la transición a través de las cadenas de suministro" de la Fundación Ellen MacArthur [7], la sección 1.2.6, sobre Teoría de juegos, está basada en el libro de texto "Sistemas multiagente: Fundamentos algorítmicos, lógicos, y de teoría de juegos" [8] de Shoham y Leyton-Brown, la sección 1.2.3, sobre Blockchain, está basada en la revisión de literatura de Ferdous *et al.* [9], la sección 1.2.4, sobre consenso en las cadenas de bloques, está basada en la revisión de literatura de Xiao *et al.* [6], la sección 1.2.7, sobre métodos formales, está basada en el libro "Usando Z, Especificación, Refinamiento y Demostraciones" de Woodcock y Davies [10]. Hemos traducido el título de cada publicación para mantener el idioma del texto, el título original se encuentra en la bibliografía.

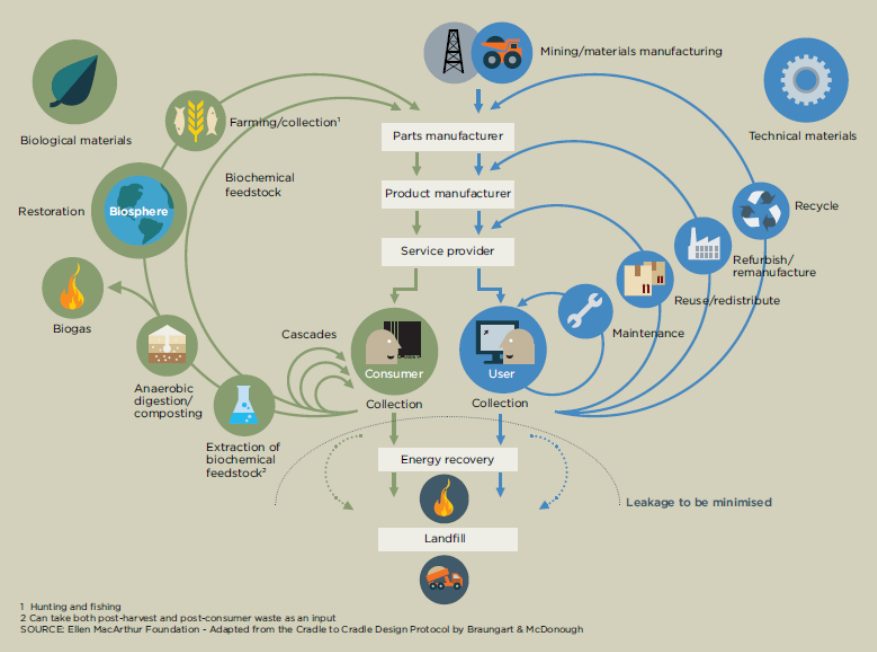

Figura 1.1: Economía Circular: un sistema industrial restaurativo por diseño [7].

Parques ecoindustriales

Los parques ecoindustriales implementan los principios de la Ecología Industrial, contienen, dentro de sus límites geográficos, un conjunto de empresas en las que, por coherencia con los principios de la Ecología Industrial, la administración promueve el uso compartido de la infraestructura, y el tratamiento sostenible de los subproductos y de los desechos. Esto resulta en el establecimiento de relaciones “simbióticas” entre las empresas participantes, lo que facilita un mejor aprovechamiento de los recursos, como energía, agua y materias primas, y deriva en una producción más “limpia”, que reduce la contaminación industrial, incluso por desechos peligrosos o tóxicos. Algunas empresas en estos parques están dedicadas exclusivamente a la gestión de residuos.

Cadenas de suministro sostenibles

En las empresas que componen las cadenas de suministro sostenibles, la administración promueve un consumo de recursos tal que el desperdicio generado en cada procedimiento sea el mínimo, en procedimientos como los de logística, los de almacenamiento, y los de embalaje y compra, mediante la reducción, la reutilización, y el reciclaje (3R) de materiales, a esto le denominan “consumo ecológico”. Además, la administración implementa políticas internas de gestión ambiental, y de cooperación con otras administraciones.

Cadenas de suministro circulares —*Closed-loop* SC—

Son conocidas también como sistemas, o flujos de material, circulares. Así como en las empresas en los parques ecoindustriales, la administración de las cadenas de suministro circulares promueve el tratamiento sostenible de los subproductos y de los desechos, pero, además, en las cadenas circulares, el consumidor es considerado parte de la cadena. En

algunas de estas cadenas hay más de un proveedor del mismo tipo de recurso, y en todas, el objetivo principal consiste en la reducción, la reutilización, y el reciclaje de materiales, para esto, la administración normalmente implementa procedimientos de logística inversa[4], y operaciones de diversificación en mercados secundarios.

La aplicación de esta configuración requiere de nuevos modelos de negocio, y de técnicas de diseño, que promuevan la integridad, la actualización, la reparación, la restauración, la remanufacturación, y el reciclaje de los recursos; en otras palabras, es necesario evitar la obsolescencia y la degradación de los recursos. Estos modelos, y técnicas, pueden ser biomiméticas, o de diseño ecológico. Un ejemplo de modelo es el modelo de topología de red para las cadenas de suministro. Un ejemplo de diseño es el diseño de productos como servicios —*Product-Service Systems*—. En cualquier caso, el retorno de la inversión en materiales, o energía, no necesariamente es inmediato.

1.2.3. Blockchain

Un *blockchain*, o cadena de bloques, es una base de datos de arquitectura descentralizada, que consta de una secuencia de bloques enlazados, en la que cada bloque contiene una serie de transacciones. Cada cierto tiempo, un nuevo bloque es agregado a la cadena[5], el protocolo de consenso, implementado por el sistema distribuido, determina la duración de este tiempo. La siguiente lista describe las seis propiedades que cualquier protocolo de consenso debe exhibir para garantizar la integridad de la cadena de bloques.

Propiedades

1. *Consistencia del estado de la cadena.* Corresponde a la capacidad para lograr un consenso distribuido sobre el estado de la cadena, esta propiedad evita la dependencia de una tercera entidad de confianza.

2. *Inmutabilidad e irreversibilidad del estado de la cadena.* Cada transacción es irreversible, por lo que cada bloque es inmutable, esto se logra, al menos después de cierto tiempo de que el bloque es aceptado. Sin embargo, para que esto sea posible, el protocolo requiere la participación de un gran número de nodos[6]. Esto también permite que los contratos inteligentes sean inmutables[7] y que mediante estos sea posible el despliegue y la ejecución de programas, también inmutables.

3. *Persistencia de los datos.* Idealmente, cada bloque es almacenado en cada nodo de la red [12], si el número de nodos participantes es lo suficientemente alto, la persistencia de los datos está garantizada.

4. *Documentación de la procedencia de los datos.* Cada transacción que haya sido aceptada en la cadena de bloques debe estar firmada mediante criptografía de clave pública, la autenticidad de cada transacción está garantizada por la firma digital en tal transacción.

5. *Control de datos distribuido.* Corresponde a la capacidad de almacenamiento, y a la capacidad de recuperación de los datos almacenados, garantizadas por el protocolo de consenso.

[4] En el diccionario de Cambridge, el término "Logística inversa" se refiere a cualquier procedimiento mediante el que cualquier recurso pueda ser devuelto, del consumidor, al productor.

[5] Cada nueva transacción es transmitida de punto a punto; idealmente, cada bloque debe ser almacenado en cada dispositivo que esté conectado a la red. Cada bloque es identificado con un hash generado a partir del contenido del bloque, que incluye el hash del bloque anterior, cada bloque queda enlazado al bloque anterior [12].

[6] En cualquier cadena de bloques, un "nodo" es cualquier dispositivo tecnológico mediante el que cualquier agente interactúe en la comunidad subyacente a la cadena de bloques.

[7] Un contrato inteligente es un script transaccional, compuesto por un conjunto de cláusulas, y preparado para que estas sean ejecutadas automáticamente [12].

6. *Transparencia.* El estado de la cadena de bloques, así como cualquier transacción que haya sido aceptada, puede ser verificado por cualquier usuario con acceso a la cadena de bloques; por lo tanto, cualquier cadena de bloques garantiza la transparencia, y como consecuencia, promueve la responsabilidad.

Tipos de cadenas de bloques

Hay dos tipos de cadena de bloques predominantes, el de las cadenas de bloques públicas y el de las cadenas de bloques privadas. El tipo de cadena de bloques depende del dominio de aplicación para el que se implemente.

Cadena de bloques pública. En una cadena de bloques pública, cualquier usuario puede producir y verificar bloques, así como modificar el estado de la cadena al efectuar transacciones. Esto significa que, en una cadena de bloques pública, cada transacción es accesible para cualquiera. Esto puede ser contraproducente en escenarios en los que se deba preservar la privacidad de las transacciones.

Cadena de bloques privada. En una cadena de bloques privada, no cualquier usuario puede producir y verificar bloques, o efectuar transacciones, en los dos casos, el usuario debe estar autorizado, por lo tanto, este tipo de cadena de bloques es el adecuado en escenarios en los que se deba preservar la privacidad de las transacciones.

Capas de las cadenas de bloques

Un sistema distribuido de cadena de bloques está constituido por componentes con funciones muy variadas, como recopilar transacciones, propagar bloques, minar, alcanzar el consenso, entre otras. Ferdous *et al.* las han agrupado en cuatro capas, según su función.

1. La *capa de red* es la que incluye a los componentes con funciones como conectar con la red subyacente, permanecer en la red (seguir el protocolo), propagar y recibir transacciones, propagar y recibir bloques, entre otras.

2. La *capa de consenso* es la que implementa las propiedades que exige el protocolo de consenso, en esta capa se determina el orden de los bloques.

3. La *capa de aplicación* es la que permite la interpretación de los datos en la cadena de bloques tal como lo requiera el dominio de aplicación.

4. La *capa de meta-aplicación* es la que facilita la interpretación de los datos en la cadena de bloques para aplicaciones complementarias, a esta capa Ferdous *et al.* también la identifican como “capa semántica”.

1.2.4. Consenso en las cadenas de bloques

En cualquier red subyacente a una cadena de bloques, cada participante puede ser tanto un cliente, al emitir una transacción, como un servidor, al verificarla. La estructura de datos de cualquier cadena de bloques consta de una serie de bloques ordenada cronológicamente, en la que cada bloque está enlazado al anterior mediante un hash. Cada bloque contiene un paquete de transacciones válidas y consistentes entre sí. Una transacción puede considerarse un registro público, el registro de una transferencia de un valor. El objetivo de un protocolo de consenso es garantizar que cada uno de los nodos participantes esté de acuerdo con

un historial de transacciones. Xiao *et al.* identifican los componentes en el cuadro 1.1, de cualquier protocolo de consenso, y definen una serie de requisitos para cualquiera de estos protocolos.

Cuadro 1.1: Componentes de un protocolo de consenso.

Componente	Propósito
Proposición del nuevo bloque	Generar el nuevo bloque, junto con la prueba de trabajo o de participación correspondiente.
Propagación de la información	Difundir los bloques a través de la red.
Verificación del último bloque recibido	Verificar las pruebas y las transacciones en el último bloque recibido.
Finalización del último bloque recibido	Aceptar, en consenso, el último bloque recibido.
Mecanismo de incentivos	Emitir moneda y promover la participación honesta.

Requisitos del consenso

- *Terminación.* En cada nodo confiable[8], cualquier nueva transacción debe poder ser descartada o aceptada en la cadena de bloques, dentro de un bloque.
- *Acuerdo.* Cada nueva transacción, y el bloque que la contiene, deben ser aceptados por todos los nodos confiables, o descartados por todos los nodos confiables. Cada nodo confiable debe asignar el mismo número de secuencia a un bloque aceptado.
- *Validez.* Cualquier nodo que reciba un bloque válido, debe aceptarlo.
- *Integridad.* En cada nodo confiable, cada transacción aceptada debe ser coherente con el resto. La cadena de bloques debe estar ordenada cronológicamente, y cada bloque debe estar enlazado al bloque anterior mediante un hash.

El protocolo de consenso de Nakamoto

Cada vez que un agente recibe y verifica un nuevo bloque, el agente lo anuncia a los demás, de los cuales, cada uno solicita el bloque si este extiende su cadena local. Cada agente, al recibirlo, lo verifica, y así el bloque puede ser propagado por toda la red. Al recibir un bloque, cada agente puede aceptarlo o puede descartarlo para incluirlo en su cadena de bloques local, después de aceptarlo también puede descartarlo, pero la probabilidad de que esto suceda, con el tiempo, disminuye exponencialmente. Los componentes en el cuadro 1.1, para el protocolo de consenso de Nakamoto en particular, corresponden a los siguientes.

- *Prueba de trabajo —Proof-of-Work, PoW—.* Cada bloque debe incluir su solución de la prueba de trabajo, esto permite, mediante una función hash, verificar el nivel de dificultad del procedimiento de generación del bloque, en otras palabras, la prueba de trabajo garantiza que el periodo de tiempo que tarda la generación de cada bloque sea de 10 minutos, aproximadamente.
- *Regla de difusión.* Cada agente, al generar un bloque, o recibirlo, debe anunciarlo inmediatamente, y debe transmitirlo a cualquier agente que lo solicite. Cada agente también, al efectuar una transacción, o recibirla, debe transmitirla a los otros agentes.

[8] En cualquier cadena de bloques, un nodo "confiable" es cualquier nodo que no sea operado con la intención de dirigir un ataque cualquiera en la red subyacente a la cadena de bloques.

- *Regla de verificación.* Cada agente, antes de transmitir un bloque, o agregarlo a su cadena local, debe verificar la coherencia de las transacciones que contiene, y debe verificar su solución de la prueba de trabajo. Cada agente también, al recibir una transacción, debe verificarla.
- *Regla de la cadena más larga.* En caso de bifurcaciones, la cadena más larga sería la cadena correcta, por consenso.
- *Retribución por la generación del bloque y comisión por transacción.* Cada agente, al construir un bloque, puede incluir en el bloque una transacción denominada "transacción base", que emite una cierta cantidad de moneda y la deposita en la cuenta del agente, junto con la comisión por cada transacción que haya incluido en el bloque.

El periodo de tiempo que tarda la generación de cada bloque se logra mantener en 10 minutos, aproximadamente, ajustando la dificultad del procedimiento de generación cada 2 016 bloques, esto permite que cada bloque sea propagado lo suficiente antes de que se transmita el siguiente. Sin embargo, en caso de bifurcaciones, la regla de la cadena más larga permite solucionar la bifurcación.

La prueba de trabajo funciona como medida de seguridad ante los ataques sybil[9], ya que la solución de la prueba de trabajo requiere de una inversión real en recursos, y la regla de la cadena más larga, en caso de bifurcaciones, exigiría que la cadena en la que se ha invertido más, sea la cadena correcta. La remuneración por la generación del bloque y la comisión por transacción también promueven la minería[10] honesta, y la remuneración por la generación del bloque facilita la emisión de nueva moneda.

El despliegue del Bitcoin ha evidenciado las virtudes del protocolo de consenso de Nakamoto, sin embargo, el protocolo tiene debilidades. (1) En términos de rendimiento, el costo de la seguridad es muy alto, por ejemplo, la comunidad de Bitcoin procesa, en promedio, 7 transacciones por segundo, mientras que VISA procesa, en promedio, 2 500 transacciones por segundo. (2) En términos energéticos, la red sería ineficiente, ya que cualquier protocolo que exija la prueba de trabajo, y que aplique la regla de la cadena más larga, requiere de una inversión alta en energía por parte de la red subyacente, por ejemplo, la red de Bitcoin consume más energía eléctrica que la República Checa [9]. (3) La red subyacente sería susceptible a ataques eclipse[11], sería necesario implementar medidas de seguridad adicionales, para proteger las conexiones de punto a punto —P2P—. (4) La red subyacente sería susceptible a la minería egoísta[12]. (5) La red subyacente podría exhibir una tendencia a la centralización, por ejemplo, en 2 018, más del 50 % de la potencia de cómputo en la comunidad de Bitcoin fue controlada por ocho granjas de minería, y más del 50 % de la potencia de cómputo en la comunidad de Ethereum fue controlada por cinco granjas de minería.

Protocolos de consenso con prueba de participación —*Proof-of-Stake*, PoS—

En las redes que implementan un protocolo de consenso con prueba de participación, la capacidad de participación de cada agente en el proceso de consenso es relativa a la cantidad de *tokens* que el agente posee. A diferencia de la prueba de trabajo, la prueba de participación permite que la red subyacente sea eficiente, en términos energéticos. En estas redes, la participación en el proceso generalmente requiere de una inversión en criptomoneda, en

[9] En una red de naturaleza pública y seudónima, como la de la comunidad de Bitcoin, un ataque sybil podría iniciar con la apertura de múltiples cuentas por parte de uno o varios adversarios organizados, pero para dirigir uno de estos ataques, y que tal ataque fuese exitoso, si la red exige la prueba de trabajo, y aplica la regla de la cadena más larga, el o los adversarios necesitarían controlar más del 50 % del total del poder de cómputo dedicado a la minería.

[10] Se le denomina "minería" al procedimiento mediante el que cada bloque es generado.

[11] En una red de naturaleza pública, y de punto a punto, como la red de Bitcoin, uno o varios adversarios organizados podrían tomar ventaja de los problemas de conectividad en la red.

[12] La minería egoísta consiste en la violación de la regla de difusión, al violarla, uno o varios adversarios organizados podrían amplificar la proporción del poder de cómputo que controlan en la red.

lugar de una inversión alta en energía, por parte del agente, y la participación es proporcional a esta inversión. Esta inversión funciona como medida de seguridad ante los ataques sybil. A los agentes que participan en el proceso de consenso normalmente se les denomina agentes verificadores. Xiao *et al.* han identificado cuatro clases de pruebas de participación: prueba de participación encadenada, prueba de participación dirigida por comités, prueba de participación tolerante a fallas bizantinas, y prueba de participación delegada.

Prueba de participación encadenada. Los protocolos que requieren pruebas de esta clase heredan algunos de los componentes del protocolo de consenso de Nakamoto, como el de la propagación de la información, el de la validación del último bloque recibido, y el de la finalización del último bloque recibido (i.e., la regla de la cadena más larga). Estos protocolos, para poder participar en el proceso de consenso, exigen una inversión en criptomoneda en lugar de una inversión alta en energía, por parte del agente. El agente debe participar en la generación de una prueba computacionalmente exhaustiva que, por lo general, debe ser resuelta para una serie de bloques, cada uno generado por un agente diferente. La red subyacente podría ser susceptible a ataques del 51 %[13], sin embargo, estos protocolos permiten disuadir estos ataques mediante penalidades que podrían provocar la pérdida de la inversión del adversario, o la denegación de futuras ofertas de participación del adversario. Peercoin y Nxt fueron algunos de los primeros sistemas en los que se implementó una cadena de bloques con prueba de participación encadenada.

Prueba de participación dirigida por comités. En las redes en las que la participación es dirigida por un comité, por lo general, el tiempo está dividido en rondas, cada bloque es generado por un comité, y en cada ronda, el comité es restablecido. Los protocolos que requieren pruebas de esta clase, para poder participar en el proceso de consenso, exigen una inversión en criptomoneda por parte del agente, y heredan la regla de la cadena más larga, debido a esto último, la red subyacente sería susceptible a ataques del 51 %, por otro lado, en la red subyacente, sería conveniente implementar una regla que limite el tamaño del comité, de lo contrario, la red podría sufrir por problemas de rendimiento. La regla adicional podría limitar el tamaño del comité al exigir un requisito adicional a los agentes interesados en participar. Ouroboros, Ouroboros-Praos y Snow-White son algunos de los protocolos con prueba de participación de esta clase.

Prueba de participación tolerante a fallas bizantinas. En los protocolos que requieren pruebas de esta clase, la regla de la cadena más larga no es necesaria, en su lugar, una capa adicional, la capa que proporciona la tolerancia a fallas bizantinas[14], resuelve la finalización del último bloque recibido, de manera rápida y determinista. Esta capa, por lo general, incluye un mecanismo de puntos de control que permite sustituir la regla de la cadena más larga por la regla del punto de control más reciente. Tendermint, Algorand[15] y Casper-FFG

[13] La red subyacente sería susceptible a ataques dirigidos por uno, o varios adversarios organizados, que controlen más del 50 % del total del poder de cómputo en la red, a estos ataques se les denomina "ataques del 51 %".

[14] Se dice que una falla es bizantina si durante su ocurrencia, el sistema aparenta estar funcionando con normalidad, pero el efecto de su funcionamiento no es el esperado, una falla bizantina, e.g., podría influir en un proceso de consenso, en un sistema distribuido. Lamport *et al.* usaron el término "bizantino" por primera vez en 1 982, en su artículo sobre el problema de los generales bizantinos, para describir este comportamiento, lo describieron comparando a cada proceso en el sistema con un general bizantino. Un protocolo de consenso que es tolerante a fallas bizantinas —BFT— también es tolerante a fallas no silenciosas.

[15] Se le llamó Algorand porque utiliza "aleatoriedad algorítmica" para seleccionar el conjunto de agentes que generará el siguiente bloque. El protocolo asegura que el método de selección no sea manipulable, que sea impredecible antes del último minuto, y que después sea fácil de verificar. Además, el protocolo asegura que la probabilidad de que la cadena de bloques se bifurque sea menor a 10^{-18}. Entre otras propiedades de Algorand tenemos que: (1) la inversión en energía que el protocolo requiere es mínima, (2) el tiempo que requiere la generación de cada bloque es menor a 10 minutos y, (3) la distribución del trabajo de verificación es uniforme. El protocolo establece que, al inicio de cada fase, cada agente pueda enviar un mensaje, y al final de la misma fase, tal mensaje sea recibido por los demás. Los mensajes recibidos por un agente confiable *i*, al inicio de una fase determinada, son enviados a todos los demás antes de que la misma fase termine. La red podría particionarse arbitrariamente por un período de tiempo desconocido, durante

son algunos de los protocolos con prueba de participación de esta clase, estos protocolos toleran hasta 1/3 de participación maliciosa. En caso de que un adversario controle más de 1/3 de la participación, y pueda manipular la comunicación de tal forma que provoque un conflicto entre varios puntos de control, el protocolo Casper-FFG permite que los verificadores confiables puedan votar por uno de los puntos en conflicto, sin sufrir penalidades.

Prueba de participación delegada. Las redes en las que la participación es delegada, la participación es dirigida por un comité, en el que a cada miembro se le denomina "delegado". Cada comité es establecido mediante "elección popular", el proceso de elección es denominado "proceso de delegación", en el proceso, cada agente, para elegir, puede emitir su voto mediante una transacción. Cada agente, para ingresar al comité, necesita atraer los votos suficientes, generalmente lo logra mediante propaganda, o mediante la oferta de incentivos externos, en cualquier caso, es necesario que el agente revele su identidad. Cada delegado recibe una remuneración por el trabajo de verificación, proporcional a la cantidad de votos que acumuló. Cualquier protocolo de consenso con prueba de participación delegada, por diseño, permite controlar el tamaño de cada comité, por lo que el comité de turno podría resolver de manera segura la finalización del último bloque, así como sería resuelta en un sistema tolerante a fallas bizantinas, de esta manera, aunque cada delegado revele su identidad, el protocolo queda protegido ante cualquier ataque por parte de uno o varios adversarios organizados que controlen 1/3 o menos del total de la participación.

La prueba de participación parece ser más conveniente que la prueba de trabajo en todos los escenarios, sin embargo, cualquier protocolo con prueba de participación requiere de medidas de seguridad adicionales para proteger a la cadena de bloques ante intentos de falsificación de alguno de sus segmentos, ante intentos que no requieran de una inversión significativa. La falta de medidas de seguridad adicionales podría incentivar comportamientos irregulares por parte de cualquier agente, no necesariamente uno que controle el 50 % de la participación, e.g., (1) con la intención de efectuar un doble gasto, el agente irregular podría seguir trabajando sobre los diferentes extremos de una cadena de bloques bifurcada[16], (2) el agente irregular podría intentar organizar un ataque junto a otros agentes con una alta participación en el pasado, pero con una baja participación en el presente, (3) también con la ayuda de otros, el agente irregular podría intentar generar una cadena de bloques con una alteración en un bloque generado mientras hubo poca participación, o (4) el agente irregular podría intentar sesgar el proceso de elección para el establecimiento del comité. Además, la red subyacente podría exhibir una tendencia a la centralización, cualquier agente podría invertir sus ganancias provenientes del trabajo de verificación en más participación, esto podría facilitar que cualquier agente acumule más del 50 % del total de la participación.

1.2.5. Cadena de bloques logística

Recientemente, la tecnología de cadena de bloques ha sido implementada en plataformas desde las que una cadena de suministro es administrada. Hemos compuesto el término "cadena de bloques logística" para, en forma concisa, expresar que la administración de una cadena de suministro es asistida mediante la cadena de bloques en cuestión. Westerkamp *et al.* proponen identificar a cada producto mediante un *token* no fungible, y registrar las transformaciones de cada producto en la cadena de bloques. Según los autores, un *token* puede identificar a una unidad o a un paquete de unidades que pueda ser medido por su cantidad, peso, volumen o tamaño. Un *token* no fungible, a diferencia de un *token* que represente a una criptomoneda, es un *token* de valor único, normalmente, un *token* no fungible representa a un recurso físico [14].

---

este, un adversario *j* podría intervenir en la entrega de los mensajes, pero en cuanto la red se desparticione, el efecto provocado por *j* desaparecería [13].

[16] Si este comportamiento es replicado por los suficientes agentes, el doble gasto podría ser aceptado en la cadena de bloques principal.

La Fundación Ellen MacArthur identifica una serie de perfiles para los agentes, según sus funciones, en las redes de suministro, estos son: proveedor de materia prima —*materials manufacturer*—, fabricante de componentes —*parts manufacturer*—, fabricante de productos —*product manufacturer*—, proveedor de servicios —*service provider*—, y consumidor —*consumer or user*—. La figura 1.1 ilustra estos perfiles. Westerkamp *et al.* proponen una descripción a cada perfil en la siguiente lista, la lista es equiparable a la que identifica la fundación.

1. *Proveedor de materia prima*. Corresponde a los agentes para los que, al menos uno de sus procesos productivos, permite producir un recurso e identificarlo mediante un *token*, sin consumir otro recurso que esté identificado mediante otro *token*, en la cadena de bloques. Un proveedor de materia prima cualquiera normalmente opera con paquetes de productos en lugar de productos individuales.

2. *Fabricante de componentes y fabricante de productos*. Corresponde a los agentes para los que, al menos uno de sus procesos productivos, permite producir un recurso e identificarlo mediante un *token*, por medio del consumo de otro recurso que esté identificado mediante otro *token*, en la cadena de bloques. Un fabricante cualquiera normalmente genera un *token* para cada uno de sus productos y, además, con frecuencia genera un *token* para un conjunto de productos existentes, cada uno identificado mediante un *token*, esto para poder manipular al conjunto como un paquete, en la cadena de bloques. Claramente, la transferencia de un recurso físico cualquiera sería representada, en la cadena de bloques, mediante la transferencia del *token* que identifica al recurso.

3. *Proveedor de servicios*. Corresponde a los agentes para los que, cada uno de sus procesos productivos, permite producir un servicio e identificarlo mediante un *token*, en la cadena de bloques. Un proveedor de servicios cualquiera normalmente no altera ninguno de los productos que adquiere, pero puede generar un *token* para un conjunto de productos existentes, cada uno identificado mediante un *token*, esto para poder manipular al conjunto como un paquete, en la cadena de bloques.

4. *Consumidor*. Corresponde a los agentes para los que no hay ningún proceso productivo. Un consumidor cualquiera normalmente adquiere para utilizar, o para revender, en caso de que adquiera un producto, lo adquiere mientras este está en su vida útil.

1.2.6. Teoría de juegos

La teoría de juegos facilita el estudio de problemas en los que dos o más agentes, cada uno autodeterminado e interesado en su propio beneficio, puede intervenir en la solución del problema. El planteo de estos problemas requiere de la definición de una función de utilidad para cada agente, que cuantifique el grado de preferencia entre las diferentes acciones disponibles para el agente. Se dice que un agente es racional si este espera maximizar la utilidad que obtiene mediante sus acciones.

Al estudiar un problema mediante la teoría de juegos, es necesario definir, además de la función de utilidad, el conjunto de agentes, y el conjunto de acciones para cada uno. Cada agente actúa en función de las acciones de las que dispone, cada uno puede corresponder a una persona, un empleado, una empresa, un gobierno, entre otros. El conjunto de acciones disponibles para un agente corresponde a lo que el agente puede hacer, e.g., una acción puede corresponder al ingreso de una oferta en una subasta, a la participación en una protesta, a la venta de un activo, o al voto por un candidato determinado.

Un juego puede ser representado en "forma normal" o en "forma extensiva". En forma normal, un juego es representado mediante una matriz que determina la utilidad para cada

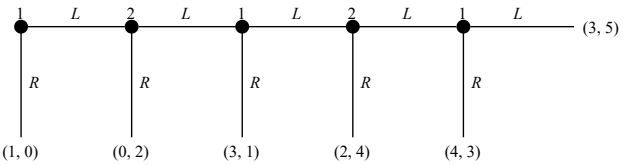

Figura 1.2: Un "juego de ciempiés". En este juego, el primero en actuar debe ser el jugador 1, debe elegir entre la acción *L* y la acción *R*, después debe actuar el jugador 2, debe elegir entre las mismas acciones, *L* y *R*, y así sucesivamente. Cada nodo terminal está identificado con una etiqueta compuesta por dos valores, la utilidad para el jugador 1 y la utilidad para el jugador 2, respectivamente. En el juego se alcanza el único equilibrio posible si el jugador 1 elige la acción *R* en su primera oportunidad.

agente y para cada acción de la que el agente dispone, en esta forma, el tiempo no está expresado explícitamente, sin embargo, es posible codificarlo en forma de acciones adicionales. En forma extensiva, un juego es representado mediante un árbol, en esta forma, el tiempo está expresado explícitamente, codificado en los nodos del árbol, o estados del juego, y cada nodo está determinado por las acciones elegidas en los estados anteriores. La figura 1.2 contiene una representación de un juego en forma extensiva. En forma normal, tradicionalmente, un juego se define como $G = (N, A, U)$, donde:

- $N = \{1, \ldots, n\}$ corresponde al conjunto de los n agentes en la población.
- A_i corresponde a un conjunto finito de acciones, el conjunto de las acciones disponibles para el agente i, y $A = A_1 \times \ldots \times A_n$, A representa el conjunto de configuraciones disponibles para la población.
- $u_i : A \to \mathbb{R}$ corresponde a la función de utilidad del agente i, y $U = (u_1, \ldots, u_n)$.

Se dice que un juego está en equilibrio —*Nash Equilibrium*, NE—, cuando cada agente elige la acción, o conjunto de acciones si el juego está en forma extensiva, mediante la que obtiene la máxima utilidad, pese a que la utilidad de cada agente pueda depender de las acciones de otros.

Definición 1.2.1 (Mejor respuesta —*Best Response*, BR—)**.** $a'_i \in BR(a_{-i}) \Leftrightarrow u_i(a'_i, a_{-i}) \geq u_i(a_i, a_{-i})\ \forall\ a_i : A_i$*, con* $a'_i \in A_i$ *y con* a_{-i} *como una configuración que no incluya una acción para i.*

Se le denomina "solución del juego" a cualquier configuración mediante la que se alcance el equilibrio.

Definición 1.2.2 (Equilibrio de Nash —*Nash Equilibrium*, NE—)**.** $\forall\ a : A \mid a = (a_1, \ldots, a_n)$ *hay equilibrio sii* $\forall\ i : N,\ a_i \in BR(a_{-i})$.

1.2.7. Métodos formales

Un método formal es un procedimiento que consiste en formular especificaciones formales, especificaciones que describen de forma precisa, mediante un lenguaje matemático, las propiedades que debe exhibir un sistema de información. Una especificación formal describe el "qué", sin restringir el "cómo", sobre lo que el sistema debe hacer, sobre sus características. Una especificación formal permite evaluar de forma precisa las características del sistema, sin necesidad de consultar fuentes carentes de legibilidad, como podría ser el código fuente del sistema, o fuentes carentes de precisión, como podría ser un documento escrito en lenguaje natural [15].

Lenguaje Z

Existen diferentes lenguajes para formular especificaciones formales, uno de ellos es el lenguaje Z, que incluye los operadores estándar de la teoría de conjuntos, y los operadores estándar de la lógica de primer orden, esto permite el cálculo de predicados, el uso de tipos[17], y el uso de técnicas de demostración mediante el lenguaje. Además, el lenguaje permite definir objetos complejos y describir sus propiedades mediante un patrón de declaración y restricción. A las expresiones que siguen este patrón se les denomina "esquemas", estos esquemas también permiten describir el estado de un sistema y las formas en que este puede cambiar.

La expresión 1.1 ilustra la forma típica de las expresiones en Z, en la expresión, Q representa a un cuantificador, universal o existencial, de esta forma podemos expresar que, para los objetos referenciados en la declaración, que satisfagan la restricción, el resultado se sostiene. La expresión 1.2 sirve como ejemplo de una expresión en Z.

$$\mathrm{Q}\ declaration \mid constraint \bullet result \tag{1.1}$$

El lenguaje permite declarar secuencias, i.e., colecciones ordenadas de objetos, como en la primera declaración en la expresión 1.2, en la declaración, *Set* corresponde al tipo de los objetos en la secuencia. El lenguaje también permite representar la cardinalidad de la secuencia, como en la restricción en la expresión 1.2[18]. La expresión 1.2, con "$\langle collection\ i \rangle$ in *collection*" afirma que la secuencia $\langle collection\ i \rangle$ es una subsecuencia de la secuencia *collection*.

$$\begin{aligned} \exists\, collection : \mathrm{seq}\ Set \bullet \forall\, i : \mathbb{N} \mid \\ 1 \leq i \land i \leq \#collection \bullet \langle collection\ i \rangle \ \mathrm{in}\ collection \end{aligned} \tag{1.2}$$

El lenguaje permite identificar al conjunto potencia de cualquier conjunto *Set*, i.e., el lenguaje permite identificar al conjunto de todos los subconjuntos de *Set*, como "$\mathbb{P}\, Set$". Los esquemas pueden ser interpretados como declaraciones, como predicados, o como conjuntos, y pueden ser expresados en notación horizontal, como en la expresión 1.3 o en notación vertical[19], como en la figura 1.3.

$$hSchema \mathrel{\widehat{=}} [declaration \mid constraint] \tag{1.3}$$

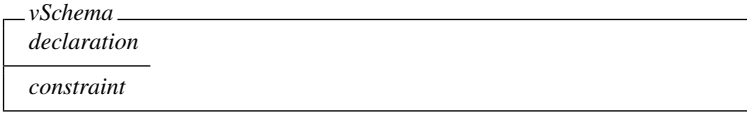

Figura 1.3: Esquema expresado en notación vertical.

[17] Cualquier conjunto maximal puede ser usado como un tipo.

[18] (1) Esta notación también permite representar la cardinalidad de cualquier conjunto. (2) "$object_i = collection\, i$" puede ser expresada también como "$object_i = collection\,(i)$". (3) El primer objeto en cualquier secuencia *collection*, si existe, es *collection* 1. (4) $0 \in \mathbb{N}$.

[19] El lenguaje permite utilizar la notación vertical para expresar definiciones genéricas, para esto en el lugar del identificador del esquema se debe colocar una expresión de la forma $[X]$ tal que X sea un parámetro útil como conjunto en la definición.

