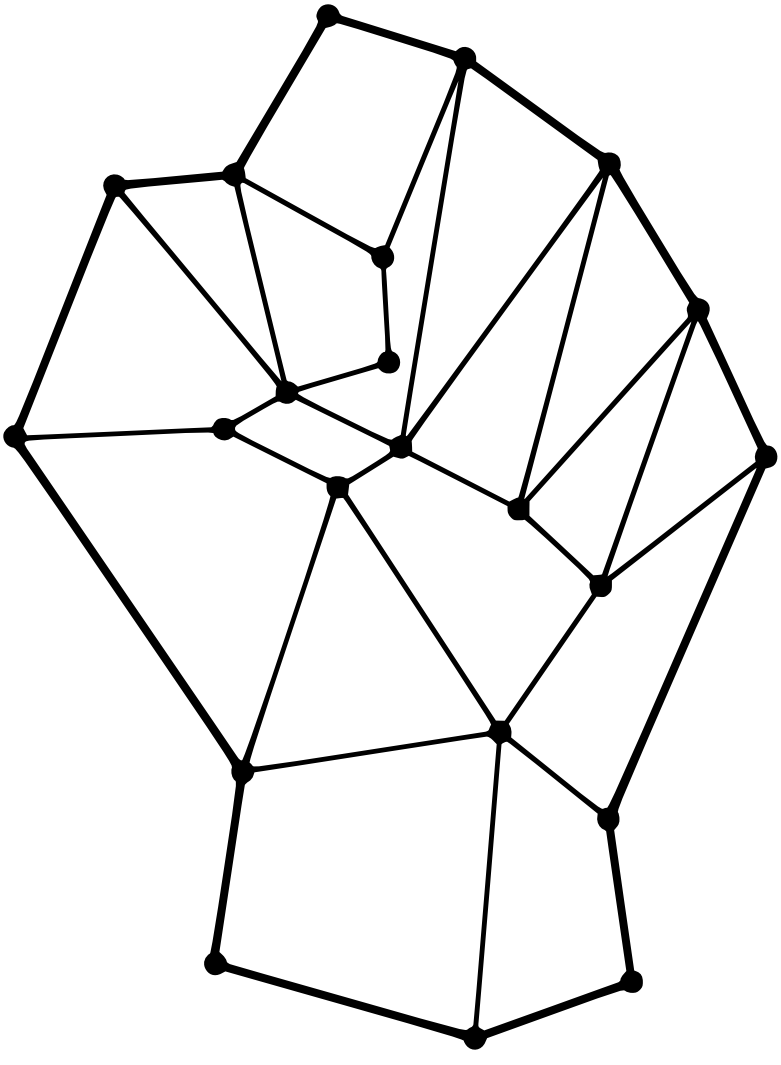
CRIPTOECONOMÍA

PRINCIPIOS FUNDAMENTALES DE BITCOIN



ERIC VOSKUIL

Editado e ilustrado por James Chiang

CRIPTOECONOMÍA

Principios fundamentales de Bitcoin

Eric Voskuil

Criptoeconomía. Principios fundamentales de Bitcoin, 2ª Edición

Versión 1.2.3, Formato de Documento Portátil (PDF)

Editor
Publicado en los Estados Unidos por Eric Voskuil

Autor
Eric Voskuil

Editor e ilustrador
James Chiang

Traductor
Diego Méndez Romero

ISBN: 979-8-9869946-2-8

ISBN 979-8-9869-9462-8
9 798986 994628

Autor

Eric Voskuil

Eric Voskuil ha realizado contribuciones importantes a Libbitcoin[1], una suite de alto rendimiento para desarrolladores en Bitcoin. Eric se graduó por el Rensselaer Polytechnic Institute[2] con una licenciatura en Informática, vendiendo su primera start-up, DesktopStandard[3], a Microsoft[4] y su segunda, BeyondTrust[5], a Veritas Capital[6]. Ha trabajado en el desarrollo del núcleo de Bitcoin desde comienzos de 2014 y da charlas en conferencias y encuentros de todo el mundo. También es emprendedor en serie, *angel investor*, especialista en artes marciales, motociclista ávido, viajero del mundo, y ex piloto de caza de la Marina Estadounidense[7].

A principios de 2020 organizó CryptoEcon[8] en Hanoi, la primera conferencia dedicada a la teoría criptoeconómica, cofundó el Libbitcoin Institute[9] para ayudar a financiar el desarrollo del núcleo de Bitcoin y la educación asociada, patrocinó el primer circuito de Bitbikers[10] por el norte de Vietnam y publicó la primera edición de *Criptoeconomía*.

Reference

[1] https://libbitcoin.info

[2] https://rpi.edu

[3] https://www.eweek.com/enterprise-apps/microsoft-buys-desktopstandard

[4] https://microsoft.com

[5] https://beyondtrust.com

[6] https://veritascapital.com

[7] https://www.navy.mil

[8] https://cryptoecon.org

[9] https://libbitcoininstitute.org

[10] https://bitbikers.org

Editor e ilustrador

James Chiang

James ha hecho contribuciones de código abierto tanto al proyecto Libbitcoin[1] como al proyecto Bitcoin Core[2]. Leyó su primer capítulo de *Criptoeconomía*, el Principio del Coste Dedicado[3], a principios de 2018 y se puso a hacer bocetos de gráficos que le ayudaran a estudiar los principios subyacentes. Actualmente está realizando investigaciones en la seguridad formal de los contratos inteligentes. James está completando su doctorado en informática en la Universidad Politécnica de Dinamarca[4] y anteriormente fue ingeniero aeroespacial en Jet Propulsion Lab[5].

Reference

[1] https://libbitcoin.info

[2] https://bitcoincore.org

[3] Capítulo: Principio del Coste Dedicado

[4] https://www.dtu.dk/english

[5] https://www.jpl.nasa.gov/

Traductor

Diego Méndez Romero

Emprendedor hiperpolíglota, matemático e ingeniero, Diego es un entusiasta de los detalles económicos, técnicos y empresariales de las criptomonedas. Actualmente dirige Agencia de Ingeniería[1], empresa con la que desde 2009 ayuda a *start-ups* y pymes a desarrollar proyectos de software, traducción y tecnologías cripto.

Diego está finalizando su Tesis Doctoral sobre inteligencia artificial[2] y comunicaciones inalámbricas entre vehículos[3] en la Universidad Carlos III de Madrid[4]. Anteriormente completó tres carreras universitarias: Ingeniería Técnica en Sistemas de Telecomunicación por la Universidad Carlos III de Madrid, así como Ciencias Matemáticas y Ciencias Empresariales por la UNED[5].

Por su labor emprendedora, Diego ha recibido entre otros galardones el Premio Iniciativa al Mejor Proyecto Empresarial[6], concedido por la revista Emprendedores[7].

Reference

[1] https://www.emprendedores.es/casos-de-exito/agencia-de-ingenieria/

[2] https://ieeexplore.ieee.org/document/9145198

[3] https://ieeexplore.ieee.org/document/8453900

[4] https://uc3m.es

[5] https://www.uned.es/universidad/inicio.html

[6] https://www.emprendedores.es/casos-de-exito/agencia-de-ingenieria/

[7] https://www.emprendedores.es

Agradecimientos

Este proyecto comenzó como una serie de tuits[1] y más tarde publicaciones en la wiki del repositorio[2] de software de Libbitcoin[3]. Eventualmente hubo tal contenido e interés que empecé a recibir peticiones de escribir un libro. Posteriormente llegaron las ofertas de traducción. Finalmente **James Chiang** intentó publicarlo. Prácticamente completó el montaje de la primera edición, incluyendo sus propias ilustraciones. Sus interesantes preguntas me llevaron a repensar el Principio de Inflación[4], lo cual dio lugar a un marco conceptual económico importante. Y, sin embargo, mis constantes añadidos y cambios en ese momento hicieron que completarlo resultara casi imposible. Al final James se dedicó a asuntos de mayor importancia, pero su labor y sus ilustraciones inspiraron la eventual publicación. No puedo darle tanto las gracias como se merece.

A lo largo del último año, **Fabrizio Armani** ha estado trabajando en una traducción al italiano. Sus comentarios contribuyeron a mejorar esta edición. Su incomodidad con la Relación de Ahorros[5] me llevó finalmente a reducir el alcance de su conclusión. He tenido la suerte de tenerle como persona de consulta para esta edición. Intento ser mi crítico más feroz cuando intento demostrar una conclusión criptoeconómica. Pero James y Fabrizio han mostrado claramente la importancia de trabajar con otra parte dedicada.

Bitcoin empezó para mí con Libbitcoin. En cuanto empecé, volé hasta España para encontrarme con **Amir Taaki**. Él había creado la comunidad de Libbitcoin y dirigió el proyecto antes de poner rumbo a Rojava[6]. Fue extremadamente paciente conmigo

Reference

[1] https://twitter.com

[2] https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics

[3] https://libbitcoin.info

[4] Capítulo: Principio de Inflación

[5] Capítulo: Relación de ahorro

[6] https://es.wikipedia.org/wiki/Amir_Taaki

mientras yo recuperaba mis habilidades con C++ y aprendía a las idiosincrasias de Bitcoin. Libbitcoin constituye una comunidad especial dentro del universo del desarrollo del núcleo de Bitcoin, y Amir merece que se le reconozca el mérito. El intento de reconciliar el bombo que rodeaba a Bitcoin con lo que yo sabía por mi experiencia con él fue lo que condujo a *Criptoeconomía*. Las elecciones realizadas en el desarrollo se relacionan directamente con los fundamentos económicos. Teníamos que explicar lo que estábamos haciendo; explicárnoslo a nosotros mismos y explicárselo los demás. En última instancia su trabajo e ideas condujeron a esta obra, por lo que resultaba apropiado y muy apreciado que aceptara proporcionar el Prefacio[1].

A menudo me refiero a **Phillip Mienk** como la persona más lista que conozco. Le fichó Microsoft[2] como parte de un grupo de egresados del prestigioso Programa de Doctorado en Informática de la University of Illinois, Urbana-Champaign[3]. Yo estaba formando un nuevo equipo de desarrollo de ese momento. No me apetecía tener que formar al nuevo empleado recién salido de la universidad que Microsoft había dejado en mi regazo. Rápidamente me di cuenta de lo afortunado que fui. Cuando lo dejé, unió fuerzas conmigo para montar una tercera *start-up*, y el día en que cerró se unió a mí en Libbitcoin. Él ha sido un socio fundamental durante la última década, siempre capaz de ir directamente al corazón de los problemas más complejos. Estoy agradecido por su apoyo durante algunos momentos difíciles y en última instancia por su contribución a esta obra.

Neill Miller de alguna manera encontró Libbitcoin y ha hecho importantes contribuciones a nuestro código de cartera y al código de interfaz del servidor, y ha mantenido nuestros servidores de la comunidad durante varios años. **Kulpreet Singh** me localizó en el Baltic Honeybadger[4] 2019 y consultó mis ideas en torno a Libbitcoin. Desde ese momento, ha hecho grandes contribuciones a nuestra suite de pruebas de bases de

Reference

[1] Capítulo: Prólogo

[2] https://microsoft.com

[3] https://cs.illinois.edu

[4] https://twitter.com/hashtag/bh2019?src=hashtag_click

datos y ha seguido trabajando en mejoras de diseño en el material subyacente. Junto con Phillip, Neill y Kulpreet han formado la columna vertebral de Libbitcoin. Sin su apoyo no sería posible pasar tanto tiempo escribiendo palabras cuando debería estar escribiendo código[1].

El Libbitcoin Institute[2] es la creación intelectual de **Thomas Pacchia**. Tom me fichó a mí y a **Lucas Betschart** para formar la organización con el propósito de recaudar dinero para financiar el desarrollo del software gratuito[3] de Libbitcoin y la educación en Bitcoin. Hizo todo el trabajo tedioso requerido para obtener el estatus 501c3[4] ante el IRS (las autoridades fiscales estadounidenses). Hasta la fecha, el IRS no ha cumplido, pero el Instituto sigue siendo un vehículo para apoyar los trabajos necesarios para promover la propuesta de valor[5] de Bitcoin. Tom y Lucas me han dado un apoyo tremendo y han sido buenos amigos.

La primera edición de *Criptoeconomía* se distribuyó exclusivamente a los asistentes de CryptoEcon[6] 2020 en Hanoi. La intención era publicarlo online rápidamente para su venta, pero la vida se interpuso. Los extras siguen en una tienda de motocicletas de la calle Tay Ho. Pero CryptoEcon, un proyecto del Libbitcoin Institute, contribuyó a difundirlo. Las contribuciones de HODL Capital[7] (a través de **Thomas Pacchia**) y Lemniscap[8] (a través de **Roderik van der Graaf**) hicieron posible la conferencia. Tom me vino a buscar a Lisboa en Building on Bitcoin[9] 2018 y Roderik me encontró en Baltic Honeybadger

Reference

[1] https://www.activism.net/cypherpunk/manifesto.html

[2] https://libbitcoininstitute.org

[3] https://es.wikipedia.org/wiki/Free_Software_Foundation

[4] https://www.irs.gov/charities-non-profits/charitable-organizations/exemption-requirements-501c3-organizations

[5] Capítulo: Propuesta de Valor

[6] https://cryptoecon.org

[7] https://www.hodl.capital

[8] https://lemniscap.com

[9] https://building-on-bitcoin.com

2019, en Riga. Ellos tomaron la iniciativa y me inspiraron a completar el libro para la conferencia.

Las personas que más han contribuido con temas inspiradores y crítica constructiva de las ideas son demasiadas para incluirlas. Incluyen organizadores de conferencias y reuniones, directores de *podcasts*, asistentes y oyentes, y el torrente aparentemente infinito de comentaristas por Twitter. He descubierto mucho más investigando ideas deficientes que con las ideas sólidas. Y, sin embargo, sin tener también voces ocasionales que te apoyen, este tipo de asunto es mucho más difícil de llevar a cabo.

Finalmente, gracias a mis amigos y a mi familia por apoyarme durante un periodo difícil.

CONTENIDO

Tabla de contenido

PRÓLOGO

Prólogo
Por Amir Taaki

La criptoanarquía[1] no es ni una estrategia para imponer una hegemonía política ni para rebatir otras posibles actitudes o agendas. Es un mero conjunto de conceptos o ideas que se puede utilizar tácticamente para implementar modos alternativos de existencia. La historia es el resultado de la voluntad y la acción humanas, pero esto siempre ocurre dentro de un marco de convicciones, creencias y representaciones que proporcionan significado y orientación a cualquier actividad que se pretenda. De esta manera, la criptoanarquía trata de armar al individuo con poderosas herramientas conceptuales para construir sus propias visiones creativas.

La economía es importante puesto que constituye el estudio de los mecanismos fundamentales de la acción humana y de sus consecuencias. La economía racional analiza la actividad humana al tiempo que acepta los límites del conocimiento. A partir de un sencillo conjunto de suposiciones, incluyendo las de que los humanos actúan[2] y prefieren las cosas antes mejor que después[3], se deducen teoremas mediante reglas de inferencia[4]. El resultado es potente, ya que es necesariamente verdadero en virtud de las suposiciones. El desarrollo de estos teoremas nos proporciona estructuras sencillas que podemos utilizar para compartimentar y analizar fenómenos más complejos.

La criptomoneda[5] emergió de la criptoanarquía y la economía de libre mercado, pero desde entonces ha superado sus propias raíces y se ha convertido en una entidad

Reference

[1] https://es.wikipedia.org/wiki/Criptoanarquismo
[2] https://en.wikipedia.org/wiki/Action_axiom
[3] https://en.wikipedia.org/wiki/Time_preference
[4] https://es.wikipedia.org/wiki/Regla_de_inferencia
[5] https://es.wikipedia.org/wiki/Criptomoneda

contemporánea con características peculiares. Esto nos ha obligado a revisitar nuestras propias ideas y suposiciones acerca de cómo se interrelacionan esas disciplinas. El nuevo campo de estudio se denomina criptoeconomía.