Al decorar de la forma s' al identificador de un esquema s, el identificador de cada componente del esquema hereda la decoración, e.g., $\forall\, s' : Sch \bullet c' \in Set$, con $Sch \mathrel{\widehat{=}} [c : Set]$. En los esquemas que describen un cambio de estado, por convención, los pares de componentes identificados de la forma v, v' corresponden al mismo componente, el componente sin decorar representa el valor antes del cambio, y el otro representa el valor después del cambio.

Los esquemas que describen un cambio de estado pueden contener componentes de entrada y componentes de salida, y por convención, el identificador de cada entrada debe terminar con el símbolo de interrogación, e.g., $v?$, y el identificador de cada salida debe terminar en el símbolo de exclamación, e.g., $v!$.

1.3. Definición del problema

La Fundación Ellen MacArthur, establecida en 2 010, trabaja en la transición hacia una economía circular, "inspirando" a las generaciones del presente en el replanteamiento, rediseño y construcción del futuro [7]. Según la fundación, la tecnología es clave en la transición, especialmente en el rastreo de recursos y en la organización de la logística inversa. La dificultad de garantizar disponibilidad, calidad y consistencia de los datos relativos a los recursos sigue siendo un obstáculo importante, a nivel nacional y global [7]. Esta es una parte fundamental del problema que tratamos en este trabajo.

Las cadenas de suministro gestionan 2/3 del comercio global y, por otro lado, el alcance de la tecnología de cadena de bloques en el ámbito de las redes de suministro se desconoce [4]. Creemos que podemos contribuir con la solución del problema mediante esta tecnología, según la propiedad de "documentación de la procedencia de los datos" de las cadenas de bloques, mediante esta tecnología, en cualquier cadena de suministro, cualquier agente, incluso si es un consumidor, podría acceder a información confiable sobre la composición y la procedencia de cualquier recurso, información que además facilitaría las operaciones de coordinación y de logística.

Sabemos que, para que nuestra contribución sea efectiva, es necesario incluir al consumidor e incentivar la participación en la solución. Creemos que al ofrecer una plataforma que facilite las labores en las cadenas de suministro, una plataforma en la que se disponga de una criptodivisa, sería posible implementar un mecanismo de incentivos adecuado para tratar el problema. Un mecanismo de incentivos adecuado, además, debería evitar que la participación en la solución pueda generar un costo de oportunidad importante para cualquier organización.

La aceptación de la propiedad de "documentación de la procedencia de los datos" de las cadenas de bloques, requiere de flexibilidad por parte de cada organización participante en las medidas de seguridad de la información. En algunos casos, esta propiedad podría implicar algún tipo de vulnerabilidad, e.g., un competidor cualquiera podría explotar la información que sea publicada en la cadena de bloques, por otro lado, para muchos de los consumidores de algunas organizaciones, en especial de la industria alimenticia, podría ser de interés conocer la procedencia de los recursos que consumen [14].

Al considerar todo esto nos preguntamos: *¿Es posible diseñar un mecanismo de incentivos tal que la oferta de una criptodivisa que lo implemente acelere significativamente la transición hacia una economía circular?* Esta es nuestra pregunta de investigación. Claramente, el mecanismo debería cumplir con la restricción de racionalidad individual[20], en otras palabras, el mecanismo debería incentivar la participación en la solución, a pesar de los costos de oportunidad inherentes a la participación, si los hay.

[20] Esto para que sea más atractivo participar que no participar en el "juego" [8].

Sin embargo, la implementación de un mecanismo de incentivos no evita que la utilidad de cada agente dependa no solo de sus propias acciones, y tampoco facilita la predicción del efecto del comportamiento de cada agente en la utilidad que el agente obtiene, por lo que para abordar el problema es necesario considerar escenarios con múltiples agentes, y para abordarlo es adecuado un método experimental, en lugar de un método exclusivamente analítico. La sección 3.1, sobre la metodología, describe el procedimiento utilizado para responder a la pregunta de investigación.

Hipótesis. *En toda matriz de agentes racionales*[21]*, (para cualquier combinación de agentes) que emula el comportamiento de una economía de recursos no perecederos*[22]*, si en ella existe un mecanismo de incentivos autosuficiente*[23] *que promueva la transición hacia una economía circular, entonces a partir de cierto tiempo, la matriz exhibe una aceleración de la transición.*

[21] Un agente es racional si prefiere la estrategia mediante la que puede obtener la máxima utilidad.

[22] El lado derecho de la figura 1.1 ilustra el manejo de los recursos no perecederos en una economía circular.

[23] Un mecanismo de incentivos es autosuficiente si su mantenimiento no requiere de una inversión constante por parte de su desarrollador.

2

Justificación, objetivos, y alcance

Este capítulo justifica nuestra investigación desde tres dimensiones diferentes: innovación, impacto y profundidad; además, incluye la descripción de los objetivos y el alcance de la investigación, y describe los entregables a partir de las contribuciones en cada uno.

2.1. Justificación

Profundidad

Considerando la topología de las redes de suministro y la dinámica de las cadenas de suministro circulares, para resolverlo, hemos decidido reducir el problema de "formular una definición de circularidad para utilizarla como criterio de circularidad" a un problema trivial, el problema de "encontrar un Autómata Finito con ε-Transiciones —*ε Nondeterministic Finite Automaton*, ε-NFA—[24]", un autómata mediante el que sea posible reconocer las transacciones "circulares" en el historial de transacciones".

Es posible representar mediante un ε-NFA el conjunto de todas las posibles secuencias de transacciones circulares, si se dispone de una definición de circularidad en términos "transaccionales", en otras palabras, es posible describir mediante un ε-NFA el comportamiento que promovería el mecanismo de incentivos, de esto trata el capítulo 4, trata del modelo circular de red de suministro.

Innovación

Hasta ahora, no existe una definición de "circularidad" generalmente aceptada [11]. Hemos definido un modelo genérico de negocio con configuración circular, para extraer de este, una definición formal de circularidad, y poder utilizarla como criterio en el reconocimiento de las transacciones circulares en el historial de transacciones.

[24] Un autómata es una máquina abstracta, una máquina de estados, con un conjunto finito de estados, un conjunto finito de símbolos de entrada, y una función de transición. Uno de los estados del conjunto es su estado inicial, y un subconjunto del conjunto de estados corresponde al conjunto de estados de aceptación. La función de transición determina el cambio de estado cada vez que un símbolo de entrada es procesado [16].

Hemos diseñado un método experimental que permite analizar el efecto de un mecanismo de incentivos en un sistema dinámico, y hemos especificado una extensión para ser implementada junto a un protocolo de consenso con prueba de participación tolerante a fallas bizantinas, que permite implementar cualquier mecanismo de incentivos, si el mecanismo no requiere de más información que el mecanismo propuesto en este documento.

Hasta ahora no se ha desplegado un sistema de criptodivisa que promueva una transición hacia una economía con énfasis en los recursos. Creemos que esto puede cambiar con la oferta de un sistema de criptodivisa como el propuesto en este documento.

Impacto

Creemos que con el desarrollo de nuestra investigación hemos contribuido en dos ámbitos principalmente, en el ámbito ambiental y en el ámbito académico. En el ámbito ambiental, hemos contribuido al ofrecer una alternativa que pueda acelerar la transición hacia una economía sostenible, una alternativa de alcance global, y en el ámbito académico, hemos contribuido al proponer un marco de trabajo que puede facilitar el diseño y el análisis de nuevos mecanismos de incentivos, y también al proponer una arquitectura que facilita la implementación de tales mecanismos.

2.2. Objetivo general

El objetivo general de este trabajo es *diseñar un mecanismo de incentivos, de alcance global, que acelere la transición hacia una economía circular*, creemos que antes de alcanzarlo, es necesario alcanzar los objetivos en la siguiente lista, estos son los objetivos específicos de este trabajo.

2.2.1. Objetivos específicos

1. Generar un marco de trabajo que facilite el diseño y el análisis de “cripto-mecanismos” de incentivos.

2. Especificar una arquitectura que facilite la implementación de “cripto-mecanismos” de incentivos.

3. Formular una definición de circularidad para utilizarla como criterio en el reconocimiento de transacciones circulares.

4. Diseñar un mecanismo que pueda incentivar la participación en la transición hacia una economía circular.

2.3. Alcance

En una economía circular, el sistema industrial debe ser regenerativo y restaurativo, el progreso económico no debe destruir el medio ambiente, y debe preservar el valor económico, social y ambiental de cada recurso [11]. La transición de una economía lineal a una economía circular equivale a un cambio de paradigma, un cambio en el que intentamos contribuir al ofrecer una alternativa que facilite la gestión sostenible de inventarios de recursos no perecederos, en particular. El diseño de esta alternativa parte de la configuración de cadena de suministro circular, parte de esta configuración porque consideramos que esta es la que está más alineada con los objetivos de este trabajo.

En la literatura, varios autores han identificado una serie de debilidades en la red de la comunidad de Bitcoin que están fuera de la problemática abordada en la investigación, por ejemplo, la red es susceptible a ataques del 51 % [6], la prueba de trabajo, junto con la regla de la cadena más larga, requiere de una inversión alta en energía por parte de la comunidad [9], el último bloque no es confiable debido a que, frecuentemente, la cadena de bloques se bifurca [17], y otros de carácter político, como la prohibición de "minar" decretada por un gobierno (como sucedió en China), o económico, como la inestabilidad del tipo de cambio.

3

Metodología y plan de trabajo

Este capítulo describe la metodología aplicada en la investigación, describe la implementación del método científico en la investigación y la aplicación de los métodos formales en la descripción de la propuesta. Las últimas secciones del capítulo contienen la documentación sobre los entregables y el cronograma.

3.1. Metodología

La sección 1.3, sobre la definición del problema, establece la hipótesis de la investigación. Según la hipótesis, la propuesta en este documento es implementable como solución de la problemática descrita en la sección 1.3. El diseño de la investigación es de tipo cuantitativo, hemos desarrollado un sistema de simulación mediante el que hemos recopilado los conjuntos de datos necesarios para el análisis estadístico de la influencia de la distribución de la población, según la clase de cada agente, en el efecto del sistema de criptodivisa. La documentación de este análisis se encuentra en el capítulo 6.

El desarrollo de los capítulos 4, 5 y 7 es teórico/analítico, los capítulos 4 y 5 describen las herramientas que hemos construido mediante las que hemos desarrollado este trabajo. El capítulo 4 establece un criterio de circularidad, necesario en la implementación del mecanismo de incentivos, el capítulo 5 describe el modelo de juego, un modelo que permite representar el ciclo de vida de cualquier recurso y que, mediante un conjunto de estas representaciones, también permite obtener una instantánea de cualquier sistema económico, una instantánea con un nivel de detalle suficiente para el desarrollo de este documento. El trabajo de diseño del mecanismo de incentivos y de diseño del método experimental inicia en el modelado del juego. El capítulo 7 describe una arquitectura de cadena de bloques que permite implementar el mecanismo de incentivos[25].

El lenguaje de modelado que utilizamos está inspirado en el lenguaje Z[26], un lenguaje utilizado en las especificaciones formales. El lenguaje que utilizamos no está más que inspirado en el lenguaje Z porque, pese a que el lenguaje Z nos ofrece recursos que nos han

[25] Cada capítulo se desarrolla en un contexto diferente, el capítulo 5 en el contexto del sistema económico (un modelo de juego), el capítulo 6 en el contexto del sistema de simulación, y los capítulos 4 y 7 en el contexto del sistema de criptodivisa.

[26] Un lenguaje para especificaciones, refinamientos y demostraciones [10].

resultado muy convenientes (estos los hemos utilizado), hemos decidido mantener un lenguaje formal más tradicional para mantener un lenguaje más legible y compacto. La sección 1.2.7, sobre métodos formales, introduce los recursos del lenguaje Z que hemos utilizado.

Nuestra intención es que la documentación de este trabajo esté autocontenida, con esto queremos decir que, nuestra intención es que las secciones de antecedentes, marco teórico y otras incluyan el contenido que sea relevante en este trabajo, aunque haya sido desarrollado con base en trabajos de otros autores. Con el propósito de ser concisos, hemos decidido redactar el texto "de abajo hacia arriba", con esto queremos decir que hemos iniciado con las secciones más técnicas, y hemos finalizado con las más literarias, tal como se refleja en la organización del cronograma de actividades.

3.2. Entregables

La lista a continuación describe cada entregable, cada uno de ellos corresponde a un capítulo de este documento. El desarrollo de cada uno de estos capítulos, en conjunto, permite responder a la pregunta de investigación, establecida en la sección 1.3.

Modelo circular de red de suministro. Este capítulo contiene la descripción de un modelo genérico de negocio con configuración circular, y un criterio de circularidad, extraído del modelo de negocio, y formulado a partir del lenguaje de un Autómata Finito con ε-Transiciones —*ε Nondeterministic Finite Automaton*, ε-NFA—. El criterio de circularidad facilita el reconocimiento de las transacciones que derivan de la actividad económica de las cadenas de suministro afines al modelo genérico descrito en el capítulo.

Mecanismo de incentivos. El objetivo de este capítulo es proponer un mecanismo que pueda incentivar la participación en la transición hacia una economía circular. El mecanismo propuesto en este capítulo está construido sobre un modelo de juego en forma normal, y puede ser desplegado en un sistema dinámico. Este capítulo contiene un análisis teórico del mecanismo, un análisis del equilibrio de Nash.

Análisis estadístico del efecto del mecanismo de incentivos. Este capítulo contiene los resultados de un análisis estadístico mediante el que hemos evaluado el efecto del mecanismo de incentivos, una descripción detallada del método utilizado para el análisis, y la descripción del sistema de simulación mediante el que hemos recopilado los conjuntos de datos necesarios para el análisis. El método requiere dos series de experimentos, mediante las que hemos evaluado el efecto en el sistema económico, sistema que incluye el mecanismo de incentivos, de diferentes poblaciones. En la primera serie, la "serie experimental", el sistema de simulación implementa el mecanismo de incentivos, mientras que, en la segunda serie, la "serie de control", el sistema de simulación no implementa el mecanismo de incentivos. El capítulo finaliza con la interpretación de los resultados del análisis.

Cripto-mecanismo de incentivos. Este capítulo describe una arquitectura de cadena de bloques que permite implementar el mecanismo de incentivos para cualquier cadena de suministro, la arquitectura consta de una serie de capas, e incluye una extensión del protocolo de consenso. Este capítulo también describe un modelo de aplicación mediante el que es posible, para cualquier cadena de suministro, registrar un modelo de negocio tal que sea posible implementar sobre este, el mecanismo de incentivos. El capítulo incluye un esquema de minería alternativo, y describe una serie de propiedades que la arquitectura exhibe, y que garantizan la integridad de la cadena de bloques.

3.3. Cronograma de actividades

La siguiente es la lista de actividades mediante las que hemos desarrollado los entregables. Cada actividad está indexada mediante la fecha de finalización que le corresponde, fecha en la que el documento correspondiente fue entregado.

2019 08 07 Modelo circular de red de suministro

2019 08 14 Descripción formal del entorno

2019 08 21 Definición de circularidad

2019 09 28 Redacción 1

2019 10 07 Modelo de juego y diseño del mecanismo de incentivos

2019 10 28 Análisis del mecanismo de incentivos

2019 11 28 Redacción 2

2020 06 21 Diseño del método experimental

2020 07 21 Modelo del sistema de simulación

2020 08 21 Análisis de datos

2020 09 21 Redacción 3

2020 10 07 Análisis de complejidad

2020 10 28 Descripción formal del "criptomecanismo" de incentivos

2020 11 28 Redacción 4

Fix the money and the rest will follow.

—Lawrence Lepard

4

Modelo circular de red de suministro

Sinopsis. Este capítulo contiene la descripción de un modelo genérico de negocio con configuración circular, y un criterio de circularidad, extraído del modelo de negocio, y formulado a partir del lenguaje de un Autómata Finito con ε-Transiciones —*ε Nondeterministic Finite Automaton*, ε-NFA—. El criterio de circularidad facilita el reconocimiento de las transacciones que derivan de la actividad económica de las cadenas de suministro afines al modelo genérico descrito en el capítulo.

4.1. Modelo de negocio

La Fundación Ellen MacArthur, en su artículo *Hacia la Economía Circular, vol. 3* [7], presenta un diagrama que ilustra la dinámica del manejo de los recursos en una economía circular, tal diagrama corresponde a la figura 1.1.

Definición 4.1.1 (Recurso)**.** *Cualquier mercancía registrable en una cadena de bloques logística.*

Este capítulo contiene la descripción de un modelo genérico de negocio con configuración circular adecuado para cualquier cadena de suministro tal que su modelo de negocio esté orientado a la manufactura de recursos no perecederos, por lo tanto, en casos en los que la orientación sea otra, será necesario desarrollar otro modelo de negocio y extraer de este, un nuevo criterio de circularidad.

La configuración circular, para las cadenas de suministro, permite estimular una dinámica como la ilustrada en la figura 1.1. Con frecuencia, para facilitar las operaciones bajo esta configuración, se implementa un mecanismo de logística inversa, como tal, este mecanismo podría facilitar el rastreo de cada recurso que sea tratado por la cadena de suministro. El modelo de negocio que hemos descrito en este capítulo refleja una configuración circular, y requiere, en la cadena de suministro, de un nodo adicional, un nodo que corresponda al consumidor.

El modelo requiere de una serie de perfiles, la definición de cada uno es la que propone la Fundación Ellen MacArthur. Hemos identificado como "productor" a cualquier fabricante, sea de componentes o de productos, y hemos clasificado como "perfiles internos" a los per-

files “productor”, “proveedor de materia prima” y “proveedor de servicios”, y como “perfil externo” al perfil “consumidor”.

Definición 4.1.2 (Interno)**.** *(a) El perfil de cualquier agente es interno, si el agente es un (1) “productor”, (2) “proveedor de materia prima” o (3) “proveedor de servicios”, en la cadena de suministro. (b) Cualquier agente es interno si su perfil es interno. (c) Un subconjunto del conjunto de los agentes en cualquier cadena de suministro corresponde a una “cadena de suministro interna” si cada agente en la cadena de suministro pertenece al subconjunto sii su perfil es interno.*

Definición 4.1.3 (Externo)**.** *(a) El perfil de cualquier agente es externo, si el agente es un (4) “consumidor”. (b) Cualquier agente es externo si su perfil es externo. (c) Un subconjunto del conjunto de los agentes en cualquier cadena de suministro corresponde a una “cadena de suministro externa” si cada agente en la cadena de suministro pertenece al subconjunto sii su perfil es externo.*

4.2. Entorno: Dinámica del sistema económico

El modelo del historial de transacciones, mediante el que desarrollamos esta investigación, consta de un grafo de transacciones, específicamente un multigrafo dirigido $\mathbb{G} = (V, E)$, donde V corresponde al conjunto de nodos y E corresponde al conjunto de aristas. Cada nodo representaría a un agente y cada arista representaría a una transacción del agente proveedor al agente consumidor. La dirección de la transferencia del recurso en cada transacción determinaría la dirección de la arista correspondiente.

Definición 4.2.1 (V)**.** *Conjunto de nodos en el multigrafo dirigido G. Cada nodo en el conjunto representa a un agente.*

En cualquier cadena de bloques “típica”, cada transacción puede registrar n entradas, cada una correspondiente a un monto y una dirección diferente, y m salidas, cada una correspondiente a un monto y una dirección diferente [18], pero en nuestro modelo, cada arista en $\mathbb{G}$ corresponde a una “transacción unitaria”, i.e., una arista entre el nodo que representa al agente proveedor y el nodo que representa al agente consumidor, para distinguir entre una transacción en la cadena de bloques y una transacción unitaria, hemos denominado “transacción múltiple” a cualquier transacción n por m[27].

Este modelo del historial de transacciones es una abstracción, no una especificación, el esquema E en la expresión 4.1 representa la estructura de cualquier transacción en el modelo. En la cadena de bloques, la estructura de una transacción podría permitir registrar otros datos, además de las n entradas y las m salidas, el esquema E incluye solo los componentes necesarios para el desarrollo de esta investigación.

$$E \triangleq [i; j; k; \omega; t; \sigma] \tag{4.1}$$

En la expresión 4.1, $i : V$ identifica al agente proveedor, $j : V$ identifica al agente consumidor, $k : V$ identifica al recurso, $\omega : \mathbb{N}$ identifica al monto transferido de j a i, por lo tanto, i corresponde al origen del recurso en la transacción, $t : \mathbb{N}$ identifica a la marca de tiempo en el que se efectúa la transacción, esta marca de tiempo puede ser interpretada como el identificador del bloque al que corresponde la transacción, y $\sigma : \text{seq}\,\mathbb{N}$ identifica a una secuencia de identificadores, que podría estar vacía, en la que cada uno correspondería a una transacción.

[27] Claramente, en nuestro modelo, para representar una transacción múltiple, sería necesario definir un conjunto de transacciones unitarias.

Si es posible reconocer a cada transacción que contribuya en el cambio de paradigma, entonces es posible remunerar tal contribución al agente que corresponda, proponemos reconocer a cada una de las transacciones en $\mathbb{G}$ que contribuya, mediante alguna de las propiedades que deba exhibir la trayectoria del recurso a la que pertenece, si tal trayectoria es determinada por la logística de una red con configuración circular.

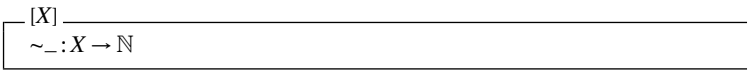

Figura 4.1: A través de todo el documento, la expresión "$\sim x$" y el identificador del objeto x son intercambiables.

Definición 4.2.2 (Trayectoria)**.** *Cualquier secuencia de transacciones unitarias σ en la que,* $\forall\, \iota : \mathbb{N} \mid \iota < \#\sigma \bullet \exists\, e, e' : E \mid \sim e = \sigma(\iota) \land \sim e' = \sigma(\iota + 1) \bullet \forall\, e'' : E \mid e'' \neq e \land e'' \neq e' \bullet i' = j \land k' = k \land t' < t \land \neg (k'' = k \land t' < t'' \land t'' < t)$.

El criterio de circularidad que hemos propuesto requiere de una definición de "trayectoria", la definición 4.2.2. La definición permite trabajar con la "circularidad" como una propiedad posible de cualquier trayectoria. Según la definición, la trayectoria de un recurso corresponde a una secuencia, ordenada cronológicamente, de transacciones, que solo incluye cada una de las transacciones mediante las que el producto fue transferido durante su "ciclo de vida".

4.3. Criterio de circularidad

Definición 4.3.1 (L(4.2))**.** *Lenguaje del autómata 4.2, el lenguaje equivale a un conjunto de secuencias tal que cada secuencia en él pueda ser reconocida por el autómata.*

Hemos formulado una definición de circularidad *ad hoc*, i.e., una definición que funciona como criterio en el reconocimiento de trayectorias "circulares", exclusivamente para el modelo de negocio que hemos desarrollado. Hemos formulado la definición mediante el lenguaje L(4.2), un lenguaje que equivale al conjunto de todas las posibles trayectorias "circulares".

Definición 4.3.2 (Circularidad)**.** *Una trayectoria cualquiera es circular sii tal trayectoria pertenece al conjunto L(4.2).*

Las etiquetas de las transiciones en el autómata 4.2 están codificadas para simplificar su expresión. Cada etiqueta (j,i) puede ser interpretada como el valor de $f(e)$, tal que e representa la transacción a evaluar en la trayectoria, transacción en la que el recurso es transferido de una cuenta con perfil i a otra con perfil j. Hemos decidido representar a cada perfil con el índice que le corresponde en la siguiente lista: (1) Proveedor de materia prima, (2) Productor, (3) Proveedor de servicios, (4) Consumidor. El cuadro 4.1 describe a cada una de estas etiquetas.

Cuadro 4.1: Descripción de cada etiqueta correspondiente a una transición en la figura 4.2.

Etiqueta	Perfil de la cuenta de destino	Perfil de la cuenta de origen
$(3,4)$	Proveedor de servicios	Consumidor
$(2,4)$	Productor	Consumidor
$(1,4)$	Proveedor de materia prima	Consumidor
$(4,4)$	Consumidor	Consumidor
$(4,3)$	Consumidor	Proveedor de servicios
$(3,3)$	Proveedor de servicios	Proveedor de servicios
$(3,2)$	Proveedor de servicios	Productor
$(2,2)$	Productor	Productor
$(2,1)$	Productor	Proveedor de materia prima

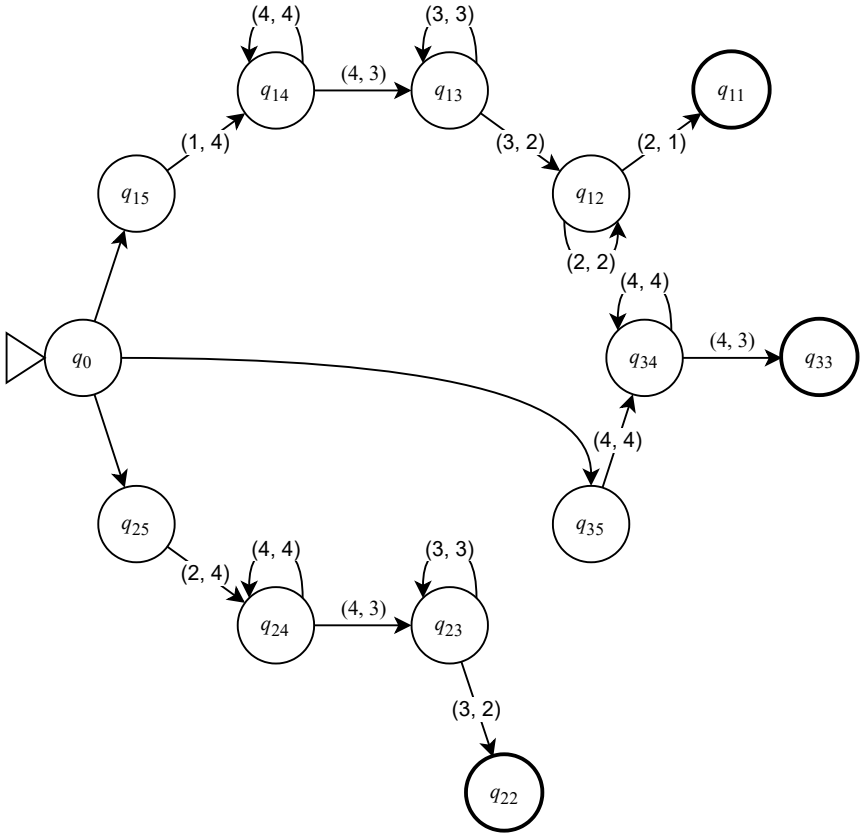

Figura 4.2: (Autómata 4.2). ε-NFA para el reconocimiento de trayectorias circulares. Las transiciones sin etiqueta son ε-transiciones, el estado inicial es q_0 y el conjunto de estados de aceptación es $\{q_{11}, q_{22}, q_{33}\}$.

El autómata 4.2 permite analizar cada trayectoria concluida en un bloque determinado, examina cada una de las transacciones identificada en una trayectoria, en orden cronológico, desde la más reciente hasta la menos reciente. En el autómata, este orden es expresado mediante la dirección de las transiciones. Según la definición 4.3.2, por extensión, "circularidad" es la propiedad de cualquier transacción que esté incluida en una "trayectoria circular". El ejemplo 4.3.3 ilustra el procesamiento de la trayectoria en la figura 4.3, en el ejemplo, el último estado que se alcanza es un estado de aceptación, por lo que el autómata reconoce a

la trayectoria como circular.

Ejemplo 4.3.3. Supongamos que en la trayectoria descrita en la figura 4.3, la cuenta de Cenizo es de perfil "productor", la cuenta de Jacinto es de perfil "proveedor de servicios" y la cuenta de Simposio es de perfil "consumidor". Sea $e_3 : E$ la transacción entre Cenizo y Jacinto, sea $e_2 : E$ la transacción entre Jacinto y Simposio, sea $e_1 : E$ la transacción entre Simposio y Cenizo, y sea $f : E \to \mathbb{N} \times \mathbb{N}$ tal que $f(e_3) = (3,2)$, $f(e_2) = (4,3)$ y $f(e_1) = (2,4)$, según la función de transición δ del autómata 4.2: (1) $\delta\big(q_0, \varepsilon\big) = q_{25}$ y $\delta\big(q_{25}, (2,4)\big) = q_{24}$, por lo tanto, a partir de la transacción más reciente en la secuencia, e_1, se alcanza el estado q_{24}; (2) $\delta\big(q_{24}, (4,3)\big) = q_{23}$, por lo tanto, a partir de la siguiente transacción en la secuencia, e_2, se alcanza el estado q_{23}; y (3) $\delta\big(q_{23}, (3,2)\big) = q_{22}$, por lo tanto, a partir de la siguiente transacción en la secuencia, e_3, se alcanza el estado de aceptación q_{22}. La trayectoria descrita en la figura 4.3 sería circular.

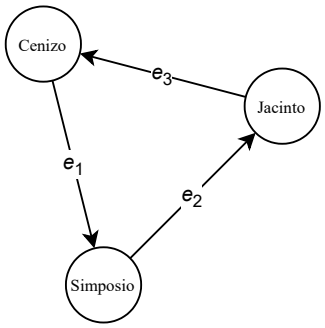

Figura 4.3: Tres transacciones que componen la secuencia "circular" $\langle \sim e_3, \sim e_2, \sim e_1 \rangle$. En la primera, e_3, Jacinto le compra a Cenizo una docena de botellas de cerveza de la marca Rabia, la marca que ella produce, en la segunda, e_2, Simposio compra una de esas cervezas en la tienda de Jacinto, y en la tercera, e_1, Cenizo le compra a Simposio el envase que contenía la cerveza para reutilizar el vidrio.

Lo propuesto en este capítulo aplica para cualquier cadena de suministro, tal que su modelo de negocio esté orientado a la manufactura de recursos no perecederos, en otros casos será necesario redefinir el autómata 4.2, y esto podría requerir de una serie de perfiles diferente. Creemos que el resto de lo propuesto en este capítulo podría aplicar para cualquier cadena de suministro, independientemente de la orientación de su modelo de negocio.

Never doubt that a small group of thoughtful, committed, citizens can change the world. Indeed, it is the only thing that ever has.

—Margaret Mead

5

Mecanismo de incentivos

Sinopsis. El objetivo de este capítulo es proponer un mecanismo que pueda incentivar la participación en la transición hacia una economía circular. El mecanismo propuesto en este capítulo está construido sobre un modelo de juego en forma normal, y puede ser desplegado en un sistema dinámico. Este capítulo contiene un análisis teórico del mecanismo, un análisis del equilibrio de Nash.

5.1. Entorno: Modelo de juego

La teoría de juegos facilita el estudio de problemas en los que dos o más agentes, cada uno autodeterminado e interesado en su propio beneficio, puede intervenir en la solución del problema [8]. Un sistema económico es un sistema dinámico, un sistema que evoluciona con el paso del tiempo, pero pese a esto, es posible formular un algoritmo de aprendizaje que determine el comportamiento de cada agente de forma que facilite el alcance del equilibrio en un sistema dinámico [8].

Encontrar un algoritmo de aprendizaje que facilite el alcance del equilibrio no es relevante, sin embargo, que sea posible encontrarlo, nos permitió optar por un modelo de "juego" multiagente, un modelo de "juego" no solo para dos agentes, como medio para encontrar un mecanismo de incentivos que pueda promover el consumo sostenible de cada recurso.

Cada "juego" descrito mediante el modelo permite analizar el ciclo de vida de un recurso por separado, registrado o no registrado, en el sistema de criptodivisa y, mediante un conjunto de estas descripciones es posible representar a cualquier sistema económico[28]. El modelo, en forma normal, corresponde a $G = (N, A, \theta, R)$, donde:

- $N = \{1, \ldots, n\}$ sea el conjunto de los n agentes en la población.
- A_i sea un conjunto finito de acciones, de las acciones disponibles para el agente i, y $A = A_1 \times \ldots \times A_n$. A sería el conjunto de configuraciones disponibles para la población[29].

[28] En cualquier sistema, cada agente podría participar en más de uno de estos juegos simultáneamente, y el conjunto de juegos en el sistema variaría con el paso del tiempo.

[29] Una configuración en A corresponde a una posible combinación de acciones generada por parte de la población, una por cada agente.

- $\theta : N \to \Theta$ sea la función que permite obtener el perfil de cualquier agente, Θ sería el conjunto de perfiles. Si $\theta(i) \neq 4$ entonces el agente i es interno, y si $\theta(i) = 4$ entonces el agente i es externo, según la serie de perfiles en la sección 1.2.5.

- $r_i : A \to \mathbb{R}$ sea la función que permite obtener la utilidad para cualquier agente i, y $R = (r_1, \ldots, r_n)$.

La función de utilidad r_i cuantifica el valor, en términos monetarios, que el juego genera para el agente i según las expectativas del agente i, en otras palabras, según el efecto que el agente i espera experimentar mediante cada acción de las que dispone. La función de utilidad de cada agente refleja el efecto del mecanismo de incentivos en la utilidad del agente, hemos establecido dos "dimensiones" en las que podemos ubicar a cualquier factor que influya en la utilidad del agente, las dimensiones "ingreso/egreso" e "intrínseco/extrínseco", el ingreso y el egreso extrínsecos corresponderían a los producidos por el mecanismo de incentivos. El ejemplo 5.2.1 describe el ciclo de vida de un recurso y el efecto del mecanismo en este, lo describe mediante el modelo de juego.

Cuadro 5.1: Componentes de la función de utilidad, de cada agente i, y para cada configuración a, i.e., para todo $i : N$; $a : A$. En cualquier juego, extrínseco es cualquier valor monetario sii es transferido de o a el agente debido al mecanismo de incentivos, e intrínseco es cualquier valor monetario que no sea extrínseco. A través de todo el documento, "utilidad" e "ingreso" son términos intercambiables, e "inversión" y "egreso" también, son términos intercambiables.

	v Intrínseca	w Extrínseca	Bruta
ˇ Utilidad	$\check{v}_i(a)$	$\check{w}_i(a)$	$\check{v}_i(a) + \check{w}_i(a)$
ˆ Inversión	$\hat{v}_i(a)$	$\hat{w}_i(a)$	$\hat{v}_i(a) + \hat{w}_i(a)$
Utilidad neta	$\check{v}_i(a) - \hat{v}_i(a)$	$\check{w}_i(a) - \hat{w}_i(a)$	

En cada juego, el objetivo de cada agente i es obtener la máxima utilidad neta, esta puede ser calculada como lo describe la expresión 5.1, mediante cuatro componentes inherentes a la configuración a, la utilidad extrínseca, la utilidad intrínseca, la inversión extrínseca y la inversión intrínseca[30].

- $\check{w}_i : A \to \mathbb{R}$. La utilidad extrínseca, corresponde a la remuneración que el mecanismo de incentivos determina para el agente i, en función de la configuración. El criterio de la función está definido en los cuadros 5.4 y 5.5.

- $\check{v}_i : A \to \mathbb{R}$. La utilidad intrínseca, corresponde al valor monetario que el juego produce para el agente i, en función de la configuración, sin tomar en cuenta el valor monetario que el mecanismo de incentivos produce. El criterio de la función está definido en el cuadro 5.3.

- $\hat{w}_i : A \to \mathbb{R}$. La inversión extrínseca, corresponde al valor monetario que el mecanismo de incentivos extrae del agente i, en función de la configuración. El criterio de la función está definido en los cuadros 5.4 y 5.5.

- $\hat{v}_i : A \to \mathbb{R}$. La inversión intrínseca, corresponde al valor monetario que el juego extrae del agente i, en función de la configuración, sin tomar en cuenta el valor monetario que el mecanismo de incentivos extrae. El criterio de la función está definido en el cuadro 5.3.

[30] El agente i podría esperar, al elegir una acción mediante la que pueda contribuir, experimentar un efecto adverso, en este caso, la expectativa influiría en el valor representado mediante el componente $\hat{v}_i(a)$.

$$r_i(a) = \left(\check{v}_i(a) + \check{w}_i(a)\right) - \left(\hat{v}_i(a) + \hat{w}_i(a)\right) \tag{5.1}$$

$$\forall\, i : N;\, a : A.$$

Al definir la función de utilidad como en la expresión 5.1, podemos evaluar la remuneración que el mecanismo de incentivos determina, para cualquier configuración a' en cuanto a cualquier otra configuración a, como en la expresión 5.2. En esta expresión podemos interpretar, para el juego, y para el agente i, a $\check{v}_i(a) + \check{w}_i(a)$ como la utilidad bruta, y a $\hat{v}_i(a) + \hat{w}_i(a)$ como la inversión bruta, mientras que podemos interpretar a $\check{w}_i(a) - \hat{w}_i(a)$ como la utilidad extrínseca neta, y a $\check{v}_i(a) - \hat{v}_i(a)$ como la utilidad intrínseca neta.

$$\begin{aligned} &r_i(a') \geq r_i(a) \Leftrightarrow \\ &\left(\check{w}_i(a') - \hat{w}_i(a')\right) \geq \left(\check{v}_i(a) - \hat{v}_i(a)\right) - \left(\check{v}_i(a') - \hat{v}_i(a')\right) + \left(\check{w}_i(a) - \hat{w}_i(a)\right) \end{aligned} \tag{5.2}$$

$$\forall\, i : N;\, a, a' : A.$$

5.1.1. Diseño del mecanismo de tokenización

El diseño del mecanismo de incentivos propuesto en la sección 5.2 requiere de una medida de seguridad, en particular, ante un ataque sybil[31], un ataque mediante el que el adversario podría intentar recibir una remuneración, sin ameritarla. Como medida de seguridad, hemos diseñado otro mecanismo, el "mecanismo de tokenización", un mecanismo basado en el axioma 5.1.2.

Definición 5.1.1 (Mecanismo de tokenización)**.** *Conjunto de reglas del protocolo de consenso sobre la administración monetaria.*

El mecanismo de tokenización permitiría que desde cualquier cadena de suministro sea posible definir una criptodivisa, y luego administrarla[32] para que la transferencia de la remuneración, correspondiente a cualquier recurso, pueda ser efectuada mediante una criptodivisa definida desde una cadena de suministro. Eso sí, para garantizar que la transferencia de cada remuneración sea efectuada mediante una criptodivisa definida desde una cadena de suministro, no debería existir una criptodivisa nativa[33].

Axioma 5.1.2. *El valor monetario de cualquier recurso es relativo a la razón entre su demanda y su oferta.*

[31] Un ejemplo de ataque sybil podría ser uno que inicie con la apertura de múltiples cuentas por parte de uno o varios adversarios organizados, desde las que posteriormente, algunos efectúen transacciones que generen trayectorias circulares, sin que mediante ellas transfieran algún recurso físico.

[32] Administrar la emisión de moneda, inclusive. Actualmente, el despliegue de una nueva criptodivisa, para la que el desarrollador pueda administrar su emisión, está al alcance de cualquier internauta.

[33] En un escenario como el descrito en el ejemplo de ataque sybil, el mecanismo de tokenización garantizaría que el valor de la criptodivisa del adversario, esté disgregado del valor de las otras criptodivisas, el adversario sí recibiría la remuneración, pero la recibiría en la criptodivisa administrada por el usuario que registro el recurso ficticio.

Según el axioma 5.1.2, para que la administración no requiera de la confianza por parte de la comunidad de usuarios, la criptodivisa debería estar respaldada, podría estar respaldada por la producción de la cadena de suministro, en este caso, el administrador de la cadena de suministro debería estar dispuesto siempre a aceptar cualquier transferencia en la criptodivisa de la cadena de suministro como forma de pago.

Definición 5.1.3 (Criptodivisa logística)**.** *Cualquier criptodivisa que esté respaldada por la producción de una cadena de suministro.*

La inexistencia de una criptodivisa nativa, en el sistema de criptodivisa, permitiría que la transferencia de cada remuneración sea efectuada mediante una criptodivisa logística, esto es necesario para garantizar la seguridad del mecanismo de incentivos, pero podría generar un costo indeseable para cualquier administrador que implemente el mecanismo de incentivos. Como solución a este problema, proponemos desarrollar un conjunto de herramientas que permitan contrarrestar el costo indeseable, si lo hay. Tales herramientas trabajarían con el sistema de criptodivisa, y estarían disponibles para cualquier administrador que implemente el mecanismo de incentivos.

Definición 5.1.4 (Herramientas de tokenización)**.** *Conjunto de herramientas mediante las que es posible contrarrestar cualquier costo que derive de la implementación del mecanismo de incentivos.*

Una de las funciones de las herramientas de tokenización, que permitiría generar valor para contrarrestar cualquier costo que derive de la implementación del mecanismo de incentivos, sería la de facilitar las labores inherentes a la administración de la criptodivisa correspondiente, otras funciones podrían facilitar la automatización de algunos procesos comunes a través de las cadenas de suministro, procesos que derivan de las labores de logística, de gestión del inventario, de previsión y planificación de la demanda, entre otras.

5.1.2. Comportamiento

Es necesario reconocer al menos dos estrategias elegibles por cada agente en el sistema económico, la estrategia mediante la que el agente contribuye en la transición hacia la Economía Circular, y la estrategia mediante la que el agente no contribuye. La oferta de un mecanismo de tokenización podría incentivar la participación en el sistema de criptodivisa, pero el costo de implementación del mecanismo de incentivos podría desincentivar la contribución en la transición hacia la Economía Circular, por lo que conviene reconocer una tercera estrategia elegible, para tomarla en cuenta en el análisis[34], la estrategia mediante la que el agente no contribuye en la transición, pero sí participa en el sistema de criptodivisa.

En cada juego, para cada participante, debe existir una acción que describa los detalles, relevantes para esta investigación, sobre la adquisición del recurso por parte del participante, una acción que pueda ser identificada con una estrategia, para esto hemos definido la siguiente lista de propiedades[35]. Cada una de las propiedades en la lista es exhibida por al menos una acción. El cuadro 5.2 define a cada acción disponible en función de sus propiedades, y la ecuación 5.3 permite reconocer el perfil para el que cada acción está disponible.

1. Uso de la cuenta

2. Uso del mecanismo de tokenización

[34] El acceso a las herramientas de tokenización requeriría de la implementación del mecanismo de incentivos, pero el acceso al mecanismo de tokenización no la requeriría. El tratamiento de la tercera estrategia nos permitió reconocer como una necesidad, la oferta de las herramientas de tokenización.

[35] La lista incluye la propiedad "participación en el trabajo de minería" para poder tomar en cuenta en el análisis, a cualquier utilidad o inversión inherente a la participación en el trabajo de minería.

3. Contribución en la transición hacia la Economía Circular

4. Participación en el trabajo de minería

Es ideal que, la inversión en recursos, en recursos energéticos inclusive, que el trabajo de minería requiera sea la mínima, por coherencia con el paradigma de la Economía Circular, por otro lado, la implementación de un protocolo que exija la prueba de trabajo requeriría a posteriori de una inversión alta en energía por parte de la red subyacente, por lo tanto, no conviene implementar un protocolo de este tipo. Además, la inexistencia de una criptodivisa nativa evita que sea posible implementar un esquema de minería remunerativa como parte del protocolo, por lo que proponemos un esquema de minería *ad honorem*, un esquema en el que el trabajo de minería sea delegado a los agentes que estén interesados en la oferta del sistema de criptodivisa[36].

Cualquier agente debería recibir la remuneración si y solo si elige una acción que exhiba la tercera propiedad[37]. La siguiente lista describe cada combinación de propiedades correspondiente a alguna de las acciones, relevantes para esta investigación, disponibles en el sistema económico, el cuadro 5.2 contiene una versión sistemática de la descripción. Cualquier combinación que no esté en la lista no corresponde a una acción disponible en el sistema económico.

- 0. Corresponde a cualquier transacción que no sea efectuada mediante el sistema de criptodivisa.
- 1000. Corresponde a cualquier transacción que no contribuya en la transición hacia la Economía Circular, que sea efectuada mediante el sistema de criptodivisa, por un agente que no haya usado el mecanismo de tokenización y que no participe en el trabajo de minería.
- 1100. Corresponde a cualquier transacción que no contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que haya usado el mecanismo de tokenización, pero que no participe en el trabajo de minería.
- 1010. Corresponde a cualquier transacción que contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que no haya usado el mecanismo de tokenización y que no participe en el trabajo de minería.
- 1110. Corresponde a cualquier transacción que contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que haya usado el mecanismo de tokenización, pero que no participe en el trabajo de minería.
- 1001. Corresponde a cualquier transacción que no contribuya en la transición hacia la Economía Circular, que sea efectuada mediante el sistema de criptodivisa, por un agente que no haya usado el mecanismo de tokenización, pero que participe en el trabajo de minería.
- 1101. Corresponde a cualquier transacción que no contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que haya usado el mecanismo de tokenización y que participe en el trabajo de minería.

[36] Sin embargo, es necesario considerar que, el hecho de que el trabajo de minería no sea remunerado, puede influir en el interés de cualquier agente por participar. El efecto de la participación en el trabajo de minería, por parte del agente i, para la configuración a, influye en el valor representado mediante el componente $\hat{v}_i(a)$.

[37] Según nuestra definición de circularidad, una acción contribuye a la Economía Circular si contribuye en la generación de una trayectoria que sea reconocida por el autómata 4.2. Una acción es descrita por la tercera propiedad si también es descrita por la primera propiedad, esto porque cualquier contribución es identificada como tal, según nuestra definición de circularidad.

- 1011. Corresponde a cualquier transacción que contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que no haya usado el mecanismo de tokenización, pero que participe en el trabajo de minería.

- 1111. Corresponde a cualquier transacción que contribuya en la transición hacia la Economía Circular, que sea efectuada por un agente que haya usado el mecanismo de tokenización y que participe en el trabajo de minería.

Cuadro 5.2: Descripción de cada una de las acciones disponibles en el modelo de juego. Cada columna representa a una acción, y cada acción está definida por las propiedades en 1 que le corresponden.

Propiedad									
Uso de la cuenta	0	1	1	1	1	1	1	1	1
Uso del mecanismo de tokenización	0	0	1	0	1	0	1	0	1
Contribución a la Economía Circular	0	0	0	1	1	0	0	1	1
Participación en la minería	0	0	0	0	0	1	1	1	1

$$A_i = \begin{cases} 0, 1100, 1110, 1101, 1111 & \theta(i) \neq 4 \\ \\ 0, 1000, 1010, 1001, 1011 & \theta(i) = 4 \end{cases} \tag{5.3}$$

En función de la descripción de las acciones en el cuadro 5.2, podemos reconocer a la estrategia 1, mediante la que el agente contribuye en la transición hacia la Economía Circular, caracterizada por las acciones 1010, 1110, 1011 y 1111; a la estrategia 2, mediante la que el agente participa en el sistema de criptodivisa, pero no contribuye en la transición hacia la Economía Circular, caracterizada por las acciones 1000, 1100, 1001 y 1101; y a la estrategia 3, mediante la que el agente no participa en el sistema de criptodivisa, caracterizada por una sola acción, la acción 0.

Criterio de decisión

La tupla $(\upsilon_i, \psi_i, \dot{\upsilon}_i, \dot{\psi}_i, \mathring{\upsilon}_i, \mathring{\psi}_i)$ representa el criterio de decisión para cada agente i, esta está compuesta por dos componentes por cada estrategia, tales que reflejen la preferencia del agente por una u otra estrategia. Según el cuadro 5.3, $\mathring{\upsilon}_i : \mathbb{R}$ y $\mathring{\psi}_i : \mathbb{R}$ corresponden respectivamente a la utilidad intrínseca y a la inversión intrínseca al aplicar la estrategia 1, $\dot{\upsilon}_i : \mathbb{R}$ y $\dot{\psi}_i : \mathbb{R}$ corresponden respectivamente a la utilidad intrínseca y a la inversión intrínseca al aplicar la estrategia 2, y $\upsilon_i : \mathbb{R}$ y $\psi_i : \mathbb{R}$ corresponden respectivamente a la utilidad intrínseca y a la inversión intrínseca al aplicar la estrategia 3.

Cuadro 5.3: Criterio de las funciones $\check{\nu}_i$ y $\hat{\nu}_i$ para la acción a_i (en la configuración a) tal que no implique participación en el trabajo de minería.

a_i	$\check{\nu}_i(a)$	$\hat{\nu}_i(a)$
0	υ_i	ψ_i
1000	$\dot{\upsilon}_i$	$\dot{\psi}_i$
1100	$\dot{\upsilon}_i$	$\dot{\psi}_i$
1010	$\mathring{\upsilon}_i$	$\mathring{\psi}_i$
1110	$\mathring{\upsilon}_i$	$\mathring{\psi}_i$

La tupla, mediante la expresión 5.4, nos permite identificar como[38] $\mathring{\Delta}_i : \mathbb{R}$ a la utilidad intrínseca neta obtenida mediante la estrategia 1, como $\dot{\Delta}_i : \mathbb{R}$ a la utilidad intrínseca neta obtenida mediante la estrategia 2, y como $\Delta_i : \mathbb{R}$ a la utilidad intrínseca neta obtenida mediante la estrategia 3, para el agente i.

$$\begin{aligned} \mathring{\Delta}_i &= \mathring{v}_i - \mathring{\psi}_i, \\ \dot{\Delta}_i &= \dot{v}_i - \dot{\psi}_i, \\ \Delta_i &= v_i - \psi_i \end{aligned} \tag{5.4}$$

Ningún componente del criterio de decisión representa alguna utilidad o inversión inherente a la participación en el trabajo de minería. El cuadro 5.3 permite suponer que el componente $\check{v}_i(a)$ refleja la utilidad inherente a la participación en el trabajo de minería, y que el componente $\hat{v}_i(a)$ refleja la inversión inherente a la participación en el trabajo de minería, para cada agente i y configuración a. La siguiente lista describe algunas condiciones que pueden influir en el criterio de decisión.

- Al implementar una configuración circular, el diseño del producto puede ser más costoso, puede requerir diferentes procesos, materiales, o incluso el habilitamiento de una cadena de suministro inversa [7].
- Con frecuencia, el diseño del producto se prefiere simple, y se varía poco. El consumo de productos descartables puede ser percibido como más "exclusivo" [7].
- El almacenamiento de recursos que estén finalizando su ciclo de vida podría comprometer el volumen de ventas, ya que requeriría de espacio que podría ser ocupado en el almacenamiento de recursos que estén iniciando su ciclo de vida [7].
- Un sistema de criptodivisa puede facilitar la descentralización de la economía, y una cadena de bloques puede permitir obtener información muy acertada sobre la oferta y la demanda de cada recurso que haya sido registrado en ella, por lo que puede facilitar una mejor distribución de los recursos [4].
- Una cadena de bloques también puede facilitar la coordinación y la automatización de una cadena de suministro, incluso si esta es altamente sofisticada, en términos de verificación, regulación, financiación, e intercambio de información. Esto, finalmente, puede promover la eficiencia la cadena de suministro [4].
- La implementación de una cadena de bloques puede comprometer la seguridad y la privacidad de la información que sea registrada en ella [4].

Haller *et al.* estudiaron las tendencias de consumo en el año 2 020, según el reporte en el que publicaron los resultados del estudio, es plausible que ahora exista un conjunto de agentes interesados en el cambio de paradigma, un conjunto de agentes que eventualmente participen y contribuyan con el cambio, y que tal evento provoque que emerja el comportamiento colectivo descrito en la hipótesis. En el reporte, los autores expresan lo siguiente.

"Los consumidores cada vez más adoptan causas sociales, buscan productos y marcas que se alineen con sus valores. Cerca de seis de cada 10 consumidores entrevistados están dispuestos a cambiar sus hábitos de compra para reducir su impacto ambiental. Cerca de ocho de cada 10 entrevistados indican que la sustentabilidad es importante para ellos. Y para aquellos que indican que es muy/extremadamente importante, más del 70 % pagarían un

[38] En este documento, cada componente decorado mediante el símbolo $\mathring{}$ corresponde a un concepto relativo a la estrategia 1, y cada componente decorado mediante el símbolo $\dot{}$ corresponde a un concepto relativo a la estrategia 2.

extra de 35 %, en promedio, para marcas que son sustentables y responsables con el medio ambiente." [19]

"Las compañías de comercio minorista y productos de consumo en todo el mundo han incrementado su foco en la sustentabilidad en los últimos cinco años. Desde el 2 014, las inversiones globales sustentables y responsables con el medio ambiente han crecido 68 % y llegan ahora a los 30 billones de USD. Cada vez más, el conocimiento sobre cuestiones ambientales globales está cambiando los hábitos del consumidor sin importar donde vivan." [19]

"Con la sustentabilidad al frente y al centro, los consumidores hacen más que solo revisar la lista de ingredientes en una etiqueta. Ellos quieren detalles del origen, cómo son hechos y procesados los productos, también el cómo son entregados. De los consumidores entrevistados, el 73 % indica que la rastreabilidad de productos es importante para ellos. De los que dicen que este criterio es muy importante, 71 % pagaría un sobreprecio por ello. Los compradores también buscan información sobre las políticas de sustentabilidad corporativas. Muchos quieren garantías de que las marcas apoyan el reciclaje, fondean causas caritativas, o toman otras acciones que demuestren responsabilidad social." [19]

5.2. Diseño del mecanismo de incentivos

El diseño del mecanismo de incentivos, mediante una implementación consistente con la expresión 5.5, podría promover la participación y la contribución por parte de cada agente, sea interno o sea externo, para promover la participación, el sistema de criptodivisa debe implementar las funciones del dinero[39] al menos tanto como cualquier sistema de criptodivisa disponible hasta ahora, y para promover la contribución, cada agente, sea interno[40] o sea externo, al contribuir, debe poder recibir una remuneración. En la expresión 5.5, $\nabla : (\operatorname{seq} \mathbb{N}) \times \Theta \to \mathbb{R}$ corresponde al cálculo de la remuneración para cualquier agente i, según su perfil $\theta(i)$ y la trayectoria σ del recurso. En la expresión, φ corresponde al valor monetario del recurso, $\ell_{-4} : (\operatorname{seq} \mathbb{N}) \to \mathbb{N}$ corresponde al cálculo de la cardinalidad de la cadena interna y $\ell_4 : (\operatorname{seq} \mathbb{N}) \to \mathbb{N}$ corresponde al cálculo de la cardinalidad de la cadena externa[41].

$$\nabla\big(\sigma, \theta(i)\big) = \begin{cases} \check{h}_{-4} \cdot \frac{\varphi}{\ell_{-4}(\sigma)} & \theta(i) \neq 4 \\ \check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)} & \theta(i) = 4 \end{cases} \tag{5.5}$$

$$\forall\, i : N;\ \sigma : \operatorname{seq} \mathbb{N};\ \theta(i) : \Theta \bullet \exists\, \check{h}_{-4}, \check{h}_4 : [0,1];\ \varphi : \mathbb{R}.$$

Cada coeficiente $\check{h}_{-4}$ y $\check{h}_4$ define la remuneración en función del valor monetario del recurso. Cada administrador que implemente el mecanismo de incentivos debe determinar el valor de cada coeficiente, junto con el valor monetario del recurso, que corresponde al costo por el que lo adquirirá el primer agente externo en la trayectoria. El cálculo en la expresión 5.5 permite determinar la proporción del valor monetario del recurso que sería remunerado

[39] El dinero tradicional sirve como (1) medio de intercambio, (2) reserva de valor y (3) unidad de medida [20].

[40] Es necesario para cada agente interno, si la cadena de suministro no es monolítica, i.e., una cadena en la que no existe una coalición ente varios agentes internos.

[41] Con cardinalidad de la cadena nos referimos a la cantidad de agentes que la componen. El subíndice 4 indica que el valor es relativo al perfil 4, y el subíndice −4 indica que el valor no es relativo al perfil 4, que lo es a los otros perfiles.

a cada agente al final del ciclo de vida del recurso, en función de $\check{h}_{-4}$ si el agente es interno, o en función de $\check{h}_4$ si el agente es externo[42].

Cuadro 5.4: Criterio de $\check{w}_i$ y $\hat{w}_i$ para el agente i, en función de la configuración a (de la acción a_i) en el caso $\theta(i) \neq 4$, con $\check{h}_{-4} : [0,1]$ como el *ratio* que define la remuneración para la cadena interna, con $\varphi : \mathbb{R}$ como el valor monetario del recurso, y con $\sigma : \text{seq}\,\mathbb{N}$ como la trayectoria del recurso. El criterio de $\hat{h}_{-4} : N \to [0,1]$ determina la proporción que cada agente invierte para habilitar la transferencia de la remuneración a la cadena interna. El criterio de $\hat{h}_4 : N \to [0,1]$ determina la proporción que cada agente invierte para habilitar la transferencia de la remuneración a la cadena externa. El criterio de $h_0 : N \to \mathbb{R}$ correspondería al cálculo del valor, interpretado como valor monetario, de las herramientas de tokenización, para cada agente.

a_i	$\check{w}_i(a)$	$\hat{w}_i(a)$
0	0	0
1100	$h_0(i)$	0
1110	$\check{h}_{-4} \cdot \frac{\varphi}{\ell_{-4}(\sigma)} + h_0(i)$	$\big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big) \cdot \varphi$
1101	$h_0(i)$	0
1111	$\check{h}_{-4} \cdot \frac{\varphi}{\ell_{-4}(\sigma)} + h_0(i)$	$\big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big) \cdot \varphi$

En el cuadro 5.4, el componente $\check{w}_i(a)$ toma en cuenta la remuneración que obtiene el agente i, y el valor para el agente i, interpretado como valor monetario, de las herramientas de tokenización; y el componente $\hat{w}_i(a)$ toma en cuenta el valor, también interpretado como valor monetario, que el agente i invierte para habilitar la transferencia de la remuneración. En la práctica, el mecanismo de tokenización permitiría emitir nueva moneda, la suficiente para evitar que uno, al menos uno, de los agentes deba transferir un monto desde su "cuenta" corriente para habilitar la transferencia de la remuneración, sin embargo es necesario que el componente $\hat{w}_i(a)$ tome en cuenta el valor que el agente invierte para habilitar la transferencia de la remuneración, esto porque la emisión de nueva moneda podría influir en el valor monetario de la moneda existente, emitida por la administración[43].

Cuadro 5.5: Criterio de $\check{w}_i$ y $\hat{w}_i$ para el agente i, en función de la configuración a (de la acción a_i) en el caso $\theta(i) = 4$, con $\check{h}_4 : [0,1]$ como el *ratio* que define la remuneración para la cadena externa, con $\varphi : \mathbb{R}$ como el valor monetario del recurso, y con $\sigma : \text{seq}\,\mathbb{N}$ como la trayectoria del recurso. El criterio de $\hat{h}_{-4} : N \to [0,1]$ determina la proporción que cada agente invierte para habilitar la transferencia de la remuneración a la cadena interna. El criterio de $\hat{h}_4 : N \to [0,1]$ determina la proporción que cada agente invierte para habilitar la transferencia de la remuneración a la cadena externa. El criterio de $h_0 : N \to \mathbb{R}$ correspondería al cálculo del valor, interpretado como valor monetario, de las herramientas de tokenización, para cada agente.

a_i	$\check{w}_i(a)$	$\hat{w}_i(a)$
0	0	0
1000	0	0
1010	$\check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)}$	$\big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big) \cdot \varphi$
1001	0	0
1011	$\check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)}$	$\big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big) \cdot \varphi$

El cuadro 5.4 incluye el componente $h_0(i)$, el componente representa el valor para el

[42] Esta diferenciación disuade a cualquier agente de intentar influir significativamente en el monto por cualquiera de las remuneraciones que pueda obtener; y disuade a cualquier agente externo de intentar manipular, después de la implementación, la remuneración que cualquier agente interno pueda recibir, y a la inversa. La sección 7.2.2 profundiza en esta característica, mediante las proposiciones 7.2.4, 7.2.5, 7.2.6 y 7.2.7.

[43] Esto podría afectar a cualquier agente que posea parte de la moneda existente, ya que podría provocar un efecto inflacionario, en otras palabras, podría provocar la pérdida del poder adquisitivo mediante la moneda, o inversamente, el incremento del costo de los recursos en tal moneda, para los consumidores y los productores en cualquier cadena de suministro.

agente i, interpretado como valor monetario, de las herramientas de tokenización. El cuadro 5.5 no lo incluye porque solo es relevante para los agentes internos, el componente $\check{v}_i(a)$ toma en cuenta cualquier utilidad que pueda derivar del uso del sistema de criptodivisa, interpretada como valor monetario, para cualquier agente i, si es externo, según la configuración a.

El sistema de inecuaciones 5.6 expresa que, el sistema de criptodivisa debe implementar un mecanismo de incentivos mediante el que sea posible que cada agente, al contribuir en la transición, reciba una remuneración. El ejemplo 5.2.1 ilustra el ciclo de vida de un recurso cualquiera, y el efecto del mecanismo de incentivos en la utilidad de cada participante.

$$\begin{aligned} h_0(i) &> 0, \\ \check{h}_{-4} &> 0, \\ \check{h}_4 &\geq 0 \end{aligned} \tag{5.6}$$

$$\forall\, i : N \bullet \exists\, \check{h}_{-4}, \check{h}_4 : [0,1].$$

Ejemplo 5.2.1. Al describir el ciclo de vida de la cerveza en el ejemplo 4.3.3 mediante el modelo de juego, si suponemos que las tres transacciones son efectuadas mediante un sistema de criptodivisa, que Cenizo y Jacinto enlazan sus cuentas para establecer una cadena de suministro, implementan el mecanismo de incentivos e implementan las herramientas de tokenización, según la expresión 5.5, con $\check{h}_{-4} = 0{,}006$ y $\check{h}_4 = 0{,}012$, entonces podríamos definir a N como $\{1,2,3\}$, con (1) Cenizo, (2) Jacinto y (3) Simposio; y a los perfiles de agente como $\theta(1) = 2$, $\theta(2) = 3$ y $\theta(3) = 4$; para cada acción a_i, correspondiente al agente i, del cuadro 5.2 podríamos inferir que $a_i = 1110$ si $i = 1$, $a_i = 1110$ si $i = 2$ y $a_i = 1010$ si $i = 3$. Si también suponemos que Simposio compra la cerveza en ¢10, Jacinto compra la docena de botellas en ¢96 y Cenizo compra el envase a Simposio[44] en ¢0; y que Cenizo y Jacinto consideran que las herramientas de tokenización contribuyen en ¢0,1 a cada uno en este ciclo, entonces, según la expresión 5.1, $r_1(a_1,\ldots,a_3) = 2{,}07$, $r_2(a_1,\ldots,a_3) = 2{,}07$ y $r_3(a_1,\ldots,a_3) = 2{,}06$. El cuadro 5.6 desglosa la utilidad de cada agente.

Cuadro 5.6: Desglose de la utilidad de cada agente i en el ejemplo 5.2.1, sea $a : A$ tal que $a = a_1,\ldots,a_3$. Adicionalmente, se supone que Cenizo invierte ¢6 en cada cerveza que vende, y que cada una de estas cervezas genera un bienestar equivalente a ¢12 para Simposio.

i	$\check{v}_i(a)$	$\check{w}_i(a)$	$\hat{v}_i(a)$	$\hat{w}_i(a)$	$r_i(a)$
1	8	$0{,}006 \cdot \frac{10}{2} + 0{,}1$	6	$(0{,}002 + 0{,}004) \cdot 10$	2,07
2	10	$0{,}006 \cdot \frac{10}{2} + 0{,}1$	8	$(0{,}002 + 0{,}004) \cdot 10$	2,07
3	12	$0{,}012 \cdot \frac{10}{1}$	10	$(0{,}002 + 0{,}004) \cdot 10$	2,06

5.3. Análisis del mecanismo de incentivos

El comportamiento de la población "ideal", sería el de una población que genera trayectorias circulares, solamente. Creemos que, en cualquier población, bajo el efecto del mecanismo de incentivos, a partir de cierto tiempo, el comportamiento de la población cambiaría, se aproximaría al comportamiento de la población ideal, en otras palabras, a partir de cierto tiempo, la actividad de la población se concentraría en un subconjunto de posibles juegos en los que cada agente obtendría la utilidad neta máxima, para él, al contribuir en la transición.

[44] Simposio vende el envase para obtener la remuneración.

En otras palabras, en cualquier juego de tal subconjunto, se alcanzaría el "equilibrio" si cada agente en el juego contribuye en la transición, según la definición 1.2.2, la definición de Equilibrio de Nash. La proposición 5.3.1 afirma que un juego con esta propiedad es posible, la demostración de la proposición puede facilitar el cálculo del valor para los *ratios* $\check{h}_{-4}$ y $\check{h}_4$ en la expresión 5.5, el corolario 5.3.2 resume cada una de las expresiones en la demostración que pueda facilitarlo.

La expresión 5.7 afirma, sin pérdida de generalidad[45] que, en los casos (a) $\mathring{a}_i = 1100 \wedge a_i = 0$, (b) $\mathring{a}_i = 1000 \wedge a_i = 0$, (c) $\mathring{a}_i = 1110 \wedge a_i = 1100$ o (d) $\mathring{a}_i = 1010 \wedge a_i = 1000$, para cada posible configuración que genere una trayectoria circular, para cada agente i que contribuya en la transición o solo participe en el sistema de criptodivisa, la utilidad es mayor o igual que al no contribuir o no participar, respectivamente. La expresión 5.7, con "$i = j \veebar \mathring{a}_j = a_j$" afirma que si las acciones $\mathring{a}_j$ y a_j difieren, lo hacen solo en el recurso al que se refieren, e i y j identifican diferentes agentes, o afirma que las acciones $\mathring{a}_j$ y a_j difieren, e i y j identifican al mismo agente. En la misma expresión, con "$\mathring{a}_i \approx a_i$" afirmamos que las acciones $\mathring{a}_i$ y a_i se refieren a recursos con funciones idénticas o en su defecto no se refieren a un recurso.

Proposición 5.3.1. *En cada juego existe al menos una solución que satisface la expresión 5.7, para cada agente, independientemente de su perfil.*

$$\begin{aligned}
&\forall\, i,j : N; (\mathring{a}_1,\ldots,\mathring{a}_n),(a_1,\ldots,a_n) : A \mid i = j \veebar \mathring{a}_j = a_j \\
&\quad \bullet\ \mathring{a}_i \approx a_i \wedge r_i(\mathring{a}_1,\ldots,\mathring{a}_n) \geq r_i(a_1,\ldots,a_n) \wedge \\
&\qquad \begin{cases} \theta(i) \neq 4 \wedge \big((\mathring{a}_i = 1110 \wedge a_i = 1100) \vee (\mathring{a}_i = 1100 \wedge a_i = 0)\big) \vee \\ \theta(i) = 4 \wedge \big((\mathring{a}_i = 1010 \wedge a_i = 1000) \vee (\mathring{a}_i = 1000 \wedge a_i = 0)\big) \end{cases}
\end{aligned} \tag{5.7}$$

Demostración.

1. *Según la expresión 5.7:* para cada par de posibles configuraciones que solo difieran en la acción que corresponde al agente i, existe al menos una solución que satisface la inecuación $r_i(\mathring{a}_1,\ldots,\mathring{a}_n) \geq r_i(a_1,\ldots,a_n)$.
2. *En el caso b, según el punto 1, la expresión 5.1 y los cuadros 5.3 y 5.5:* $\theta(i) = 4 \wedge \Big(\dot{v}_i + 0\Big) - \Big(\dot{\psi}_i + 0\Big) \geq \Big(v_i + 0\Big) - \Big(\psi_i + 0\Big)$.
3. *En el caso b, según el punto 2 y la expresión 5.4:* $\theta(i) = 4 \wedge \Delta_i \leq \dot{\Delta}_i$.
4. *En el caso a, según el punto 1, la expresión 5.1 y los cuadros 5.3 y 5.4:* $\theta(i) \neq 4 \wedge \Big(\dot{v}_i + h_0(i)\Big) - \Big(\dot{\psi}_i + 0\Big) \geq \Big(v_i + 0\Big) - \Big(\psi_i + 0\Big)$.
5. *En el caso a, según el punto 4 y la expresión 5.4:* $\theta(i) \neq 4 \wedge \Delta_i - h_0(i) \leq \dot{\Delta}_i$.
6. *En el caso d, según el punto 1, la expresión 5.1 y los cuadros 5.3 y 5.5:* $\theta(i) = 4 \wedge \Big(\dot{v}_i + \check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)}\Big) - \Big(\dot{\psi}_i + \big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big)\cdot\varphi\Big) \geq \Big(\dot{v}_i + 0\Big) - \Big(\dot{\psi}_i + 0\Big)$.
7. *En el caso d, según el punto 6 y la expresión 5.4:* $\theta(i) = 4 \wedge \dot{\Delta}_i \leq \mathring{\Delta}_i + \check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)} + \big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big)\cdot\varphi$.
8. *En el caso c, según el punto 1, la expresión 5.1 y los cuadros 5.3 y 5.4:* $\theta(i) \neq 4 \wedge \Big(\dot{v}_i + \big(\check{h}_{-4} \cdot \frac{\varphi}{\ell_4(\sigma)} + h_0(i)\big)\Big) - \Big(\dot{\mathring{\psi}}_i + \big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big)\cdot\varphi\Big) \geq \Big(\dot{v}_i + h_0(i)\Big) - \Big(\dot{\psi}_i + 0\Big)$.
9. *En el caso c, según el punto 8 y la expresión 5.4:* $\theta(i) \neq 4 \wedge \dot{\Delta}_i \leq \mathring{\Delta}_i + \check{h}_{-4} \cdot \frac{\varphi}{\ell_4(\sigma)} - \big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big)\cdot\varphi$.
10. *Según los puntos 1, 3 y 7:* la expresión de la inecuación para el caso b es consistente con la expresión de la inecuación para el caso d; existe al menos una solución[46], tal que $\theta(i) = 4$, para la inecuación.

[45] Los casos para la otra alternativa serían (a) $\mathring{a}_i = 1101 \wedge a_i = 0$, (b) $\mathring{a}_i = 1001 \wedge a_i = 0$, (c) $\mathring{a}_i = 1111 \wedge a_i = 1101$, (d) $\mathring{a}_i = 1011 \wedge a_i = 1001$. Según el esquema de minería, podemos distinguir una u otra alternativa.