Las criptomonedas como Bitcoin representan un tipo de dinero que simultáneamente es global, está libre de censura, y es de acceso abierto para todo el mundo, por primera vez en la Historia humana. También se están realizando grandes avances en la tecnología de anonimización, no solo para las criptomonedas sino también para otros instrumentos financieros y actividades humanas. Por consiguiente, la criptomoneda constituye un fenómeno único con sus propias características merecedoras de estudio.

La importancia de la economía reside en que nos proporciona una ventana para comprender las actividades de los seres humanos. Esto significa que podemos hacer planes acerca de dónde aplicar nuestros recursos y nuestros conocimientos técnicos. A la actual generación de empresas de cripto le falta esta dimensión estratégica y no estará preparada para aprovechar las nuevas tendencias geopolíticas. Actualmente, hay demasiada divergencia en el enfoque: la industria de la criptografía no es lo suficientemente selectiva.

Los conceptos de la teoría de la evolución nos pueden ayudar a predecir qué tipo de estrategias organizativas ganarán a más largo plazo. Por ejemplo, la Teoría de selección r/K[1] explica que, después de los grandes eventos de extinción, los primeros organismos en ocupar nichos son las especies con grandes cifras de jóvenes que maduran rápidamente y reciben poca inversión de recursos procedentes de los padres (seleccionados por r)[2]. Sin embargo, su ventaja es superada a más largo plazo por los organismos que tienen menos jóvenes y más especializados para los nichos, y que tardan más en madurar (seleccionados por K)[3]. Estos cripto-organismos seleccionados por K son

Reference

[1] https://es.wikipedia.org/wiki/Teor%C3%ADa_de_la_selecci%C3%B3n_r/K

[2] https://es.wikipedia.org/wiki/Teor%C3%ADa_de_la_selecci%C3%B3n_r/K#Selecci%C3%B3n_R

[3] https://es.wikipedia.org/wiki/Teor%C3%ADa_de_la_selecci%C3%B3n_r/K#Selecci%C3%B3n_K

los que estarán mejor adaptados para aprovechar los nuevos nichos económicos que se están abriendo.

Otra hipótesis de la teoría de la evolución es la hipótesis de la Reina Roja[1], a saber, que los organismos se encuentran en una batalla constante por evolucionar. Es decir, tenemos que adaptarnos constantemente y evolucionar en un entorno que cambia continuamente y tiene agentes que no dejan de evolucionar.

Esto lo hacemos por medio del proceso de aplicar nuestro conocimiento para encontrar patrones y construir modelos conceptuales, modificando esos modelos según el *feedback* para mejorar su precisión o ampliar sus paradigmas subyacentes.

La actual cosecha de empresas de cripto se extinguirá bastante pronto. En su lugar, emergerá una nueva generación de organizaciones. Estas tendrán mucha capacidad de adaptación, sintonizarán con las tendencias geopolíticas, y se optimizarán para sobrevivir en un estado de desequilibrio perpetuo. Para resistir en esas condiciones, esta nueva generación debería fundarse en una síntesis que combine la astucia de la criptoeconomía y la propia criptoanarquía – que en el fondo es una doctrina sencilla: el motor del cambio histórico no es la mera innovación tecnológica, sino los conceptos, los modelos y las ideas que nos conceden poder sobre la realidad material.

Mi experiencia con Eric se remonta a 2013 cuando empezamos a trabajar en software del sistema Bitcoin[2] que era tanto rápido como escalable. Eric es un desarrollador de primer nivel que puede hacer, él solito, el trabajo de un equipo completo para crear software de nivel de producción – una habilidad muy poco frecuente. También ha vivido una amplia gama de experiencias, desde pilotar aviones para la Marina estadounidense hasta fundar múltiples empresas de éxito. Combina unos intensos conocimientos prácticos con un

Reference

[1] https://es.wikipedia.org/wiki/Hip%C3%B3tesis_de_la_Reina_Roja

[2] https://github.com/libbitcoin

robusto enraizamiento teórico y un profundo interés y conocimiento de política y economía.

Las singulares percepciones de Eric en conceptos fundamentales nos dotan de un marco esencial para guiar la orientación futura del campo de la criptoeconomía. Aplica con rigor la teoría económica racional a las criptomonedas, y se aventura más allá de lo financiero para explicar cómo la actividad humana da forma a este futuro.

PREFACIO

Prefacio

Esto empezó como una forma de evitar tener que reescribir las mismas ideas a impulsos de 140 caracteres[1]. Acordes con ese entorno, los temas eran lo más cortos posibles e informales. No pretendía escribir un libro, y tampoco podría hacerlo. La mayoría de los temas (incluido este) los escribí en mi teléfono, en un vuelo, en tren o en una cafetería. Muchos son observaciones rápidas que surgen del conocimiento íntimo del código del núcleo de Bitcoin o de mucho estudio autodidacta y larga experiencia en diversas disciplinas.

Con el tiempo los temas empezaron a interaccionar, brotó una taxonomía necesaria, y lo que había sido un proceso informal de observación ad hoc empezó a convertirse en trabajo. **Los temas son lo más cortos posibles y presuponen cierto conocimiento tanto de Bitcoin como de economía**. He hecho un esfuerzo sincero por racionalizar las relaciones y la terminología, pero sigo concentrándome en la consistencia[2] y la expansión de la comprensión. Afortunadamente, otros se han venido uniendo para ayudar con la ilustración, la revisión y la publicación.

He utilizado los términos Cataláctica[3] y Praxeología[4] para describir la disciplina subyacente. La gente también utiliza el término Economía Austríaca[5]. Cada uno de ellos los considero poco satisfactorios, así que he empezado a referirme a la disciplina como

Reference

[1] https://es.wikipedia.org/wiki/Twitter

[2] https://en.wikipedia.org/wiki/Consistency

[3] https://es.wikipedia.org/wiki/Catalaxia

[4] https://es.wikipedia.org/wiki/Praxeolog%C3%ADa

[5] https://es.wikipedia.org/wiki/Escuela_austriaca

"Economía Racional" (no confundir con el racionalismo[1] económico), un sistema basado por completo en el razonamiento[2] deductivo a partir de un conjunto de axiomas[3].

Fue Mises[4] quien estableció explícitamente la Economía como sistema sobre una base racional, pero este enfoque no impregna toda la Escuela Austríaca (que es anterior a Mises). Rothbard[5] añade rigor y claridad a Mises, deduciendo algunas nuevas conclusiones importantes. Sin embargo, Mises (como la mayoría de los humanos) comete errores sustantivos[6], a los que Rothbard desafortunadamente da continuidad. Otros errores amplificados habitualmente dentro de la Escuela Austríaca son claros fallos de interpretación.

En cada caso en el que yerra Mises, está criticando el dinero fiduciario estatal[7]. En otras palabras, parece sacrificar su objetividad ante su pasión. Y, sin embargo, su sistema racional, aplicado adecuadamente, expone fácilmente los errores. El dinero estatal merece crítica, y los *bitcoiners* rara vez pierden oportunidad de hacerlo. No obstante, se merece una crítica *precisa*; cualquier otra cosa resulta contraproducente. Con un análisis correcto, se pueden identificar fuerzas relevantes específicas, tanto en el dinero fiduciario monopolístico (por ejemplo, el dólar) como en el dinero fiduciario de mercado (por ejemplo, el Bitcoin). Este clase de buen análisis puede limitar malgastar un precioso capital en propuestas irracionales[8].

Reference

[1] https://en.wikipedia.org/wiki/Economic_rationalism
[2] https://es.wikipedia.org/wiki/Razonamiento_deductivo
[3] https://es.wikipedia.org/wiki/Axioma
[4] https://es.wikipedia.org/wiki/Ludwig_von_Mises
[5] https://es.wikipedia.org/wiki/Murray_Rothbard
[6] Capítulo: Principio de Inflación
[7] Capítulo: Taxonomía del dinero
[8] Capítulo: Falacia de la Reserva Plena

Un proceso estrictamente racional no solo expone los errores, sino que también produce nuevos e interesantes descubrimientos[1] y simplificaciones[2], no solo en Bitcoin sino en la teoría económica de carácter general. Los temas forman un grafo en el cual ningún orden global parece adecuado. La tabla de contenido es un orden mal impuesto. Si bien se ha procurado cierta progresión, recomiendo leer los temas tal y como fueron escritos, como curiosidad.

Reference

[1] Capítulo: Propiedad de resistencia a la censura

[2] Capítulo: Principio de Depreciación

INTRODUCCIÓN

Introducción

¿Crees que sabes algo acerca de Bitcoin y la Economía Austríaca[1]? En ese caso, puedes estar listo/a para *Criptoeconomía*. Esta no es una obra para los no iniciados. No es una narrativa y está exenta de opiniones. El contenido es denso: no se repite. No es una contribución para la cámara de resonancia, no te enseñará cómo configurar un monedero, ni el precio futuro, ni qué hacer.

La *criptoeconomía* aplica principios racionales de economía a Bitcoin, demostrando deficiencias y complejidades innecesarias en ellos, y en ideas comunes en torno al Bitcoin. Mejorará tu comprensión de ambos. Bitcoin requiere una disciplina nueva, rigorosa y exhaustiva. **Es esta.**

Bitcoin es algo nuevo. Parece desafiar el entendimiento. ¿Ha habido alguna vez una oferta fija de dinero? ¿Existe otro caso de coste de producción que varíe directamente con el precio del producto? ¿Hay algo más que tenga una tasa competitiva, pero fija, de facilidad de transacción? Para ver más allá del bombo, entender la propuesta de valor, el modelo de seguridad y el comportamiento económico, esta puede ser tu única fuente.

El Bitcoin es economía, tecnología y seguridad. Sin incorporar todos estos aspectos, se cometerán errores. Han intentado explicarlo economistas, tecnólogos, expertos en seguridad, e incluso numerólogos[2]. Cada cual aporta una perspectiva limitada, y no logra incorporar aspectos esenciales. El autor se vio con una cualificación única para integrarlos.

Su trabajo en Bitcoin comenzó con un monedero físico. Pasó un año echando amenazas, trabajando con expertos en diseño electrónico, explotación del hardware y vigilancia

Reference

[1] https://es.wikipedia.org/wiki/Escuela_austriaca

[2] https://twitter.com/100trillionusd

estatal. Eligió la librería de software Libbitcoin[1], ya que el prototipo de Satoshi no estaba factorizado para la programación y estaba financiado en gran medida por la Bitcoin Foundation[2], un consorcio corporativo. Posteriormente se dedicó a Libbitcoin, eventualmente escribiendo o editando todas sus ~500.000 líneas de código. Pocos tienen una experiencia comparable con una pila de Bitcoin tan completa.

Como piloto de caza con experiencia de combate en la Marina estadounidense[3], ha vivido las amenazas procedentes de los estados. Se convirtió en instructor de tácticas de cazabombardero (Strike Fighter Tactics Instructor)[4], donde su actividad principal fue el análisis de tácticas y la presentación de amenazas. También asesoró a la Marina en la red de Strike Fighter Training System[5], Joint Strike Fighter[6], primeras armas GPS[7], y sistemas de F/A-18[8]. Su comprensión de la naturaleza física de toda la seguridad se vio mejorada por décadas de formación en artes marciales japonesas, logrando clasificaciones de cinturón negro en cinco disciplinas.

Su licenciatura[9] y experiencia en informática, junto con su amplia experiencia empresarial, fundando varias empresas. Ha trabajado en IBM[10] y como Arquitecto Principal en Microsoft[11], dos de las mayores empresas del mundo. Esta última adquirió su primera *start-up*, y la segunda fue adquirida por Veritas Capital[12]. Se le han concedido

Reference

[1] https://libbitcoin.info
[2] https://bitcoinfoundation.org
[3] https://www.navy.mil
[4] https://en.wikipedia.org/wiki/United_States_Navy_Strike_Fighter_Tactics_Instructor_program
[5] https://www.globalsecurity.org/military/library/policy/navy/ntsp/SFTS.htm
[6] https://en.wikipedia.org/wiki/Joint_Strike_Fighter_program
[7] https://en.wikipedia.org/wiki/Guided_bomb#Satellite
[8] https://es.wikipedia.org/wiki/McDonnell_Douglas_F/A-18_Hornet
[9] https://www.rpi.edu
[10] https://ibm.com
[11] https://microsoft.com
[12] https://www.veritascapital.com

tres patentes estadounidenses[1] relacionadas. Eventualmente se convirtió en un *angel investor*, compartiendo su experiencia con otros emprendedores.

Como CTO (Director de Tecnología)[2] de su primera empresa, publicó tres avisos de seguridad informática a través del Computer Emergency Response Team[3]. Cada uno de ellos lo dedujo enteramente leyendo la documentación para el usuario. Posteriormente, obtuvo un puesto en el consejo asesor del DHS[4] Open Vulnerability Assessment Language[5] por su trabajo en la programación de parches informáticos. En años recientes, descubrió deficiencias sustantivas en la seguridad de cada una de las tres iteraciones de un popular monedero físico de "elementos seguros", nuevamente revisando la documentación para el usuario.

Treinta años de estudio autodidacta en la economía de libre mercado se vieron reforzados con numerosos viajes por el mundo. En sus visitas a más de 80 países, ha interactuado con personas en cinco continentes. Viajando, a menudo aún en moto sin más que una mochila al hombro, obtiene una íntima comprensión de las realidades económicas mundiales. Desde los cambistas del mercado negro de Zimbabue, pasando por los cafeteros tanzanos, los refugiados venezolanos, los pastores mongoles, los músicos de jazz de Okinawa, los monjes de Lao, etc. – el mundo no es como a menudo se le presenta.

La capacidad de integrar estas experiencias, diversas y relevantes, dieron lugar a *Criptoeconomía*. Esta es tu próxima parada.

Reference

[1] https://www.uspto.gov

[2] https://en.wikipedia.org/wiki/Chief_technology_officer

[3] https://en.wikipedia.org/wiki/CERT_Coordination_Center

[4] https://dhs.gov

[5] https://oval.cisecurity.org

MODELO DE SEGURIDAD

Axioma de resistencia

En la lógica moderna, un axioma[1] es una premisa, no puede ser probada. Se trata de una suposición inicial a la luz de la cual se pueden probar otras cosas. Por ejemplo, en la geometría euclídea[2] uno no puede probar que las líneas paralelas nunca se crucen. Sencillamente, esto define esa geometría particular.

Probar afirmaciones sobre Bitcoin exige basarse en sistemas axiomáticos, específicamente las matemáticas[3], la probabilidad[4] y la catalláctica[5], y, por consiguiente, en las suposiciones en las que se basan. Sin embargo, Bitcoin también se basa en un axioma que no se encuentra en estos sistemas.