[46] $\Delta_i \leq \dot{\Delta}_i \leq \mathring{\Delta}_i + \check{h}_4 \cdot \frac{\varphi}{\ell_4(\sigma)} + \big(\hat{h}_{-4}(i) + \hat{h}_4(i)\big)\cdot\varphi$

11. *Según los puntos 1, 5 y 9:* la expresión de la inecuación para el caso a es consistente con la expresión de la inecuación para el caso c; también existe al menos una solución[47], tal que $\theta(i) \neq 4$, para la inecuación. □

Corolario 5.3.2. *Cualquier solución que, según las expresiones 5.1 y 5.4, y los cuadros 5.3, 5.4 y 5.5, satisfaga la expresión 5.7, requiere que, en el juego, para cada agente i,* $\theta(i) = 4$ *y* $\check{h}_4 \geq \left(\dot{\Delta}_i - \mathring{\Delta}_i - (\hat{h}_{-4}(i) + \hat{h}_4(i))\cdot\varphi\right)\cdot\frac{\ell_4(\sigma)}{\varphi}$, *o* $\theta(i) \neq 4$, $\check{h}_{-4} \geq \left(\dot{\Delta}_i - \mathring{\Delta}_i + (\hat{h}_{-4}(i) + \hat{h}_4(i))\cdot\varphi\right)\cdot\frac{\ell_4(\sigma)}{\varphi}$ *y* $h_0(i) \geq \left(\Delta_i - \dot{\Delta}_i\right)$.

A pesar de que la implementación del mecanismo de incentivos según el corolario 5.3.2 pueda facilitar que el comportamiento de la población se aproxime al comportamiento de la población ideal, no lo garantiza. Cada interacción puede causar un "efecto mariposa", un efecto difícil de predecir, en un juego posterior. El capítulo 6 contiene un análisis estadístico del efecto del mecanismo de incentivos, y una descripción del sistema de simulación mediante el que pudimos recopilar los datos necesarios para el análisis estadístico.

[47] $\Delta_i - h_0(i) \leq \dot{\Delta}_i \leq \mathring{\Delta}_i + \check{h}_{-4}\cdot\frac{\varphi}{\ell_4(\sigma)} - \left(\hat{h}_{-4}(i) + \hat{h}_4(i)\right)\cdot\varphi$

Power tends to corrupt and absolute power corrupts absolutely.

—Lord Acton

6

Análisis estadístico del efecto del mecanismo de incentivos

Sinopsis. Este capítulo contiene los resultados de un análisis estadístico mediante el que hemos evaluado el efecto del mecanismo de incentivos, una descripción detallada del método utilizado para el análisis, y la descripción del sistema de simulación mediante el que hemos recopilado los conjuntos de datos necesarios para el análisis. El método requiere dos series de experimentos, mediante las que hemos evaluado el efecto en el sistema económico, sistema que incluye el mecanismo de incentivos, de diferentes poblaciones. En la primera serie, la "serie experimental", el sistema de simulación implementa el mecanismo de incentivos, mientras que, en la segunda serie, la "serie de control", el sistema de simulación no implementa el mecanismo de incentivos. El capítulo finaliza con la interpretación de los resultados del análisis.

6.1. Diseño del método experimental

El diseño del método experimental requiere dos series de experimentos, mediante las que hemos evaluado el efecto en el sistema económico, sistema que incluye el mecanismo de incentivos, de la distribución de la población según la clase de cada agente. El cuadro 6.1 contiene la descripción de cada clase.

En cada una de las simulaciones en la primera serie, la "serie experimental", el sistema de simulación implementa el mecanismo de incentivos, y en cada una de las simulaciones en la segunda serie, la "serie de control", el sistema de simulación no implementa el mecanismo de incentivos. Hemos fijado el tamaño de la población en 512 agentes y el tiempo de simulación en 256 iteraciones, las suficientes para que cada simulación alcance la estabilidad.

El diseño es monofactorial, el factor controlado es la distribución de la población. Hemos definido 24 tratamientos, cada tratamiento corresponde a una combinación de los niveles disponibles para las variables χ_0, χ_1, χ_2 y χ_3, una combinación tal que $\chi_0 \neq \chi_1 \neq \chi_2 \neq \chi_3$, para que la distribución sea diferente en cada tratamiento. Cada variable χ_i representa la cardinalidad del conjunto de agentes de clase *i* para el tratamiento. El tamaño de la población se fijó en 512, por lo que la suma de los niveles en cada tratamiento debió ser 512, los

establecimos en[48] 384, 96, 24 y 8.

Cuadro 6.1: Definición de cada clase, según la expresión 5.4. El valor inicial, tanto de $\dot{\Delta}_i - \Delta_i$ como de $\mathring{\Delta}_i - \dot{\Delta}_i$, para cada agente i es aleatorio, dentro del rango correspondiente. Cada agente inicia con cierta predisposición a favor de alguna estrategia, la predisposición depende de la clase del agente. La última columna indica la estrategia favorecida.

Clase	$\dot{\Delta}_i - \Delta_i$				$\mathring{\Delta}_i - \dot{\Delta}_i$				Predisposición
0	[	−255,	0	[	[	−255,	0	[	$3 > 2, 2 > 1$
1	[	−255,	0	[	]	0,	255	]	$3 > 2, 1 > 2$
2	]	0,	255	]	[	−255,	0	[	$2 > 3, 2 > 1$
3	]	0,	255	]	]	0,	255	]	$2 > 3, 1 > 2$

Hemos evaluado 384 observaciones para cada serie, 16 observaciones para cada uno de los 24 tratamientos, y cada observación ha sido obtenida mediante una simulación completa. Los cuadros 6.2, 6.3 y 6.4 desglosan la configuración de cada tratamiento, el valor que corresponde a cada variable en cada tratamiento.

Cuadro 6.2: Configuración de cada tratamiento, del 1 al 8.

Variable	1	2	3	4	5	6	7	8
χ_0	8	8	8	8	8	8	24	24
χ_1	24	24	96	96	384	384	8	8
χ_2	96	384	24	384	24	96	96	384
χ_3	384	96	384	24	96	24	384	96

Cuadro 6.3: Configuración de cada tratamiento, del 8 al 16.

Variable	9	10	11	12	13	14	15	16
χ_0	24	24	24	24	96	96	96	96
χ_1	96	96	384	384	8	8	24	24
χ_2	8	384	8	96	24	384	8	384
χ_3	384	8	96	8	384	24	384	8

Cuadro 6.4: Configuración de cada tratamiento, del 16 al 24.

Variable	17	18	19	20	21	22	23	24
χ_0	96	96	384	384	384	384	384	384
χ_1	384	384	8	8	24	24	96	96
χ_2	8	24	24	96	8	96	8	24
χ_3	24	8	96	24	96	8	24	8

La variable de respuesta $y_\iota(\jmath)$ corresponde a la cantidad de transacciones circulares entre la cantidad total de transacciones, en cada tratamiento ι y observación $\jmath$, al completar la última iteración. Hemos decidido evaluar la hipótesis mediante un análisis de varianza de la media μ_ι de cada variable de respuesta y_ι.

$$\forall\, i,j : \{1,\ldots,24\} \bullet \mu_i \approx \mu_j \qquad (H_0)$$

[48] Hemos distribuido los 512 de la siguiente manera: (1) $384 = 512 \cdot 3/4$; (2) $96 = 512 \cdot 1/4 \cdot 3/4$; (3) $24 = 512 \cdot 1/4 \cdot 1/4 \cdot 3/4$; (4) $8 = 512 \cdot 1/4 \cdot 1/4 \cdot 1/4$.

$$\exists\, i,j : \{1,\ldots,24\} \mid \mu_i \not\approx \mu_j \qquad (H_1)$$

Aceptar la hipótesis original, la que hemos establecido en el capítulo 1, equivale a aceptar "$H_0 \wedge \neg H_0'$", i.e., aceptar H_0 y rechazar H_0', tal que H_0' y H_1' correspondan a la hipótesis nula y a la hipótesis alternativa, respectivamente, para la serie de control. En este escenario, podríamos decir que, si el mecanismo de incentivos interviene, a partir de cierto tiempo, una cantidad significativa de transacciones contribuye en la transición hacia una economía circular, independientemente de la distribución de la población.

6.2. Modelo del sistema de simulación

El sistema de simulación emula una dinámica económica promovida por la demanda y la oferta de recursos. Cada agente, para cada tipo de recurso, puede disponer de más de, tanto como, o de menos de lo que requiere. El sistema, para cada simulación, registra un historial de transacciones, y completa 256 iteraciones. En el historial, cada transacción corresponde a la transferencia de un recurso, de un agente que no lo requiere a otro agente que sí lo requiere, transferencia mediante la que el agente que sí lo requiere maximiza su utilidad.

Cada transacción es registrada junto con una marca de tiempo que la relaciona con la iteración en la que fue efectuada. El sistema de simulación marca a cada transacción, en función de la predisposición del agente que intenta efectuarla, como una transacción "efectuada mediante el sistema de criptodivisa" o como una transacción "no efectuada mediante el sistema de criptodivisa".

En cada simulación para la serie experimental, en cada transacción, el agente proveedor transfiere al agente consumidor, una remuneración por contribuir en la transición, si la transacción deriva de una acción inherente a la estrategia 1, por otro lado, en cada simulación para la serie de control, en cada transacción, el agente proveedor no transfiere remuneración alguna por contribuir en la transición, el mecanismo de incentivos permanece inactivo.

El sistema de simulación, mediante un algoritmo de aprendizaje, permite que lo que sucede en cada iteración pueda ser diferente de lo que sucedió en la iteración anterior. El algoritmo de aprendizaje, al cabo de cada iteración, aplica un ajuste al criterio de decisión de cada agente, un ajuste tal que, al cabo de cierto tiempo, el agente obtenga una utilidad neta mayor, o igual en el peor caso, que la que habría obtenido sin el ajuste, en otras palabras, el algoritmo de aprendizaje provoca que el equilibrio sea alcanzado, esto para garantizar la calidad de cada observación. El apéndice B contiene una descripción formal del sistema de simulación.

6.3. Análisis de datos

Cada una de las gráficas en las figuras 6.1 y 6.2, según los datos recopilados mediante cada una de las simulaciones[49], refleja el comportamiento de la media de la variable de respuesta en cada iteración, en la serie experimental. La gráfica en el cuadro 6.1 refleja el comportamiento en el tratamiento 1, tratamiento en el que 384 de los 512 agentes iniciaron con cierta predisposición para contribuir con el cambio de paradigma, y la gráfica en la figura 6.2 refleja el comportamiento en el tratamiento 24, tratamiento en el que solo 8 de los 512 agentes iniciaron con cierta predisposición para contribuir con el cambio de paradigma.

[49] El apéndice D contiene los conjuntos de datos correspondientes a la última iteración, en cada tratamiento, para las dos series.

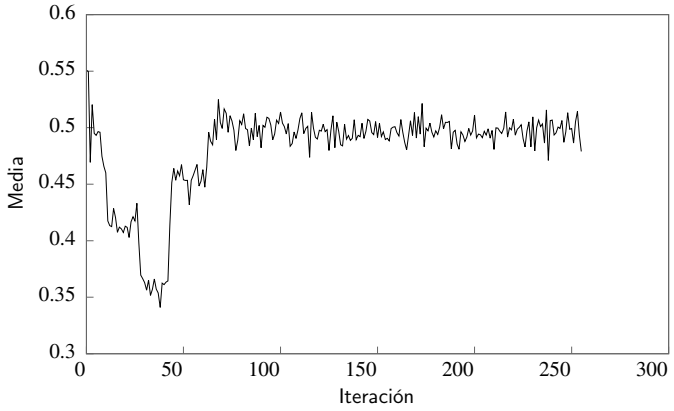

Figura 6.1: Media de la variable de respuesta en la serie experimental, para el tratamiento 1, en cada iteración. En este tratamiento, 384 de los 512 agentes inician con predisposición para contribuir en la transición hacia la Economía Circular.

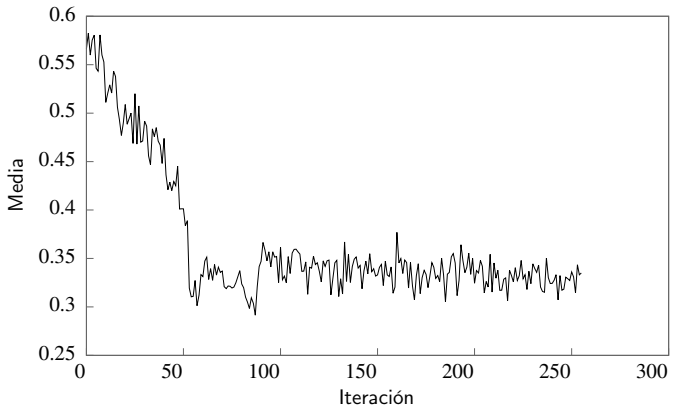

Figura 6.2: Media de la variable de respuesta en la serie experimental, para el tratamiento 24, en cada iteración. En este tratamiento, solo 8 de los 512 agentes inician con predisposición para contribuir en la transición hacia la Economía Circular.

Cada una de las gráficas en las figuras 6.3 y 6.4, según los datos recopilados mediante cada una de las simulaciones, refleja el comportamiento de la media de la variable de respuesta durante el tiempo transcurrido, en la serie de control. La gráfica en la figura 6.3 refleja el comportamiento en el tratamiento 1, tratamiento en el que 384 de los 512 agentes inician con cierta predisposición para contribuir con el cambio de paradigma, y la gráfica en la figura 6.4 refleja el comportamiento en el tratamiento 24, tratamiento en el que solo 8 de los 512 agentes iniciaron con cierta predisposición para contribuir con el cambio de paradigma.

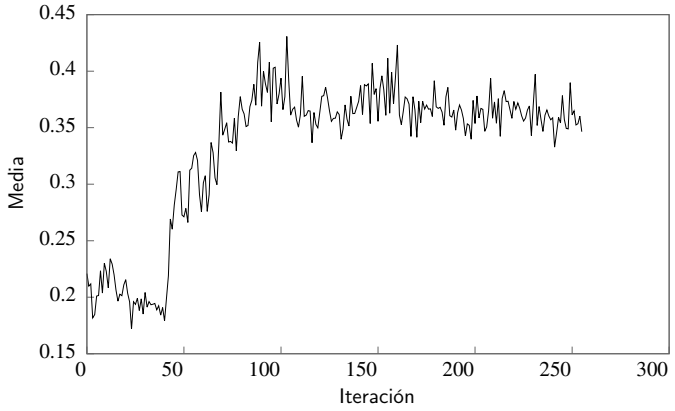

Figura 6.3: Media de la variable de respuesta en la serie de control, para el tratamiento 1, en cada iteración. En este tratamiento, 384 de los 512 agentes inician con predisposición para contribuir en la transición hacia la Economía Circular.

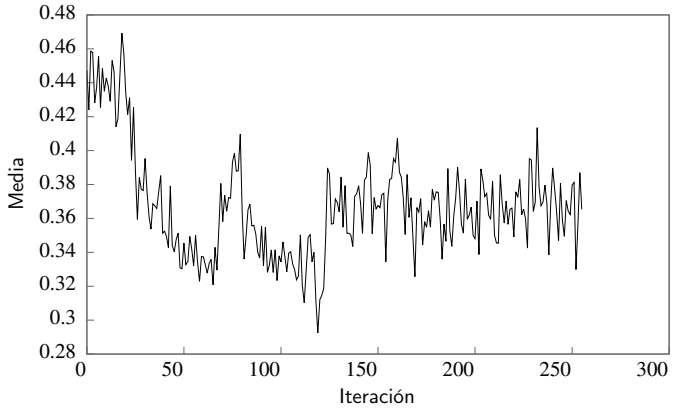

Figura 6.4: Media de la variable de respuesta en la serie de control, para el tratamiento 24, en cada iteración. En este tratamiento, solo 8 de los 512 agentes inician con cierta predisposición para contribuir en la transición hacia la Economía Circular.

El cuadro 6.7 resume el conjunto de los datos recopilados mediante la serie experimental. Establecimos el nivel de significancia para evaluar la hipótesis nula en 0,1, i.e., para aceptar la hipótesis nula, el valor[50] p debe ser mayor a 0,1.

El cuadro 6.5 resume los resultados del análisis de varianza para la serie experimental. Según el cuadro, no hay suficiente evidencia para rechazar la hipótesis nula, el valor p es mayor que el nivel de significancia que establecimos, $0{,}11 > 0{,}1$, por lo que hemos concluido que no hay evidencia de que la distribución de la población, según la clase de cada agente, influye en el efecto del mecanismo de incentivos.

[50] En el análisis de varianza para la serie de control, por convención, F es el *ratio* entre la media de los cuadrados "entre los tratamientos" y la media de los cuadrados "dentro de los tratamientos", y el valor p es la probabilidad de obtener un valor para F mayor o igual que el obtenido en el análisis si la hipótesis nula es verdadera. En el análisis de varianza para la serie experimental, F' es el *ratio* entre la media de los cuadrados "entre los tratamientos" y la media de los cuadrados "dentro de los tratamientos", y el valor p' es la probabilidad de obtener un valor para F' mayor o igual que el obtenido en el análisis si la hipótesis nula es verdadera.

Cuadro 6.5: Resultados del análisis de varianza para la serie experimental. Con "Entre" nos referimos a "entre los tratamientos" y con "Dentro" a "dentro de los tratamientos".

Origen de las variaciones	Entre	Dentro	Total
Suma de cuadrados	4,441 221 129	49,973 609 67	54,414 830 8
Grados de libertad	23	360	383
Media de los cuadrados	0,193 096 571	0,138 815 582	
F	1,391 029 504		
Valor p	0,110 237 936		
Valor crítico para F	1,412 826 725		

El cuadro 6.8 resume el conjunto de los datos recopilados mediante la serie de control. Establecimos el nivel de significancia para evaluar la hipótesis nula en 0,1.

El cuadro 6.6 resume los resultados del análisis de varianza para la serie de control. Según el cuadro, hay suficiente evidencia para rechazar la hipótesis nula, el valor p' es menor que el nivel de significancia que establecimos, $0{,}09 < 0{,}1$, por lo que hemos concluido que hay evidencia de que la distribución de la población, según la clase de cada agente, influye en el efecto del mecanismo de incentivos.

Cuadro 6.6: Resultados del análisis de varianza para la serie de control. Con "Entre" nos referimos a "entre los tratamientos" y con "Dentro" a "dentro de los tratamientos".

Origen de las variaciones	Entre	Dentro	Total
Suma de cuadrados	4,449 017 286	48,120 487 55	52,569 504 83
Grados de libertad	23	360	383
Media de los cuadrados	0,193 435 534	0,133 668 021	
F'	1,447 133 972		
Valor p'	0,085 512 403		
Valor crítico para F'	1,412 826 725		

Si aceptamos la hipótesis H_0, la hipótesis nula que corresponde a la serie experimental, la serie en la que el sistema de criptodivisa incluye el mecanismo de incentivos[51], y rechazamos la hipótesis H_0', la hipótesis nula que corresponde a la serie de control, la serie en la que el sistema de criptodivisa no incluye el mecanismo de incentivos, entonces debemos aceptar la hipótesis planteada en el capítulo 1.

Sin embargo, la aceptación de la hipótesis es discutible. Creemos que, al implementar otro modelo de sistema de simulación, y a partir de los resultados del análisis para cada serie, volver a evaluar la hipótesis, aun con un nivel de significancia del 0,05, podríamos obtener suficiente evidencia para aceptar la hipótesis original. Creemos que es necesario continuar investigando.

[51] El mecanismo, según las expresiones B.4 y B.6, es autosuficiente y promueve la estrategia 1.

Cuadro 6.7: Resumen del análisis de varianza para la serie experimental

Tratamiento	Sumatoria	Media	Varianza
1	7,663 2	0,478 950 00	0,162 503 708
2	6,287 0	0,392 937 50	0,173 192 876
3	6,118 1	0,382 381 25	0,166 785 434
4	6,239 4	0,389 962 50	0,186 943 215
5	4,869 7	0,304 356 25	0,090 167 284
6	8,927 8	0,557 987 50	0,141 087 428
7	7,283 8	0,455 237 50	0,157 223 111
8	6,746 5	0,421 656 25	0,170 576 103
9	4,999 4	0,312 462 50	0,140 774 720
10	9,798 5	0,612 406 25	0,123 610 286
11	4,185 0	0,261 562 50	0,139 127 711
12	7,797 4	0,487 337 50	0,132 494 869
13	5,094 8	0,318 425 00	0,148 102 535
14	4,418 3	0,276 143 75	0,147 159 880
15	8,082 3	0,505 143 75	0,149 012 465
16	4,905 6	0,306 600 00	0,148 722 044
17	4,119 1	0,257 443 75	0,142 302 645
18	3,791 9	0,236 993 75	0,102 391 705
19	6,437 6	0,402 350 00	0,175 807 313
20	5,141 3	0,321 331 25	0,131 122 454
21	5,319 4	0,332 462 50	0,121 035 176
22	2,873 4	0,179 587 50	0,079 583 715
23	8,304 2	0,519 012 50	0,076 024 780
24	5,360 5	0,335 031 25	0,125 822 524

Cuadro 6.8: Resumen del análisis de varianza para la serie de control

Tratamiento	Sumatoria	Media	Varianza
1	5,543 4	0,346 462 50	0,133 543 235
2	9,384 4	0,586 525 00	0,156 757 775
3	7,294 4	0,455 900 00	0,165 259 696
4	7,668 4	0,479 275 00	0,141 934 615
5	3,686 0	0,230 375 00	0,110 571 697
6	2,803 7	0,175 231 25	0,107 728 930
7	8,330 9	0,520 681 25	0,160 844 891
8	4,177 6	0,261 100 00	0,140 677 543
9	6,396 6	0,399 787 50	0,163 601 432
10	7,607 1	0,475 443 75	0,130 864 881
11	5,775 6	0,360 975 00	0,151 001 751
12	6,072 3	0,379 518 75	0,159 992 752
13	4,149 2	0,259 325 00	0,130 214 981
14	7,347 1	0,459 193 75	0,151 996 078
15	5,104 0	0,319 000 00	0,148 028 853
16	6,848 2	0,428 012 50	0,140 536 783
17	1,511 3	0,094 456 25	0,061 260 581
18	5,420 5	0,338 781 25	0,133 734 512
19	4,815 0	0,300 937 50	0,123 293 959
20	5,661 2	0,353 825 00	0,126 244 575
21	5,759 2	0,359 950 00	0,151 367 913
22	5,423 8	0,338 987 50	0,067 788 804
23	5,903 9	0,368 993 75	0,124 466 189
24	5,845 9	0,365 368 75	0,126 320 077

In crypto we trust.

—Anónimo

7

Cripto-mecanismo de incentivos

Sinopsis. Este capítulo describe una arquitectura de cadena de bloques que permite implementar el mecanismo de incentivos para cualquier cadena de suministro, la arquitectura consta de una serie de capas, e incluye una extensión del protocolo de consenso. Este capítulo también describe un modelo de aplicación mediante el que es posible, para cualquier cadena de suministro, registrar un modelo de negocio tal que sea posible implementar sobre este, el mecanismo de incentivos. El capítulo incluye un esquema de minería alternativo, y describe una serie de propiedades que la arquitectura exhibe, y que garantizan la integridad de la cadena de bloques.

7.1. Arquitectura

Este capítulo contiene una descripción formal del mecanismo de incentivos compatible con la arquitectura en capas identificada por Ferdous *et al.*, compuesta por una capa de red, una capa de consenso, una capa de aplicación, y una capa de meta-aplicación [9].

Definición 7.1.1 (Aplicación)**.** *Representación, en una cadena de bloques, de cualquier modelo de negocio.*

Además de las funciones que tradicionalmente son implementadas en la capa de red, no hemos identificado alguna otra función que sea requerida en esta capa por el mecanismo de incentivos, por otro lado, la capa de aplicación implementa las funciones inherentes a cualquier cadena de bloques logística, y también las funciones inherentes a cualquier sistema de criptodivisa "tradicional".

Definición 7.1.2 (Extensión del protocolo de consenso)**.** *Conjunto de reglas que habilitan al protocolo de consenso para soportar el desarrollo y el funcionamiento de cada aplicación.*

La capa de meta-aplicación es equivalente al conjunto de aplicaciones inscritas, por otro lado, la extensión del protocolo de consenso permite implementar, de forma segura, el registro de recursos y el mecanismo de tokenización, ya que restringe la administración de cada aplicación, para que cada una sea administrada solamente por el usuario que la ha inscrito.

7.1.1. Capa de consenso

El protocolo implementado en esta capa, además de determinar cada una de las funciones inherentes al consenso, debe permitir que el sistema de criptodivisa pueda satisfacer cada uno de los casos de uso en la siguiente lista.

1. Un usuario, al intentar abrir una cuenta, debe poder especificar el perfil de la cuenta.

2. Un usuario, al registrar un recurso, debe hacerlo desde una cuenta con perfil de administración.

3. Un administrador, al intentar registrar un recurso, en el registro correspondiente al recurso, debe poder incluir un contrato inteligente, un contrato que requiera que el saldo en el contrato sea 0 después de la ejecución, ergo, las transacciones que genere tal contrato sean incluidas en un único bloque.

4. Un administrador, antes de inscribir un contrato, debe disponer de un lenguaje de programación lo suficientemente potente para programar el contrato. Un lenguaje turing-completo sería más que suficiente.

5. Un administrador *i*, debe poder inscribir solo una aplicación, y al intentar inscribirla, debe poder definir una y solo una divisa en la aplicación, y posteriormente solo *i* debe poder emitir moneda en esa divisa.

6. Un usuario, al intentar efectuar una transacción *e*, debe poder incluir en *e* una referencia a una trayectoria.

7. Un usuario *i*, al intentar certificar una transacción *e*, si el monto está en una divisa que fue definida desde la cuenta *j*, la cuenta desde la que *e* fue efectuada, y mediante *e* se intenta transferir el monto hacia la cuenta *j*, entonces *i* no verifica el monto, por lo que el monto puede ser mayor al saldo disponible en *j*, en la misma divisa.

8. Un usuario, al intentar efectuar una transacción *e*, debe poder incluir en *e* una comisión para el agente que la registre en la cadena de bloques.

9. Un usuario, al intentar construir un bloque, por coherencia con el paradigma de la Economía Circular, no debe requerir de la solución de la prueba de trabajo, debido a la inversión que requiere conseguirla, en términos energéticos.

10. Un usuario, al intentar generar un bloque *b*, debe poder elegir las transacciones que incluye en *b*, pero antes de incluirlas debe certificarlas.

Según el caso de uso 9, el mecanismo de incentivos no puede ser implementado como parte de un protocolo de consenso que exija la prueba de trabajo, esto nos permite descartar que el protocolo implementado pueda ser el de Nakamoto. Por otro lado, si el protocolo exige la prueba de participación encadenada, o la prueba de participación dirigida por comités, por diseño, el protocolo requeriría de una inversión en criptomoneda por cada agente que intente participar en el proceso de consenso, y si el protocolo exige la prueba de participación delegada, por diseño, el protocolo requeriría que cada delegado reciba una remuneración por el trabajo de minería [6], por lo que creemos que es conveniente que el mecanismo de incentivos, tal como lo hemos propuesto, sea implementado como parte de un protocolo de consenso con prueba de participación tolerante a fallas bizantinas.

7.1.2. Implementación de la extensión del protocolo de consenso

Esta sección describe una extensión del protocolo de consenso que permite implementar el mecanismo de incentivos propuesto, junto con cada una de las características que requiere su implementación. Las expresiones 7.1, 7.2, 7.3, 7.4 y 7.5 constituyen la descripción formal de la extensión, pero solamente para el componente que permite la certificación de las transacciones correspondientes a transferencias monetarias.

La extensión del protocolo de consenso establece que cada aplicación[52] debe ser inscrita junto a una cuenta i desde la que la aplicación pueda ser administrada, esto quiere decir que, por protocolo, (7.1) el registro de recursos, y (7.2) la emisión de moneda, serían posibles solo desde la cuenta de aplicación.

$$\forall\, e : E \bullet k \notin K(j,t) \Rightarrow \big(\theta(j) = 5 \wedge i = j\big) \tag{7.1}$$

Según la expresión 4.1, los componentes i, j, k y t existen en el esquema E.

El perfil del agente es "de aplicación", o 5 en la expresión 7.1, si el agente es un administrador. La expresión 7.1, mediante $K : V \times \mathbb{N} \rightarrow \mathbb{P}\, V$, afirma que "$k \notin K(j,t)$", i.e., el recurso k no pertenece al conjunto de recursos que posee el agente j en el tiempo t.

Definición 7.1.3 (Cuenta de aplicación)**.** *Cualquier cuenta mediante la que una aplicación sea administrada.*

El empaquetamiento de insumos se reflejaría en las entradas y salidas de cada transacción. Cualquier agente i podría recibir un conjunto de insumos para producir un recurso k, mediante una transacción múltiple, o varias, y el agente i podría entregar el producto k, mediante otra transacción múltiple e, cada salida mediante la que el agente i recibió un insumo para producir el recurso k correspondería a una entrada de la transacción múltiple e.

Implementación del mecanismo de tokenización

Cualquier agente de aplicación podría emitir moneda, según la expresión 7.2, para esto solo es necesario que el agente efectúe una transacción mediante la que transfiera un monto desde su cuenta j hacia su cuenta j, un monto que puede ser mayor al saldo disponible. Sin embargo, esto es posible solo si la transferencia está en la criptodivisa que corresponde a la aplicación que administra.

Cada aplicación permitiría registrar cualquier cantidad de recursos, y con cada uno permitiría registrar un contrato inteligente[53]. Según el axioma 5.1.2, el valor de cada moneda dependería, no solo del volumen de producción correspondiente a la aplicación M, también dependería de la cantidad de moneda que fuese emitida desde la aplicación M.

[52] Cada aplicación debe poder ser administrada con la asistencia de las herramientas de tokenización.
[53] Claramente, el agente de aplicación podría decidir no registrar toda la producción.

$$\forall\, e : E \bullet \omega > \vartheta(j,t) \Rightarrow \big(\theta(j) = 5 \wedge i = j\big) \tag{7.2}$$

Según la expresión 4.1, los componentes i, j, ω y t existen en el esquema E.

La expresión 7.2, mediante $\vartheta : V \times \mathbb{N} \rightarrow \mathbb{N}$, afirma que "$\omega > \vartheta(j,t)$", i.e., el monto ω transferido por el agente j es mayor al saldo del agente j en el tiempo t. El valor de cada criptodivisa debe estar disgregado del valor de las otras criptodivisas para garantizar la seguridad del mecanismo de incentivos, por lo que, en cada transacción múltiple, el monto correspondiente a cualquiera de las entradas debe estar en la criptodivisa que esté el monto correspondiente a cada una de las otras entradas.

Definición 7.1.4 (Recurso inteligente)**.** *Recurso inscrito en una cadena de bloques, recurso tal que su inscripción incluya un contrato inteligente.*

En el capítulo 5 hemos propuesto respaldar a cada moneda con la producción de la cadena de suministro desde la que fue emitida. En este capítulo proponemos que, mediante la extensión del protocolo de consenso, sea posible incluir el registro de un contrato inteligente en el registro de cualquier recurso, en la cadena de bloques. Esto permitiría agilizar las operaciones sobre los dos componentes, sobre el recurso y sobre el contrato que le corresponde.

Definición 7.1.5 (S_j)**.** *Conjunto de transacciones que el agente j ha firmado y que han sido aceptadas en la cadena de bloques.*

$$\forall\, e : E \bullet e \notin S_j \Rightarrow \theta(j) = 6 \tag{7.3}$$

Según la expresión 4.1, el componente j existe en el esquema E.

En la expresión 7.3, el perfil del agente es 6 cuando el agente es un recurso inteligente. La extensión del protocolo de consenso requiere que al menos los perfiles 5 y 6 estén definidos en la capa de consenso.

La circulación de una criptodivisa por cada aplicación podría comprometer el buen funcionamiento, como medio de intercambio, de cualquiera de las criptodivisas, una solución a este problema podría ser inscribir al menos una aplicación mediante la que desde una casa de intercambio sea posible administrar una criptodivisa "neutral", una criptodivisa que sea aceptada por casi cualquier agente como forma de pago, esto se podría lograr más fácilmente si esta criptodivisa estuviera respaldada por otra divisa, externa al sistema de criptodivisa, y que sea generalmente aceptada.

Interacción usuario-contrato

Definición 7.1.6 (Contrato circular)**.** *Cualquier contrato inteligente incluido en la inscripción de un recurso inteligente, que implemente el mecanismo de incentivos propuesto en la expresión 5.5.*

Cualquier agente que contribuya en la generación de una trayectoria circular puede ejecutar el contrato circular correspondiente[54] si no ha sido ejecutado. Para garantizar esto, como lo establece la expresión 7.4, el saldo en cualquier contrato circular debe ser 0 después de la ejecución del contrato. Cualquier agente, que ejecute un contrato circular, debe incluir en cada transacción que sea generada por la ejecución, una referencia a la trayectoria que habilitó la ejecución, a fin de facilitar la certificación de cada transacción. En la expresión 4.1, la referencia está identificada como σ.

$$\begin{aligned} &\forall\, e : E;\, t' : \mathbb{N} \mid \theta(j) = 6 \bullet \\ &\qquad t < t' \Rightarrow \vartheta(j, t') = 0 \end{aligned} \tag{7.4}$$

Según la expresión 4.1, los componentes j y t existen en el esquema E.

Entonces, por consenso, cada agente i debe certificar a cada transacción antes de incluirla en un bloque, esto consiste en verificar sobre el agente j que intenta efectuarla, según las expresiones 7.1 y 7.2: que posee el recurso o el monto que intenta transferir, según corresponda; y según la expresión 7.3: que ha firmado la transacción, esto lo debe verificar mediante la llave pública de j. Adicionalmente, si la transacción fue generada a partir de un recurso circular, i debe verificar, según la expresión 7.4: que cada una de las transacciones que transfieren la remuneración sea incluida en el bloque que son incluidas las otras; según la expresión 7.5: (1) que j contribuyó en la trayectoria del recurso, (2) que la trayectoria es circular, y (3) que la distribución de la remuneración es consistente con la expresión 5.5.

Definición 7.1.7 (C)**.** *Conjunto de los recursos inteligentes.*

$$\begin{aligned} &\forall\, e : E \mid \theta(j) = 6 \bullet \exists\, e' : E;\, \kappa : C \mid \\ &\quad i = j' \land j = k' \land k' = {\sim}\kappa \land \langle {\sim} e' \rangle \,\mathsf{in}\, \sigma \bullet \sigma \in L(M) \land \omega \geq \nabla\big(\sigma, \theta(i)\big) \end{aligned} \tag{7.5}$$

Con $L(M)$ como el lenguaje de la aplicación desde la que el recurso k' fue inscrito. Según la expresión 4.1, los componentes i, j, j', k', ω y σ existen en el esquema E.

En la expresión 7.5, κ representa al recurso desde el que se transfiere la remuneración. En la implementación de la expresión[55] "$\sigma \in L(M)$" puede ser útil considerar que el autómata 4.2, es equivalente a la expresión regular

$$(3,4)(4,4)^*(4,3) + (2,4)(4,4)^*(4,3)(3,3)^*(3,2) + (1,4)(4,4)^*(4,3)(3,3)^*(3,2)(2,2)^*(2,1).$$

[54] Probablemente, el agente que ejecute el contrato sea el que complete la trayectoria circular que habilite la ejecución. Cada usuario podría disponer de una herramienta que facilite la revisión de la trayectoria de cualquier recurso.

[55] La implementación de esta expresión correspondería a la verificación automatizada de la contribución con el cambio de paradigma. La verificación automatizada es necesaria para la automatización de la transferencia de la remuneración, para evitar dificultades en la transferencia. La incertidumbre sobre la transferencia de la remuneración podría anular el efecto del mecanismo de incentivos.