Satoshi alude a esto en una afirmación[6] temprana:

> >No hallaréis en la criptografía una solución a los problemas políticos.
>
> Sí, pero podemos ganar una batalla importante en la carrera armamentística y capturar un nuevo territorio de libertad durante varios años.
>
> Los gobiernos son buenos decapitando redes con control centralizado como Napster, pero las redes P2P puras como Gnutella y Tor parecen estar resistiendo bastante bien.
>
> *Satoshi Jue Nov 6 15:15:40 EST 2008*

Reference

[1] https://es.wikipedia.org/wiki/Axioma

[2] https://es.wikipedia.org/wiki/Geometr%C3%ADa_euclidiana

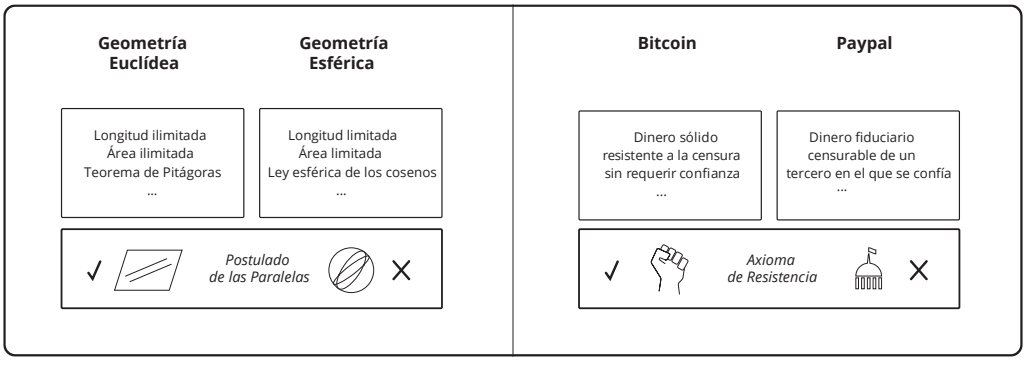
[3] https://en.wikipedia.org/wiki/Zermelo%E2%80%93Fraenkel_set_theory

[4] https://es.wikipedia.org/wiki/Axiomas_de_probabilidad

[5] https://es.wikipedia.org/wiki/Catalaxia

[6] http://satoshi.nakamotoinstitute.org/emails/cryptography/4

En otras palabras, existe una suposición de que es *posible* que un sistema resista el control estatal. Esto no se acepta como un hecho sino que se considera una suposición razonable, debido al comportamiento de sistemas similares en los que basar el sistema.



Alguien que no acepte el axioma de resistencia está contemplando un sistema totalmente distinto al de Bitcoin. Si uno supone que *no es posible* que un sistema resista los controles estatales, las conclusiones no tienen sentido en el contexto del Bitcoin – al igual que las conclusiones en la geometría esférica[1] contradicen las euclídeas. ¿Cómo puede Bitcoin estar exento de permisos[2] o ser resistente a la censura[3] sin el axioma? La contradicción le lleva a uno a cometer errores obvios[4] en un intento de racionalizar el conflicto.

Es habitual que la gente se refiera cínicamente a un sistema de tipo similar a Bitcoin que omita el axioma de resistencia como "otro PayPal más", una designación que no está libre de mérito. Confinity[5] intentó originalmente crear un sistema con una propuesta de

Reference

[1] https://es.wikipedia.org/wiki/Geometr%C3%ADa_esf%C3%A9rica

[2] Capítulo: Principio de Ausencia de Permisos

[3] Capítulo: Propiedad de resistencia a la censura

[4] Capítulo: Error de Hearn

[5] https://en.wikipedia.org/wiki/Confinity

valor[1] similar a Bitcoin. Al no haberlo logrado, descartó el axioma, construyendo el PayPal[2] que conocemos hoy.

Reference

[1] Capítulo: Propuesta de Valor

[2] https://en.wikipedia.org/wiki/PayPal

Propiedad de resistencia a la censura

La resistencia a la censura es una consecuencia de las comisiones por transacciones. Imponer el cumplimiento de una censura es indistinguible de imponer el cumplimiento de una bifurcación blanda, con la potencia de hash mayoritaria rechazando los bloques no censores. Sin esta imposición de su cumplimiento, las transacciones son confirmadas sobre una base de racionalidad económica a pesar de la subjetividad individual de la minera.

Una minera mayoritaria es rentable financieramente. Como tal, no tiene coste adquirir los medios de censura. Puesto que la minería constituye necesariamente un rol anónimo[1], siempre es posible que un actor adquiera una potencia de hash mayoritaria, la despliegue, y la controle en un momento dado. Como se demuestra en la Falacia de la Prueba de Trabajo[2], las bifurcaciones duras no se pueden utilizar para desalojar al censor de manera selectiva y, por el contrario, aceleran el derrumbamiento de la moneda.

En el caso de la censura activa, pueden originarse comisiones en las transacciones que no logren confirmarse. Esta prima de comisión genera un mayor beneficio potencial para las mineras que confirmen transacciones censuradas. A un nivel suficiente, esta oportunidad produce una mayor competencia y, por consiguiente, aumenta la tasa de hash global.

Si la potencia de hash no censora y en aumento supera la del censor, la imposición de la censura fracasa. Así, el censor se enfrenta a la elección de subvencionar las operaciones o abandonar la empresa. Solamente el estado puede subvencionar las operaciones a perpetuidad, ya que puede exigir impuestos. Al mismo tiempo, se beneficia al conservar

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

[2] Capítulo: Falacia de la Prueba de Trabajo

su propio régimen monetario. **El estado debe consumir impuestos hasta al menos el nivel de la prima de comisión para mantener la imposición de la censura.**

Una moneda sin comisiones integradas o bien no lograría censurar, o bien desarrollaría un mercado de comisiones aparte. Como se demuestra en la Falacia de las Comisiones Aparte[1], no es necesario que las comisiones estén integradas; sin embargo, la integración de las comisiones constituye una técnica importante para su carácter anónimo. En cualquiera de ambos casos, la resistencia a la censura se origina solamente a partir de la prima de comisión. Esta porción de subvención de la recompensa del bloque no contribuye a la resistencia a la censura porque el censor recibe la misma subvención que las demás mineras.

Es posible que la imposición de la censura pudiera producir un derrumbamiento del precio, haciendo que el sensor soporte pérdidas en las operaciones. Sin embargo, en este caso se ha logrado su objetivo, sin que la economía tenga la oportunidad de contrarrestar la acción del censor. Este derrumbamiento podría lograrse por un coste despreciable sin más que demostrar la intención de censurar. También es posible que una bifurcación blanda por censura pudiera producir un *aumento* de precio, en tanto las empresas de los mercados legales dieran la bienvenida a la aprobación estatal asociada. No obstante, para que la moneda sobreviva, su economía tiene que seguir generando una prima de comisión suficiente para superar en potencia al censor.

No se puede demostrar que la economía vaya a generar suficientes comisiones para superar en potencia al censor. De manera parecida, no se puede demostrar que un censor vaya a tener la disposición y la capacidad de subvencionar operaciones a cualquier nivel dado. Por consiguiente, no es posible probar la resistencia a la censura. Por este motivo, la resistencia al control estatal es axiomática[2].

Reference

[1] Capítulo: Falacia de las Comisiones Aparte

[2] Capítulo: Axioma de resistencia

Riesgo de Centralización

Una debilidad[1] del Bitcoin se produce por la centralización y la compartición de recursos. Las fuerzas que producen minería acumulada se llaman presiones pro-compartición de recursos[2]. Mientras que la compartición de recursos debilita la seguridad de la confirmación, la centralización debilita la seguridad de las reglas de consenso. La debilidad es el resultado de que haya menos personas con las que compartir el riesgo[3].

El riesgo de consenso se comparte solamente entre los comerciantes activos, ya que son las personas con la capacidad de negarse a intercambiar propiedad por unidades que no sean conformes a sus reglas. Las fuerzas financieras que reducen el número de comerciantes se llaman presiones de centralización. El problema de la delegación es que a menudo viene emparejada con la centralización, como es típico de los monederos[4] web. El monedero no solo posee las unidades guardadas sino que también controla la validación de las unidades recibidas en intercambios. **Esto último reduce el poder sobre las reglas de consenso a una persona para todos los monederos del servicio.**

Las presiones de centralización incluyen:

- El descuento por dificultad de uso.
- El descuento por cerrar operaciones en la cadena.

Si el cambio le resulta difícil a un cliente, el comerciante tiene que aplicar descuentos a la mercancía para aceptar la moneda. Si el cambio le resulta difícil al comerciante, se incurre

Reference

[1] Capítulo: Modelo de Seguridad Cualitativa

[2] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[3] Capítulo: Principio de la Compartición de Riesgos

[4] https://bitcoin.org/en/wallets/web

en un coste adicional. Cuando remitir pagos a un tercero de confianza reduzca la magnitud de su descuento y/o coste, aumentará el rendimiento del capital.

La transferencia soporta comisiones, lo cual también obliga a que un comerciante aplique descuentos a la mercancía. Cuando utilizar un intermediario de confianza para cerrar transferencias fuera de la cadena reduzca las comisiones, y, por tanto, el descuento, aumentará el rendimiento del capital del comerciante.

La centralización se manifiesta como:

- Procesadores de pagos
- Monederos web y otros monederos basados en la confianza
- APIs alojadas para acceder a la cadena

En un entorno bajo en amenazas[1], el comerciante tiene un incentivo financiero reducido en subvencionar la seguridad del Bitcoin. A medida que aumente el coste de las alternativas[2], el descuento se vuelve inevitable. En ese momento, el cliente decide pagar un mayor precio o el comerciante cierra el negocio ya que el capital busca rentabilidades de mercado.

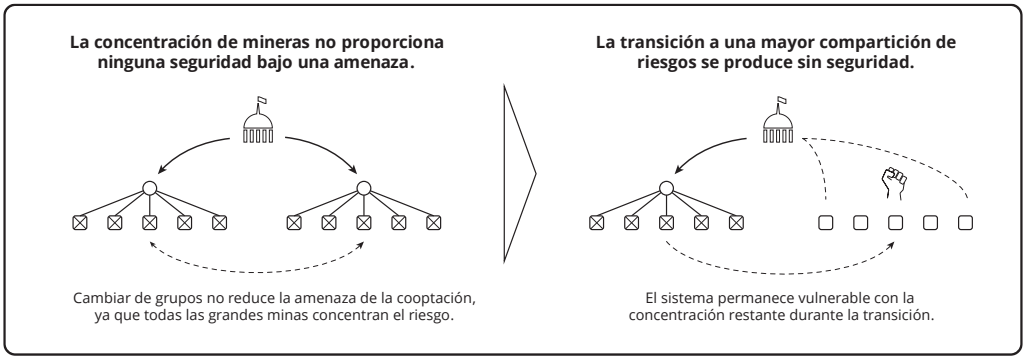
Reference

[1] Capítulo: Paradoja del Nivel de Amenaza

[2] https://en.wikipedia.org/wiki/Foreign_exchange_controls

Falacia de las Cucarachas

Existe una teoría que afirma que la agregación no reduce sustancialmente la seguridad permitida por la compartición de riesgos[1] porque las mineras y la economía se dispersarán según sea necesario, de manera parecida a como se dispersan las cucarachas cuando una luz las molesta. **La irracionalidad de la teoría implica que la seguridad existe realmente porque podría existir.** Esto supone esencialmente un rechazo de la Paradoja del Nivel de Amenaza[2], que implica que la seguridad evoluciona con el tiempo bajo una amenaza persistente.



La teoría se basa en que las machacadoras se cambien de bando de mineras. Esto se basa en la Falacia del Equilibrio de Poder[3], que modela a las mineras incorrectamente como la amenaza. Un movimiento de potencia de hash desde una mina a otra no reduce la compartición de recursos ni el riesgo asociado[4] a ella. El riesgo es que los estados coopten

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

[2] Capítulo: Paradoja del Nivel de Amenaza

[3] Capítulo: Falacia del Equilibrio de Poder

[4] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

grandes cantidades de potencia de hash, reduciendo sustancialmente el coste del ataque. Es un error asumir que los estados no colaboran[1] para defender el señoreaje[2].

> El Fondo Monetario Internacional (IMF) es una organización de 189 países, que trabajan para fomentar la cooperación monetaria global...
>
> *imf.org*

Como tal, uno no puede asumir que pueda existir una gran mina fuera del control[3] estatal. Una reducción en la compartición de recursos requiere un aumento en el número de mineras, específicamente de aquellas dispuestas y capaces de realizar operaciones encubiertas[4]. Esto requiere que las machacadoras sufran el mayor coste asociado a una compartición de recursos reducida.

Sin embargo, no cabe esperar que las personas trabajen en contra de su interés financiero. Para que aumente la compartición de riesgos, deberán revertirse las presiones financieras en contra de esta. Asumir lo contrario es económicamente irracional.

La teoría también ignora la centralización económica y la delegación. Es un error asumir que la economía pueda descentralizarse rápidamente, y la des-delegación sería muy probablemente inviable en caso de que ataques estatales como controles[5] de divisas restrinjan habitualmente la transferencia.

Reference

[1] http://www.imf.org/external/index.htm

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

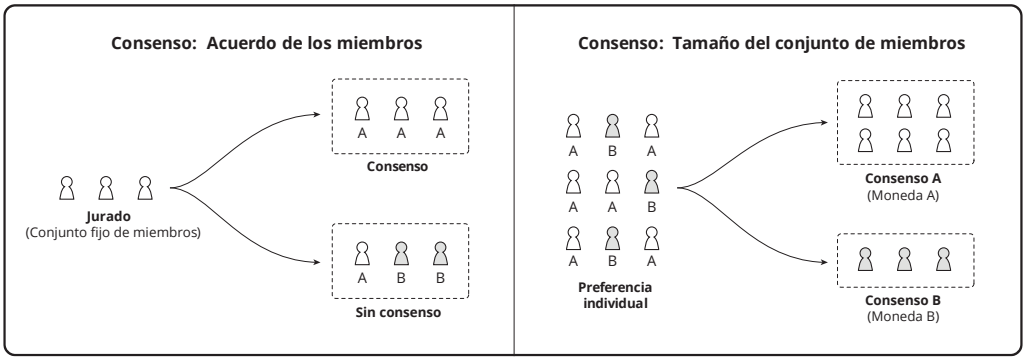
[3] Capítulo: Paradoja del Nivel de Amenaza

[4] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/

[5] https://en.wikipedia.org/wiki/Foreign_exchange_controls

Propiedad de Consenso

Las personas conciben generalmente el consenso en el contexto de un conjunto fijo de participantes, como un jurado[1]. En ese modelo, el consenso implica que todos los participantes tengan que estar de acuerdo. **Pero, puesto que la participación en Bitcoin no requiere permisos y, por consiguiente, no es fija, siempre existe un acuerdo completo, implícito en la participación.** En este modelo, el consenso se refiere a la magnitud de los participantes (economía), no a una condición de acuerdo.



Un consenso puede fragmentarse[2] o consolidarse[3]. En general, un mayor consenso proporciona una mayor utilidad y una mayor seguridad al compartirse el riesgo[4] de manera más amplia.

Reference

[1] https://en.m.wikipedia.org/wiki/Hung_jury

[2] Capítulo: Principio de Fragmentación

[3] Capítulo: Principio de Consolidación

[4] Capítulo: Principio de la Compartición de Riesgos

Principios Criptodinámicos

La criptodinámica es un término acuñado aquí con el propósito de referirnos fácilmente a los principios fundamentales de Bitcoin. Tiene la intención tanto de informar la idea de Bitcoin como de diferenciarlo de otras tecnologías. Los principios constituyen el subconjunto mínimo de principios criptoeconómicos necesarios para lograr este objetivo.

Si bien no es demasiado importante el nombre que se elija, a continuación se proporciona una justificación del mismo.

Cripto[1]

> "Una criptomoneda es un [dinero] que utiliza criptografía fuerte para asegurar transacciones financieras, controlar la creación de unidades adicionales, y verificar la transferencia de las [unidades]."
>
> *Wikipedia*

Dinámica[2]

> "La dinámica es la rama de la matemática aplicada [...] que se ocupa del estudio de las fuerzas [...] y su efecto sobre el movimiento."
>
> *Wikipedia*

Reference

[1] https://es.wikipedia.org/wiki/Criptomoneda

[2] https://es.wikipedia.org/wiki/Din%C3%A1mica

Cripto + Dinámica

La criptodinámica es el conjunto de fuerzas que aseguran las transacciones de Bitcoin mediante el control de (1) la definición de las unidades, y (2) la transferencia de las unidades.

Principios

La fuerza de seguridad de naturaleza totalmente humana. Las personas deben actuar para asegurar cualquier cosa, incluido Bitcoin. Como sistema económico, la seguridad de Bitcoin solo puede esperar que las personas actúen de manera económicamente racional (interés propio). Como tal, las fuerzas de seguridad de Bitcoin están totalmente basadas en las acciones en interés propio de personas individuales, específicamente:

- Compartición de riesgos[1]
- Hundimiento de Energía[2]
- Regulación de potencia[3]

Estas fuerzas dependen de las demás, por orden. Sin compartición de riesgos, no se puede hundir energía en el sistema para regular la potencia de un censor. Con estas tres fuerzas intactas, Bitcoin puede ser seguro. Sin ninguna de ellas, una tecnología no es Bitcoin.