7.1.3. Capa de meta-aplicación

La capa de meta-aplicación estaría compuesta por cada aplicación que sea inscrita. Según la extensión del protocolo de consenso, cada aplicación debe ser inscrita junto a una cuenta de aplicación, una cuenta desde la que la aplicación pueda ser administrada, la inscripción consta de una descripción del modelo del negocio, y una descripción de la cuenta de aplicación. La descripción del modelo del negocio permite que cada recurso herede los componentes de la aplicación desde la que sea registrado. El modelo de negocio debe ser descrito en forma de un ε-NFA extendido $M = (Q, \Theta, \Sigma, \delta, q_0, F, \nabla)$, donde:

- Q sea el conjunto finito de estados.
- Θ sea el conjunto finito de perfiles.
- Σ sea el conjunto finito de símbolos de entrada, tales que $\forall\, \imath : \mathbb{N};\ e : \Sigma \mid$

$$0 < \imath \land \imath \leq \#e \bullet e(\imath) \in \Theta.$$

- $\delta : Q \times \Sigma \to Q$ sea la función de transición.
- $q_0 : Q$ sea el estado inicial.
- F sea el conjunto de estados finales[56].
- $\nabla : (\text{seq}\, \mathbb{N}) \times \Theta \to \mathbb{R}$ sea la función que permite calcular la remuneración para cualquier agente, según el perfil del agente y la trayectoria del recurso.

La descripción de una aplicación, mediante un ε-NFA extendido, requiere de la definición de una función, identificada como f en la expresión 7.6, que permita interpretar a cualquier transacción, si corresponde a la transferencia de un recurso, como un símbolo de entrada del autómata[57].

El mecanismo de incentivos debería ser especificado mediante la función ∇, y podría ser especificado como en la expresión 5.5. Para esto último, el agente de aplicación necesitaría determinar el valor monetario φ del recurso, y las proporciones $\check{h}_{-4}$ y $\check{h}_4$ del valor monetario del recurso que serían retornadas en forma de remuneración a la cadena interna y a la cadena externa, respectivamente[58].

Implementación del mecanismo de incentivos

La inexistencia de una criptodivisa nativa evita que sea posible implementar un esquema de minería remunerativa como parte del protocolo, por lo que el esquema de minería debe ser no remunerativo, debe ser un esquema en el que el trabajo de minería sea delegado a un comité compuesto por agentes que estén interesados en la oferta del sistema de criptodivisa. En otras palabras, el protocolo de consenso no debe promover, de forma explícita, la participación en la minería.

Al registrar un recurso que el agente de aplicación espera recuperar, con el recurso, el agente debe poder registrar un contrato inteligente que implemente el mecanismo de incentivos. Si el mecanismo se implementa según la definición de la función ∇ en la expresión

[56] $F \subseteq Q$.

[57] Además, la descripción de la aplicación podría incluir una "lista de exclusión", una lista de agentes o criptodivisas para las que el agente de aplicación podría decidir denegar cualquier transacción, o una "lista de inclusión", una lista de los únicos agentes o criptodivisas para las que el agente de aplicación podría decidir lo contrario.

[58] Aunque el agente de aplicación especifique el mecanismo de incentivos como en la expresión 5.5, debería poder elegir una combinación de valores que no satisfaga la expresión 5.6, también debería poder elegir una combinación de valores que no satisfaga el corolario 5.3.2.

5.5, para que el contrato sea ejecutado con éxito, antes de que sea ejecutado, el agente i debe transferir al recurso el valor monetario de $\left(\hat{h}_{-4}(i) + \hat{h}_4(i)\right) \cdot \varphi$ para que el contrato, al ser ejecutado, pueda generar una transacción por cada cuenta referenciada en la trayectoria, en la que transfiera el valor monetario que corresponde a la cuenta, según la expresión 5.5, desde la cuenta del recurso.

$$C \triangleq [M, f] \tag{7.6}$$

La expresión 7.6, identifica los componentes de un recurso inteligente, cada recurso debe heredar los componentes de la aplicación[59] desde la que sea registrado. Cualquier recurso inteligente, mediante la implementación de $f : E \to \Sigma$, permitiría interpretar a cualquier transacción mediante la que haya sido transferido, como un símbolo de entrada. El saldo en cualquier contrato circular debe ser 0 después de la ejecución del contrato, por lo que es necesario que cada una de las transacciones que sea generada por un contrato circular esté integrada a las otras, mediante una transacción múltiple.

El contrato de cada recurso circular debe poder ser ejecutado solo una vez, pero un nuevo contrato debe poder ser registrado con cada nuevo recurso, aunque este haya sido generado a partir de otro que haya finalizado su ciclo. Al ejecutar el contrato de uno de estos recursos circulares, el saldo para el recurso debe ser consumido por completo, esto debería impedir que el contrato sea ejecutado nuevamente. El acceso a las herramientas de tokenización podría ser administrado mediante una aplicación de licenciamiento, desde la aplicación, cada licencia podría ser registrada como un recurso, en la cadena de bloques. El ejemplo 7.1.8 describe el efecto del comportamiento de los agentes en el escenario del ejemplo 4.3.3 al ejecutar el mecanismo de incentivos.

Ejemplo 7.1.8. El escenario del ejemplo 4.3.3 es posible solo si antes, (1) Cenizo, (2) Jacinto y (3) Simposio abren sus cuentas en el sistema de criptodivisa, con $\theta(1) = 2$, $\theta(2) = 3$ y $\theta(3) = 4$ respectivamente, y después acumulan un saldo suficiente para efectuar cada transacción, supongamos que ahora, en el tiempo t_0, $\vartheta(1, t_0) = 150$, $\vartheta(2, t_0) = 100$ y $\vartheta(3, t_0) = 50$, y para enlazar las tres cuentas y establecer una cadena de suministro, uno de los tres, supongamos Cenizo, inscribe una aplicación con identificador 4, con una cuenta de aplicación. Cenizo registra la docena de botellas de cerveza en el sistema de criptodivisa mediante la cuenta de aplicación y con cada cerveza, ella registra un contrato inteligente que implementa el mecanismo de incentivos según la expresión 5.5, con $\varphi = 10$, $\check{h}_{-4} = 0{,}006$ y $\check{h}_4 = 0{,}012$, por lo que adquiere una licencia ℓ que le permite implementar las herramientas de tokenización, podemos modelar la adquisición mediante la transacción unitaria e_0, con $j = 4$ y $k = \ell$, según la expresión 4.1, y luego efectúa, para cada cerveza b, una transacción, con $i = b$, $j = 4$ y $\omega = 0{,}12$, según la expresión 4.1, en la que transfiere la remuneración al recurso. Luego Jacinto efectúa la compra de la docena de botellas de cerveza a Cenizo, podemos modelar la compra mediante las transacciones unitarias $e_1, \ldots, e_{12}$, donde, por medio de la transacción e_b Jacinto adquiere la unidad b, con $i = 1$, $j = 2$, $k = b$ y $\omega = 8$, según la expresión 4.1. Luego Simposio efectúa la compra de la cerveza identificada como 5 a Jacinto, podemos modelar la compra mediante la transacción unitaria e_{13}, con $i = 2$, $j = 3$, $k = 5$ y $\omega = 10$, según la expresión 4.1. Luego Cenizo efectúa la compra del envase de la cerveza identificada como 5 a Simposio, podemos modelar la compra mediante la transacción unitaria e_{14}, con $i = 3$, $j = 1$, $k = 5$ y $\omega = 0$, según la expresión 4.1. Finalmente, Simposio ejecuta el contrato de la cerveza identificada como 5, y así genera tres transacciones unitarias, una con $i = 5$, $j = 1$, $\omega = 0{,}03$ y $\sigma = \langle \sim e_{14}, \sim e_{13}, \sim e_1 \rangle$, otra con $i = 5$, $j = 2$, $\omega = 0{,}03$ y $\sigma = \langle \sim e_{14}, \sim e_{13}, \sim e_1 \rangle$, y otra con $i = 5$, $j = 3$, $\omega = 0{,}12$ y $\sigma = \langle \sim e_{14}, \sim e_{13}, \sim e_1 \rangle$, según la expresión 4.1. Las últimas tres transacciones unitarias equivalen a la transacción múltiple mediante la que la remuneración sería transferida desde la cuenta del recurso hacia cada una de las cuentas referenciadas en la trayectoria.

[59] M representa a los componentes del ε-NFA extendido.

7.2. Integridad de la cadena de bloques

Las cadenas de bloques, por diseño, garantizan la consistencia y la inmutabilidad de cada transacción [9], y además, por protocolo, requieren que cada agente firme, mediante su llave privada, cada transacción que intente efectuar [12], sin embargo, la implementación del mecanismo de incentivos propuesto requiere de la extensión del protocolo de consenso descrita en la sección 7.1.2, y por lo tanto, de medidas de seguridad adicionales. El mecanismo de tokenización funciona como una de estas medidas de seguridad, en particular ante ataques sybil, y es complementado por el esquema de minería, tal como es propuesto en la sección 7.2.1.

7.2.1. Esquema de minería

Es ideal que la inversión en recursos que la minería requiera sea la mínima, por coherencia con el paradigma de la Economía Circular, por lo que conviene evitar la necesidad de pruebas como la PoW. Además, la inexistencia de una criptodivisa nativa evita que sea posible implementar un esquema de minería remunerativa como parte del protocolo de consenso, por lo que el esquema de minería debe ser no remunerativo y a la vez consistente con el protocolo[60], por lo tanto, el esquema debe ser uno en el que el trabajo de minería sea delegado a un comité compuesto por agentes que estén interesados en la oferta del sistema de criptodivisa.

Definición 7.2.1 (Agente certificador)**.** *Cualquier agente que participe actualmente en el trabajo de generación de bloques.*

Cada agente certificador debe poder elegir las transacciones que incluye en cada bloque, y cada transacción debe estar certificada, mediante el procedimiento descrito en la sección 7.1.2, antes de ser incluida en un bloque, además es importante que cualquier agente que intente efectuar una transacción pueda determinar una comisión para el agente certificador [21]. Estas características complementan al mecanismo de tokenización como medida de seguridad. El ejemplo 7.2.2 describe el procedimiento de certificación aplicado a cada una de las transacciones en el ejemplo 7.1.8.

Ejemplo 7.2.2. En el escenario del ejemplo 7.1.8, Cenizo registra la docena de botellas de cerveza en la cuenta de aplicación en el tiempo t_1, por lo tanto, $\theta(4) = 5$; y para cada cerveza b, $b \in K(4,t_1)$. Luego, sin necesidad de un saldo en la cuenta de aplicación, Cenizo puede transferir el monto para cada remuneración a la cuenta del recurso b que corresponde, mediante la transacción unitaria e'_b, al hacerlo, $e'_b \in S_4$. Luego transfiere las botellas de cerveza a su cuenta de usuario, en el tiempo t_2, por lo tanto, para cada cerveza b, $b \in K(1,t_2)$. Luego en el tiempo t_3, $\vartheta(2,t_3) \geq 96$, por lo que Jacinto puede comprar la docena de botellas de cerveza, al hacerlo, para cada cerveza b, $b \in K(2,t_3)$, y $\{e_1,\ldots,e_{12}\} \subseteq S_2$. Luego en el tiempo t_4, $\vartheta(3,t_4) \geq 8$, por lo que Simposio puede comprar la cerveza identificada como 5, al hacerlo, $5 \in K(3,t_4)$, y $e_{13} \in S_3$. Luego Cenizo adquiere el envase por ¢0, en el tiempo t_5, por lo tanto, $5 \in K(1,t_5)$, y $e_{14} \in S_1$. Finalmente, en el tiempo t_6 Simposio ejecuta el contrato de la cerveza identificada como 5, y así genera y emite una transacción múltiple equivalente a las transacciones unitarias e''_1, e''_2 y e''_3, con $0{,}03 + 0{,}03 + 0{,}12 = \vartheta(b,t_6)$; según la expresión 4.1, con la trayectoria σ compuesta por transacciones efectuadas por Cenizo, Jacinto y Simposio, y con $\sigma \in L(4.2)$.

[60] Un usuario que trabaje en una cadena de suministro, podría contratar a un usuario, o a varios, como agente certificador, aunque el sistema de criptodivisa no ofrezca una herramienta que facilite esta operación.

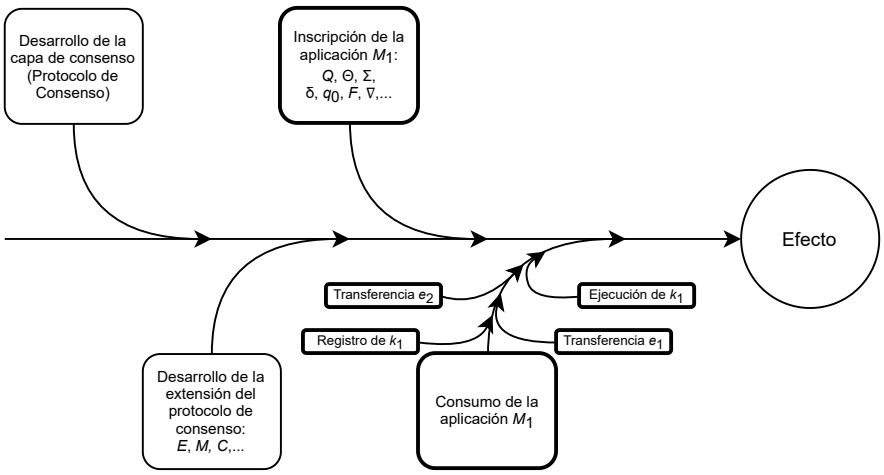

Figura 7.1: Diagrama causal de Ishikawa, para esta investigación, la "promoción de la Economía Circular" sería el efecto, y las fases de desarrollo del sistema de criptodivisa, y la inscripción y el consumo de las aplicaciones serían las causas. El protocolo de consenso garantiza la integridad de los eventos de inscripción y consumo. El contrato inteligente k_1 es registrado desde la aplicación M_1.

7.2.2. Integridad del mecanismo de incentivos

Esta sección contiene un análisis sobre otras de las medidas de seguridad que sostiene, de forma implícita, la arquitectura propuesta en este capítulo, si el mecanismo de incentivos es implementado según la expresión 5.5. Cada medida está expresada en forma de proposición y su demostración correspondiente. El diagrama en la figura 7.1, ilustra las relaciones causales relevantes en cada demostración.

Proposición 7.2.3. *Cualquier agente puede calcular la remuneración que obtendría de cualquier trayectoria circular en la que pueda contribuir.*

Demostración.

1. *Según la propiedad 3 de las cadenas de bloques, en la sección 1.2.3:* cada bloque sería almacenado en cada nodo de la red.
2. *Según la sección 7.1.2, sobre la extensión del protocolo de consenso:* mediante la extensión sería posible incluir el registro de cualquier contrato inteligente en el registro de cualquier recurso, en la cadena de bloques.
3. *según los puntos 1 y 2:* la información necesaria para calcular cualquier remuneración estaría disponible para cualquier usuario. □

La propiedad expresada en la proposición 7.2.3 es importante porque para que la oferta de cualquier remuneración provoque el efecto esperado, es necesario que la información relevante sobre la oferta sea accesible.

Antes de abordar las siguientes proposiciones, es necesario considerar que cualquier mecanismo de incentivos definido en la capa de meta-aplicación debe ser implementado como un contrato inteligente, así, por consenso, cada mecanismo que sea implementado sería inmutable. Esto garantiza que el consumo de cada aplicación sea seguro[61]. Además, cualquier transacción que sea generada mediante la ejecución de un contrato, debe ser certificada antes de ser aceptada en la cadena de bloques, por consenso.

[61] El consumo de la aplicación es seguro, por esto el consumo de la aplicación está remarcado en el diagrama causal en la figura 7.1.

Proposición 7.2.4. *Al implementar el mecanismo de incentivos según la expresión 5.5, la remuneración esperada por cualquier agente interno por contribuir en la generación de una trayectoria circular, disminuye si la cantidad de agentes internos que contribuyan en la generación de tal trayectoria, aumenta.*

Demostración.

1. Sea $r_1 : \mathbb{R}$ la remuneración esperada por cualquier agente interno en el escenario a, y sea $n : \mathbb{N}$ la cardinalidad de la cadena interna en el escenario a.
2. Sea $r_2 : \mathbb{R}$ la remuneración esperada por cualquier agente interno en el escenario b, y sea $m : \mathbb{N}$ la cantidad de agentes internos adicionales en el escenario b (en este escenario, la cardinalidad de la cadena interna es mayor que en el escenario a, lo demás es como en el escenario a).
3. *Supongamos, en términos de la expresión 5.5, que:* $n > 0$, $\check{h}_{-4} > 0$ y $\varphi > 0$.
4. Sea $x : \mathbb{R}$ tal que $x = \frac{n+m}{n}$.
5. *Según los puntos 1, 2 y la expresión 5.5:* $r_1 = \check{h}_{-4} \cdot \frac{\varphi}{n}$.
6. *Según los puntos 1, 2 y la expresión 5.5:* $r_2 = \check{h}_{-4} \cdot \frac{\varphi}{n+m}$.
7. *Según el punto 5:* $r_1 \cdot n = \check{h}_{-4} \cdot \varphi$.
8. *Según el punto 6:* $r_2 \cdot (n + m) = \check{h}_{-4} \cdot \varphi$.
9. *Según los puntos 7 y 8:* $r_1 \cdot n = r_2 \cdot (n + m)$.
10. *Según los puntos 4 y 9:* $r_1 = r_2 \cdot x$.
11. *Según el punto 10:* $r_1 > \frac{r_2 \cdot x}{x}$.
12. *Según el punto 11:* $r_1 > r_2$. □

La propiedad expresada en la proposición 7.2.4 es importante porque al mantenerla, disuade la extensión innecesaria de la cadena interna. El valor monetario de la remuneración para los agentes internos podría diluirse en escenarios con cantidades altas de agentes internos.

Proposición 7.2.5. *Al implementar el mecanismo de incentivos según la expresión 5.5, la remuneración esperada por cualquier agente externo por contribuir en la generación de una trayectoria circular, disminuye si la cantidad de agentes externos que contribuyan en la generación de tal trayectoria, aumenta.*

Demostración.

1. Sea $r_1 : \mathbb{R}$ la remuneración esperada por cualquier agente externo en el escenario a, y sea $n : \mathbb{N}$ la cardinalidad de la cadena externa en el escenario a.
2. Sea $r_2 : \mathbb{R}$ la remuneración esperada por cualquier agente externo en el escenario b, y sea $m : \mathbb{N}$ la cantidad de agentes externos adicionales en el escenario b (en este escenario, la cardinalidad de la cadena interna es mayor que en el escenario a, lo demás es como en el escenario a).
3. *Supongamos, en términos de la expresión 5.5, que:* $n > 0$, $\check{h}_4 > 0$ y $\varphi > 0$.
4. Sea $x : \mathbb{R}$ tal que $x = \frac{n+m}{n}$.
5. *Según los puntos 1, 2 y la expresión 5.5:* $r_1 = \check{h}_4 \cdot \frac{\varphi}{n}$.
6. *Según los puntos 1, 2 y la expresión 5.5:* $r_2 = \check{h}_4 \cdot \frac{\varphi}{n+m}$.
7. *Según el punto 5:* $r_1 \cdot n = \check{h}_4 \cdot \varphi$.
8. *Según el punto 6:* $r_2 \cdot (n + m) = \check{h}_4 \cdot \varphi$.
9. *Según los puntos 7 y 8:* $r_1 \cdot n = r_2 \cdot (n + m)$.
10. *Según los puntos 4 y 9:* $r_1 = r_2 \cdot x$.
11. *Según el punto 10:* $r_1 > \frac{r_2 \cdot x}{x}$.
12. *Según el punto 11:* $r_1 > r_2$. □

La propiedad expresada en la proposición 7.2.5 es importante porque, al mantenerla, disuade la extensión innecesaria de la cadena externa. El valor monetario de la remuneración para los agentes externos podría diluirse en escenarios con cantidades altas de agentes externos.

Proposición 7.2.6. *Al implementar el mecanismo de incentivos según la expresión 5.5, la remuneración esperada por cualquier agente interno, por contribuir en la generación de una trayectoria circular, es independiente de la cantidad de agentes externos que contribuyan en la generación de tal trayectoria.*

Demostración.
1. Sea $r_m : \mathbb{R}$ la remuneración esperada por cualquier agente interno en el escenario a, sea $n : \mathbb{N}$ la cardinalidad de la cadena interna en el escenario a, y sea $m : \mathbb{N}$ la cardinalidad de la cadena externa en el escenario a.
2. Sea $r_{m+1} : \mathbb{R}$ la remuneración esperada por cualquier agente interno en el escenario b, en términos del punto 1, sea n la cardinalidad de la cadena interna en el escenario b, y en términos del punto 1, sea $m + 1$ la cardinalidad de la cadena externa en el escenario b (en este escenario, hay un agente adicional en la cadena externa, lo demás es como en el escenario a).
3. *Según los puntos 1, 2 y la expresión 5.5:* $r_m = \check{h}_{-4} \cdot \frac{\varphi}{n}$.
4. *Según los puntos 1, 2 y la expresión 5.5:* $r_{m+1} = \check{h}_{-4} \cdot \frac{\varphi}{n}$.
5. *Según los puntos 3 y 4:* $r_m = r_{m+1}$. □

La propiedad expresada en la proposición 7.2.6 es importante porque al mantenerla evita que, para cualquier contrato circular, después de que este fuese registrado, cualquier agente externo pueda manipular la remuneración que cada agente interno recibiría.

Proposición 7.2.7. *Al implementar el mecanismo de incentivos según la expresión 5.5, la remuneración esperada por cualquier agente externo, por contribuir en la generación de una trayectoria circular, es independiente de la cantidad de agentes internos que contribuyan en la generación de tal trayectoria.*

Demostración.
1. Sea $r_n : \mathbb{R}$ la remuneración esperada por cualquier agente externo en el escenario a, sea $n : \mathbb{N}$ la cardinalidad de la cadena interna en el escenario a, y sea $m : \mathbb{N}$ la cardinalidad de la cadena externa en el escenario a.
2. Sea $r_{n+1} : \mathbb{R}$ la remuneración esperada por cualquier agente externo en el escenario b, en términos del punto 1, sea $n + 1$ la cardinalidad de la cadena interna en el escenario b, y en términos del punto 1, sea m la cardinalidad de la cadena externa en el escenario b (en este escenario, hay un agente adicional en la cadena interna, lo demás es como en el escenario a).
3. *Según los puntos 1, 2 y la expresión 5.5:* $r_n = \check{h}_4 \cdot \frac{\varphi}{m}$.
4. *Según los puntos 1, 2 y la expresión 5.5:* $r_{n+1} = \check{h}_4 \cdot \frac{\varphi}{m}$.
5. *Según los puntos 3 y 4:* $r_n = r_{n+1}$. □

La propiedad expresada en la proposición 7.2.7 es importante porque al mantenerla evita que, para cualquier contrato circular, después de que este fuese registrado, cualquier agente interno pueda manipular la remuneración que cada agente externo recibiría.

Proposición 7.2.8. *La ejecución exitosa de cualquier contrato circular requiere de una trayectoria circular, la trayectoria del recurso con el que el contrato fue registrado.*

Demostración.
1. Sea $\sigma : \text{seq}\,\mathbb{N}$ tal que σ no sea circular.
2. En términos del punto 1, sea $e : E$ tal que σ sea la trayectoria referenciada en e, y sea $k' : V$ tal que k' sea un contrato circular y e sea generada por la ejecución exitosa de k'.
3. Sea $\kappa : C$ tal que $k' = \sim\kappa$.
4. *Según los puntos 2, 3 y la expresión 7.5:* $\sigma \in L(4.2)$.

5. *Según el punto 1 y la definición 4.3.2:* $\sigma \notin L(4.2)$.
6. Hay contradicción entre los puntos 4 y 5. □

Proposición 7.2.9. *La remuneración puede ser transferida, de un recurso inteligente cualquiera a un agente cualquiera, solo si el agente contribuyó en la generación de la trayectoria circular que habilitó la ejecución exitosa del contrato que fue registrado con el recurso.*

Demostración.
1. Sea $\sigma : \text{seq}\,\mathbb{N}$ tal que σ sea circular, sea $i'' : V$ tal que i'' no haya contribuido en la generación de σ, sea $e : E$ tal que σ sea la trayectoria referenciada en e, y sea $k' : V$ tal que k' sea un contrato circular y e sea generada por la ejecución exitosa de k'.
2. *Supongamos, en términos del punto 1 y la expresión 4.1, por contradicción:* $\exists\, e' : E \mid \langle \sim e' \rangle \,\text{in}\, \sigma \wedge j' = i''$.
3. *Según el punto 1, y las expresiones 4.1 y 7.5:* $\forall\, e' : E \mid \langle \sim e' \rangle \,\text{in}\, \sigma \bullet j' \neq i''$.
4. Hay contradicción entre los puntos 2 y 3. □

La implementación del mecanismo de incentivos propuesto requiere de las propiedades expresadas en las proposiciones 7.2.8 y 7.2.9. Estas propiedades permitirían la transferencia de la remuneración, solo si la contribución del agente al que es transferida es la esperada.

Proposición 7.2.10. *Cualquier agente, para cualquier token fungible que esté registrado en el sistema de criptodivisa, puede identificar al agente que emitió el token.*

Demostración.
1. Sean $i' : V$ y $\phi : \mathbb{N}$ tales que, ϕ sea un *token* fungible emitido por i'.
2. Sean $e : E$ y $f(e) : \mathbb{N}$ tales que, el monto que es transferido mediante e esté en la criptodivisa $f(e)$.
3. *Supongamos, por contradicción, que:* no es posible identificar al agente que emitió el *token* ϕ.
4. *Según el punto 1 y el caso de uso 5 en la sección 7.1.1, sobre la capa de consenso:* existe una y solo una criptodivisa en la que el agente i' puede emitir moneda.
5. *Según la sección 7.1.2, sobre la extensión del protocolo de consenso:* en cada transacción múltiple, el monto correspondiente a cualquiera de las entradas debe estar en la criptodivisa que esté el monto correspondiente a cada una de las otras entradas.
6. *Según los puntos 2, 4, 5 y la expresión 4.1:* $\forall\, e, e'' : E \mid e \neq e'' \bullet \exists\, n : \mathbb{N};\ \varsigma : \text{seq}\,\mathbb{N} \mid n \leq \#\varsigma \wedge \big(2 \leq \#\varsigma \Rightarrow \exists\, e' : E \mid \sim e = \varsigma(n) \wedge \sim e' = \varsigma(n-1) \wedge i' = j \wedge t' < t \wedge f(e) = f(e') \wedge \neg\,(i'' = j \wedge t' < t'' \wedge t'' < t)\big)$.
7. Hay contradicción entre los puntos 3 y 6. □

La propiedad expresada en la proposición 7.2.10 es importante porque al mantenerla, la criptodivisa correspondiente a cada *token* fungible permanece inmutable, esto garantiza que el valor de cada criptodivisa permanezca disgregado del valor de las otras criptodivisas, lo que permite que el mecanismo de tokenización funcione como medida de seguridad ante ataques sybil.

Proposición 7.2.11. *Cada contribución que sea remunerada mediante un contrato que sea circular y que requiera que las transacciones que genere sean incluidas en un único bloque, puede ser remunerada solo una vez.*

Demostración.
1. Sean $i,j : V$ tales que j sea un recurso inteligente que implementa el mecanismo de incentivos según la expresión 5.5.
2. *Supongamos, en términos de la expresión 4.1, por contradicción:* $\exists\, e, e' : E \mid i' = i \wedge j' = j \wedge \omega' = \omega \wedge t' \neq t \wedge \omega > 0$.
3. *Según el punto 2 y la expresión 7.4:* $\big(t < t' \Rightarrow \vartheta(j', t') = 0\big) \wedge \big(t' < t \Rightarrow \vartheta(j, t) = 0\big)$.

4. *Según los puntos 1 y 2:* $\theta(j) = 6 \wedge \theta(j') = 6$.
5. *Según los puntos 2 y 3:* $\vartheta(j,t) = 0 \vee \vartheta(j',t') = 0$.
6. *Según los puntos 2 y 5:* $\omega > \vartheta(j,t) \vee \omega' > \vartheta(j',t')$.
7. *Según los puntos 4 y 6:* $\omega > \vartheta(j,t) \wedge \theta(j) = 6 \vee \omega' > \vartheta(j',t') \wedge \theta(j') = 6$.
8. Hay contradicción entre el punto 7 y la expresión 7.2. □

La propiedad expresada en la proposición 7.2.11 es importante porque, al mantenerla, garantiza que exista un procedimiento que evite el doble cobro de las remuneraciones. Sin embargo, para cualquier contrato, aunque al desarrollarlo se haya seguido tal procedimiento, y ya haya sido ejecutado, es posible volver a habilitarlo al volver a transferir el monto requerido por el mecanismo de incentivos que implemente.

En resumen, la arquitectura propuesta en este capítulo permite que el mecanismo de incentivos, si sigue la expresión 5.5, sea implementado de forma segura. La arquitectura (7.2.8, 7.2.9, 7.2.11) evita que cualquier agente pueda recibir una remuneración sin haber contribuido como el agente de aplicación lo espera, (7.2.4, 7.2.5) evita que cualquier agente pueda influir significativamente en el monto por cualquiera de las remuneraciones que pueda obtener, (7.2.6, 7.2.7) evita que después de la implementación, cualquier agente externo pueda manipular la remuneración que cualquier agente interno pueda recibir, y a la inversa, y (7.2.10) evita que cualquier criptodivisa obtenga valor a partir de otra criptodivisa.

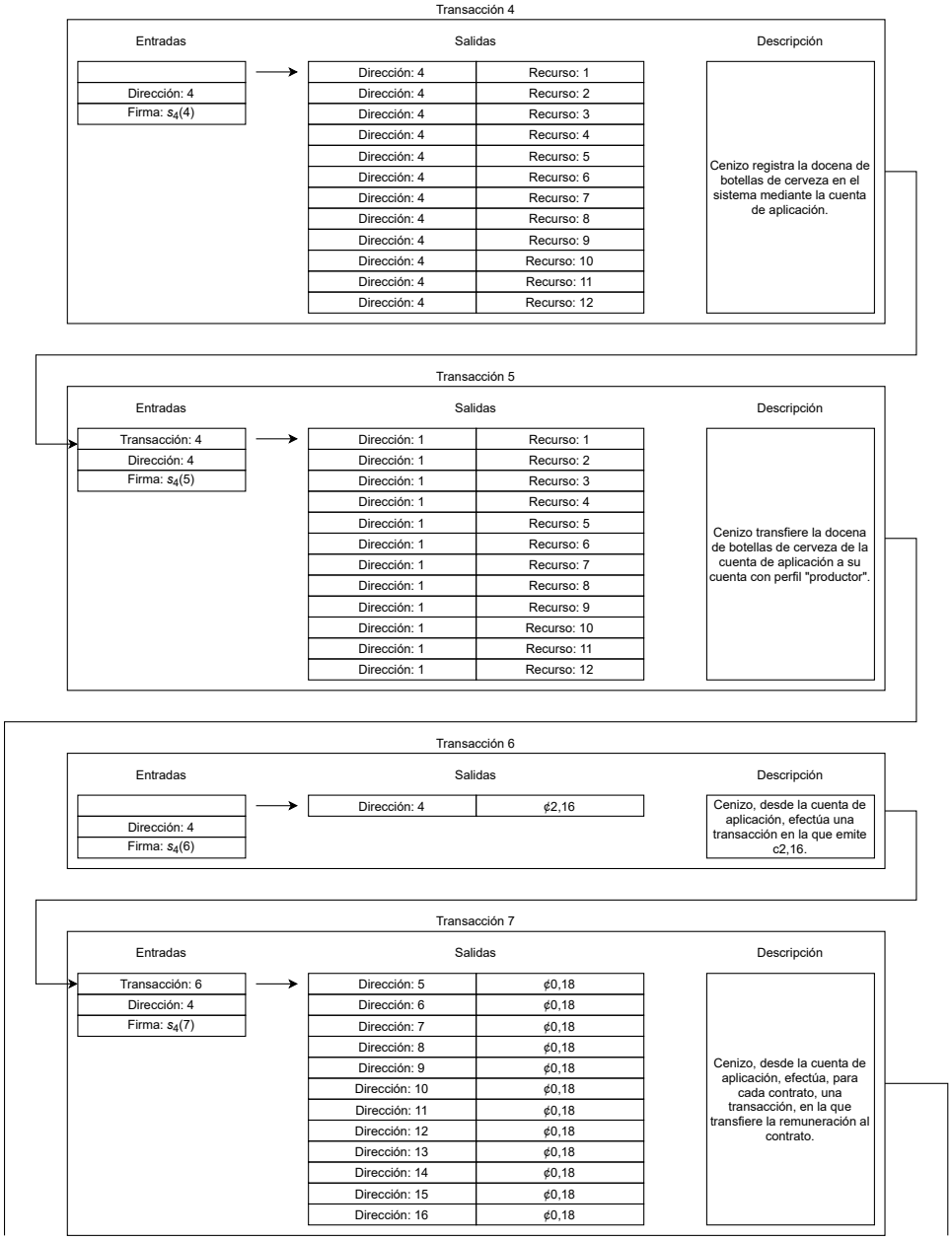

Figura 7.2: Representación gráfica de cada transacción múltiple en la primera serie de transacciones en el ejemplo 7.1.8, $s_i(e')$ representa la firma del agente i en la transacción múltiple e'.

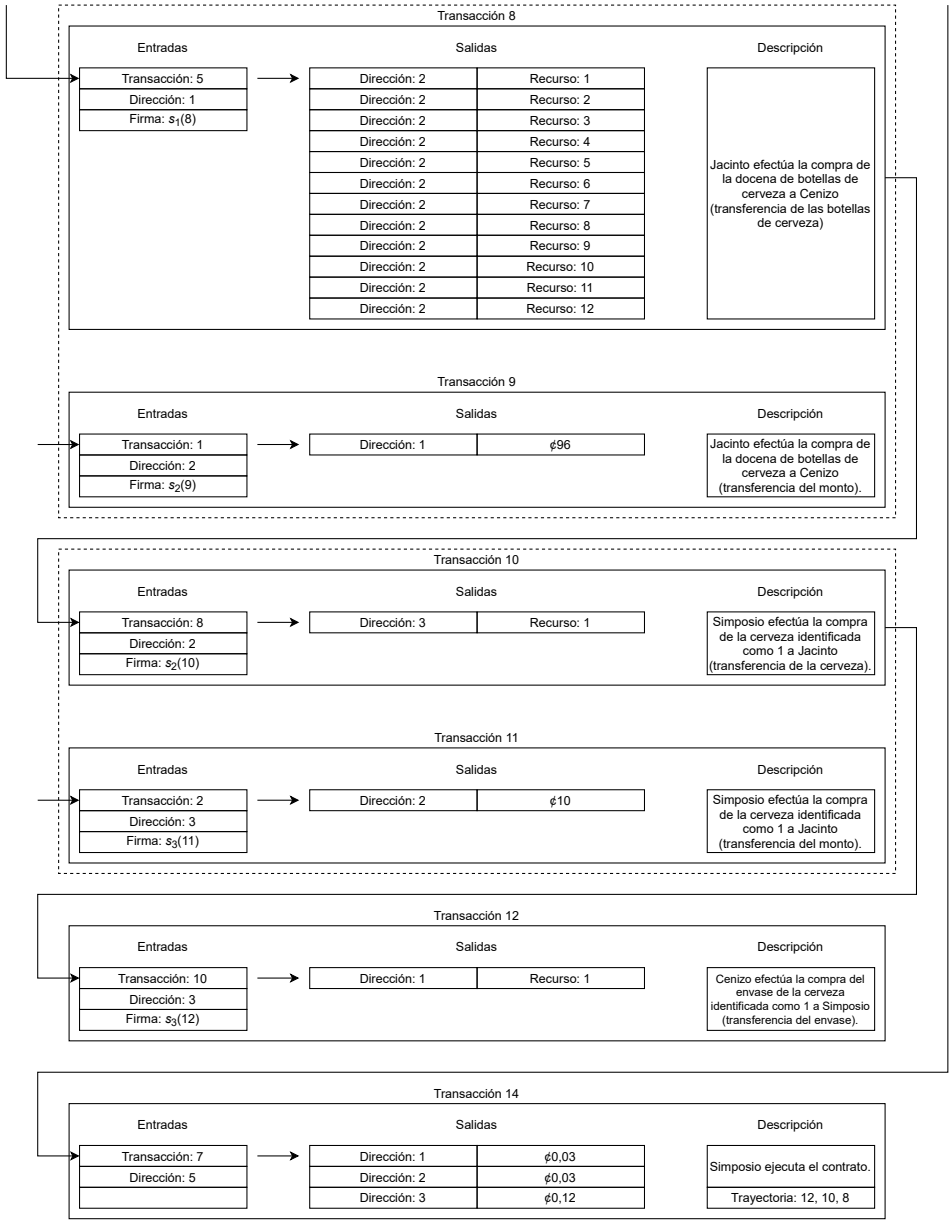

Figura 7.3: Representación gráfica de cada transacción múltiple en la última serie de transacciones en el ejemplo 7.1.8, $s_i(e')$ representa la firma del agente i en la transacción múltiple e'.

8

Epílogo

Este capítulo contiene una sección sobre el trabajo relacionado con nuestra investigación, otra sección sobre detalles varios de nuestra investigación que ameritan ser discutidos, otra sección sobre cuestiones varias que están fuera del alcance de esta investigación, pero de las que se puede obtener valor, mediante investigación adicional, y finalmente una sección que resume nuestras conclusiones.

8.1. Trabajo relacionado

Esta sección contiene una descripción breve sobre algunos proyectos de investigación o de desarrollo, que comparten algunas características con nuestro trabajo, la sección incluye un análisis comparativo de cada uno de estos trabajos[62] con el nuestro, el propósito del análisis es evidenciar la necesidad de proponer un enfoque diferente para abordar la problemática descrita en la sección 1.3.

8.1.1. Bitcoin

La primera cadena de bloques que fue implementada fue la cadena de bloques de Bitcoin [9], en el artículo "Bitcoin: un sistema de punto a punto de divisa electrónica" [22], Nakamoto, el desarrollador del sistema de criptodivisa, describe las generalidades del protocolo de consenso que es implementado en el sistema, el protocolo de consenso de Nakamoto.

Nakamoto especifica que el costo inherente al funcionamiento del sistema es cubierto por los "mineros", los agentes que trabajan en la generación y en la verificación de cada bloque en la cadena de bloques, y a la vez, el sistema implementa un mecanismo de incentivos que promueve la participación en el trabajo de minería. El mecanismo de incentivos permite que el minero, al generar un nuevo bloque, incluya en este una transacción mediante la que emita

[62] La sección 8.1.1, sobre Bitcoin, está basada en el artículo con título "Bitcoin: un sistema de punto a punto de divisa electrónica" [22] de Nakamoto, la sección 8.1.2, sobre Ethereum, está basada en los artículos "Ethereum: Una plataforma de próxima generación para el desarrollo de aplicaciones descentralizadas con contratos inteligentes" [23] de Buterin, "Un libro de transacciones descentralizado, seguro y de propósito general" [24] de Wood, y "Una especificación técnica de Ethereum" [25] de Dameron. Hemos traducido el título de cada publicación para mantener el idioma del texto, el título original se encuentra en la bibliografía.

cierta cantidad, establecida por el protocolo, de bitcoins y los deposite en su cuenta.

El artículo de Bitcoin describe las generalidades del protocolo de consenso de Nakamoto, según el artículo, en la red de Bitcoin, (1) cada agente debe transmitir cada transacción que reciba, o que intente efectuar, a tantos agentes como pueda, (2) cada agente que intente generar un nuevo bloque, debe elegir cada una de las transacciones que incluirá en este, (3) cada agente que intente generar un nuevo bloque, debe intentar generar la prueba de trabajo para el nuevo bloque, (4) al lograrlo, debe incluirla en el nuevo bloque, y transmitir el bloque a tantos agentes como pueda, (5) cada agente debe aceptar cada bloque que reciba, pero solo si cada una de las transacciones que contiene es válida, y no está en un bloque anterior, y (6) el bloque es aceptado por el agente, si el agente incluye el hash del bloque en el siguiente bloque que genere.

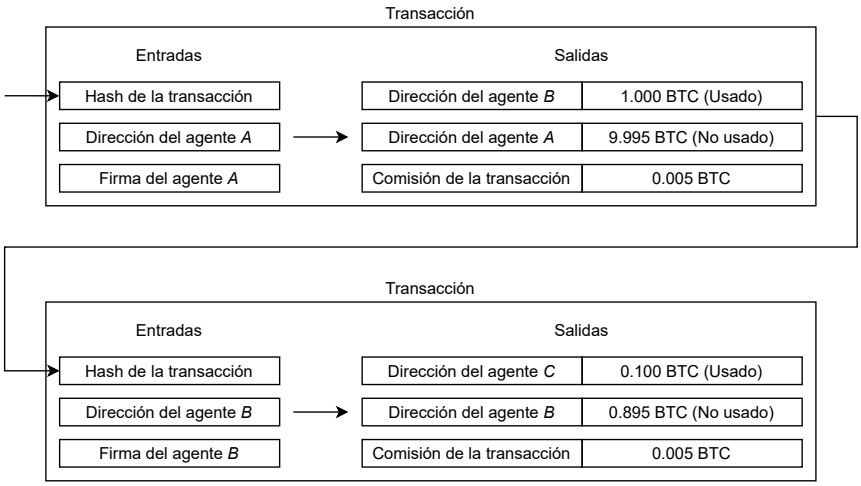

Figura 8.1: Ejemplo de dos transacciones, una entre *A* y *B*, y otra entre *B* y *C*. En la red de Bitcoin, la estructura de las transacciones indica la cantidad a transferir, los remitentes y los destinatarios. En la transacción del agente *A* al agente *B*, la entrada corresponde a la dirección de la cuenta de origen, que corresponde a la clave pública de *A*, y la firma de *A*, que es calculada a partir de la clave privada de *A*. En la misma transacción, las salidas corresponden al monto a transferir, la dirección de la cuenta que recibe el monto, que corresponde a la clave pública de *B*, y la dirección de la cuenta que recibe el cambio, que posiblemente corresponda a una dirección de *A*. [21].

Cada agente sigue la regla de la cadena más larga, debe generar el siguiente bloque a partir de la cadena más larga. Si al menos dos agentes transmiten versiones diferentes del siguiente bloque y lo hacen simultáneamente, de los demás, algunos podrían recibir una primero y otros la otra, la cadena de bloques se bifurcaría, en este caso cada uno debe trabajar sobre la primera versión que recibió, y almacenar la otra en caso de que posteriormente la mayoría continúe trabajando sobre esta. En caso de que un agente no reciba un bloque, debe solicitarlo al recibir el que le sigue. El protocolo no requiere que cada nueva transacción deba ser transmitida a cada uno de los agentes en la red, pero sí que deba ser transmitida a los suficientes para ser aceptada en la cadena de bloques.

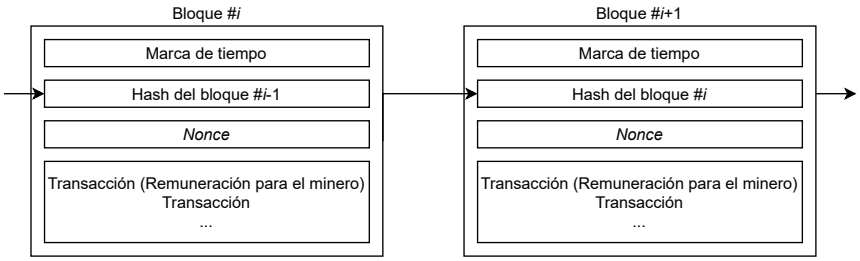

Figura 8.2: Una secuencia de bloques en la cadena de bloques. La prueba de trabajo requiere que el minero encuentre un número único —*number used once, nonce*— en función del hash actual, el hash del bloque anterior (los hashes son calculados usando SHA-256) y la serie de transacciones incluidas en el bloque. Las comisiones en el bloque se suman a la remuneración por la generación del bloque [21].

Sin embargo, la información disponible en la cadena de bloques de Bitcoin[63] no es suficiente para establecer un criterio o una definición concisa de circularidad que permita el reconocimiento de las transacciones que contribuyan con la "circularización" de la economía[64], por lo tanto, para obtener tal definición es necesario disponer de una estructura de datos más amplia, una estructura que permita registrar información adicional sobre cada transacción. Creemos que una estructura de datos que soporte el registro de la actividad en una cadena de suministro podría ser lo suficientemente amplia, afortunadamente la tecnología de cadena de bloques ya ha sido implementada por múltiples cadenas de suministro[65].

8.1.2. Ethereum

Ethereum es una plataforma de desarrollo de aplicaciones construida sobre una base de datos de arquitectura de cadena de bloques. La plataforma está transicionando a un protocolo con prueba de participación, la criptodivisa nativa de la plataforma es el Ether, por lo que el trabajo de minería es remunerado en ethers. La finalización del último bloque recibido es resuelta mediante la regla del subárbol más pesado —*The Greedy Heaviest-Observed Sub-Tree*, GHOST— que establece que, dentro del subárbol más pesado, la cadena más larga es la cadena correcta, dentro del subárbol más pesado de los subárboles de un árbol de bloques con el bloque génesis como raíz. Con la regla GHOST, el periodo de tiempo que tarda la generación de cada bloque es menor que con la regla de la cadena más larga, por lo que la regla GHOST permite un mayor volumen de transacciones por segundo [6].

La plataforma puede ser interpretada como una máquina virtual sobre la que es posible desarrollar aplicaciones distribuidas denominadas "contratos inteligentes", aplicaciones integradas a la cadena de bloques, sin que sea necesario desarrollar más que la última capa de la aplicación. El concepto de "contrato inteligente" es implementado por primera vez en esta plataforma, la plataforma soporta un lenguaje de programación turing-completo, mediante el que es posible desarrollar cualquier contrato inteligente.

La cadena de bloques de Ethereum permite registrar información tan diversa como la que es posible registrar en una base de datos relacional. La plataforma también suele ser descrita como una máquina de estados de propósito general, en la que cada transacción efectuada influye en la transición de un estado a otro. Al estado inicial se le denomina "estado génesis".

La prueba de participación parece ser más conveniente que la prueba de trabajo en todos

[63] La referencia del desarrollador (de Bitcoin) contiene la documentación sobre la estructura de datos de la cadena de bloques de Bitcoin [18].

[64] Esto está demostrado en el apéndice A, mediante un contraejemplo de la proposición: *Existe* $f : (\text{seq}\,\mathbb{N}) \to \mathbb{C}$ *tal que para cada* $\sigma : \text{seq}\,\mathbb{N}$ *(secuencia de transacciones bitcoin),* $f(\sigma) \in \mathbb{C}$ *si* σ *es circular, y* $f(\sigma) \notin \mathbb{C}$ *de lo contrario.*

[65] El artículo "Cadenas de bloques en todas partes: Un caso de uso en la cadena de suministro farmacéutica" describe un caso de aplicación [26].

los escenarios, sin embargo, el protocolo de consenso de Ethereum establece que la minería debe ser remunerativa y que, para participar en el proceso de consenso, es necesaria una inversión en ethers por parte del agente interesado. El diseño del mecanismo de tokenización descrito en la sección 5.1.1 no considera la existencia de una criptodivisa nativa mediante la que sea posible implementar un esquema de minería remunerativa, y el protocolo de consenso debe permitir que el sistema de criptodivisa pueda satisfacer los casos de uso descritos en la sección 7.1.1, por lo que creemos que para implementar el mecanismo de incentivos tal como lo hemos diseñado, es conveniente considerar un protocolo diferente.

8.2. Discusión

Según la Fundación Ellen MacArthur, la tecnología es clave en la transición, especialmente en el rastreo de recursos y en la organización de la logística inversa. La dificultad de garantizar disponibilidad, calidad y consistencia de los datos relativos a los recursos sigue siendo un obstáculo importante [7], por otro lado, según la propiedad de "documentación de la procedencia de los datos" de las cadenas de bloques, mediante esta tecnología, cualquier agente podría acceder a información confiable sobre la composición y la procedencia de cualquier recurso, información que además facilitaría las operaciones de coordinación y de logística. Creemos que, mediante una alternativa de solución sin cadena de bloques, la alternativa podría presentar dificultades en el rastreo de recursos, en el alcance de la solución[66], en el establecimiento de la confianza[67], en el costo de mantenimiento del mecanismo de incentivos[68], entre otras.[69]

La inexistencia de una criptodivisa nativa, en el sistema de criptodivisa, posibilita que la transferencia de cada remuneración sea efectuada mediante una criptodivisa logística, esto es necesario para garantizar la seguridad del mecanismo de incentivos[70]. Nuestra propuesta de solución ante este requerimiento consiste en la implementación del mecanismo de tokenización, un mecanismo que puede facilitar la autonomía económica de cualquier cadena de suministro. Esta solución podría incentivar la inscripción de grandes cantidades de aplicaciones. Cada aplicación inscrita, por protocolo, podría permitir la implementación de un mecanismo de incentivos que promueva, o no, el consumo sostenible, un mecanismo de incentivos que, aunque promueva el consumo sostenible, podría ser diferente del mecanismo de incentivos propuesto en este documento, eventualmente, la oferta de un sistema de criptodivisa como el propuesto en este documento podría contribuir en la conformación de un extenso ecosistema de mecanismos.

Sin embargo, la circulación de una criptodivisa por cada aplicación, pese a que cada criptodivisa esté respaldada por la producción[71] de la cadena de suministro subyacente, podría comprometer la función de "medio de intercambio" del sistema. Una medida complementaria que podría contribuir en la solución a este problema consiste en la inscripción de al menos una aplicación mediante la que una casa de intercambio pueda administrar una criptodivisa "neutral", una criptodivisa que sea aceptada por casi cualquier agente como forma de pago, esto se podría lograr más fácilmente si la criptodivisa neutral estuviera respaldada por otra divisa, externa al sistema de criptodivisa, y que sea generalmente aceptada, como el Bitcoin.

[66] En caso de que el alcance de la solución fuese global, probablemente, el mantenimiento del sistema sería altamente costoso.

[67] Si la administración del sistema requiere de centralización.

[68] En especial, si el sistema implementa un mecanismo puramente fiat y el mecanismo es mantenido por el Estado, a menos que se establezca otro mecanismo que permita financiar el mecanismo de incentivos, tal vez mediante penalizaciones.

[69] Un ejemplo de sistema transaccional a partir de el que se podría desarrollar una alternativa podría ser similar a la plataforma de VISA, otro ejemplo de sistema transaccional que ejemplifica una alternativa es el de los *ecoins*, con una implementación en Costa Rica, otra en Panamá, y otra en Perú.

[70] Garantiza la seguridad ante ataques sybil.

[71] Cada criptodivisa, en lugar de estar respaldada directamente por la producción de la cadena de suministro subyacente, podría estar respaldada por cada acción bursátil emitida desde la cadena de suministro subyacente.

Creemos que, en cualquier población, bajo el efecto del mecanismo de incentivos, a partir de cierto tiempo, la actividad de la población se concentraría en un subconjunto de "juegos" en los que cada agente obtendría la utilidad neta máxima al contribuir en la transición hacia la Economía Circular. Es necesario considerar que cada agente, al completar una transacción, puede reconfigurar su criterio de decisión con el objetivo de incrementar la utilidad que obtendrá en la siguiente transacción, la complejidad de un algoritmo mediante el que sea posible encontrar una nueva configuración para cada agente[72] sería de no menos de $O(n_1 \cdot n_2 \cdot n_3)$, tal que n_1 sea a la cantidad de agentes en el sistema, n_2 sea a la cantidad de bloques aceptados hasta alcanzar el equilibrio, y n_3 sea a la cantidad de posibles configuraciones para el criterio de decisión de cada agente. La complejidad parece ser lineal, pero el dominio de ninguno de los parámetros está acotado.

Sin embargo, es posible formular un algoritmo de aprendizaje que determine el comportamiento de cada agente de forma que facilite el alcance del equilibrio en un sistema dinámico [8], que sea posible formularlo, nos permitió optar por un modelo de "juego" multiagente, un modelo que nos permitió obtener el corolario 5.3.2 que aunque no lo garantiza, si se sigue al implementar el mecanismo de incentivos, puede facilitar que el comportamiento de la población se aproxime al comportamiento de la población ideal, no lo garantiza porque cada interacción puede causar un "efecto mariposa", un efecto difícil de predecir, en un juego posterior, y el efecto que provoque cualquier algoritmo de aprendizaje, que facilite el alcance del equilibrio, en el comportamiento, puede ser muy diferente del efecto que provocaría la experiencia que pueda adquirir un usuario cualquiera del sistema de criptodivisa.

Hemos desarrollado, un análisis estadístico que considerara la dinámica del sistema económico como un todo, y hemos formulado un algoritmo de aprendizaje que es implementado por el sistema de simulación, un algoritmo que permite alcanzar el equilibrio, para poder garantizar que el comportamiento de cada agente es racional, sin embargo, para formular un algoritmo de complejidad menor que la estimada anteriormente, hemos asumido ciertas características que restringen la libertad de cada agente, descritas en la sección B.1, sobre las limitaciones del sistema de simulación, las características 10, 11 y 12. Creemos que sería posible evaluar la hipótesis a partir de un conjunto de datos para cada serie generado mediante un sistema de simulación que implemente un algoritmo de aprendizaje que no requiera asumir características restrictivas, o evaluar la hipótesis mediante un método analítico, a partir del algoritmo que hemos formulado, o a partir de otro que no requiera asumir características restrictivas.

Según el análisis estadístico del efecto del mecanismo de incentivos, documentado en el capítulo 6, podemos aceptar la hipótesis original, la que hemos establecido en el capítulo 1, sin embargo, la aceptación de la hipótesis es discutible, no solo por las características del algoritmo de aprendizaje que restringen la libertad de cada agente, también porque hemos establecido el nivel de significancia para evaluar la hipótesis nula en 0,1. Si estableciéramos el nivel de significancia en 0,05, entonces no podríamos aceptar la hipótesis original, ya que según los resultados del análisis para la serie experimental, no habría evidencia suficiente para rechazar la hipótesis nula, el valor p sería mayor que el nivel de significancia, $0{,}11 > 0{,}05$, y según los resultados del análisis para la serie de control, tampoco habría evidencia suficiente para rechazar la hipótesis nula, el valor p' también sería mayor que el nivel de significancia, $0{,}09 > 0{,}05$.

8.3. Conclusiones

Una contribución relevante de este trabajo es la técnica mediante la que hemos obtenido el modelo del sistema económico, un sistema dinámico, el modelo se encuentra en el capítulo 5. El modelo permite el análisis del sistema mediante una definición del equilibrio para

[72] Equivale al orden del cómputo requerido por el análisis del equilibrio en el entorno.

juegos estáticos con dos jugadores. Otra contribución relevante de este trabajo es la técnica mediante la que hemos definido la función de utilidad que se encuentra en el capítulo 5, la técnica consistió en establecer dos dimensiones en las que sea posible ubicar cualquier factor que pueda influir en la utilidad de cada agente, incluso los factores relativos al mecanismo de incentivos, las dimensiones "ingreso/egreso" e "intrínseco/extrínseco".

Otra contribución relevante de este trabajo, más que los resultados del análisis de datos, es el diseño del método experimental, la pregunta de investigación establecida en el capítulo 1, para ser abordada mediante un análisis de varianza, requiere de un diseño de experimentos no intuitivo, el diseño del método experimental que se encuentra en el capítulo 6 lo permite, independientemente del origen de los conjuntos de datos. Otra contribución relevante de este trabajo, más que la definición de circularidad que se encuentra en el capítulo 4, es la técnica mediante la que la hemos obtenido, la búsqueda de un autómata finito mediante el que sea posible reconocer una propiedad de las transacciones que contribuyan con el cambio de paradigma.

Hemos propuesto un mecanismo de incentivos, de alcance global, que esperamos pueda estimular una dinámica que acelere la transición hacia una economía circular, mediante la incentivación de cierto comportamiento local. Creemos que un sistema de criptodivisa como el propuesto en este documento permitiría el diseño de mecanismos mediante los que otros comportamientos podrían ser incentivados. Esto confirma la importancia de la propiedad de "transparencia", de las cadenas de bloques, en especial cuando el sistema de criptodivisa permite estimular una dinámica en particular.

8.4. Trabajo futuro

La aceptación de la hipótesis es discutible, por lo que consideramos necesario explorar la posibilidad de evaluar la hipótesis mediante un método analítico, a partir del algoritmo de aprendizaje que hemos formulado, o a partir de otro algoritmo que no requiera asumir características restrictivas. En caso de que se determine que para evaluarla es más apropiado un análisis experimental, similar al desarrollado en el capítulo 6, creemos que podríamos establecer el nivel de significancia en 0,05 y aun así obtener evidencia suficiente para aceptar la hipótesis planteada en el capítulo 1 si se remueve algunas de las características restrictivas, como las 2, 6, 11 y 12[73] descritas en la sección B.1, sobre las limitaciones del sistema de simulación, y se vuelve a evaluar la hipótesis a partir de los resultados del análisis para cada serie. Las características 11 y 12 podrían ser removidas mediante otro algoritmo de aprendizaje, o un algoritmo evolutivo.

Creemos que es importante caracterizar al conjunto de mecanismos de incentivos que sean implementables bajo la arquitectura propuesta en este documento y, a partir de este conjunto, investigar sobre el soporte para un conjunto más extenso. Esperamos, en el futuro, tener oportunidad de desarrollar un prototipo de sistema de criptodivisa que, mediante su desarrollo, nos permita refinar la arquitectura propuesta es el capítulo 7. Creemos que también puede ser importante investigar a profundidad la compatibilidad entre el mecanismo de incentivos propuesto en este documento y un protocolo de consenso diferente de uno con prueba de participación tolerante a fallas bizantinas, e investigar sobre el soporte necesario para la implementación de aplicaciones mediante las que sea posible incentivar la participación en el trabajo de minería.

[73] La 2 es sobre el límite en la cantidad de tipos de recurso. La 6 es sobre el monto que cada agente requiere para transferir cada uno de sus recursos. La 11 es sobre lo que, de facto, cada agente está dispuesto a invertir. La 12 es sobre la reacción, también de facto, de cada agente ante un competidor.

Bibliografía

[1] P. E. de la Nación, "Estado de la nación 2020," 2020. [Online]. Available: https://estadonacion.or.cr

[2] G. Nobre and E. Tavares, "Scientific literature analysis on big data and internet of things applications on circular economy: a bibliometric study," *Scientometrics*, 02 2017.

[3] M. Slater. (2017) Towards perma-circular currencies? why a regenerative economy calls for new forms of money. [Online]. Available: https://www.community-exchange.org/home/towards-perma-circular-currencies-why-a-regenerative-economy-calls-for-new-forms-of-money

[4] *Token Economics: Designing The Digital Economy*. Pallars 193, 8005, Barcelona, Spain: Systems Academy, 03 2017. [Online]. Available: https://systemsacademy.io/token-economics-book

[5] "Ecoins lanza su app que facilita encontrar centros de acopio y canjear puntos por descuentos," *El Mundo CR*, 03 2020. [Online]. Available: https://www.elmundo.cr/tendencias/ecoins-lanza-su-app-que-facilita-encontrar-centros-de-acopio-y-canjear-puntos-por-descuentos/

[6] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *CoRR*, vol. abs/1904.04098, 2019. [Online]. Available: http://arxiv.org/abs/1904.04098

[7] "Towards the circular economy 3—accelerating the scale-up across global supply chains," 2014. [Online]. Available: http://www.ellenmacarthurfoundation.org/books-and-reports

[8] Y. Shoham and K. Leyton-Brown, "Introduction to noncooperative game theory: Games in normal form," *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*, pp. 47–88, 2008.

[9] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *Journal of Network and Computer Applications*, vol. 182, p. 103035, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521000618

[10] J. Woodcock and J. Davies, *Using Z: Specification, Refinement, and Proof*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1996.

[11] D. Masi, S. Day, and J. Godsell, "Supply chain configurations in the circular economy: A systematic literature review," *Sustainability*, vol. 9, p. 1602, 09 2017.

[12] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," 04 2017, pp. 12–23.

[13] J. Chen, S. Gorbunov, S. Micali, and G. Vlachos, "Algorand agreement: Super fast and partition resilient byzantine agreement," Cryptology ePrint Archive, Report 2018/377, 2018, https://eprint.iacr.org/2018/377.

[14] M. Westerkamp, F. Victor, and A. Küpper, "Blockchain-based supply chain traceability: Token recipes model manufacturing processes," *CoRR*, vol. abs/1810.09843, 2018. [Online]. Available: http://arxiv.org/abs/1810.09843

[15] J. M. Spivey, "An introduction to Z and formal specifications," *Softw. Eng. J*, 1989.

[16] J. E. Hopcroft, R. Motwani, and J. D. Ullman, "Finite automata," *Introduction to Automata Theory, Languages, and Computation (3rd Edition)*, pp. 37–84, 2006.

[17] S. Micali, "ALGORAND: the efficient and democratic ledger," *CoRR*, vol. abs/1607.01341, 2016. [Online]. Available: http://arxiv.org/abs/1607.01341

[18] K. Okupski, "Bitcoin developer reference," 07 2016.

[19] K. Haller, J. Lee, and J. Cheung, "Meet the 2020 consumers driving change," 2020. [Online]. Available: https://www.ibm.com/thought-leadership/institute-business-value/report/consumer-2020

[20] B. Carruthers, "The meanings of money: A sociological perspective," *Theoretical Inquiries in Law*, vol. 11, 01 2010.

[21] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. PP, 06 2017.

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 03 2009.

[23] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[24] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger eip-150 revision (759dccd - 2017-08-07)," 2017. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[25] M. Dameron, "An ethereum technical specification," 2018.

[26] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, May 2017, pp. 772–777.

[27] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 6–24.

A

"Circularidad" en la cadena de bloques de Bitcoin

A.1. Sinopsis

Esta sección demuestra que *a partir de solo la estructura de datos de una cadena de bloques como la subyacente a la red de Bitcoin, no es posible formular un criterio de circularidad*, lo demuestra mediante un contraejemplo de la proposición A.1.1, así, el aumento de complejidad que implica el uso de una estructura más amplia, como la que implementa cualquier cadena de suministro, queda justificado.

Proposición A.1.1. *Existe* $f : (\text{seq}\,\mathbb{N}) \to \mathbb{C}$ *tal que para cada* $\sigma : \text{seq}\,\mathbb{N}$ *(secuencia de transacciones bitcoin),* $f(\sigma) \in \mathbb{C}$ *si* σ *es circular, y* $f(\sigma) \notin \mathbb{C}$ *de lo contrario.*

A.2. Marco teórico

El criterio de f depende del formato de las transacciones. Según la referencia del desarrollador de Bitcoin, el formato exige un identificador de la transacción, la versión del protocolo de consenso, el origen de los fondos y la cardinalidad del origen, el destino de los fondos y la cardinalidad del destino, y una marca de tiempo [18].

El destino de los fondos consta de una lista de "salidas", y la cardinalidad del destino corresponde a la cantidad de estas salidas. Cada salida incluye el monto en satoshis[74] a ser transferido, un script de llave y la longitud del script en bytes.

El origen de los fondos consta de una lista de "entradas", cada una consume una salida de una transacción anterior, y la cardinalidad del origen corresponde a la cantidad de estas entradas. Cada entrada incluye un script de firma y la longitud del script en bytes, un número de secuencia, y una referencia a una salida anterior compuesta del identificador de la transacción a la que pertenece y un índice que permite ubicar la salida en la transacción.

El script de llave en cada salida contiene una serie de restricciones que deben ser satisfechas por el script de firma en la entrada que la consume. El formato típico del script de llave es `OP_DUP OP_HASH160` $\#k$ k `OP_EQUALVERIFY OP_CHECKSIG`, tal que k sea la dirección del destinatario y $\#k$ la longitud en bytes de la dirección, cada uno de los otros elementos

[74] 1 satoshi equivale a 10^{-8} bitcoins [27]

corresponde a un código de operación que el protocolo requiere para mantener la integridad de cada transacción. El formato típico del script de firma es *#s s* tal que *s* sea la firma del agente que efectuó la transacción y *#s* la longitud de la firma en bytes.

A.3. Demostración

Sea $e_3 : E$ la transacción entre Cenizo y Jacinto descrita en el cuadro A.1, sea $e_2 : E$ la transacción entre Jacinto y Simposio descrita en el cuadro A.1, y sea $e_1 : E$ la transacción entre Simposio y Cenizo descrita en el cuadro A.1. Sea $e'_3 : E$ una transacción cualquiera entre Cenizo y Jacinto, sea $e'_2 : E$ una transacción cualquiera entre Jacinto y Simposio, y sea $e'_1 : E$ una transacción cualquiera entre Simposio y Cenizo. Sea $\sigma_1 : \text{seq}\,\mathbb{N}$ tal que $\sigma_1 = \langle \sim e_1, \sim e_2, \sim e_3 \rangle$ la secuencia compuesta por una referencia a cada transacción efectuada en el escenario a, y sea $\sigma_2 : \text{seq}\,\mathbb{N}$ tal que $\sigma_2 = \langle \sim e'_1, \sim e'_2, \sim e'_3 \rangle$ la secuencia compuesta por una referencia a cada transacción efectuada en el escenario b.

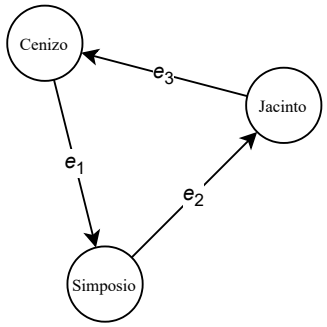

Figura A.1: Diagrama para la secuencia de transacciones descrita en el cuadro A.1. La dirección de cada arista representa la dirección de la transferencia del monto correspondiente.

Cuadro A.1: Conjunto de las transacciones que componen una secuencia "circular". En la primera transacción, Jacinto le compra a Cenizo una docena de botellas de cerveza de la marca Rabia, la marca que ella produce, en envase de vidrio, en la segunda transacción, Simposio compra una de esas cervezas en la tienda de Jacinto, y en la tercera transacción, Cenizo le compra a Simposio el envase que contenía la cerveza para reutilizar el vidrio.

	Jacinto→Cenizo	Simposio→Jacinto	Cenizo→Simposio
Identificador	J_1	J_2	J_3
Cantidad de entradas	1	1	1
Entrada			
Salida anterior	ι_1	ι_2	ι_3
Longitud del script de firma	ℓ_1	ℓ_3	ℓ_5
Script de firma	*JacSigScr*	*SimSigScr*	*CenSigScr*
Número de secuencia	n_1	n_2	n_3
Cantidad de salidas	1	1	1
Salida			
Monto	v_1	v_2	v_3
Longitud del script de llave	ℓ_2	ℓ_4	ℓ_6
Script de llave	*CenKeyScr*	*JacKeyScr*	*SimKeyScr*
Marca de tiempo	t_1	t_2	t_3

Claramente σ_1 es circular y σ_2 no lo es, según el paradigma de la Economía Circular[75],

[75] La figura 1.1 ilustra la dinámica del manejo de los recursos en una economía circular.

pero $f(\sigma_1) \in \mathbb{C} \Rightarrow f(\sigma_2) \in \mathbb{C}$ para cualquier criterio de f ya que no hay diferencia entre los registros para el escenario a y los registros para el escenario b, por lo que a partir del registro de cada transacción en la cadena de bloques subyacente a la red de Bitcoin no es posible obtener un criterio de f tal que $f(\sigma_1) \in \mathbb{C}$ y $f(\sigma_2) \notin \mathbb{C}$.

B

Modelo del sistema de simulación

El sistema de simulación emula una dinámica económica promovida por la demanda y la oferta de tres tipos de recurso, según su función. Cada agente, para cada tipo de recurso, puede disponer de más de, tanto como, o de menos de lo que requiere. La expresión B.1, mediante la definición de $\nu_1 : V \to \mathbb{N}$, $\nu_2 : V \to \mathbb{N}$ y $\nu_3 : V \to \mathbb{N}$, permite representar a la demanda y a la oferta, de cada agente, y de los tipos de recurso 1, 2 y 3, e.g., el agente 1, para el tipo de recurso 2, dispone de más de lo que requiere si $\nu_2(1) > 0$, dispone de tanto como lo que requiere si $\nu_2(1) = 0$, o dispone de menos de lo que requiere si $\nu_2(1) < 0$.

$$
\begin{aligned}
&\exists\, V' : \operatorname{seq} V \mid \#V' = \#V \bullet \forall\, i : V \mid \langle i \rangle \text{ in } V' \bullet \\
&\quad \exists\, x, x', y, y', z, z' : \mathbb{N} \mid \\
&\qquad\qquad i = x \;+ 8 \cdot y \;+ 64 \cdot z \;\land \\
&\qquad\qquad V'(i) = x' + 8 \cdot y' + 64 \cdot z' \land \\
&\qquad\qquad \nu_1(i) = x - x' \land \\
&\qquad\qquad \nu_2(i) = y - y' \land \\
&\qquad\qquad \nu_3(i) = z - z'
\end{aligned}
\tag{B.1}
$$

Según la expresión B.1, para cada tipo de recurso existe una función biyectiva entre el conjunto de las cantidades, una por cada agente, correspondiente a la demanda del agente por el tipo de recurso, y el conjunto de las cantidades, una por cada agente, correspondiente a la oferta del agente por el tipo de recurso.

$$
\begin{aligned}
\mathring{\Delta}_i(t) &= \mathring{v}_i(t) - \mathring{\psi}_i(t), \\
\dot{\Delta}_i(t) &= \dot{v}_i(t) - \dot{\psi}_i(t), \\
\Delta_i(t) &= v_i(t) - \psi_i(t)
\end{aligned}
\tag{B.2}
$$

$$\forall\, i : V;\, t : \mathbb{N} \bullet t = 0 \Rightarrow v_i(t) > \psi_i(t) \land \psi_i(t) > 0 \land \dot{v}_i(t) > \dot{\psi}_i(t) \land \dot{\psi}_i(t) > 0 \land \mathring{v}_i(t) > \mathring{\psi}_i(t) \land \mathring{\psi}_i(t) > 0.$$

El criterio de decisión de cada agente varía en función del tiempo. El criterio, en el modelo del sistema de simulación, corresponde al criterio de v_i, ψ_i, $\dot{v}_i$, $\dot{\psi}_i$, $\mathring{v}_i$ y $\mathring{\psi}_i : \mathbb{N} \to \mathbb{N}$ de cada agente i. La expresión B.2, mediante la definición de $\mathring{\Delta}_i$, $\dot{\Delta}_i$ y $\Delta_i : \mathbb{N} \to \mathbb{Z}$, describe el cálculo de la utilidad intrínseca neta obtenida mediante la estrategia 1, la estrategia 2 y la estrategia 3, respectivamente.