No se puede asumir[4] que, dada la incorporación de estas fuerzas, una implementación de Bitcoin pueda ser asegurada. Además, una puede ser más susceptible de aseguramiento

Reference

[1] Capítulo: Principio de la Compartición de Riesgos
[2] Capítulo: Falacia de la Prueba de Participación
[3] Capítulo: Propiedad de resistencia a la censura
[4] Capítulo: Axioma de resistencia

que otra. **Solamente puede afirmarse que, dada la incorporación de estas fuerzas, una tecnología es un Bitcoin; y que sin ellas, no lo es.**

La posibilidad de seguridad permitida por estas fuerzas puede denominarse "seguridad criptodinámica". Así, por ejemplo, una "cadena de bloques sujeta a permisos" viola el principio de compartición de riesgos, una tecnología estrictamente de prueba de participación (*proof of stake*) viola el principio de hundimiento de energía, y un dinero que se base enteramente en la subvención para remunerar las confirmaciones viola el principio de regulación de potencia. Ninguno de ellos es seguro desde un punto de vista criptodinámico.

Principio de Riesgo de Custodia

Cuando un contrato representa un activo, el contrato constituye un derecho reclamable contra el custodio del activo. Este derecho reclamable a menudo se llama un título, con la pretensión implícita de que el derecho reclamable está "protegido" en el caso de que el custodio no entregue a cambio el activo en virtud de los términos del contrato. El valor monetario del título es el del activo subyacente menos los costes del cambio y de hacer valer el derecho reclamable.

El riesgo de custodia es un aspecto central de cualquier dinero[1]. La utilidad de un dinero se ve limitada por la fiabilidad de su custodio. Al ser humano, no se puede asegurar la fiabilidad de un custodio. En el caso del dinero estatal, el único custodio es el estado. Según se demuestra en Principio de Reserva[2], el dinero estatal existe con el propósito de acumular una reserva[3]. Esto proporciona una ventaja para el estado solamente porque se puede abolir su papel de custodio tanto mediante la liquidación de la reserva como de la emisión de títulos fraudulentos. En otras palabras, la suspensión de pagos del custodio es la razón del dinero estatal.

El valor monetario de una unidad de Bitcoin es estrictamente una función de lo que puede adquirir en intercambios. Si ningún comerciante lo acepta, una unidad no es útil para su propietario. Bitcoin no tiene custodio, pero en aras de establecer un principio general, uno podría considerar el conjunto de todos los comerciantes como el custodio colectivo de Bitcoin. Como tal, el riesgo de custodio se reparte por toda la economía.

En el caso de Bitcoin, los comerciantes ofrecen su propia propiedad a cambio del dinero. Como tal, no hay ninguna titulización implícita de la propiedad. Un comerciante puede

Reference

[1] Capítulo: Taxonomía del dinero

[2] Capítulo: Principio de Reserva

[3] Capítulo: Definición de reserva

dejar de aceptar dinero, lo cual reduce la utilidad del dinero. Esto se puede considerar un riesgo de custodio, pero no una suspensión de pagos ya que comerciante no ha aceptado ninguna obligación de hacer intercambios por el dinero. Según se muestra en Principio de Fragmentación[1], la cambiante aceptación de los comerciantes es la naturaleza de una división.

Según se demuestra en Falacia de la Cadena de Bloques[2], la "tecnología de cadena de bloques" no puede ofrecer ninguna defensa respecto de la suspensión de pagos del custodio. Un activo "tokenizado" es un título. La oportunidad de fraude o robo por el custodio, ya sea de manera directa o por imposición del estado, no se ve reducida. **Al igual que sucede con los dineros mercancía, como el oro, la reducción del riesgo de custodia permitida por Bitcoin no es una consecuencia de la tecnología ni de una obligación contractual, sino del tamaño de su economía.** Irónicamente, el "título" (*security*, en inglés) es lo que es inseguro.

Reference

[1] Capítulo: Principio de Fragmentación

[2] Capítulo: Falacia de la Cadena de Bloques

Error de Hearn

Existe una teoría de que un estado no puede prohibir cosas populares.

Esto implica que el alto volumen de transacciones permite una defensa eficaz contra ataques y coacciones. Esto a su vez implica que Bitcoin puede ser asegurado aceptando la fuerza centralizante de un volumen muy grande de transacciones.

La teoría es inválida, ya que está basada en la observación empírica pero se apoya en un error fáctico. **Es evidente que los estados en realidad prefieren prohibir cosas populares.** A continuación se muestra una breve lista de cosas populares habitualmente prohibidas:

- Drogas
- Juegos de apuestas
- Prostitución
- Religión
- Discursos
- Reuniones
- Intercambios
- Migraciones
- Armas
- Trabajos
- Libros
- Dinero

Este error puede originarse por no aceptar el Axioma de Resistencia[1] al seguir trabajando en Bitcoin. Esto probablemente produzca disonancia cognitiva[2]. La consiguiente búsqueda de alivio puede llevar a este error. Sin embargo, el error termina por volverse innegable, lo cual puede hacer que se deje todo por el enfado[3].

Reference

[1] Capítulo: Axioma de resistencia

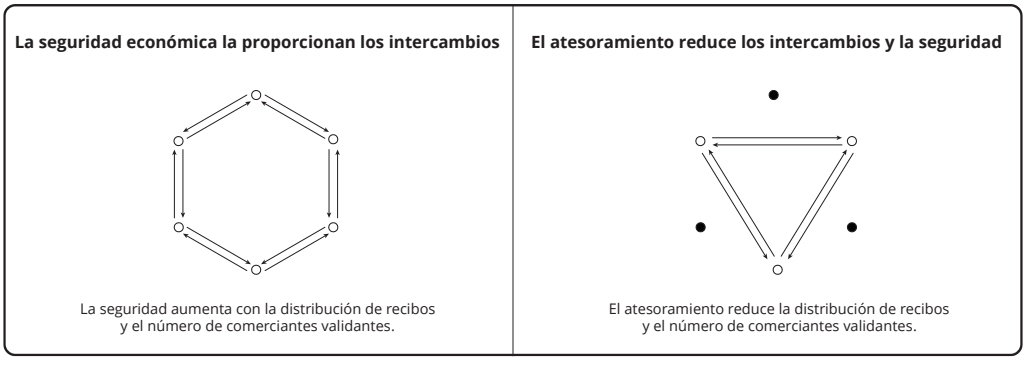
[2] https://en.wikipedia.org/wiki/Cognitive_dissonance

[3] https://en.wikipedia.org/wiki/Wikipedia:Rage_quit

Falacia del Atesoramiento

Existe una teoría de que un mayor nivel de atesoramiento produce un mayor nivel de seguridad en una moneda. Esto se parece a la Falacia del *Dumping*[1] pero no necesariamente se basa en una división.

La supuesta ventaja de seguridad por un nivel elevado de atesoramiento proviene de la teoría de que un propietario tiene voz en la validación y podría actuar para evitar que la economía acepte lo que los propietarios consideran colectivamente dinero inválido. Sin embargo, los propietarios no están actuando salvo que intercambien unidades por algo y, en este caso, es el comerciante el que impone el cumplimiento de reglas de consenso. **La posibilidad de que los propietarios puedan actuar al unísono no aumenta este nivel cero de control. Por consiguiente, la teoría es inválida.**



Un aumento solo se puede expresar en relación con un nivel básico. Si se puede convencer a una persona de que hay una mayor seguridad en el sistema por un mayor nivel colectivo de atesoramiento, la teoría sostiene que la persona podría decidir atesorar más de lo que resultaría óptimo en otro caso (es decir, el nivel básico de la persona). Esto supone un coste individual real con un supuesto beneficio social. En otras palabras, la teoría

Reference

[1] Capítulo: Falacia del *Dumping*

depende de un comportamiento económico irracional, incluso si el beneficio en seguridad fuera real, y, por consiguiente, es inválida.

La teoría implica que menos intercambios en la moneda producirán una mayor seguridad. Esto es lo contrario de lo que sucede. Como se muestra en Modelo de Seguridad Cualitativo[1], la imposición del cumplimiento de una regla de consenso requiere intercambios continuados. El precio de una unidad de la moneda en otra mercancía[2] o dinero es arbitrario pero aumenta temporalmente si se convence a los individuos para que se comprometan con la falacia. Este aumento repercute solamente en beneficio de los propietarios existentes. La teoría de que el precio solo puede aumentar es un error especulativo relacionado, explorado en Falacia Lunar[3]. Incluso un aumento general, perpetuo y demostrable de los precios no validaría esta teoría, ya que estaría relacionada solamente con un aumento temporal relativo causado por decisiones individuales subóptimas desde un punto de vista financiero.

Reference

[1] Capítulo: Modelo de Seguridad Cualitativa

[2] Capítulo: Principio de Inflación

[3] Capítulo: Falacia Lunar

Falacia del Arbitraje entre Jurisdicciones

Existe una teoría en el sentido de que, puesto que es improbable que todos los estados se adhirieran a una prohibición del Bitcoin, la moneda sobreviviría por el movimiento de la minería y demás actividades a estados permisivos.

Aquellos que no cumplan, operan en el mercado negro[1] desde la perspectiva de la autoridad prohibidora. Otro estado que infrinja una prohibición se considera un estado en rebeldía[2] desde esta perspectiva. Una prohibición es una acción política sencilla contra la cual Bitcoin no ofrece ninguna protección.

Existe una falacia relacionada[3] en el sentido de que una acción de este tipo tendría una dificultad imposible en el caso en que Bitcoin fuera popular. Esta es la idea de que Bitcoin está asegurado mediante el voto, lo cual reduce su modelo de seguridad al del status quo del dinero estatal, eliminado la propuesta de valor[4] de Bitcoin.

Por definición, las operaciones en el mercado legal se ven eliminadas por una prohibición. Por consiguiente, la teoría implica que Bitcoin está asegurado en última instancia por la protección de los estados en rebeldía. Esto también se reduce a la seguridad obtenida mediante el voto. Además, los estados poderosos tienen muchas herramientas[5] para forzar a los demás, todas las que hay antes de llegar a la guerra abierta, e incluso la guerra abierta. Estas herramientas se emplean habitualmente en diversas guerras, como las guerras contra las drogas, el blanqueo de dinero y el terrorismo. Una prohibición del

Reference

[1] https://es.wikipedia.org/wiki/Mercado_negro

[2] https://es.wikipedia.org/wiki/Estado_canalla

[3] Capítulo: Error de Hearn

[4] Capítulo: Propuesta de Valor

[5] https://en.m.wikipedia.org/wiki/United_States_embargoes

Bitcoin podría entrar fácilmente bajo el paraguas de las justificaciones de todos estos conflictos internacionales existentes.

Sin embargo, Bitcoin está diseñado específicamente para funcionar sin permiso de ningún estado. Su funcionamiento continuado como dinero en el mercado negro podría llevar a uno o varios estados a intentar suprimirlo mediante censura[1]. Si bien esto podría intentarlo un estado en solitario, es habitual que los estados colaboren en defensa de la capacidad tributaria[2] de sus divisas. Este es el propósito del Fondo Monetario Internacional[3].

Una acción de este tipo se puede ejecutar con máxima eficacia[4] desde una única ubicación geográfica. En este escenario, los estados en rebeldía no ofrecen ninguna defensa salvo en la medida en que no solamente estén dispuestos a renunciar a la ventaja fiscal de sus propias divisas, sino también a donar impuestos recaudados para resistir a la censura. **No se puede asumir que los estados en rebeldía puedan superar en potencia a la autoridad censora, y depender de ellos en cualquier medida reduce el Bitcoin a un dinero asegurado mediante la política.** Por consiguiente, la teoría es inválida.

Reference

[1] Capítulo: Principio de los Otros Medios

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] https://www.imf.org

[4] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

Principio de los Otros Medios

Bitcoin es un acto de resistencia[1], un intento de "ganar un nuevo territorio de libertad." La libertad se contrae por la presión constante de financiación obligatoria del estado. Típicamente la libertad se expande con el derramamiento de sangre, con el objetivo específico de reducir el poder estatal. Bitcoin no puede eliminar la necesidad de riesgo personal para lograr este objetivo. Sin embargo, mediante la compartición de riesgos[2], podría llegar a reducir el impuesto[3] que constituye la inflación sin derramar sangre. Esto no eliminará la fiscalidad con carácter general; sin embargo, podría reducir el poder estatal al dar mayor visibilidad a los impuestos.

Este conflicto entre el estado y los individuos por el control del dinero[4] recorrerá hasta cuatro fases anticipadas por el modelo de seguridad[5] de Bitcoin. Estas pueden solaparse y variar regionalmente pero cada una de ellas es claramente identificable.

1. Luna de miel
2. Mercado negro
3. Competencia
4. Capitulación

Reference

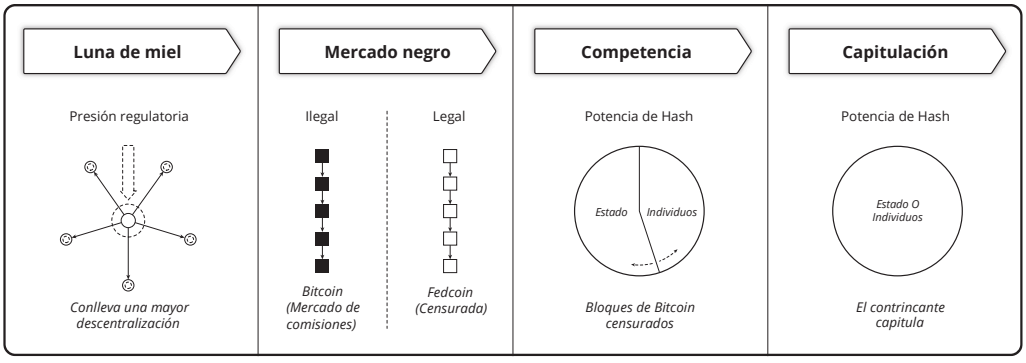
[1] Capítulo: Axioma de resistencia

[2] Capítulo: Principio de la Compartición de Riesgos

[3] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[4] Capítulo: Taxonomía del dinero

[5] Capítulo: Modelo de Seguridad Cualitativa



La fase de luna de miel se caracteriza por el deseo de las agencias estatales de retener el control regulador sobre el movimiento de dinero y títulos. Para tal fin, se aplica presión en puntos de agregación. A medida que aumenta la presión sobre las mineras que hacen *pooling* y los comerciantes centralizados, aumenta el coste y disminuye la utilidad. A continuación, el dinero necesariamente pasa a estar más distribuido para evitar estos gastos.

A medida que se hace evidente que los controles en los puntos de agregación resultan una imposición insuficiente para el cumplimiento, y aflora la conciencia de que el señoreaje[1] está en riesgo, la transacción con Bitcoin y la minería complementaria de Bitcoin se ilegalizan[2]. En la medida en que los estados colaboren para proteger sus divisas, esto podría convertirse en una "Guerra contra el Bitcoin" de carácter global. Esto podría coincidir con la adopción de un nuevo dinero oficial, es decir, Fedcoin[3]. El objetivo sería dar la apariencia de adherirse a un dinero "más seguro" que el Bitcoin al tiempo que se retiene el señoreaje y las ventajas de vigilancia de los sustitutos electrónicos para las divisas estatales.

Reference

[1] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[2] Capítulo: Error de Hearn

[3] Capítulo: Objetivos del Fedcoin

Asumiendo una resistencia suficiente, Bitcoin persistiría con independencia del Fedcoin como dinero en el mercado negro. En este momento, el estado concluye que la única táctica eficaz es competir como minera. Dado que la minería es necesariamente anónima[1], no hay ninguna manera[2] de que la economía evite la participación estatal en la minería. Así, Bitcoin entraría en la fase competitiva[3], con el estado intentando un ataque perpetuo por el 51%.

Aparte de la imposición del cumplimiento continuada desde la fase del mercado negro, la fase competitiva se caracteriza por una batalla pacífica entre el estado y los individuos usando potencias de hash. El estado opera con pérdidas al rechazar las transacciones censuradas. Estas pérdidas se compensan con ingresos fiscales. La presión de las comisiones por las transacciones censuradas aumenta[4] hasta que la subvención fiscal de la minería estatal se compense con ese nivel de comisiones. **Llegados a este punto, aumentan los impuestos y las comisiones por transacciones censuradas hasta que se rinda una de las partes del conflicto.**

De esta manera, Bitcoin puede llegar a ganar una guerra por otros medios[5]. No cabe asumir que esta capitulación sea perpetua. Según está implícito en la Paradoja del Nivel de Amenaza[6], el dinero probablemente circule paulatinamente hasta fases anteriores a medida que disminuya la amenaza.

Reference

[1] Capítulo: Principio de los Datos Públicos

[2] Capítulo: Falacia de la Prueba de Trabajo

[3] Capítulo: Principio de los Otros Medios

[4] Capítulo: Propiedad de resistencia a la censura

[5] https://en.wikiquote.org/wiki/Carl_von_Clausewitz

[6] Capítulo: Paradoja del Nivel de Amenaza

Principio de la Resistencia a las Patentes

Al contrario que los derechos de reproducción (*copyright*), la patente es una fuerza contraria al mercado. Un auténtico *copyright* es un acuerdo contractual entre el comprador y el vendedor en el que la patente constituye exclusivamente una concesión estatal de monopolio[1]. La patente no es un "ataque" por el titular de la patente, es una distorsión que actúa como una presión pro-compartición de recursos[2] y creada por el estado.

El proceso de minería es muy competitivo. La protección de monopolios en el uso de algoritmos[3] eficientes de minado constituye una fuerte presión pro-compartición de recursos contra el mercado. Bitcoin está asegurado por personas que resisten[4] contra las fuerzas anti-mercado. La resistencia asume un mayor riesgo[5] cuando la minera tiene mucha compartición de recursos y/o es no anónima[6].

Si las personas no resisten contra tales fuerzas, no hay seguridad[7] en el dinero. A medida que aumenta el nivel de amenaza[8], la consecuencia de infringir las patentes no supone un riesgo mayor que la propia minería. **Por consiguiente, el impacto de las patentes es irrelevante en lo que respecta a la seguridad del dinero.**

Reference

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/p/1075

[2] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[3] https://patents.google.com/patent/WO2015077378A1

[4] Capítulo: Axioma de resistencia

[5] Capítulo: Principio de la Compartición de Riesgos

[6] Capítulo: Principio de los Datos Públicos

[7] Capítulo: Modelo de Seguridad Cualitativa

[8] Capítulo: Paradoja del Nivel de Amenaza

Principio de Ausencia de Permisos

Bitcoin está diseñado[1] para operar sin permisos de ninguna autoridad. Su propuesta de valor[2] está basada totalmente en esta propiedad.

Un mercado se puede dividir en una categoría con permisos y otra categoría sin permisos desde la perspectiva del estado. Para referirnos a ellas con facilidad, el primero a menudo se denominará "mercado legal" y el segundo, "mercado negro". Los intercambios en el mercado legal, por definición, requieren permisos, y el mercado negro no los requiere.

Por una sencilla cuestión de definición, **las operaciones de Bitcoin no pueden estar en el mercado legal y a la vez estar exentas de permisos.** Cualquier persona que opere en el mercado legal necesita permiso para hacerlo. Por consiguiente, Bitcoin es inherentemente un dinero del mercado negro. Su arquitectura de seguridad necesariamente asume que está operando sin permiso estatal[3].

La seguridad de Bitcoin no se extiende a los sistemas de mercados legales. Cualquier sistema que dependa de la propuesta de valor de Bitcoin también debe estar en el mercado negro.

Reference

[1] Capítulo: Principios Criptodinámicos

[2] Capítulo: Propuesta de Valor

[3] Capítulo: Principio de los Otros Medios

Falacia del Dilema del Prisionero

Existe una teoría en el sentido de que, ante la elección de si adherirse a una prohibición del Bitcoin, los estados individuales se enfrentan a un dilema del prisionero[1]. Una prohibición significativa implica que uno o varios estados (la "prisión") impondrán el cumplimiento de sanciones económicas[2] (al menos) contra otros estados (los "prisioneros") que pudieran pasarse a Bitcoin como divisa de reserva[3].

Asumimos que los prisioneros que pudieran decidirse por utilizar Bitcoin son socios comerciales. En otras palabras, su utilización como divisa de reserva requiere un socio con el que realizar transacciones.

La utilidad ordinal[4] es una implicación del valor subjetivo[5]. No se observan empates[6] en los resultados, lo que implica un dilema fuerte. Se evalúan tanto las suposiciones de conocimiento simétrico como asimétrico.

El resultado si hay una decisión individual pro-Bitcoin (Primo) :

- Sanción económica.
- Sin socios comerciales (que utilicen el dólar).
- Una divisa de reserva inutilizable (no hay socios comerciales).

Reference

[1] https://es.wikipedia.org/wiki/Dilema_del_prisionero

[2] https://www.cfr.org/backgrounder/what-are-economic-sanctions

[3] https://es.wikipedia.org/wiki/Moneda_de_reserva

[4] https://en.wikipedia.org/wiki/Ordinal_utility

[5] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

[6] https://en.wikipedia.org/wiki/Tie_(draw)

El resultado si hay una decisión mutua pro-Bitcoin (Recompensa) :

- Sanción económica.
- Sanción económica del socio comercial.
- Una divisa de reserva no sujeta a la fiscalidad que representa el señoreaje.

El resultado si hay una decisión individual pro-dólar (Tentación) :

- Sin sanción económica.
- Sanción económica del socio comercial.
- Una divisa de reserva sujeta a la fiscalidad que representa el señoreaje.

El resultado si hay una decisión mutua pro-dólar (Castigo) :

- Sin sanción económica.
- Sin sanción económica del socio comercial.
- Una divisa de reserva sujeta a la fiscalidad que representa el señoreaje.

Dilema simétrico fuerte con relaciones ordinales de los resultados

Brasil\Irlanda	Bitcoin	Dólar
Bitcoin	R\R	C\T
Dólar	T\P	C\C

Para que se considere un dilema del prisionero, debe verificarse T > R > C > P, donde:

- T > R y C > P implican que el dólar es la estrategia dominante para cada uno.
- R > C implica que cada uno prefiere la decisión mutua pro-Bitcoin a la decisión mutua pro-dólar.

Podemos concluir que se cumple C > P, ya que la sanción individual implica que no hay pagos internacionales y, por consiguiente, no hay beneficios de una reserva de divisas extranjeras[1], y presumiblemente las sanciones son poco deseables.

Para determinar si se cumplen R > C y T > R, se requiere un método objetivo para relacionar solamente el señoreaje y las sanciones, ya que presumiblemente las sanciones son poco deseables. Esto se puede obtener mediante la observación de que el oro no está sujeto ni a señoreaje[2] ni a sanciones. En otras palabras, el oro proporciona las ventajas anteriormente indicadas del Bitcoin sin las sanciones. Y, sin embargo, no se eligió el oro (y se abandonó anteriormente en favor del dólar), lo que implica que el resultado de la decisión pro-dólar se prefiere al de la decisión pro-oro y, por tanto, a la decisión pro-Bitcoin. Por consiguiente, no se verifica ninguna de las estrategias[3]. **Por consiguiente, no hay dilema.**

Dilema asimétrico fuerte con relaciones ordinales de los resultados

Brasil\Irlanda	Bitcoin	Dólar
Bitcoin	Rf\Rc	Pf\Tc
Dólar	Tf\Pc	Cf\Cc

Para que se considere un dilema del prisionero, debe ser verdadero que Ti > Ri > Ci > Pi (i puede tomar los valores f, de fila, o c, de columna), donde:

- Tf > Rf y Cf > Pf
- Tc > Rc y Cc > Pc

Reference

[1] https://en.wikipedia.org/wiki/Foreign-exchange_reserves

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] https://es.wikipedia.org/wiki/Estrategia_dominante

- Rf > Cf y Rc > Cc

Si se verifican todas estas relaciones, entonces la decisión individual pro-dólar se prefiere a la pro-Bitcoin, y se prefiere la decisión mutua pro-Bitcoin. Dado que estas son las mismas relaciones evaluadas en el escenario simétrico, no hay dilema.

Otras suposiciones

La relación oro-Bitcoin supone que los costes de compensación[1], de transportar el oro y de confirmar el Bitcoin, son despreciables[2] en el contexto de las liquidaciones internacionales. La compensación requiere el movimiento periódico de solo los desequilibrios de pago entre los estados.

> ... cualquier corrección de un desequilibrio económico se aceleraría y normalmente no sería necesario esperar al punto en el que se necesitarían transportar cantidades sustanciales de oro de un país a otro.
>
> *gold.org*

Se ha preferido el dólar al oro a pesar de tener un peso parecido, un tamaño significativamente mayor, y el señoreaje. La relación oro-Bitcoin supone que no hay diferencias en volatilidad y liquidez, aunque el oro objetivamente supera[3] al Bitcoin en ambos aspectos. Dado que el oro y el Bitcoin son dineros estables[4], no se asume ninguna rentabilidad especulativa para ninguno de ellos. Otras propiedades monetarias del oro, del Bitcoin y del dólar se suponen equivalentes o no relevantes para ser divisa de reserva estatal.

Reference

[1] https://es.wikipedia.org/wiki/Compensaci%C3%B3n_(finanzas)

[2] https://www.gold.org/about-gold/history-of-gold/the-gold-standard

[3] https://coinweek.com/bullion-report/bitcoin-vs-gold-10-crystal-clear-comparisons

[4] Capítulo: Propiedad de Estabilidad

Falacia de la Clave Privada

Las claves privadas no aseguran el Bitcoin, aseguran las unidades de Bitcoin. **El control de claves privadas es aplicable a la seguridad individual, no a la seguridad del sistema.** Quienquiera que controle las claves es el propietario, y Bitcoin proporciona seguridad para ese propietario, incluso si se roban las claves. La validación descentralizada asegura el consenso y la potencia de hash mayoritaria distribuida asegura la confirmación, pero la seguridad de las claves privadas es el problema del propietario.

Falacia de la Prueba de Trabajo

Los comerciantes adquieren los servicios de minería que satisfacen sus reglas por una comisión satisfactoria. Existe una teoría que afirma que los servicios de minería están subordinados a estos intercambios. Esta subordinación a veces se describe como "asimetría" o "regla de los usuarios". Esta teoría lleva a personas a creer que la minería se puede realizar con una fuerte compartición de recursos en tanto los comerciantes no estén centralizados, ya que la economía puede controlar el comportamiento de la minería, haciendo que el sistema sea seguro. La consecuencia de esta teoría inválida es la complacencia en relación con la inseguridad causada por la compartición de recursos.

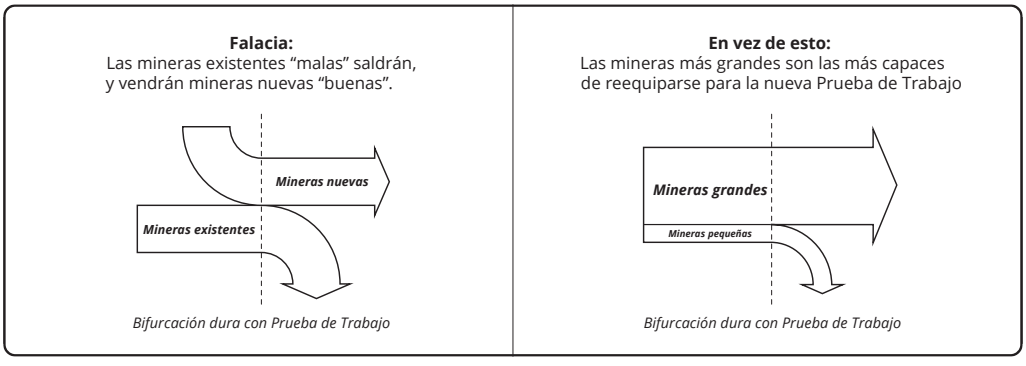
Las mineras controlan la selección de las transacciones, mientras que los comerciantes controlan la propiedad ofrecida a cambio. Si alguna parte de la economía está insatisfecha con las selecciones de las mineras, puede poner su propiedad a la venta en una moneda dividida con una regla de trabajo diferente que deje obsoletos todos los equipos físicos de machacado (*grinding*). Este se describe típicamente como una bifurcación dura con prueba de trabajo.

Según esta teoría, las mineras entonces sufren una pérdida catastrófica a causa de la inversión de capital irrecuperable en equipos físicos muy especializados. La bifurcación dura puede incluir un ajuste de dificultad que permita seguir realizando confirmaciones a pesar de una supuesta caída significativa en la tasa de hash. A causa de la menor dificultad y una supuesta falta de equipos físicos especializados, más individuos son capaces de minar. Esto introduce nuevas mineras en el negocio y reduce la compartición de recursos.

Se ha dicho que esta capacidad de la economía de generar una pérdida de capital en sus socios comerciales constituye una asimetría única en comparación con otros mercados. Por ejemplo, una comunidad que compra manzanas no puede "destruir" sin más los huertos de todos sus proveedores. **La teoría no reconoce que no hay ninguna asimetría**

en los intercambios. Si los compradores deciden que no van a comprar manzanas de los huertos existentes, ciertamente pueden hacerlo.

De manera análoga, los huertos tienen la opción de no venderlas. El precio es la resolución continua de esta tensión. Esta es exactamente la misma dinámica que existe en cualquier mercado.



La teoría tampoco considera la ausencia de identidad. Supone que la pérdida de capital hará que salgan las mineras "malas" que haya y que entren las mineras "buenas". Esto es una suposición no defendible. No hay ninguna razón para creer que las mineras existentes saldrán ni hay ninguna razón para creer que las nuevas mineras no tomarían las mismas decisiones que las mineras anteriores dado que están en el mismo negocio, suponiendo siquiera que uno pudiera notar la diferencia. Al menos en el escenario de las manzanas, uno sabe a quién le está comprando manzanas y puede discriminar; esto no es posible en Bitcoin.

La teoría tampoco considera la economía de la minería. Hay una ventaja en favor de la proximidad[1] que produce una mayor rentabilidad del capital para las mineras con mayor potencia de hash. Por consiguiente, las mineras más grandes son más rentables que las

Reference

[1] Capítulo: Fallo Lógico de la Prima de Proximidad

mineras pequeñas. Por tanto, las mineras más grandes estarán mejor capitalizadas que su competencia de menor tamaño. Cuando se produce el cambio de regla, las mineras que permanezcan serán aquellas que puedan permitirse los reequipamientos, que serán las más grandes.

Es irracional suponer que todas las mineras se irán sin más. ¿Esperaríamos que todos los productores de manzanas fueran sustituidos por nuevos productos de manzanas? ¿En la minería, no resultan ventajas importantes sobre los recién llegados la experiencia técnica, las instalaciones, los contratos de energía, los procesos y la maquinaria no especializada? Las mineras existentes tienen una ventaja inherente respecto de sus supuestos sustitutos. Esto significa que tienen un mayor acceso a capital. Por tanto, no solo las mineras más grandes terminan teniendo menos competencia, sino que todas las mineras existentes que permanezcan tienen una ventaja sobre las mineras nuevas.

La teoría tampoco considera que los comerciantes necesitan minería. La minería no se sustituye mediante división, y retiene el control completo de la selección de transacciones. Así, por ejemplo, si las mineras "malas" resultan ser estados que están atacando a la moneda, el propio estado y las mineras cooptadas continuarán con la misma perturbación, a un menor coste energético. Puesto que las demás mineras fracasan debido a lo que efectivamente constituye un impuesto del 100%, el coste energético del atacante sigue disminuyendo. Mediante la división no se pueden producir servicios de minería que sean "buenos" para los comerciantes.