B.1. Limitaciones del sistema de simulación

Como todo modelo, el modelo del sistema de simulación difiere, en algunas características, del sistema modelado, en este caso, un sistema económico, en el que la población dispone de un sistema de criptodivisa que puede implementar el mecanismo de incentivos propuesto. La siguiente lista describe algunas de las características del sistema de simulación.

1. En el sistema de simulación, las cadenas de suministro son volátiles. Cada cadena de suministro, junto con sus características, emerge de la actividad inherente al tratamiento correspondiente, y cada transacción es efectuada entre un agente proveedor de servicios y otro agente consumidor.

2. El sistema de simulación emula la oferta de solo tres tipos de recurso, según su función.

3. El sistema de simulación no implementa nuestro criterio de circularidad, la circularidad de cada transacción es determinada en función del criterio de decisión del consumidor.

4. El conjunto de las acciones disponibles en el sistema de simulación, descrito en el cuadro B.1, difiere ligeramente del conjunto de las acciones disponibles en el modelo de juego, descrito en el cuadro 5.2. No es necesario, para evaluar la hipótesis, que el sistema de simulación exhiba alguna característica inherente al mecanismo de tokenización, o al trabajo de minería, sin embargo sí es necesario distinguir entre una transacción mediante la que se reciba un insumo que sea sostenible y una transacción mediante la que se entregue un producto que sea sostenible, esto porque el agente que recibe la remuneración es el agente consumidor.

5. El monto es registrado en una divisa neutral, para cada transacción.

6. El monto requerido para transferir cualquier recurso, es independiente del tipo del recurso.

7. No hay límite para lo que cualquier agente puede invertir, en una o más iteraciones.

8. El valor representado mediante el componente $\check{v}_i(a)$, según el cuadro 5.1, toma en cuenta cualquier utilidad que pueda derivar del uso del sistema de criptodivisa, interpretada como valor monetario, para cualquier agente i, sea interno o sea externo, según la configuración a.

9. El sistema de simulación no emula, para agente alguno, el efecto de la participación en la minería. Si se quiere, para cada agente i y configuración a, se puede suponer que el componente $\check{v}_i(a)$, según el cuadro 5.1, refleja la utilidad inherente a la participación en la minería, y que el componente $\hat{v}_i(a)$, según el cuadro 5.1, refleja la inversión inherente a la participación en la minería.

10. El algoritmo de aprendizaje requiere la equiparación del valor monetario de los insumos al costo de la inversión intrínseca en un solo recurso, para cada venta.

11. Según el algoritmo de aprendizaje, ningún agente está dispuesto a invertir más de lo que haya decidido invertir previamente, esto implica que, si un proveedor decidiera incrementar su utilidad bruta, esta sería mayor que lo que cualquier posible consumidor estuviera dispuesto a invertir.

12. Según el algoritmo de aprendizaje, cada proveedor, en caso de competir con otro, decidiría mejorar su oferta y no compartir la utilidad. Esto minimizaría el valor monetario del recurso.

B.2. Historial de transacciones

El sistema de simulación, para cada simulación, registra un historial de transacciones, y completa 256 iteraciones. Hemos tratado a cada historial como un multigrafo dirigido $\widetilde{\mathbb{G}} = (V, \widetilde{E})$, como en el capítulo 4, el capítulo sobre el modelo circular de red de suministro. En el modelo del sistema de simulación, cada transacción es una transacción unitaria, definida por un agente proveedor $i : V$, un agente consumidor $j : V$, un descriptor del recurso $w : W$, una marca de tiempo $t : \mathbb{N}$, y otro descriptor $a : \widetilde{A}$ de la acción de la que deriva la transacción.

$$\widetilde{E} \triangleq [i; j; w; t; a] \tag{B.3}$$

$W = \{1, 2, 3\}$, el recurso es de tipo 1, de tipo 2, o de tipo 3. El conjunto $\widetilde{A}$, el conjunto de las acciones disponibles en el sistema de simulación, está definido en el cuadro B.1.

Cada transacción en $\widetilde{E}$, corresponde una transferencia efectuada en la iteración t, de un recurso de tipo w, de un agente i que no requiere el recurso, a otro agente j que sí requiere el recurso, y deriva de una acción a mediante la que el agente j maximiza su utilidad. La expresión B.4, mediante la definición de $z : V \times V \times \mathbb{N} \times \widetilde{A} \to \mathbb{Z}$, permite interpretar a $z(i, j, t, a)$ como la utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t, transacción que deriva de la acción a.

$$\begin{aligned} &\forall e : \widetilde{E} \bullet \\ &\quad z(i,j,t,a) = \max_{\forall\, i' : V;\, a' : \widetilde{A}} \begin{cases} z(i', j, t, a') \mid \\ \qquad \nu_w(j) < 0 \wedge \nu_w(i') > 0 \end{cases} \end{aligned} \tag{B.4}$$

Según la expresión B.3, los componentes i, j, w, t y a existen en el esquema $\widetilde{E}$.

La siguiente lista describe cada combinación de propiedades correspondiente a alguna de las acciones disponibles en el sistema de simulación, el cuadro B.1 contiene una versión sistemática de la descripción. Cualquier combinación que no esté en la lista no corresponde a una acción disponible en el sistema de simulación.

- 0. Corresponde a cualquier transacción que no sea efectuada mediante el sistema de criptodivisa.

- 100. Corresponde a cualquier transacción que sea efectuada mediante el sistema de criptodivisa, en la que se transfiera un insumo que no sea sostenible, de un producto que no sea sostenible.
- 110. Corresponde a cualquier transacción que sea efectuada mediante el sistema de criptodivisa, en la que se transfiera un insumo que no sea sostenible, de un producto que sea sostenible.
- 101. Corresponde a cualquier transacción que sea efectuada mediante el sistema de criptodivisa, en la que se transfiera un insumo que sea sostenible, de un producto que no sea sostenible.
- 111. Corresponde a cualquier transacción que sea efectuada mediante el sistema de criptodivisa, en la que se transfiera un insumo que sea sostenible, de un producto que sea sostenible.

Cuadro B.1: Descripción del conjunto de acciones disponibles en el sistema de simulación. Cada columna corresponde a una acción, y cada acción está definida por las propiedades en 1 que le corresponden.

Propiedad					
Uso de la cuenta	0	1	1	1	1
El recurso es insumo de otro recurso que es sostenible	0	0	1	0	1
El recurso es sostenible	0	0	0	1	1

En cada simulación para la serie experimental, cada agente transfiere una remuneración por contribuir en la transición, si mediante la estrategia 1 obtiene la máxima utilidad neta que puede obtener, por otro lado, en cada simulación para la serie de control, ningún agente transfiere la remuneración por contribuir en la transición, el mecanismo de incentivos permanece inactivo. La expresión B.5, mediante la definición de $\widetilde{\nabla} : V \times \mathbb{N} \to \mathbb{Z}$ y la definición de $\widetilde{\nabla}' \to V \times \mathbb{N} \to \mathbb{Z}$ permite identificar como $\widetilde{\nabla}(i,t)$ para la serie experimental, o $\widetilde{\nabla}'(i,t)$ para la serie de control, a la remuneración que transfiere el agente i en la iteración t. Las funciones $\widetilde{\nabla}$ y $\widetilde{\nabla}'$, por construcción, implementan las restricciones expresadas en el corolario[76] 5.3.2.

$$\widetilde{\nabla}\ (i,t) = \begin{cases} 0 & \mathring{\Delta}_i(t) - \dot{\Delta}_i(t) \leq 1 \vee \Delta_i(t) \geq \mathring{\Delta}_i(t) \\ \\ \mathring{\Delta}_i(t) - \dot{\Delta}_i(t) - 1 & \mathring{\Delta}_i(t) - \dot{\Delta}_i(t) > 1 \wedge \Delta_i(t) < \mathring{\Delta}_i(t) \end{cases} \tag{B.5}$$

$$\widetilde{\nabla}'(i,t) = 0$$

$$\forall\, i : V;\, t : \mathbb{N}.$$

La expresión B.6 facilita la reinterpretación de $z(i,j,t,a)$ como la diferencia, para el agente j, entre la utilidad bruta esperada, tomando en cuenta la remuneración por contribuir en la transición, si aplica, y la inversión intrínseca requerida, de la transferencia de un recurso del agente i al agente j en la iteración t, diferencia que es maximizada mediante la acción a.

[76] El cálculo de la remuneración según la expresión B.5 equivale al cálculo de la remuneración según la expresión 5.5 con $\theta(i) = 3$, $\ell_{-4}(\sigma) = 1$, $\ell_4(\sigma) = 1$, $\varphi = \mathring{\upsilon}_i$, $\check{h}_{-4} = 0$ y $\check{h}_4 = \left((\mathring{\upsilon}_i - \mathring{\psi}_i) - (\dot{\upsilon}_i - \dot{\psi}_i) - 1\right)\frac{1}{\dot{\upsilon}_i}$.

Si la transacción deriva de la acción 0, la máxima utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t equivale a $v_j(t) - v_i(t)$, de lo contrario, la utilidad no es superior o el agente i no permite la acción 0.

$$\begin{aligned} z(i,j,t,a) = v_j(t) - v_i(t) \wedge \\ a = 0 \wedge \\ \left(v_j(t) - v_i(t) \geq \dot{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \wedge \\ \left(v_j(t) - v_i(t) \geq \mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(v_j(t) - v_i(t) \geq \dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(v_j(t) - v_i(t) \geq \mathring{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \vee \end{aligned}$$

Si la transacción deriva de la acción 100, la máxima utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t equivale a $\dot{v}_j(t) - \dot{v}_i(t)$, de lo contrario, la utilidad no es superior o el agente i no permite la acción 100.

$$\begin{aligned} z(i,j,t,a) = \dot{v}_j(t) - \dot{v}_i(t) \wedge \\ a = 100 \wedge \\ \left(\dot{v}_j(t) - \dot{v}_i(t) \geq \mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \dot{v}_i(t) \geq v_j(t) - v_i(t) \vee v_i(t) - \psi_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \dot{v}_i(t) \geq \dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \dot{v}_i(t) \geq \mathring{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \vee \end{aligned}$$

Si la transacción deriva de la acción 110, la máxima utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t equivale a $\mathring{v}_j(t) - \dot{v}_i(t)$, de lo contrario, la utilidad no es superior o el agente i no permite la acción 110.

$$\begin{aligned} z(i,j,t,a) = \mathring{v}_j(t) - \dot{v}_i(t) \wedge \\ a = 110 \wedge \\ \left(\mathring{v}_j(t) - \dot{v}_i(t) \geq \dot{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \dot{v}_i(t) \geq \mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \dot{v}_i(t) \geq \dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \dot{v}_i(t) \geq v_j(t) - v_i(t) \vee v_i(t) - \psi_i(t) \leq 0\right) \vee \end{aligned}$$

Si la transacción deriva de la acción 101, la máxima utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t equivale a $\dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t)$, de lo contrario, la utilidad no es superior o el agente i no permite la acción 101.

$$\begin{aligned} z(i,j,t,a) = \dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \wedge \\ a = 101 \wedge \\ \left(\dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \dot{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq v_j(t) - v_i(t) \vee v_i(t) - \psi_i(t) \leq 0\right) \wedge \\ \left(\dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \mathring{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \vee \end{aligned}$$

Si la transacción deriva de la acción 111, la máxima utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t equivale a $\mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t)$, de lo contrario, la utilidad no es superior o el agente i no permite la acción 111.

$$\begin{aligned} z(i,j,t,a) = \mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \wedge \\ a = 111 \wedge \\ \left(\mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \dot{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq v_j(t) - v_i(t) \vee v_i(t) - \psi_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \dot{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \vee \mathring{v}_i(t) - \mathring{\psi}_i(t) \leq 0\right) \wedge \\ \left(\mathring{v}_j(t) - \mathring{v}_i(t) + \widetilde{\nabla}(i,t) \geq \mathring{v}_j(t) - \dot{v}_i(t) \vee \dot{v}_i(t) - \dot{\psi}_i(t) \leq 0\right) \end{aligned}$$

Según la expresión B.3, los componentes i, j, t y a existen en el esquema $\widetilde{E}$. $\forall\, e : \widetilde{E}$.

(B.6)

Esta descripción del historial de transacciones permite, si se interpreta a $E_{\imath\,\jmath}$ como el conjunto de transacciones para el tratamiento $\imath$ y la observación $\jmath$, obtener la definición formal B.7 de la variable de respuesta del diseño del método experimental[77].

$$y_\imath(\jmath) = \frac{\#\{e : \widetilde{E} \mid e \in E_{\imath\,\jmath} \land t = 255 \land a \in \S_1\}}{\#\{e : \widetilde{E} \mid e \in E_{\imath\,\jmath} \land t = 255\}} \tag{B.7}$$

Según la expresión B.3, los componentes t y a existen en el esquema $\widetilde{E}$.
$\forall\, \imath : \{1,\ldots,24\};\ \jmath : \{1,\ldots,16\} \bullet \exists\, y_\imath(\jmath) : \mathbb{R}$.

B.3. Algoritmo de aprendizaje

El algoritmo de aprendizaje implementa una heurística, la heurística B.3.1, que permite, al cabo de cada iteración t, aplicar un ajuste al criterio de decisión de cada agente i mediante el que, al cabo de cierto tiempo, i obtenga una utilidad neta mayor, o igual en el peor caso, que la que habría obtenido sin el ajuste. La operación de ajuste está descrita en el esquema B.1. El algoritmo de aprendizaje permite que lo que sucede en cada iteración pueda ser diferente de lo que sucedió en la iteración anterior.

Heurística B.3.1. *En cada iteración t (en la primera iteración, $t = 0$), (a) cada agente i debe definir el valor monetario $w_i(t)$ que está dispuesto a invertir en una venta, como $w_i(t) = v_j(t)$ si $v_j(t) \leq w_i(t')$, o como $w_i(t) = w_i(t-1)$ si no, donde $v_j(t)$ sea el costo de la mínima inversión requerida por la venta, $w_i(t')$ sea el costo de la última inversión en la venta si la hubo, o sea 0 si no; y (b) cada agente i debe definir el valor monetario $v_i(t)$ correspondiente a la utilidad que espera de una venta, como $v_i(t) = v_i(t-1) - f_i(t)$, donde $f_i(t) = 1$ si $u_i(t) < u_i(-1) \land v_i(t-1) - 1 > w_i(t)$, o $f_i(t) = 0$ si no, tal que $u_i(t)$ sea el volumen de ventas actual; con $w_i(-1)$ como la estimación inicial de la inversión en la venta, $v_i(-1)$ como la utilidad esperada inicialmente, y $u_i(-1)$ como el volumen de ventas esperado.*

La implementación de la heurística B.3.1 requiere de la equiparación del valor monetario de los insumos al costo de la inversión intrínseca, para cada recurso. Según la heurística, sobre el costo de la inversión intrínseca, ningún agente está dispuesto a invertir más de lo que decide, y lo decide en función de la inversión intrínseca mínima hasta la iteración actual; y sobre el valor monetario correspondiente a la utilidad intrínseca, para cualquier agente, este valor solo puede mantenerse o disminuir, disminuye solo si el agente no vende el volumen esperado, que es el máximo volumen posible, mientras sea mayor a la inversión intrínseca. Si el valor monetario correspondiente a la utilidad intrínseca aumentara, sería mayor que lo que cualquier posible consumidor estuviera dispuesto a invertir.

En cualquier iteración, si existiera un proveedor i del tipo w de recurso, por el valor monetario φ, y para i hubiera ventas del tipo w, pero el volumen de estas no fuera el máximo posible, entonces existiría al menos otro proveedor j del tipo w por el valor monetario φ; por lo tanto, para mejorar su oferta, el proveedor i tendría que actualizar el valor monetario que corresponde a la utilidad bruta esperada de la venta. Esto puede provocar un efecto de "juego de ciempiés", puede provocar que, en cada iteración, cada proveedor deba decidir entre (a) "mejorar su oferta y no compartir la utilidad", y correr el riesgo de que el otro proveedor decida igual; y (b) "no mejorar su oferta y compartir la utilidad", y correr el riesgo de que el otro proveedor decida diferente.

[77] El sistema de simulación, para cada simulación, completa 256 iteraciones, la primera es la iteración 0 y la última es la iteración 255.

Según la heurística B.3.1, cada proveedor decidiría mejorar su oferta y no compartir la utilidad. La heurística provocaría que el valor monetario del recurso sea minimizado, sin embargo, también provoca que el equilibrio sea alcanzado. Es importante que la heurística provoque que el equilibrio sea alcanzado porque para que cada observación sea de calidad, cada agente debe elegir su mejor respuesta. El ejemplo B.3.3 ilustra el efecto de la heurística en el criterio de decisión de cuatro agentes.

Proposición B.3.2. *En toda matriz de agentes que emula el comportamiento económico de una población, mediante la implementación de la heurística B.3.1 por parte de cada agente, a partir de cierto tiempo, cada agente permanece en equilibrio.*

Demostración.

1. Sea $i : V$ tal que i no alcanza el equilibrio.
2. *Según el punto b y la expresión B.2:* $\forall\, i : V;\ t_0 : \mathbb{N} \bullet 0 < w_i(t_0) < v_i(t_0)$.
3. *Según los puntos b y 1:* $\forall\, t_1 : \mathbb{N} \bullet \exists\, t_2 : \mathbb{N} \mid t_1 < t_2 \land v_i(t_2) < v_i(t_1)$.
4. *Según el punto 3:* $\exists\, t_3 : \mathbb{N} \mid v_i(t_3) = 2$, y $\exists\, t_4 : \mathbb{N} \mid t_3 < t_4 \land v_i(t_4) < v_i(t_3)$.
5. Hay contradicción entre los puntos 2 y 4, por lo que, si cada agente implementa la heurística B.3.1, cada agente, a partir de cierta iteración, permanece en equilibrio. □

Ejemplo B.3.3. En un escenario con los agentes (1) Cenizo, (2) Jacinto, (3) Simposio y (4) Gerónimo, tal que en cada iteración, cada agente i pueda conceder, para cada agente j de los otros, un recurso del tipo que j requiere, solo mediante la estrategia 3, según la heurística B.3.1, si (en la iteración 0) $v_1(0) = 20$, $\psi_1(0) = 12$, $v_2(0) = 18$, $\psi_2(0) = 8$, $v_3(0) = 16$, $\psi_3(0) = 14$, $v_4(0) = 12$ y $\psi_4(0) = 10$, entonces (en la iteración 10), $v_1(10) = 11$, $\psi_1(10) = 10$, $v_2(10) = 10$, $\psi_2(10) = 8$, $v_3(10) = 11$, $\psi_3(10) = 10$, $v_4(10) = 11$ y $\psi_4(10) = 10$. El monto por el que vende cada agente se aproxima al monto por el que vende Jacinto, el monto más bajo. Jacinto puede vender por este monto y aun así obtener la mayor utilidad neta total, incluso mayor que la utilidad neta que obtuvo en la iteración 0, ya que es el agente con el monto de compra menor. El detalle de los movimientos en cada iteración aparece en el cuadro B.2.

Cuadro B.2: Desglose de el monto de venta v_i, el monto de compra ψ_i, el proveedor p_i y la utilidad neta total u_i de cada agente i en el ejemplo B.3.3, desde la iteración 0 hasta la iteración 10. En la iteración 6, Cenizo cambia de proveedor, cambia a Gerónimo por Jacinto, esto porque Jacinto disminuye el monto por el que vende. En esta iteración, Jacinto vende por el monto que vende Gerónimo, por lo tanto, la utilidad neta total de Jacinto aumenta, y la de Gerónimo disminuye.

v_1	ψ_1	p_1	u_1	v_2	ψ_2	p_2	u_2	v_3	ψ_3	p_3	u_3	v_4	ψ_4	p_4	u_4
20	12	4	0	18	8		0	16	14	4	0	12	10		4
19	12	4	0	17	8		0	15	12	4	0	12	10		4
18	12	4	0	16	8		0	14	12	4	0	12	10		4
17	12	4	0	15	8		0	13	12	4	0	12	10		4
16	12	4	0	14	8		0	13	12	4	0	12	10		4
15	12	4	0	13	8		0	13	12	4	0	12	10		4
14	12	2	0	12	8		2	13	12	4	0	12	10		2
13	12	2	0	11	8		1	13	12	4	0	11	10		1
12	11	2	0	10	8		3	12	11	2	0	11	10	2	0
11	10	2	0	10	8		3	11	10	2	0	11	10	2	0
11	10	2	0	10	8		3	11	10	2	0	11	10	2	0

Learn

$s?, \dot{s}?, \mathring{s}?,$
$s!, \dot{s}!, \mathring{s}! : \mathrm{seq}\,\mathbb{N}$
$\upsilon_0, \ldots, \upsilon_n, \psi_0, \ldots, \psi_n, \dot{\upsilon}_0, \ldots, \dot{\upsilon}_n, \dot{\psi}_0, \ldots, \dot{\psi}_n,$
$\mathring{\upsilon}_0, \ldots, \mathring{\upsilon}_n, \mathring{\psi}_0, \ldots, \mathring{\psi}_n, \upsilon'_0, \ldots, \upsilon'_n, \psi'_0, \ldots, \psi'_n,$
$\dot{\upsilon}'_0, \ldots, \dot{\upsilon}'_n, \dot{\psi}'_0, \ldots, \dot{\psi}'_n, \mathring{\upsilon}'_0, \ldots, \mathring{\upsilon}'_n, \mathring{\psi}'_0, \ldots, \mathring{\psi}'_n,$
$t, t' : \mathbb{N}$

(a) $t' = t + 1$

(b) $\forall\, i : V$

$$\bullet\ s!(i) = \begin{cases} \hat{\varkappa}_3(i,t) & \hat{\varkappa}_3(i,t) > 0 \\ s?(i) & \hat{\varkappa}_3(i,t) \leq 0 \end{cases}$$

$$\wedge\ \dot{s}!(i) = \begin{cases} \hat{\varkappa}_2(i,t) & \hat{\varkappa}_2(i,t) > 0 \\ \dot{s}?(i) & \hat{\varkappa}_2(i,t) \leq 0 \end{cases}$$

$$\wedge\ \mathring{s}!(i) = \begin{cases} \hat{\varkappa}_1(i,t) & \hat{\varkappa}_1(i,t) > 0 \\ \mathring{s}?(i) & \hat{\varkappa}_1(i,t) \leq 0 \end{cases}$$

(c) $\forall\, i : V \bullet \exists\, v, w : \mathbb{N} \mid v = \check{\varkappa}_1(i,t) \wedge w = \mathring{s}!(i) \bullet$
$\left(\mathring{\psi}'_i = w \wedge \ \ 0 < w \wedge w \leq \mathring{\psi}'_i \vee \mathring{\psi}'_i = \mathring{\psi}_i \wedge (0 \geq w \vee w > \mathring{\psi}'_i)\right) \wedge$
$\left(\mathring{\upsilon}'_i = \ v \wedge \mathring{\psi}'_i < \ v \vee \mathring{\upsilon}'_i = \mathring{\upsilon}_i \wedge \mathring{\psi}'_i \geq v\right)$

(d) $\forall\, i : V \bullet \exists\, v, w : \mathbb{N} \mid v = \check{\varkappa}_2(i,t) \wedge w = \dot{s}!(i) \bullet$
$\left(\dot{\psi}'_i = w \wedge \ \ 0 < w \wedge w \leq \dot{\psi}'_i \vee \dot{\psi}'_i = \dot{\psi}_i \wedge (0 \geq w \vee w > \dot{\psi}'_i)\right) \wedge$
$\left(\dot{\upsilon}'_i = \ v \wedge \dot{\psi}'_i < \ v \vee \dot{\upsilon}'_i = \dot{\upsilon}_i \wedge \dot{\psi}'_i \geq v\right)$

(e) $\forall\, i : V \bullet \exists\, v, w : \mathbb{N} \mid v = \check{\varkappa}_3(i,t) \wedge w = s!(i) \bullet$
$\left(\psi'_i = w \wedge \ \ 0 < w \wedge w \leq \psi'_i \vee \psi'_i = \psi_i \wedge (0 \geq w \vee w > \psi'_i)\right) \wedge$
$\left(\upsilon'_i = \ v \wedge \psi'_i < \ v \vee \upsilon'_i = \upsilon_i \wedge \psi'_i \geq v\right)$

Figura B.1: Descripción de la operación que ajusta el criterio de decisión para cada estrategia, y para cada agente, al cabo de cada iteración. El costo $s!(i)$ corresponde al costo de la inversión intrínseca hecha por el agente i mediante la estrategia 3, El costo $s?(i)$ corresponde al costo homólogo, en la iteración anterior. Si el costo actual es 0, se toma el costo anterior, para cada agente. Los costos $\dot{s}?(i)$ y $\dot{s}!(i)$ corresponden al costo de la inversión intrínseca hecha por el agente i mediante la estrategia 2, en la iteración actual y en la iteración anterior, respectivamente, y los costos $\mathring{s}?(i)$ y $\mathring{s}!(i)$ corresponden al costo de la inversión intrínseca hecha por el agente i mediante la estrategia 1, en la iteración actual y en la iteración anterior, respectivamente. Los pares de componentes identificados de la forma v, v' corresponden al mismo componente en el sistema de simulación, el componente sin decorar representa el valor antes de la operación, y el otro representa el valor después de la operación, e.g., t identifica a la iteración anterior, y t' identifica a la iteración actual.

La expresión c en el esquema B.1 describe el ajuste, para cada agente, del criterio de decisión para la estrategia 1, la operación implementa la heurística B.3.1. En el esquema, la expresión c describe, para cada agente, (1) el cálculo de la inversión intrínseca esperada, el cálculo es descrito mediante la función $\hat{\varkappa}_1$, definida en la expresión B.9; y describe (2) el cálculo de la utilidad intrínseca esperada, el cálculo es descrito mediante la función $\check{\varkappa}_1$, definida en la expresión B.12. El criterio para las estrategias 2 y 3 es ajustado, para cada agente, de la misma forma, las expresiones d y e en el esquema describen las operaciones correspondientes.

Es posible actualizar la utilidad intrínseca esperada y la inversión intrínseca predefinida, solo una de las dos, o ninguna, para cada estrategia y cada agente, la actualización depende de las restricciones que corresponden en cada caso, aunque en cualquiera, la inversión intrínseca predefinida debe ser positiva, y la utilidad intrínseca esperada debe ser mayor que

la inversión intrínseca predefinida.

$$\begin{aligned} \S_3 &= \{0\}, \\ \S_2 &= \{100, 110\}, \\ \S_1 &= \{101, 111\} \end{aligned} \tag{B.8}$$

Cada acción disponible en el sistema de simulación pertenece a uno de los conjuntos $\S_3$, $\S_2$, $\S_1$, cada uno correspondiente a una estrategia, 3, 2 y 1 respectivamente. La expresión B.9, mediante la definición de $\hat{\varkappa}_s : V \times \mathbb{N} \to \mathbb{N}$ para cada estrategia s, permite identificar como $\hat{\varkappa}_s(i,t)$ al valor monetario más alto que el agente i transfiere para adquirir un recurso, en la iteración t, mediante la estrategia s.

$$\begin{aligned} &\hat{\varkappa}_3(i,t) \neq 0 \Leftrightarrow \exists\, m : \mathbb{N} \mid \\ &\qquad m = \max_{\forall\, e' : \widetilde{E}} \{v_{i'}(t) \mid j' = i \wedge t' = t \wedge a' \in \S_3\} \wedge \\ &\hat{\varkappa}_3(i,t) = m \\ \\ &\hat{\varkappa}_2(i,t) \neq 0 \Leftrightarrow \exists\, m : \mathbb{N} \mid \\ &\qquad m = \max_{\forall\, e' : \widetilde{E}} \{\dot{v}_{i'}(t) \mid j' = i \wedge t' = t \wedge a' \in \S_2\} \wedge \\ &\hat{\varkappa}_2(i,t) = m \\ \\ &\hat{\varkappa}_1(i,t) \neq 0 \Leftrightarrow \exists\, m : \mathbb{N} \mid \\ &\qquad m = \max_{\forall\, e' : \widetilde{E}} \{\mathring{v}_{i'}(t) \mid j' = i \wedge t' = t \wedge a' \in \S_1\} \wedge \\ &\hat{\varkappa}_1(i,t) = m \end{aligned} \tag{B.9}$$

Según la expresión B.3, los componentes j', t' y a' existen en el esquema $\widetilde{E}$. $\forall\, i : V;\, t : \mathbb{N}$.

La expresión B.10 permite identificar el volumen de ventas esperado por el agente i, i.e., la cantidad de unidades que el agente i espera transferir. La expresión, (1) mediante la definición de $\mathring{\gamma}_i : \mathbb{N} \to \mathbb{N}$, permite identificar como $\mathring{\gamma}_i(t)$ al volumen obtenido por cada agente i, mediante la estrategia 1, en cada iteración t; (2) mediante la definición de $\dot{\gamma}_i : \mathbb{N} \to \mathbb{N}$, permite identificar como $\dot{\gamma}_i(t)$ al volumen obtenido por cada agente i, mediante la estrategia 2, en cada iteración t; y (3) mediante la definición de $\gamma_i : \mathbb{N} \to \mathbb{N}$, permite identificar como $\gamma_i(t)$ al volumen obtenido por cada agente i, mediante la estrategia 3, en cada iteración t. La cantidad de unidades equivale a la cantidad de agentes que, en la iteración t, están dispuestos a adquirir un recurso que el agente i está dispuesto a transferir.

$$
\begin{aligned}
\forall\, i,j : V;\ t : \mathbb{N};\ w : W \bullet \exists\, u_w, \dot{u}_w, \mathring{u}_w : \mathbb{N} \mid \\
u_w &= \#\{j \mid \Lambda(j,t) \geq v_i(t) \wedge \nu_w(i) > 0 \wedge \nu_w(j) < 0\} \wedge \\
\dot{u}_w &= \#\{j \mid \Lambda(j,t) \geq \dot{v}_i(t) \wedge \nu_w(i) > 0 \wedge \nu_w(j) < 0\} \wedge \\
\mathring{u}_w &= \#\{j \mid \Lambda(j,t) \geq \mathring{v}_i(t) \wedge \nu_w(i) > 0 \wedge \nu_w(j) < 0\} \wedge \\
\gamma_i(t) &= u_1 + u_2 + u_3 \wedge \\
\dot{\gamma}_i(t) &= \dot{u}_1 + \dot{u}_2 + \dot{u}_3 \wedge \\
\mathring{\gamma}_i(t) &= \mathring{u}_1 + \mathring{u}_2 + \mathring{u}_3
\end{aligned}
\tag{B.10}
$$

La expresión B.11, mediante la definición de $\Lambda : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, permite identificar como $\Lambda(i,t)$ a la inversión intrínseca para la utilidad neta más alta que el agente i pueda obtener en la iteración t.

$$
\begin{aligned}
\Lambda(i,t) &= \psi_i(t) \wedge \Delta_i(t) \geq \dot{\Delta}_i(t) \wedge \Delta_i(t) \geq \mathring{\Delta}_i(t) \vee \\
\Lambda(i,t) &= \dot{\psi}_i(t) \wedge \dot{\Delta}_i(t) \geq \Delta_i(t) \wedge \dot{\Delta}_i(t) \geq \mathring{\Delta}_i(t) \vee \\
\Lambda(i,t) &= \mathring{\psi}_i(t) \wedge \mathring{\Delta}_i(t) \geq \Delta_i(t) \wedge \mathring{\Delta}_i(t) \geq \dot{\Delta}_i(t)
\end{aligned}
\tag{B.11}
$$

$$\forall\, i : V;\ t : \mathbb{N}.$$

La expresión B.12, mediante la definición de $\check{\varkappa}_s : V \times \mathbb{N} \to \mathbb{N}$ para cada estrategia s, describe el cálculo de la utilidad bruta esperada por el agente i en la iteración t, la utilidad es calculada según la heurística B.3.1. Cada función $\check{\varkappa}_s$ describe el cálculo de la utilidad al implementar la estrategia s.

$$
\begin{aligned}
&\exists\, i : V;\ t,u : \mathbb{N} \mid \\
&\qquad u = \#\{e' : \widetilde{E} \mid i' = i \wedge t' = t \wedge a' \in \S_3\} \bullet \\
&\check{\varkappa}_3(i,t) = \begin{cases} v_i(t) - 1 & u < \gamma_i(0) \\ v_i(t) & u \geq \gamma_i(0) \end{cases} \\
&\exists\, i : V;\ t,u : \mathbb{N} \mid \\
&\qquad u = \#\{e' : \widetilde{E} \mid i' = i \wedge t' = t \wedge a' \in \S_2\} \bullet \\
&\check{\varkappa}_2(i,t) = \begin{cases} \dot{v}_i(t) - 1 & u < \dot{\gamma}_i(0) \\ \dot{v}_i(t) & u \geq \dot{\gamma}_i(0) \end{cases} \\
&\exists\, i : V;\ t,u : \mathbb{N} \mid \\
&\qquad u = \#\{e' : \widetilde{E} \mid i' = i \wedge t' = t \wedge a' \in \S_1\} \bullet \\
&\check{\varkappa}_1(i,t) = \begin{cases} \mathring{v}_i(t) - 1 & u < \mathring{\gamma}_i(0) \\ \mathring{v}_i(t) & u \geq \mathring{\gamma}_i(0) \end{cases}
\end{aligned}
\tag{B.12}
$$

Según la expresión B.3, los componentes i', t' y a' existen en el esquema $\widetilde{E}$.