Por último, la teoría no reconoce las consecuencias de los seguros. Sobre la base de toda la pérdida anterior de capital experimentada por todas las mineras de una moneda dada, todas las mineras futuras de su sustituta se asegurarán contra la posibilidad de un evento parecido. Puede que se aseguren por sí mismos, pero el aumento de coste es inevitable. Esto reducirá la tasa de hash para la misma comisión hasta que la posibilidad de tal evento se considere despreciable. Así, la economía reduce su propia seguridad contra gastos por duplicado y termina teniendo las mismas mineras y una mayor compartición de recursos. Esto conforma una reducción de seguridad a dos niveles, sin beneficio alguno.

Principio de los Datos Públicos

Del Principio de Compartición de Riesgos[1] se desprende que la seguridad del sistema depende de la minería encubierta y de los intercambios. Una moneda existe como un mercado en beneficio mutuo[2] entre las mineras y los comerciantes para la confirmación de transacciones dentro de bloques a cambio de comisiones.

Las actividades necesariamente encubiertas se enumeran por cada rol:

Minera

- obtener bloques [sobre los que basarse]
- obtener transacciones no confirmadas [de las que cobrar comisiones]
- crear y distribuir bloques [para hacer que otros se basen en ellos]
- recibir pagos por confirmaciones [para financiar operaciones]

Comerciante

- obtener bloques [para validar pagos de clientes]
- obtener transacciones no confirmadas (opcional) [para anticipar pagos y comisiones]
- crear y distribuir transacciones [para obtener pagos de clientes]
- realizar pagos de confirmaciones [para compensar la confirmación]

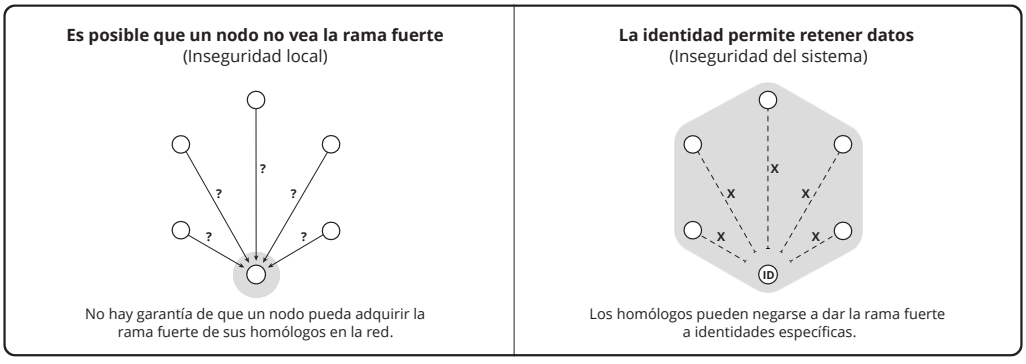
Si los bloques no se pueden obtener de manera anónima, el sistema es inseguro. La incapacidad de obtener los bloques más fuertes disponibles para otras personas es una

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

[2] Capítulo: Falacia del Equilibrio de Poder

partición de la red, lo cual implica una inseguridad localizada. Sin embargo, ni el anonimato, ni su opuesto (la identidad), pueden garantizar que uno vea la rama más fuerte en cualquier momento dado. En otras palabras, cualquier intento de mitigar la partición con la introducción de identidad es una falsa elección[1] que sacrifica la seguridad del sistema por la falsa promesa de garantizar seguridad localizada.



No es esencial que todas las mineras o comerciantes vean todas las transacciones en cualquier momento dado. Sin embargo, una visibilidad amplia es preferible ya que produce la competencia más robusta por las comisiones y la mejor información adelantada. En

otras palabras, un mercado en el que cada participante ve todas las transacciones todo el tiempo es un mercado perfecto[2]. Pedir transacciones específicas a la red, y no todas (ni información resumida sobre todas), es una fuente de contaminación y también tiene que evitarse en aras de la seguridad.

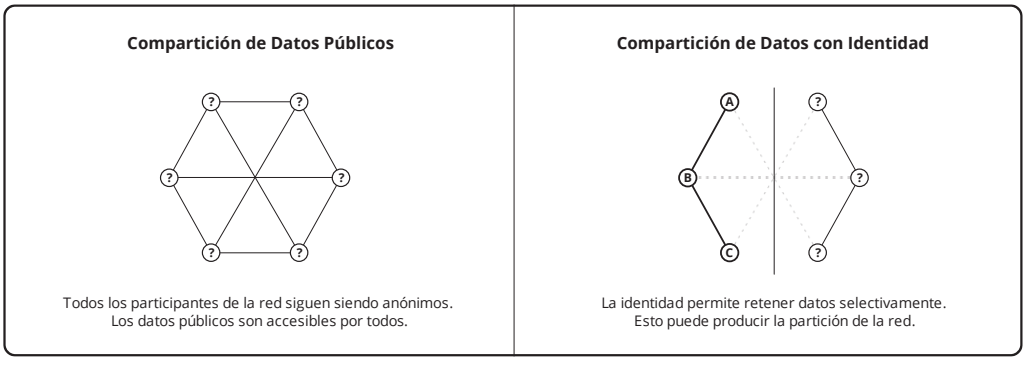
La creación de bloques y transacciones no expone la identidad de forma inherente; sin embargo, la distribución pública de cualquiera de ellos es la fuente principal de

Reference

[1] https://es.wikipedia.org/wiki/Falso_dilema

[2] https://es.wikipedia.org/wiki/Competencia_perfecta

contaminación. En la medida en que las mineras se autoidentifiquen abiertamente, están basándose en la presunción de un entorno de amenaza baja[1], no contribuyendo a la seguridad del sistema. Evitar la contaminación al diseminar los bloques y las transacciones requiere utilizar una conexión[2] anónima a un servidor de la comunidad. Esto garantiza que la red de distribución nunca tenga acceso a información identificativa.



La Prueba de Trabajo preserva el anonimato de las mineras. No hay ninguna firma asociada a la minería y la energía se presupone que es ubicua. De manera análoga, la capacidad de realizar pagos anónimos por la confirmación es la razón por la que se incluyen las comisiones de transacción. Es suficiente[3] pagar directamente a una minera (fuera de la cadena) por la confirmación; sin embargo, esto expone recíprocamente al comerciante y a la minera, y dificulta la estimación anónima de comisiones.

Bitcoin es novedoso en el sentido de que todas las transacciones financieras pueden ser validadas a partir de datos públicos y sin identidad. Los sistemas financieros centralizados se basan o bien en la confirmación en conexiones (criptográficamente identificables) a otros, o la confianza en firmas (verificables criptográficamente) en datos transmitidos. Esta es la esencia de los sistemas basados en la confianza; ciertas

Reference

[1] Capítulo: Paradoja del Nivel de Amenaza

[2] https://en.wikipedia.org/wiki/Anonymizer

[3] Capítulo: Falacia de las Comisiones Aparte

autoridades tienen secretos que los demás utilizan para verificar esa autenticidad. **La razón de la validación reside en eliminar el uso de la identidad y, por consiguiente, de la autoridad.**

Modelo de Seguridad Cualitativa

Modelo de descentralización

En Principio de la Red Social[1] se muestra que Bitcoin es una red de relaciones humanas. Esto se puede modelar como un grafo dirigido[2] en el que cada vértice representa un comerciante y cada arista representa un intercambio por Bitcoin. Las aristas indican la dirección del movimiento de la moneda y se cuantifican con el número de unidades intercambiadas. Se supone que todos los propietarios habrán sido comerciantes en el momento de recibir la moneda, incluyendo como mineras (vendiendo confirmaciones) y como receptores de donaciones caritativas (vendiendo benevolencia/fondo de comercio[3]).

Si una persona no está aceptando una moneda personalmente, o no valida personalmente la moneda aceptada, la persona no puede rechazar una moneda inválida. La persona está confiando esta tarea a una autoridad central. **Todas las personas que utilizan el mismo delegado se reducen a un mero vértice que representa al delegado.**

Durante cualquier periodo, la seguridad económica es función del número de comerciantes y la similitud de los importes intercambiados. La economía más fuerte sería la de todas las personas del mundo comerciando el mismo número de unidades en ese periodo, un ideal que puede llamarse una economía "distribuida" (o totalmente descentralizada). La más débil sería la de un delegado que aceptara todas las unidades intercambiadas en ese periodo, lo cual sería una economía "centralizada".

Reference

[1] Capítulo: Principio de la Red Social

[2] https://es.wikipedia.org/wiki/Grafo#Grafo_dirigido

[3] https://es.wikipedia.org/wiki/Fondo_de_comercio

Más específicamente, el sistema más descentralizado económicamente es el que tenga el mayor número de vértices (comerciantes) con el menor coeficiente de variación[1] en las aristas entrantes (recibos). Definiendo una función de distribución como la inversa del coeficiente de variación, obtenemos:

```
descentralización-económica = distribución(recibos) * comerciantes
```

De manera parecida a la seguridad económica, la seguridad de confirmación se puede modelar como un grafo[2] sin aristas. Cada minera está representada con un vértice en el grafo. Una machacadora no es una minera ya que la machacadora no tiene capacidad de tomar decisiones, solo está representada la minera. La potencia de hash total empleada por una minera es el peso del vértice.

Durante cualquier periodo, la seguridad de la confirmación es función del número de mineras y la similitud de la potencia de hash que dirigen. La resistencia más fuerte a la censura sería la de todas las personas del mundo minando con la misma potencia de hash en ese periodo, un ideal que puede llamarse una confirmación "distribuida" (o totalmente descentralizada). La más débil sería la de una minera con un 100% de potencia de hash, lo cual sería una confirmación "centralizada".

Más específicamente, el sistema está más descentralizado en la confirmación que tenga el mayor número de vértices (mineras) con la máxima distribución en los pesos (potencia de hash):

```
descentralización-confirmación = distribución(potencia-hash) * mineras
```

Reference

[1] https://es.wikipedia.org/wiki/Coeficiente_de_variaci%C3%B3n

[2] https://es.wikipedia.org/wiki/Grafo_nulo

Modelo de seguridad

La descentralización por sí sola no es seguridad. La seguridad es el producto de la actividad, la distribución de esa actividad, y la fracción de la humanidad que participa.

```
seguridad = actividad * distribución * participación
```

Dado que no hay límite en la humanidad, los intercambios o los cálculos, el nivel de seguridad en cada eje es ilimitado. La seguridad también es ilimitada con distribución perfecta (es decir, descentralización infinita). Un nivel mínimo de cero en cada uno se logra o bien sin participación o sin actividad. Así, la seguridad económica y de confirmación se puede definir como:

```
seguridad-económica = recibos * distribución(recibos) * [comerciantes /
humanidad]

seguridad-confirmación = potencia-hash * distribución(potencia-hash) *
[mineras / humanidad]
```

Límites del modelo

Estas relaciones no dicen nada sobre la eficacia absoluta representada por cualquier valor, ni la eficacia relativa de dos valores cualesquiera salvo que un valor mayor representa una eficacia mayor. Esto no se debe a una deficiencia del modelo. Los factores incluyen a personas, específicamente la eficacia de sus capacidades individuales para resistir[1] y su percepción de valor en el dinero. Todos los que validan o minan ofrecen cierto nivel de resistencia, pero no hay una continuidad implícita. Nos referimos a un "nivel" de seguridad, no a una "cantidad" de seguridad.

Reference

[1] Capítulo: Axioma de resistencia

Según se mostró en Principio de los Datos Públicos[1], el anonimato es una herramienta que ayuda a defender la capacidad propia de realizar intercambios y/o minar. Por tanto, el nivel de descentralización nunca puede ser medido; el modelo es una ayuda conceptual. Según se mostró en Falacia del Equilibrio de Poder[2], la seguridad que se puede permitir cada uno de los dos submodelos es complementaria e independiente del otro. Si bien las personas podrían decidir realizar intercambios y/o minar de manera independiente en el futuro, la Falacia de las Cucarachas[3] muestra que no están contribuyendo a la seguridad hasta que lo hacen. El modelo representa la seguridad que existe en ese periodo.

Reference

[1] Capítulo: Principio de los Datos Públicos

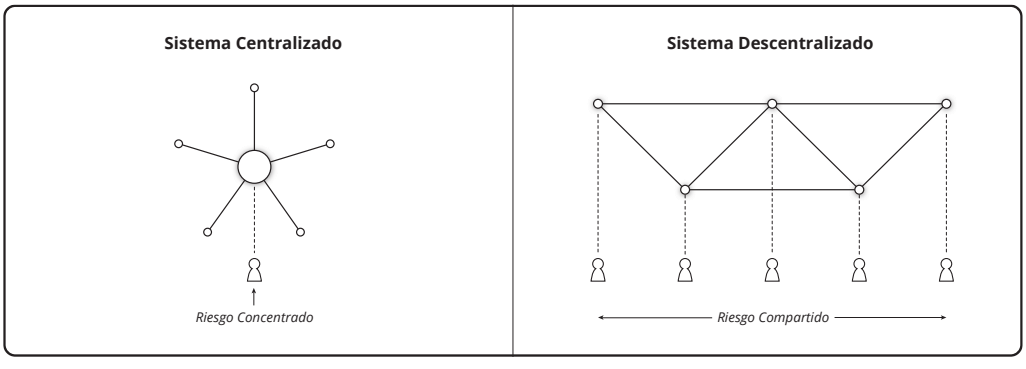
[2] Capítulo: Falacia del Equilibrio de Poder

[3] Capítulo: Falacia de las Cucarachas

Principio de la Compartición de Riesgos

Bitcoin no está asegurado por cadenas de bloques[1], potencia de hash, validación, descentralización, criptografía[2], código abierto[3] ni teoría de juegos[4]: está asegurado por personas.

La tecnología nunca es la raíz de la seguridad del sistema. La tecnología es una herramienta para ayudar a las personas a proteger lo que valoran. La seguridad exige que las personas actúen. Un servidor no se puede proteger mediante un cortafuegos si no hay una cerradura en la puerta a la sala de servidores, y una cerradura no puede proteger la sala de servidores sin un guardia que vigile la puerta, y un guardia no puede proteger la puerta sin riesgo de daño físico.



Bitcoin no es distinto, está protegido por personas que asumen un riesgo físico. Compartir este riesgo con otras personas es el propósito de la descentralización. Un

Reference

[1] https://es.wikipedia.org/wiki/Cadena_de_bloques

[2] https://es.wikipedia.org/wiki/Criptograf%C3%ADa

[3] https://es.wikipedia.org/wiki/Software_libre_y_de_c%C3%B3digo_abierto

[4] Capítulo: Falacia del Dilema del Prisionero

sistema centralizado[1] requiere que una persona[2] asuma todo el riesgo. Un sistema descentralizado divide el riesgo entre individuos[3] que componen la seguridad del sistema. Los que no entienden el valor de la descentralización muy probablemente no entiendan el papel necesario[4] que desempeñan las personas en la seguridad.

Bitcoin permite que las personas compartan el riesgo personal de aceptar monedas y minarlas. Solamente la voluntad y la capacidad de estas personas de resistir[5] es lo que puede evitar la coacción de sus nodos y la cooptación de sus minas, y esto es lo que realmente asegura al Bitcoin. Si las personas no aceptan estos riesgos, no hay ninguna seguridad efectiva en el dinero. Si muchísimas personas lo hacen, se minimiza el riesgo individual. El Bitcoin es una herramienta, no magia.