C

Código fuente (Golang) del sistema de simulación

```
1   package main; import ("os"; "sim/ca")
2
3   const OBS = 16
4   var serie = "1"
5
6   func main() {
7     serie = os.Args[1]
8     ca.REWARDENABLED = serie == "1"
9     var treats = getTreatments()
10    var i, j int
11    for i = 0; i < len(treats); i++ {
12      for j = 0; j < OBS; j++ {
13        run(treats[i], i, j)
14      }
15    }
16  }
```

Figura C.1: Rutina principal del sistema de simulación. La constante OBS almacena el número de observaciones por tratamiento. La variable *serie* indica la serie de experimentos para la que la simulación generará los datos.

```
1   package main
2
3   import ("math/rand"; "time"; "sim/ca")
4
5   // Cantidad de agentes en la simulacion
6   const N = 512
7   // Cantidad de iteraciones
8   const T = 256
9
10  func run(treat []int, trid, obid int) {
11    var grid = ca.NewGrid(N)
12    // Inicializacion del generador de numeros pseudoaleat.
13    rand.Seed(time.Now().UnixNano())
14    // Inicializacion de la matriz de agentes
15    var i, j, k, t int
16    k = 0
17    for j = range treat {
18      for i = 0; i < treat[j]; i++ {
19        grid.Add(ca.NewAgent(j), k)
20        k++
21      }
22    }
23
24    grid.Shuffle()
25    for i = 0; i < N; i++ { grid[i].Prepare(); }
26    // Busqueda y transferencia de recursos
27    var next = make([][]int, N)
28    var r, g, b int
29    // En cada iteracion
30    for t = 0; t < T; t++ {
31      // Cada agente i analiza a cada agente k
32      for j = 0; j < N; j++ {
33        // El agente i es elegido aleatoriamente
34        for _, i = range grid.Shuffled() {
35          // El arreglo "next" es inicializado si es nulo
36          if j == 0 { next[i] = grid.Shuffled(); }
37          // El agente i analiza al agente k = next[i][j]
38          grid[i].Match(next[i][j], j == 0)
39          if j == N-1 {
40            r = grid[i].RSupplier()
41            g = grid[i].GSupplier()
42            b = grid[i].BSupplier()
43
44            grid[i].Request(ca.R)
45            grid[i].Request(ca.G)
46            grid[i].Request(ca.B)
47
48            save(trid, obid, t, grid, i, r, g, b)
49          }
50        }
51      }
52      // Cada agente i ajusta su criterio de decision
53      for i = 0; i < N; i++ { grid[i].Learn(); }
54    }
55  }
```

Figura C.2: Rutina que produce una simulación, correspondiente a un tratamiento y una observación. El método *Prepare* calcula el valor que, según la expresión B.10, corresponde a $\gamma_i(0)$, $\dot{\gamma}_i(0)$ y $\hat{\dot{\gamma}}_i(0)$ para el agente i. Los métodos *RSupplier*, *GSupplier* y *BSupplier* retornan el identificador del proveedor para los tipos de recurso R, G y B respectivamente, para cualquiera de estos métodos, si el proveedor no está definido entonces el método devuelve -1. R, G y B representan los tres tipos de recurso disponibles. La rutina *save* registra el detalle de cada transacción, en cada iteración y por cada agente. El método *Learn* implementa el esquema B.1.

```
1   package ca
2
3   import ("math/rand"; "time")
4
5   // Matriz de agentes
6   type Grid []*Agent
7
8   /* Metodo constructor, inicializa la matriz de agentes,
9    * con capacidad para n agentes */
10  func NewGrid(n int) (me Grid) {
11    me = make(Grid, n)
12    return
13  }
14
15  /* Metodo que agrega la referencia de un agente a la
16   * matriz de agentes, en una posicion determinada */
17  func (me Grid) Add(agent *Agent, i int) {
18    me[i] = agent
19    agent.grid = me
20  }
21
22  /* Metodo que baraja la matriz e inicializa la oferta y
23   * la demanda de cada agente */
24  func (me Grid) Shuffle() {
25    // Inicializacion del generador de numeros pseudoaleat.
26    rand.Seed(time.Now().UnixNano())
27
28    rand.Shuffle(len(me), func(i, j int) {
29      me[i], me[j] = me[j], me[i]
30
31      me[i].SetSource(j)
32      me[j].SetSource(i)
33
34      me[i].SetTarget(i)
35      me[j].SetTarget(j)
36    })
37  }
38
39  /* Metodo que genera, baraja y retorna la secuencia de
40   * enteros entre 0 y N - 1 */
41  func (me Grid) Shuffled() []int {
42    // Inicializacion del generador de numeros pseudoaleat.
43    rand.Seed(time.Now().UnixNano())
44
45    var seq = make([]int, len(me))
46    var i = 0
47    for i = range seq {
48      seq[i] = i
49    }
50
51    rand.Shuffle(len(seq), func(i, j int) {
52      seq[i], seq[j] = seq[j], seq[i]
53    })
54
55    return seq
56  }
```

Figura C.3: "Clase" que facilita la manipulación de la matriz de agentes.

```
1  package ca
2
3  /* Interruptor que (des)habilita la oferta de la
4   * remuneracion */
5  var REWARDENABLED = false
6
7  type Agent struct {
8    ID int
9
10   V3, W3, V2, W2, V1, W1, R3, R2, R1 int
11
12   source, target *Color
13   rSupplier, gSupplier, bSupplier *Supplier
14
15   grid    Grid
16   history History
17 }
```

Figura C.4: Estructura de cada agente i, los atributos V3, W3, V2, W2, V1, W1, R3, R2, R1 corresponden a los componentes $v_i(t)$, $\psi_i(t)$, $\dot{v}_i(t)$, $\dot{\psi}_i(t)$, $\hat{v}_i(t)$, $\hat{\psi}_i(t)$, $\gamma_i(t)$, $\dot{\gamma}_i(t)$, $\hat{\gamma}_i(t)$, respectivamente, en la iteración t. Las funciones están definidas en la sección B.3.

```
1  package ca
2
3  func (me *Agent) SetSource(rgb int) {
4    var rg = rgb % 64
5    me.source.B = (rgb - rg) / 64
6    me.source.R = rg % 8
7    me.source.G = (rg - me.source.R) / 8
8  }
9
10 func (me *Agent) SetTarget(rgb int) {
11   me.ID = rgb
12   var rg = rgb % 64
13   me.target.B = (rgb - rg) / 64
14   me.target.R = rg % 8
15   me.target.G = (rg - me.target.R) / 8
16 }
```

Figura C.5: Métodos que inicializan la oferta y la demanda, respectivamente, de cada agente. R, G y B representan los tres tipos de recurso disponibles.

```
1   package ca
2
3   func (me *Agent) Match(j int, reset bool) {
4     var he = me.grid[j]
5     var value, action = me.free(he)
6     if reset {
7       me.rSupplier = nil
8       me.gSupplier = nil
9       me.bSupplier = nil
10    }
11
12    if action == -1 {
13      return
14    }
15
16    var supplier = NewSupplier(he, value, action)
17    if me.Has(R) < 0 && he.Has(R) > 0 {
18      if me.rSupplier != nil {
19        if value > me.rSupplier.value {
20          me.rSupplier = supplier
21        }
22      } else {
23        me.rSupplier = supplier
24      }
25    }
26
27    if me.Has(G) < 0 && he.Has(G) > 0 {
28      if me.gSupplier != nil {
29        if value > me.gSupplier.value {
30          me.gSupplier = supplier
31        }
32      } else {
33        me.gSupplier = supplier
34      }
35    }
36
37    if me.Has(B) < 0 && he.Has(B) > 0 {
38      if me.bSupplier != nil {
39        if value > me.bSupplier.value {
40          me.bSupplier = supplier
41        }
42      } else {
43        me.bSupplier = supplier
44      }
45    }
46  }
```

Figura C.6: Método que evalúa al agente j, permite encontrar al mejor proveedor de cada tipo de recurso. El método *free* implementa la función z, descrita en la expresión B.4. El método *Has* implementa las funciones v_1, v_2 y v_3, cada una descrita en la expresión B.1. R, G y B representan los tres tipos de recurso disponibles.

```
1   package ca
2
3   import ("math/rand"; "time")
4
5   /* Maximo valor inicial para cualquiera de los componentes
6    * del criterio de decision */
7   const MAX = 256
8
9   func NewAgent(class int) (me *Agent) {
10    me = &Agent{
11      rSupplier, gSupplier, bSupplier = nil, nil, nil
12
13      source: NewColor(),
14      target: NewColor(),
15
16      history: NewHistory(),
17    }
18
19    // Inicializacion del generador de numeros pseudoaleat.
20    rand.Seed(time.Now().UnixNano())
21
22    var d0, d1, d2 int
23    for {
24      me.V3 = rand.Intn(MAX)
25      me.W3 = rand.Intn(MAX)
26      me.V2 = rand.Intn(MAX)
27      me.W2 = rand.Intn(MAX)
28      me.V1 = rand.Intn(MAX)
29      me.W1 = rand.Intn(MAX)
30
31      d0 = me.GetDelta0()
32      d1 = me.GetDelta1()
33      d2 = me.GetDelta2()
34      if
35        (me.V3 > 0 && me.V2 > 0 && me.V1 > 0) &&
36        (me.W3 > 0 && me.W2 > 0 && me.W1 > 0) &&
37        (d0 > 0 && d1 > 0 && d2 > 0) && (
38
39        (class == 0) &&
40        (d1 - d0 > -MAX && d1 - d0 <= 0 ) &&
41        (d2 - d1 > -MAX && d2 - d1 <= 0 ) ||
42
43        (class == 1) &&
44        (d1 - d0 > -MAX && d1 - d0 <=  0) &&
45        (d2 - d1 >=    0 && d2 - d1 < MAX) ||
46
47        (class == 2) &&
48        (d1 - d0 >=    0 && d1 - d0 < MAX) &&
49        (d2 - d1 > -MAX && d2 - d1 <=  0) ||
50
51        (class == 3) &&
52        (d1 - d0 >=    0 && d1 - d0 < MAX) &&
53        (d2 - d1 >=    0 && d2 - d1 < MAX)) {
54
55        return
56      }
57    }
58  }
```

Figura C.7: Método constructor, genera un nuevo agente *i* en función de su clase. Los métodos *GetDelta0*, *GetDelta1* y *GetDelta2* permiten obtener el valor que, según la expresión B.2, corresponde a $\Delta_i(t)$, $\dot{\Delta}_i(t)$ y $\mathring{\Delta}_i(t)$, respectivamente, en la iteración *t*. Los atributos V3, W3, V2, W2, V1, W1 corresponden a los componentes $v_i(t)$, $\psi_i(t)$, $\dot{v}_i(t)$, $\dot{\psi}_i(t)$, $\mathring{v}_i(t)$, $\mathring{\psi}_i(t)$ para el agente *i* en la iteración *t*, respectivamente. Las funciones están definidas en la sección B.3.

```
1   package ca
2
3   func (me *Agent) Request(rt rune) bool {
4     if rt == R && me.rSupplier == nil ||
5        rt == G && me.gSupplier == nil ||
6        rt == B && me.bSupplier == nil {
7        return false
8     }
9
10    var he *Agent
11    var ok, value = false, 0
12    switch rt {
13    case R:
14      he = me.grid[me.rSupplier.Id()]
15      if ok, value = he.Response(rt, me.rSupplier.Action());
16      ok {
17        me.history.logreq(rt, me.rSupplier.Action(), value)
18        me.rSupplier = nil
19        return true
20      }
21    case G:
22      he = me.grid[me.gSupplier.Id()]
23      if ok, value = he.Response(rt, me.gSupplier.Action());
24      ok {
25        me.history.logreq(rt, me.gSupplier.Action(), value)
26        me.gSupplier = nil
27        return true
28      }
29    case B:
30      he = me.grid[me.bSupplier.Id()]
31      if ok, value = he.Response(rt, me.bSupplier.Action());
32      ok {
33        me.history.logreq(rt, me.bSupplier.Action(), value)
34        me.bSupplier = nil
35        return true
36      }
37    }
38
39    return false
40  }
```

Figura C.8: Método que genera una petición de transacción de un recurso de tipo rt. R, G y B representan los tres tipos de recurso disponibles. El método *logreq* registra el detalle de cada petición exitosa.

```
1   package ca
2
3   func (me *Agent) Response(rt rune, action int) (bool, int)
4   {
5     var delta, value = 0, 0
6     switch action {
7       case 111:
8         delta = me.GetDelta2() - me.GetReward()
9         value = me.V1
10      case 101:
11        delta = me.GetDelta2() - me.GetReward()
12        value = me.V1
13      case 110:
14        delta = me.GetDelta1()
15        value = me.V2
16      case 100:
17        delta = me.GetDelta1()
18        value = me.V2
19      case 0:
20        delta = me.GetDelta0()
21        value = me.V3
22    }
23
24    if delta > 0 {
25      me.history.logres(rt, action, delta)
26      return true, value
27    }
28
29    return false, value
30  }
```

Figura C.9: Método que genera una respuesta a una petición de transacción de un recurso de tipo rt. Los métodos *GetDelta0*, *GetDelta1* y *GetDelta2* permiten obtener el valor que, según la expresión B.2, corresponde a $\Delta_i(t)$, $\dot{\Delta}_i(t)$ y $\mathring{\Delta}_i(t)$, respectivamente, para el agente i en la iteración t. El método *GetReward* implementa la función $\widetilde{\nabla}$ o a la función $\widetilde{\nabla}'$, descritas en la expresión B.5, según corresponda. Los atributos V3, V2, V1 corresponden a los componentes $v_i(t)$, $\dot{v}_i(t)$, $\hat{v}_i(t)$, respectivamente, del criterio de decisión del agente i en la iteración t, las funciones están definidas en la sección B.3. El método *logres* registra el detalle de cada respuesta exitosa.

```
1   package ca
2
3   func (me *Agent) Has(rt rune) int {
4     switch rt {
5     case R:
6       return me.source.R - me.target.R
7     case G:
8       return me.source.G - me.target.G
9     default:
10      return me.source.B - me.target.B
11    }
12  }
```

Figura C.10: Método que retorna la oferta o demanda del agente, en cantidad de unidades, por un recurso de tipo rt. El método *Has* implementa las funciones v_1, v_2 y v_3, cada una descrita en la expresión B.1. R, G y B representan los tres tipos de recurso disponibles.

```
1   package main
2
3   func getTreatments() [][]int {
4     return [][]int{
5       {8, 24, 96, 384}, {8, 24, 384, 96}, {8, 96, 24, 384},
6       {8, 96, 384, 24}, {8, 384, 24, 96}, {8, 384, 96, 24},
7       {24, 8, 96, 384}, {24, 8, 384, 96}, {24, 96, 8, 384},
8       {24, 96, 384, 8}, {24, 384, 8, 96}, {24, 384, 96, 8},
9       {96, 8, 24, 384}, {96, 8, 384, 24}, {96, 24, 8, 384},
10      {96, 24, 384, 8}, {96, 384, 8, 24}, {96, 384, 24, 8},
11      {384, 8, 24, 96}, {384, 8, 96, 24}, {384, 24, 8, 96},
12      {384, 24, 96, 8}, {384, 96, 8, 24}, {384, 96, 24, 8},
13    }
14  }
```

Figura C.11: Rutina que genera y retorna un arreglo de vectores, uno por cada tratamiento, cada vector contiene cuatro enteros, uno por cada variable en el diseño del método experimental.

D

Conjuntos de datos (JSON)

Cuadro D.1: Serie experimental: Variable de respuesta para cada tratamiento y observación en la última iteración.

{1: [0.56, 0.8601, 0.8244, 0.8681, 0.8937, 0, 0.985, 0, 0.5462, 0, 0, 0, 0.8689, 0.6963, 0, 0.5605], 2: [0, 0, 0, 0.927, 0.8755, 0, 0.598, 0, 0.622, 0.8619, 0, 0.6656, 0.9103, 0.8267, 0, 0], 3: [0, 0, 0.5764, 0.8114, 0.8293, 0.9336, 0, 0.5966, 0.9797, 0, 0.7586, 0.6325, 0, 0, 0, 0], 4: [0, 0.7941, 0, 0.8459, 0, 0.8298, 0.2552, 0, 0, 1, 0, 0.6997, 0, 0.9328, 0, 0.8819], 5: [0.6417, 0, 0.7004, 0.432, 0.692, 0.6908, 0, 0.25, 0.583, 0.4302, 0, 0, 0.4496, 0, 0, 0], 6: [0, 0, 1, 0.9012, 0.957, 0.3684, 0.5085, 0.6234, 0.8555, 0.825, 0.7534, 0, 0.9488, 0.557, 0, 0.6296], 7: [0.8559, 0.8114, 0.7621, 0.5714, 0.6718, 0.2482, 0.9779, 0, 0, 0, 0.7296, 0.7824, 0, 0.8731, 0, 0], 8: [0, 0.92, 0, 0.5288, 0.9315, 0, 0, 0, 0.338, 0, 0.9531, 0.7893, 0, 0.79, 0.8508, 0.645], 9: [0, 0, 0.7094, 0, 0, 0, 0.8664, 0, 0.7342, 0.7737, 0.7992, 0, 0, 0, 0.6587, 0.4578], 10: [1, 0.9696, 0.7468, 0.6195, 0, 0, 0.5993, 1, 0, 0.8333, 0.6162, 0.9389, 0.6818, 0.449, 0.4615, 0.8826], 11: [0, 0, 0, 0, 0.6677, 0, 0.7513, 0.6698, 0, 0, 0, 0.7949, 0, 0.3013, 1, 0], 12: [0.7406, 0.465, 0.792, 0.7393, 0.8205, 0.36, 0.4739, 0.7039, 0.9835, 0.7108, 0, 0.0883, 0, 0.9196, 0, 0], 13: [0.4088, 0, 0, 0.3525, 0.8714, 0, 0, 0, 0, 0, 0.9017, 0.8561, 0.7184, 0.843, 0.1429, 0], 14: [0.7417, 0, 0, 0.7786, 0, 0, 1, 0, 0, 0.5858, 0, 0, 0, 0.473, 0, 0.8392], 15: [0.2295, 0.1532, 0.5769, 0.9414, 0, 0, 0.9103, 0.3976, 0.9153, 0, 0, 0.8065, 0.8054, 0.6085, 0.7713, 0.9664], 16: [0, 0.4641, 0.6638, 0.9785, 0, 0.6685, 0, 0.4201, 0, 0.9875, 0, 0, 0.7231, 0, 0, 0], 17: [0, 0, 0.2267, 0, 0.8685, 0.6769, 0.7828, 0, 0, 0, 0.5642, 0, 1, 0, 0, 0], 18: [0, 0, 0, 0.768, 0.254, 0.4006, 0.8979, 0, 0, 0, 0.7276, 0.433, 0, 0, 0.3108, 0], 19: [0, 0.8116, 0.5657, 0, 0, 0, 0.8085, 0, 0.7442, 0.0306, 0.8108, 0.8078, 0, 0.8882, 0.9702, 0], 20: [0.6186, 0.995, 0.8, 0, 0, 0.3866, 0, 0, 0, 0, 0, 0.4006, 0.7098, 0.4828, 0, 0.7479], 21: [0.3237, 0.4229, 0, 0.6085, 0, 0, 0.3943, 0, 0.8718, 0, 0.6964, 0.3829, 0.6189, 0, 1, 0], 22: [0.8492, 0.5167, 0, 0.638, 0, 0.1627, 0, 0, 0, 0, 0, 0, 0.2149, 0, 0, 0.4919], 23: [0.4613, 0.1532, 0.6185, 0.0929, 0.7111, 0.8065, 0.8375, 0.8357, 0.4269, 0, 0.3153, 0.4784, 0.7114, 0.3673, 0.8078, 0.6804], 24: [0, 0, 0.8522, 0.7074, 0, 0.5395, 0, 0.1107, 0.7782, 0, 0.776, 0, 0.7797, 0, 0.3636, 0.4532]}

Cuadro D.2: Serie de control: Variable de respuesta para cada tratamiento y observación en la última iteración.

{1: [0.6987, 0, 0.2714, 0.757, 0, 0, 0.7188, 0, 0, 0.6932, 0.9494, 0.4, 0, 0, 0.2326, 0.8223], 2: [0.9883, 0, 0.7839, 0.3991, 0.7635, 0.7436, 0, 0.6743, 0.9683, 0, 0.3882, 0.9554, 0, 1, 0.9913, 0.7285], 3: [0, 0, 0.645, 0.7219, 0, 0.9786, 0.7977, 0.8398, 0.3119, 0.7478, 0.3668, 0.9259, 0, 0, 0.959, 0], 4: [0, 0.589, 0.6386, 0.3568, 1, 0, 0.5115, 0.7333, 0.9399, 0, 0.7189, 1, 0, 0.4762, 0.7042, 0], 5: [0, 0, 0, 0.6654, 0, 0, 0, 0.5492, 0, 0.6394, 0, 0.8009, 0.8168, 0, 0.2143, 0], 6: [0, 0, 0, 0, 0, 1, 0, 0.4786, 0, 0, 0.6519, 0, 0, 0.6732, 0, 0], 7: [0.705, 0.2667, 0.6016, 0.8158, 0.9176, 0, 0, 0.7755, 0, 0, 0.9348, 0.8566, 0.5804, 0.8857, 0.9912, 0], 8: [0, 1, 0, 0, 0.7573, 0.0664, 0, 0.932, 0.705, 0, 0, 0.3726, 0, 0, 0.3443, 0], 9: [0, 0.8147, 0.3624, 0, 0, 0.7152, 0.9375, 0, 0.317, 0, 0.6489, 0, 0.6875, 0.9338, 0.9796, 0], 10: [0, 0.7137, 0.7928, 0.2703, 0.8988, 0, 0.5637, 0, 0.8198, 0.7262, 0.6952, 0.6667, 0.8885, 0, 0, 0.5714], 11: [0, 0.5966, 0.8168, 0, 0.8629, 0, 0.6275, 0.4305, 0, 0, 0, 0.7115, 0, 0.8844, 0, 0.8454], 12: [0, 0, 0, 0.8065, 0.766, 0, 0, 1, 0.6978, 0.7529, 0, 0.6553, 0.6172, 0, 0, 0.7766], 13: [0, 0, 0, 0.8031, 0, 0, 0.6111, 0, 0.8302, 0, 0, 0.5305, 0, 0.906, 0, 0.4683], 14: [0.5141, 0.6371, 0.7088, 0, 0.8715, 0, 0, 0.793, 0, 0, 0.935, 0.6213, 0.9483, 0.4792, 0, 0.8388], 15: [0, 0.844, 0.6907, 0, 0, 0.8526, 0, 0.754, 0.6571, 0.0556, 0, 0.8967, 0, 0.3533, 0, 0], 16: [0.5661, 0, 0.8502, 0, 0.8447, 0, 0.7895, 0.2589, 0.7819, 0.5699, 0, 0.931, 0.6406, 0, 0, 0.6154], 17: [0.3232, 0, 0, 0, 0.2395, 0, 0, 0, 0, 0.9486, 0, 0, 0, 0, 0, 0], 18: [0, 0.6762, 0, 0.7326, 0.5174, 0.757, 0.6, 0, 0, 0, 0, 1, 0, 0.5905, 0.5468, 0], 19: [0.9419, 0.6923, 0, 0.6496, 0.3983, 0.9, 0, 0, 0, 0.4327, 0.5304, 0, 0, 0, 0, 0.2698], 20: [0.5114, 0.8084, 0, 0, 0, 0.4481, 0, 0.6728, 0.9, 0.4477, 0, 0, 0, 0.8739, 0.6656, 0.3333], 21: [0, 0, 0.8056, 0.8801, 0, 0.5, 0.8462, 0, 0, 0.9163, 0, 0.5838, 0, 0.5124, 0, 0.7148], 22: [0.4985, 0.7277, 0.4901, 0.6652, 0.5336, 0.332, 0, 0.375, 0, 0.3803, 0.6098, 0, 0, 0.4873, 0.3243, 0], 23: [0, 0.3592, 0, 0.7492, 0, 0.5352, 0.77, 0.8393, 0, 0, 0.7299, 0.6961, 0.569, 0.656, 0, 0], 24: [0, 0, 0, 1, 0.5803, 0, 0, 0.6827, 0.5, 0.7279, 0.4439, 0.4978, 0.754, 0, 0, 0.6593]}

E

Semántica

Cuadro E.1: Modelo circular de red de suministro, mecanismo de incentivos, y cripto-mecanismo de incentivos.

$\mathbb{G} = (V, E)$	Modelo en forma de multigrafo dirigido, del historial de transacciones de la cadena de bloques logística, está definido en la sección 4.2, V corresponde al conjunto de nodos y E al conjunto de aristas. Cada nodo representa a un agente y cada arista a una transacción.
$E \triangleq [i; j; k; \omega; t; \sigma]$	Representación de la estructura de cualquier transacción en $\mathbb{G}$, está definida en la expresión 4.1, i identifica al agente proveedor, j al agente consumidor, k al recurso, ω al monto transferido de j a i, t a la marca del tiempo en el que la transacción es efectuada, y σ a una secuencia compuesta por un identificador por cada transacción en la secuencia.
$\sim x$	Número natural que identifica al objeto x, está declarado en el esquema 4.1.
$L(4.2)$	Lenguaje del autómata 4.2, está definido en la sección 4.3.
$G = (N, A, \theta, R)$	Modelo de juego en forma normal, está definido en la sección 5.1, un juego corresponde al ciclo de vida de cualquier recurso. $N = \{1, \ldots, n\}$ es el conjunto de los n agentes en la población, A_i es un conjunto finito de acciones, de las acciones disponibles para el agente i, $A = A_1 \times \ldots \times A_n$, r_i es la función que permite obtener la utilidad para cualquier agente i, $R = (r_1, \ldots, r_n)$, θ es la función que permite obtener el perfil de cualquier agente, y $\Theta = \{1, \ldots, 6\}$. Si $\theta(i) = 1$ entonces el agente i es un proveedor de materia prima, si $\theta(i) = 2$ entonces el agente i es un productor, si $\theta(i) = 3$ entonces el agente i es un proveedor de servicios, si $\theta(i) = 4$ entonces el agente i es un consumidor, si $\theta(i) = 5$ entonces el agente i es un agente de aplicación, si $\theta(i) = 6$ entonces el agente i es un recurso inteligente.

$\check{v}_i(a)$	Utilidad intrínseca correspondiente al agente i, en función de la configuración a, está definida en la sección 5.1.
$\check{w}_i(a)$	Utilidad extrínseca correspondiente al agente i, en función de la configuración a, está definida en la sección 5.1.
$\hat{v}_i(a)$	Inversión intrínseca correspondiente al agente i, en función de la configuración a, está definida en la sección 5.1.
$\hat{w}_i(a)$	Inversión extrínseca correspondiente al agente i, en función de la configuración a, está definida en la sección 5.1.
$v_i, v_i(t)$	Utilidad intrínseca al aplicar la estrategia 3, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\psi_i, \psi_i(t)$	Inversión intrínseca al aplicar la estrategia 3, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\dot{v}_i, \dot{v}_i(t)$	Utilidad intrínseca al aplicar la estrategia 2, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\dot{\psi}_i, \dot{\psi}_i(t)$	Inversión intrínseca al aplicar la estrategia 2, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\mathring{v}_i, \mathring{v}_i(t)$	Utilidad intrínseca al aplicar la estrategia 1, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\mathring{\psi}_i, \mathring{\psi}_i(t)$	Inversión intrínseca al aplicar la estrategia 1, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
φ	En la expresión 5.5, es el valor monetario del recurso.
σ	En la expresión 5.5, es la trayectoria del recurso.
$\ell_{-4}(\sigma)$	En la expresión 5.5, es la cantidad de agentes consumidores que componen la cadena de suministro.
$\ell_4(\sigma)$	En la expresión 5.5, es la cantidad de agentes no consumidores componen la cadena de suministro.
$\check{h}_4$	En la expresión 5.5, es el *ratio* relativo al valor monetario del recurso, corresponde a la remuneración para la cadena externa.
$\check{h}_{-4}$	En la expresión 5.5, es el *ratio* relativo al valor monetario del recurso, corresponde a la remuneración para la cadena interna.
$\hat{h}_4(i)$	*Ratio* relativo al valor monetario del recurso, corresponde al monto que el agente i invierte para habilitar la transferencia de la remuneración a la cadena externa, está definido en el cuadro 5.4.
$\hat{h}_{-4}(i)$	*Ratio* relativo al valor monetario del recurso, corresponde al monto que el agente i invierte para habilitar la transferencia de la remuneración a la cadena interna, está definido en el cuadro 5.4.
$h_0(i)$	Valor, interpretado como valor monetario, de las herramientas de tokenización, para el agente i. Está definido en el cuadro 5.4.
$P \veebar Q$	P *xor* Q, está definido en la sección 5.3.
$a \approx a'$	Las acciones a y a' se refieren a recursos con funciones idénticas o en su defecto no se refieren a un recurso. Está definido en la sección 5.3.
$\mathring{\Delta}_i, \mathring{\Delta}_i(t)$	Utilidad intrínseca neta obtenida con la estrategia 1, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\dot{\Delta}_i, \dot{\Delta}_i(t)$	Utilidad intrínseca neta obtenida con la estrategia 2, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.
$\Delta_i, \Delta_i(t)$	Utilidad intrínseca neta obtenida con la estrategia 3, correspondiente al agente i (y la iteración t), está definida en la sección 5.1.2, y redefinida en la sección B.3.

$\vartheta(i,t)$	Saldo del agente i en el tiempo t, está definido en la sección 7.1.2.
$K(i,t)$	Conjunto de recursos que posee el agente i en el tiempo t, está definido en la sección 7.1.2.
S_i	Conjunto de transacciones unitarias que el agente i ha firmado y que han sido certificadas, está definido en la sección 7.1.2.
$M = (Q,\Theta,\Sigma,\delta,q_0,F,\nabla)$	ε-NFA extendido que describe un modelo de negocio, está definido en la sección 7.1.3. Q es el conjunto finito de estados, Θ es el conjunto finito de perfiles, Σ es el conjunto finito de símbolos de entrada, δ es la función de transición, q_0 es el estado inicial, F es el conjunto de estados finales, y ∇ es la función que permite obtener la remuneración para cualquier agente, según el perfil del agente y la trayectoria del recurso.
$C \triangleq [M,f]$	Representación de la estructura de cualquier recurso inteligente, definida en la expresión 7.6. M corresponde a los componentes de un ε-NFA extendido que describe el modelo de negocio del que proviene el recurso, f es una función que permite interpretar a cualquier posible transacción, correspondiente a la transferencia del recurso, como un símbolo de entrada de M.

Cuadro E.2: Análisis estadístico del efecto del mecanismo de incentivos.

χ_0	En la sección 6.1, es la cardinalidad del conjunto de agentes de clase 0.
χ_1	En la sección 6.1, es la cardinalidad del conjunto de agentes de clase 1.
χ_2	En la sección 6.1, es la cardinalidad del conjunto de agentes de clase 2.
χ_3	En la sección 6.1, es la cardinalidad del conjunto de agentes de clase 3.
$y_\imath(\jmath)$	En la sección 6.1, es el *ratio* entre la cantidad de transacciones circulares y la cantidad total de transacciones, variable de respuesta para el tratamiento $\imath$ y la observación $\jmath$.
$\mu_\imath$	En la sección 6.1, es la media de la variable de respuesta $y_\imath$, para el tratamiento $\imath$.
H_0	Hipótesis nula en la serie experimental, establecida en la expresión H_0.
H_1	Hipótesis alternativa en la serie experimental, establecida en la expresión H_1.
H_0'	En la sección 6.1, es la hipótesis nula en la serie de control.
H_1'	En la sección 6.1, es la hipótesis alternativa en la serie de control.
p	En la sección 6.3, es el nivel de significancia para evaluar la hipótesis nula en la serie experimental.
p'	En la sección 6.3, es el nivel de significancia para evaluar la hipótesis nula en la serie de control.
$W = \{1,2,3\}$	Conjunto de los tipos de recurso en el sistema de simulación, está definido en la sección B.
$\widetilde{A}$	Conjunto de acciones disponibles en el sistema de simulación, está definido en la sección B.

$\S_3 = \{0\}$	Conjunto de acciones disponibles en el sistema de simulación, correspondiente a la estrategia 3, está definido en la sección B.2.
$\S_2 = \{1,3\}$	Conjunto de acciones disponibles en el sistema de simulación, correspondiente a la estrategia 2, está definido en la sección B.2.
$\S_1 = \{5,7\}$	Conjunto de acciones disponibles en el sistema de simulación, correspondiente a la estrategia 1, está definido en la sección B.2.
$\widetilde{\mathbb{G}} = (V, \widetilde{E})$	Modelo en forma de multigrafo dirigido, del historial de transacciones en el sistema de simulación, está definido en la sección B, V corresponde al conjunto de nodos y $\widetilde{E}$ al conjunto de aristas. Cada nodo representa a un agente y cada arista a una transacción.
$\widetilde{E} \triangleq [i; j; w; t; a]$	Representación de la estructura de cualquier transacción en $\widetilde{\mathbb{G}}$, está definida en la expresión B.3, i identifica al agente proveedor, j identifica al agente consumidor, w es el tipo del recurso transferido, t es la marca de tiempo correspondiente al tiempo en el que la transacción se efectúa, y a es la acción de la que deriva la transacción.
$E_{\imath\, \jmath}$	En la sección B.2, es el conjunto de transacciones para el tratamiento $\imath$ y la observación $\jmath$.
$z(i,j,t,a)$	Utilidad neta que el agente j obtiene de la transacción con el agente i en la iteración t, transacción que deriva de la acción a. Está definida en la sección B.2.
$\nu_1(i)$	Cálculo de la oferta y la demanda del tipo de recurso 1, para el agente i, está definida en la sección B.2.
$\nu_2(i)$	Cálculo de la oferta y la demanda del tipo de recurso 2, para el agente i, está definida en la sección B.2.
$\nu_3(i)$	Cálculo de la oferta y la demanda del tipo de recurso 3, para el agente i, está definida en la sección B.2.
Learn	Algoritmo de aprendizaje implementado en el sistema de simulación, está descrito en el esquema B.1.
$s?(i)$	Inversión intrínseca hecha por el agente i en la iteración anterior, al implementar la estrategia 3, está definida en el esquema B.1.
$s!(i)$	Inversión intrínseca hecha por el agente i en la iteración actual, al implementar la estrategia 3, está definida en el esquema B.1.
$\dot{s}?(i)$	Inversión intrínseca hecha por el agente i en la iteración anterior, al implementar la estrategia 2, está definida en el esquema B.1.
$\dot{s}!(i)$	Inversión intrínseca hecha por el agente i en la iteración actual, al implementar la estrategia 2, está definida en el esquema B.1.
$\mathring{s}?(i)$	Inversión intrínseca hecha por el agente i en la iteración anterior, al implementar la estrategia 1, está definida en el esquema B.1.
$\mathring{s}!(i)$	Inversión intrínseca hecha por el agente i en la iteración actual, al implementar la estrategia 1, está definida en el esquema B.1.
$\hat{\varkappa}_3(i,t)$	Valor monetario más alto que el agente i transfiere para adquirir un recurso, en la iteración t, mediante la estrategia 3, está definido en la sección B.3.
$\hat{\varkappa}_2(i,t)$	Valor monetario más alto que el agente i transfiere para adquirir un recurso, en la iteración t, mediante la estrategia 2, está definido en la sección B.3.
$\hat{\varkappa}_1(i,t)$	Valor monetario más alto que el agente i transfiere para adquirir un recurso, en la iteración t, mediante la estrategia 1, está definido en la sección B.3.

$\gamma_i(t)$	Volumen de ventas esperado por el agente i, i.e., la cantidad de unidades que el agente i espera transferir en la iteración t, mediante la estrategia 3, está definido en la sección B.3.
$\dot{\gamma}_i(t)$	Volumen de ventas esperado por el agente i, i.e., la cantidad de unidades que el agente i espera transferir en la iteración t, mediante la estrategia 2, está definido en la sección B.3.
$\mathring{\gamma}_i(t)$	Volumen de ventas esperado por el agente i, i.e., la cantidad de unidades que el agente i espera transferir en la iteración t, mediante la estrategia 1, está definido en la sección B.3.
$\breve{\varkappa}_3(i,t)$	Cálculo de la utilidad bruta esperada por el agente i en la iteración t, al implementar la estrategia 3, está definido en la sección B.3.
$\breve{\varkappa}_2(i,t)$	Cálculo de la utilidad bruta esperada por el agente i en la iteración t, al implementar la estrategia 2, está definido en la sección B.3.
$\breve{\varkappa}_1(i,t)$	Cálculo de la utilidad bruta esperada por el agente i en la iteración t, al implementar la estrategia 1, está definido en la sección B.3.
$\Lambda(i,t)$	Inversión intrínseca para la utilidad neta más alta que el agente i puede obtener en la iteración t, está definida en la sección B.3.