Reference

[1] https://en.wikipedia.org/wiki/Liberty_Reserve

[2] https://en.wikipedia.org/wiki/Ross_Ulbricht

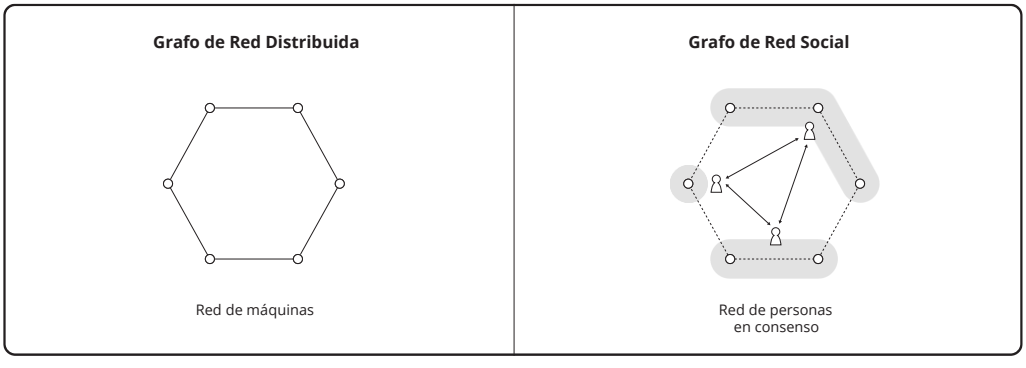
[3] https://es.wikipedia.org/wiki/BitTorrent

[4] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177

[5] Capítulo: Axioma de resistencia

Principio de la Red Social

En la terminología del artículo de Paul Baran de 1964 acerca de las redes distribuidas[1], la importancia de la topología en el diseño de redes es la capacidad de las comunicaciones de resistir la pérdida de un cierto número de nodos. Una red centralizada (en estrella) fallará con la pérdida de un nodo. Una red distribuida (malla) es más resistente. Un híbrido de estos sistemas se considera descentralizado.



En tanto que dinero, Bitcoin forma un grafo social. Solo una persona puede decidir si acepta un dinero[2] u otro en intercambios. Un conjunto de personas que comparten la misma definición de un dinero se denomina un consenso. La autoridad en un sistema monetario es el poder de definir el dinero. Bitcoin es una herramienta que pueden utilizar las personas para defenderse de la tendencia hacia la autoridad, con el fin de preservar su acuerdo y, por consiguiente, la utilidad que hay en el dinero.

En la terminología de los sistemas distribuidos, un "nodo" de Bitcoin es una persona y el sistema es dinero. No importa cuántas máquinas controle la persona, la pérdida de esa

Reference

[1] http://web.cs.ucla.edu/classes/cs217/Baran64.pdf

[2] Capítulo: Taxonomía del dinero

persona es la pérdida de un nodo en el sistema (incluidas todas las máquinas de la persona).

Un dinero centralizado no puede resistir la pérdida de una persona. Si esa única persona cambia sus reglas, el dinero original deja de existir. Según se muestra en Principio de Compartición de Riesgos[1], Bitcoin se basa en la descentralización para permitir que las personas resistan[2] a la autoridad. Esta descentralización hace que el dinero sea capaz de resistir la pérdida de más personas cuando se enfrenta a ataques estatales. Una pérdida en este sentido consiste en que la persona rechace realizar intercambios en ese dinero.

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

[2] Capítulo: Axioma de resistencia

Paradoja del Nivel de Amenaza

Según implica la Propiedad de la Suma Nula[1], presumiblemente la única forma de derrotar el subsidio externo es minar con una pérdida de capital en relación con el rendimiento del capital en el mercado. De manera similar, parece que la única forma de derrotar los impuestos, hasta e incluyendo un impuesto del 100% (prohibición), es minar más allá del alcance de la autoridad fiscal, por ejemplo en secreto. Como pasa con todos los mercados negros[2], hay un aumento de coste por la minería subversiva[3]. Competir contra la minería subsidiada multiplica el coste.

Si uno acepta el Axioma de Resistencia[4], uno tiene que asumir que tanto la fiscalidad como el subsidio se utilizarán para reducir el coste de controlar el Bitcoin. Utilizando el poder de subsidiar la minería (mediante ingresos fiscales), los estados pueden producir compartición de recursos en la región del subsidio. Una vez que la potencia de hash mayoritaria se haya concentrado, el estado puede utilizar su poder fiscal (regulador) en la región para forzar la censura.

Por consiguiente, para disfrutar de las ventajas de un Bitcoin, pareciera que las personas finalmente tendrían que minar con pérdidas. No obstante, la censura crea la oportunidad de que otros minen con beneficios en la medida en que las personas estén dispuestas a compensar este coste con comisiones. Este mercado negro es la resistencia a la censura de Bitcoin.

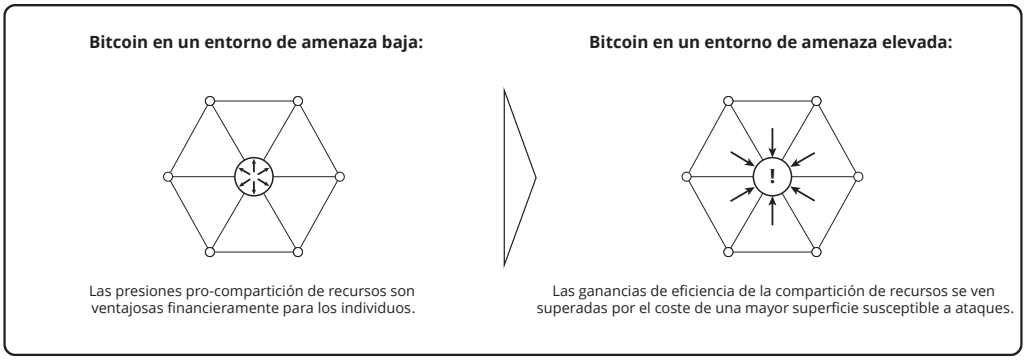
Reference

[1] Capítulo: Propiedad de la Suma Nula

[2] https://es.wikipedia.org/wiki/Mercado_negro

[3] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177

[4] Capítulo: Axioma de resistencia



Las personas pagan un precio más alto por ciertas transacciones, y con el fin de mantener ese precio más alto, el estado también tiene que sufrir los gastos, a pesar de su ineficacia.

Paradójicamente, esta herramienta funciona bien cuando el dinero está siendo atacado y mal cuando no. Si no hubiera una presión pro-compartición de recursos[1] *interna*, estos casos se equilibrarían. Pero la distribución del riesgo[2] resulta esencial para la minería subversiva, y la presión pro-compartición de recursos actúa en sentido *contrario* a la distribución. Por consiguiente, existe una superficie de ataque[3] cada vez mayor sin presión para reducirse salvo que se supriman las alternativas monetarias eficaces. La supresión[4] de las alternativas aumenta la utilidad de la recompensa a la minera en la región de supresión. La paradoja también es aplicable a las presiones pro-centralización[5].

La consecuencia esperada es que Bitcoin no estará bien preparado para ataques porque resulta desventajoso financieramente para las personas en un entorno de amenaza baja.

Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[2] Capítulo: Principio de la Compartición de Riesgos

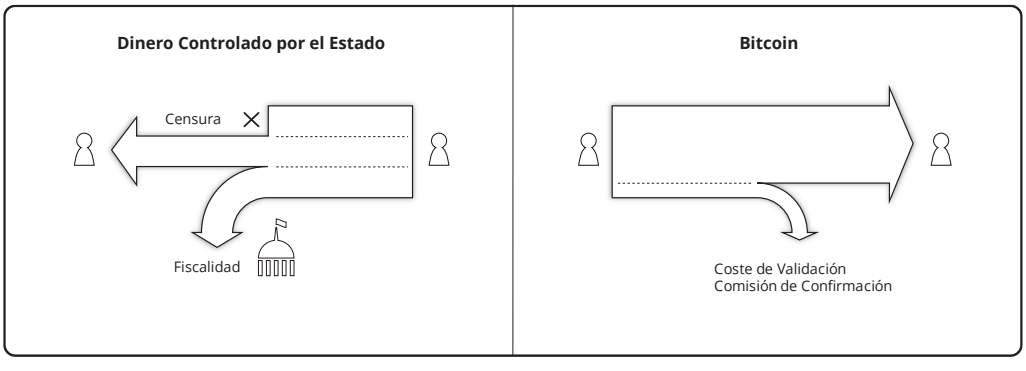
[3] https://en.wikipedia.org/wiki/Attack_surface

[4] https://en.wikipedia.org/wiki/Foreign_exchange_controls

[5] Capítulo: Riesgo de Centralización

Propuesta de Valor

El valor de Bitcoin respecto de sus alternativas se desprende directamente de quitar al estado del control tanto sobre la oferta monetaria como sobre la censura de transacciones. Las ventajas incluyen ser libres de señoreaje[1], controles[2] cambiarios, y vigilancia financiera[3]. Estas permiten que el dinero sea transferido a cualquier persona, en cualquier lugar y momento, sin necesidad de permisos de terceros.



Estas ventajas representan una reducción de costes al evitar impuestos. El señoreaje es directamente un impuesto, mientras que los controles cambiarios limitan la evasión del mismo. El propio estado a menudo proclama la independencia política[4] como objetivo en aras de limitar esta capacidad fiscal. La vigilancia financiera limita la evasión fiscal con carácter más general. **Si bien Bitcoin no puede eliminar los impuestos, y ni siquiera reducir las recaudaciones totales, sí representa un cambio en la naturaleza de la fiscalidad.** En cualquier caso, para quienes consideran al Estado como un bien social, queda la opción de financiarlo voluntariamente.

Reference

[1] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[2] https://en.m.wikipedia.org/wiki/Foreign_exchange_controls

[3] https://en.m.wikipedia.org/wiki/Know_your_customer

[4] https://www.federalreserve.gov/faqs/about_12799.htm

Sería un error asumir que estas ventajas emanan de la existencia de una tecnología más eficiente que la empleada por los dineros monopolísticos[1]. La tecnología es mucho menos eficiente[2], pero ayuda a que las personas[3] resistan contra los controles estatales. Esta resistencia[4] es lo que proporciona el valor.

Reference

[1] Capítulo: Taxonomía del dinero

[2] Capítulo: Principio de Escalabilidad

[3] Capítulo: Principio de la Compartición de Riesgos

[4] Capítulo: Axioma de resistencia

ESTATISMO

Objetivos del Fedcoin

Según implica Propuesta de Valor[1], hay dos aspectos del Bitcoin que lo ponen en la diana de los controles estatales; ambos constituyen amenazas a los ingresos fiscales.

Al combatir[2] el Bitcoin, el estado puede tratar de introducir un dinero[3] cosméticamente parecido, al que nos podemos referir como Fedcoin. Este podría introducirse como una división o como una moneda alternativa. El objetivo sería preservar los aspectos superficiales del Bitcoin al tiempo que se elimina su propuesta de valor. Esto protegería los ingresos fiscales al tiempo que permite que sus promotores hagan propaganda del Fedcoin como una alternativa "más segura" al Bitcoin. El Fedcoin en sí mismo no es relevante para el Bitcoin salvo en la medida en que el acto de obligar a utilizarlo exija resistencia[4].

Las distinciones esenciales del Fedcoin respecto del Bitcoin permiten que el estado cree arbitrariamente nuevas unidades (señoreaje[5]) y deniegue transferencias (censura). El objetivo del señoreaje se puede lograr mediante una bifurcación dura que introduzca una nueva regla de consenso. Esta regla permite que se introduzcan nuevas unidades en el caso en el que el estado haya firmado una transacción inflacionista. El objetivo de censura se puede lograr mediante una bifurcación blanda que excluya de antemano la confirmación de transacciones que no tengan la firma estatal.

Evitar que el estado obligue a utilizar estas bifurcaciones es el propósito central de la seguridad del sistema de Bitcoin. La economía protege de la bifurcación dura y las

Reference

[1] Capítulo: Propuesta de Valor

[2] Capítulo: Principio de los Otros Medios

[3] Capítulo: Taxonomía del dinero

[4] Capítulo: Axioma de resistencia

[5] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

mineras protegen de la bifurcación blanda. Los riesgos[1] asumidos por estas personas preservan el valor del dinero respecto de las alternativas controladas por el estado.

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

Falacia de la Calidad Inflacionista

Existe una teoría que afirma que la inflación de precios[1] causada por el señoreaje[2] hace que se produzcan bienes de menor "calidad" y/o menos duraderos[3]. La durabilidad es una de muchas calidades que una persona podría valorar en un bien para preferirlo a otro**. La teoría presupone necesariamente que el valor es objetivo y, por consiguiente, contradice la teoría subjetiva del valor.** Por consiguiente, la teoría es inválida.

No existe ninguna relación demostrable entre el número de unidades de dinero[4] requeridas para obtener un bien en un intercambio y las calidades de un bien que uno pudiera preferir. Una mayor riqueza (lo cual constituye una percepción, ya que el valor es subjetivo[5]), implica una menor preferencia temporal[6], según implica la teoría de la utilidad marginal[7]. Sin embargo, incluso con la suposición de un percepción errónea de riqueza creciente, una menor preferencia temporal no implica una preferencia por los bienes de menor "calidad". Solamente implica una mayor disposición a prestar una mayor porción del capital de uno. Rothbard[8] comete este "sutil" error en *What Has Government Done to Our Money (Qué le ha hecho el gobierno a nuestro dinero)*[9], un error que sigue siendo perpetuado.

Reference

[1] https://es.wikipedia.org/wiki/Inflaci%C3%B3n

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] Capítulo: Principio de Depreciación

[4] Capítulo: Taxonomía del dinero

[5] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

[6] Capítulo: Falacia de la Preferencia Temporal

[7] https://es.wikipedia.org/wiki/Utilidad_marginal

[8] https://es.wikipedia.org/wiki/Murray_Rothbard

[9] https://mises.org/library/what-has-government-done-our-money/html/p/81

> La calidad del trabajo declinará en caso de inflación por una razón más sutil: las personas se enamoran de los planes para "enriquecerse rápidamente", aparentemente a su alcance en una era de precios en constante aumento, y a menudo desdeña el esfuerzo sobrio.
>
> *Murray Rothbard: What has Government Done to Our Money*

Se supone, y ciertamente lo supone Rothbard, que las personas *siempre* prefieren enriquecerse antes que después, según implica el axioma de la preferencia temporal. Y según muestra la Hipótesis de Fisher[1], en la medida en que la inflación de precios es predecible se compensa en el tipo de interés real[2]. En la medida en que no es predecible, la conjetura de Rothbard no es aplicable.

El señoreaje es un impuesto, lo cual empobrece a las personas. Ser más pobre *aumenta* la preferencia temporal, el efecto opuesto descrito por la teoría. Todo impuesto traslada propiedad involuntariamente de unas personas a otras personas, ya que ese es su único mecanismo y objetivo real, respectivamente. Según desarrolla el propio Rothbard en su *Man, Economy and State (Hombre, Economía y Estado)*[3], la forma del impuesto es económicamente irrelevante.

> Por todos estos motivos, el objetivo de una fiscalidad uniforme resulta imposible. No es que sea sencillamente difícil de lograr en la práctica; es conceptualmente imposible y contradictoria consigo misma.
>
> *Murray Rothbard: Man, Economy and State*

Por consiguiente, ni siquiera se puede demostrar que el propio señoreaje empobrezca más a los afectados que los impuestos que presumiblemente sustituya. Solo un aumento neto en la fiscalidad implica una reducción en la riqueza.

Reference

[1] https://en.m.wikipedia.org/wiki/Fisher_hypothesis

[2] https://es.wikipedia.org/wiki/Tipo_de_inter%C3%A9s_real

[3] https://mises.org/library/man-economy-and-state-power-and-market/html/ppp/1393

Principio de Reserva

El término "reserva"[1] se refiere a un atesoramiento de capital, distinto de la porción de ahorros que se invierte. Tanto los estados como las personas atesoran capital para satisfacer los requisitos de liquidez esperados. El término "moneda de reserva"[2] se refiere a un atesoramiento estatal, requerido para la liquidación[3] de cuentas con otros estados. Las reservas dinerarias de las personas dentro de un estado generalmente están compuestas por el dinero emitido por el estado – principalmente pagarés o dinero fiduciario, con una cantidad menor en moneda[4].

Los estados compran la divisa de reserva a personas mediante el dinero monopolístico[5], los controles[6] cambiarios y la fiscalidad directa. Utilizar su propio dinero descuenta las compras en la cantidad del señoreaje[7]. Los controles cambiarios restringen o prohíben el uso de la divisa de reserva como dinero. Al tratar la divisa de reserva como propiedad pero no como dinero, el estado crea un impuesto en la aparente ganancia[8] de capitales del dinero de reserva cuando devalúa su dinero[9] contra el dinero de reserva a través de la inflación monetaria[10]. Las tasas de cambio[11] oficiales por debajo del valor de mercado crean otro impuesto sobre el uso de la divisa de reserva.

Reference

[1] Capítulo: Definición de reserva

[2] https://es.wikipedia.org/wiki/Moneda_de_reserva

[3] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)

[4] https://es.wikipedia.org/wiki/Dinero_mercanc%C3%ADa

[5] Capítulo: Taxonomía del dinero

[6] https://en.wikipedia.org/wiki/Foreign_exchange_controls

[7] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

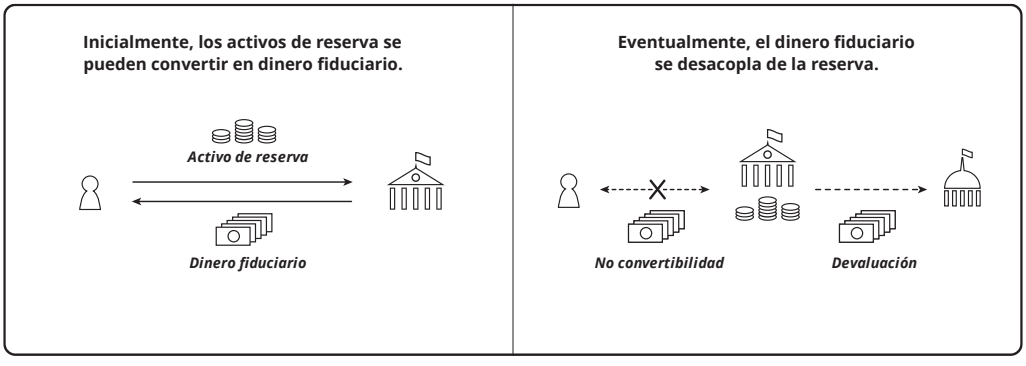
[8] https://www.investopedia.com/articles/personal-finance/081616/understanding-taxes-physical-goldsilver-investments.asp

[9] https://es.wikipedia.org/wiki/Inflaci%C3%B3n

[10] https://en.wikipedia.org/wiki/Monetary_inflation

[11] https://en.wikipedia.org/wiki/Exchange_rate#Parallel_exchange_rate

Un “patrón oro” es uno en el que el estado recauda oro como reserva de divisa extranjera, y los individuos acumulan reservas en derechos reclamables a una cantidad “estandarizada”. El dólar estadounidense fue establecido[1] como canjeable por oro a 20,67$ por onza en 1834. Durante 100 años, el estado compró y vendió oro a esta cotización. En 1934, el dólar se devaluó[2] un 60% hasta 35$ por onza. En ese momento se abolió su canjeabilidad (por las personas), y se ilegalizó que lo atesoraran o que lo utilizaran en contratos. Esta no canjeabilidad se amplió[3] a los demás estados en 1971, lo que puso fin oficialmente al patrón oro en los Estados Unidos. El dólar, que ya había dejado de ser una deuda del estado, pasó de ser una divisa representativa[4] (es decir, un pagaré) a un dinero fiduciario.



La principal reserva monetaria internacional de los EE.UU. es el oro[5] (74,5%), estando el resto en divisa extranjera y equivalentes, si bien los ciudadanos acumulan reservas principalmente en dólares. En general, los propios billetes del estado o el dinero fiduciario no se pueden utilizar como su propia reserva monetaria internacional, ya que el estado puede derogar o devaluar su pago.

Reference

[1] https://en.wikipedia.org/wiki/Coinage_Act_of_1834

[2] https://en.wikipedia.org/wiki/Gold_Reserve_Act

[3] https://es.wikipedia.org/wiki/Nixon_Shock

[4] https://es.wikipedia.org/wiki/Dinero_representativo

[5] https://es.wikipedia.org/wiki/Reserva_de_oro

El Tesoro estadounidense informa de que atesora[1] más de 8.000 toneladas métricas de oro, con un valor aproximado de 400.000 millones de dólares. El poder adquisitivo del billete de dólar estadounidense en 1834 era unas 30 veces mayor al del dólar estadounidense fiduciario de 2019.

El propósito de una divisa de reserva es la imposición fiscal. El estado primero compra el dinero de reserva con pagarés[2] negociables, posteriormente emite más pagarés que el dinero que tiene en reserva, y luego abole los pagarés y mantiene la reserva. La devaluación de los pagarés es el resultado de una emisión excesiva (señoreaje) y constituye un impuesto sobre las personas que los atesoren. El estado recauda el dinero de reserva atesorándolo, y esta reserva atesorada representa su capacidad de liquidar sus propias deudas con otros estados. Si bien la gente sigue atesorando el dinero de reserva, está sujeto a restricciones[3] de uso onerosas con el fin de preservar el beneficio fiscal del dinero monopolístico del estado. Estas restricciones se endurecen a medida que aumenta el nivel de la fiscalidad.

El uso del oro como reserva estatal no ofrece ninguna ventaja monetaria a los individuos, que deberían seguir comerciando en el dinero monopolístico. Según se demuestra en Falacia de la Divisa de Reserva[4], el Bitcoin como reserva estatal no supondría una mejora en este aspecto. Sin embargo, al contrario que el oro, la definición del Bitcoin está en manos de las personas que lo aceptan en intercambios. Con el grueso de la aceptación real del bitcóin en manos del estado, con las personas comerciando en sustitutos[5] dinerarios,

Reference

[1] https://www.treasury.gov/resource-center/data-chart-center/IR-Position/Pages/01042019.aspx

[2] https://es.wikipedia.org/wiki/Pagar%C3%A9

[3] https://www.reuters.com/article/us-venezuela-economy/venezuela-loosens-currency-exchange-controls-to-allow-forex-trading-idUSKCN1SD2NC

[4] Capítulo: Falacia de la Divisa de Reserva

[5] https://wiki.mises.org/wiki/Money_substitutes

no hay nada que limite la capacidad del estado de introducir tanto una inflación como una censura arbitrarias.

Falacia de la Divisa de Reserva

Existe una teoría que afirma que el Bitcoin terminará por ser poseído por los estados como divisa de reserva[1] y que los individuos realizarán transacciones utilizando dinero monopolístico[2] "respaldado" por Bitcoin. La teoría afirma que el volumen de transacciones resulta insuficiente para su utilización como divisa para los consumidores, pero su capacidad de evitar la inflación monetaria[3] hace del Bitcoin un activo de reserva ideal. Los bancos centrales y sus funcionarios autorizados emitirían pagarés[4] mientras mantienen el Bitcoin en reserva. Puesto que el Bitcoin no puede someterse a la inflación, la letanía de problemas producidos por el control estatal del dinero se resolvería, inaugurando una nueva era de prosperidad. Las comisiones por transacciones serían bajas mientras que el volumen de transacciones sería ilimitado.

Consideremos el escenario según se iría desarrollando. Bitcoin se convierte en una divisa[5] bastante utilizada, pero tiene problemas con el bajo volumen de transacciones, las altas comisiones y los largos tiempos de confirmación. Con el fin de obtener una reserva de bitcóin (BTC), el estado emite Certificados de Bitcoin (CB) negociables[6] a cambio de bitcóins. Esto podría lograrse incautándose de cuentas centralizadas (convirtiéndolas por la fuerza) o mediante operaciones en los mercados; ambas posibilidades se han utilizado para formar las reservas de oro. Se establece un proceso de auditoría en virtud del cual las personas puedan verificar que los CB emitidos nunca superen las reservas de BTC. Se crean leyes relativas al curso legal[7], que exigen que la gente acepte CB como pago para liquidar deudas salvo que se acuerde explícitamente lo contrario. La gente compra

Reference

[1] Capítulo: Principio de Reserva

[2] Capítulo: Taxonomía del dinero

[3] https://en.wikipedia.org/wiki/Monetary_inflation

[4] https://es.wikipedia.org/wiki/Pagar%C3%A9

[5] https://es.wikipedia.org/wiki/Moneda_(divisa)

[6] https://es.wikipedia.org/wiki/T%C3%ADtulo_de_cr%C3%A9dito#Espa%C3%B1a

[7] https://es.wikipedia.org/wiki/Curso_legal

CB con BTC para poder pagar impuestos y comprar cosas a los minoristas del mercado legal. La mayoría del BTC termina por formar parte de las reservas estatales.

Este escenario debería resultar familiar, puesto que así es como los estados acabaron teniendo el oro y la gente acabó teniendo el papel. La teoría es inválida a varios niveles.

La proporción de CB emitidos respecto de los BTC en reserva nunca puede ser auditada de manera eficaz. Incluso si las normas de consenso del Bitcoin permanecieran de alguna forma, *no hay manera* de saber cuántos CB se han emitido, y no hay posibilidad de recurso si se sospecha que se esté produciendo una devaluación. Hay que *confiar* en que el banco central se responsabilice de la emisión de CB, y, en última instancia, esto significa que todo el mundo confía en que el estado no incurra en expansión[1] cuantitativa. La historia demuestra que esto es improbable y, a pesar de todo, no constituye ninguna mejora respecto de los actuales dineros estatales.

Así pues, ¿por qué resulta que una persona no puede auditar (validar) nunca eficazmente los CB, como sí resulta posible con el BTC que sustituyen? Porque eso haría que los CB fueran indistinguibles de los BTC mantenidos en reserva. En otras palabras, el *motivo* por el cual existe una diferencia entre la moneda de curso legal y la moneda de reserva es permitir la inflación de la moneda que está siendo utilizada (impuesto[2]) mientras que se mantiene un dinero superior[3] en reserva (atesoramiento).

Además, para que exista Bitcoin tiene que haber una economía del Bitcoin descentralizada. Sin individuos que validen el BTC recibido en intercambios, no hay nadie que rechace el BTC inválido redefinido por el estado[4]. En este caso, la censura[5] y la

Reference

[1] https://es.wikipedia.org/wiki/Expansi%C3%B3n_cuantitativa

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] https://es.wikipedia.org/wiki/Ley_de_Gresham

[4] Capítulo: Objetivos del Fedcoin

[5] Capítulo: Propiedad de resistencia a la censura

inflación se pueden introducir fácilmente, lo que invalida la teoría. Solo las transacciones de Bitcoin del mercado negro y la minería pueden resistir[1] esta transición. Esto genera poca presión económica sobre el estado para que mantenga la consistencia con las reglas de consenso de Bitcoin.

La disposición en capas preserva los principios criptodinámicos[2] de la descentralización, si bien el "respaldo" es abandonarlos por completo. El Bitcoin no se puede sostener predominantemente como un dinero de respaldo para los billetes de los bancos centrales. Las personas deben realizar intercambios con él para que sea seguro.

Ciertamente es posible que las tesorerías estatales mantengan Bitcoin, pero esto no ofrece ningún escalado de transacciones ni ninguna otra ventaja para las personas.

Reference

[1] Capítulo: Axioma de resistencia

[2] Capítulo: Principios Criptodinámicos

Principio de la Banca Estatal

No hay ningún prestamista de último recurso[1] en la banca libre[2], solamente implica otro prestamista sujeto a las restricciones demostradas en la Falacia de la Nada[3]. Sin embargo, en la banca estatal este lo constituye el banco central[4], apoyado por el contribuyente. El estado recauda impuestos para proporcionar préstamos con descuento[5] a los bancos miembros[6] y a la tesorería estatal. Los préstamos deben tener descuento respecto de los tipos de mercado[7] ya que, de lo contrario, no constituye un último recurso. Los bancos siempre tienen la opción de pedir prestado a otros bancos y depositantes potenciales. La fiscalidad es necesaria para dar soporte al descuento. Así pues, si el tipo de interés económico es del 10%, el estado puede prestar a los bancos miembros al 3% y cubrir la diferencia con impuestos.

El estado tiene muchas fuentes de ingresos fiscales, pero típicamente los bancos centrales subvencionan los tipos de préstamos con descuento mediante el señoreaje[8]. Los bancos centrales son conocidos por proclamar que no "imprimen dinero", pero eso es exactamente lo que hacen. La Reserva Federal[9] ("Fed") de los Estados Unidos tiene la potestad de hacer pedidos de dinero nuevo[10] a la Oficina de Moneda y Timbre (Bureau of Engraving and Printing)[11] del Tesoro estadounidense. La Fed paga el coste de impresión[12]

Reference

[1] https://es.wikipedia.org/wiki/Prestamista_de_%C3%BAltima_instancia
[2] https://es.wikipedia.org/wiki/Banca_libre
[3] Capítulo: Falacia de la Nada
[4] https://es.wikipedia.org/wiki/Banco_central
[5] https://en.wikipedia.org/wiki/Discount_window
[6] https://en.wikipedia.org/wiki/Structure_of_the_Federal_Reserve_System
[7] https://www.frbdiscountwindow.org/pages/discount-rates/current-discount-rates
[8] https://es.wikipedia.org/wiki/Se%C3%B1oreaje
[9] https://es.wikipedia.org/wiki/Junta_de_la_Reserva_Federal
[10] https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html
[11] https://www.moneyfactory.gov/
[12] https://www.federalreserve.gov/faqs/currency_12771.htm

del "papel-moneda" (en realidad, un tejido[1]) y el valor nominal por la moneda acuñada[2]. El Tesoro no es más que el contratista que realiza el trabajo. Típicamente, la acuñación se produce de tal manera que tiene un valor nominal levemente superior a su valor de uso[3], con el fin de evitar que desaparezcan[4] las monedas. Por consiguiente, este valor de uso tiene que reducirse cuando el valor nominal se reduce en relación con él, como resultado de la devaluación del correspondiente dinero fiduciario.

Esto implica que la inflación monetaria[5] de dinero fiduciario estatal es literalmente la consecuencia de imprimir el "papel" moneda. Este proceso queda de alguna manera encubierto. La Fed no imprime primero el dinero, lo coloca en una cámara acorazada y luego lo presta. Esto resulta innecesario. En la práctica, este orden se invierte. La Fed emite préstamos con descuento, con la *presunción* de que hay dinero dentro de su cámara acorazada.

El proceso de liquidación[6] establecido por la Fed mantiene un seguimiento de cuánto dinero en la reserva de cada banco miembro. El grueso de las liquidaciones a menudo se puede compensar recíprocamente[7], pero periódicamente se tiene que mover el dinero físico.

Para reducir aún más los costes de transporte, se exige que una porción significativa de las reservas de los bancos miembros se mantenga en la cámara acorazada propia de la Fed. Esto se puede lograr mediante la compra de títulos del Tesoro (bonos (*Treasuries*)[8])

Reference

[1] https://www.moneyfactory.gov/hmimpaperandink.html
[2] https://es.wikipedia.org/wiki/Moneda
[3] https://es.wikipedia.org/wiki/Valor_de_uso
[4] https://es.wikipedia.org/wiki/Ley_de_Gresham
[5] https://en.wikipedia.org/wiki/Monetary_inflation
[6] https://en.wikipedia.org/wiki/Fedwire
[7] https://en.wikipedia.org/wiki/Set-off_(law)#Close_out_netting
[8] https://en.wikipedia.org/wiki/United_States_Treasury_security

puestos a la venta[1] por la Fed. Se trata de sustitutivos dinerarios[2] considerados suficientes para satisfacer los requisitos de reservas de los bancos miembros. Los bonos del Tesoro son deuda emitida por el Tesoro estadounidense y comprada generalmente al por mayor en el mercado continuo[3] por la Fed. La Fed reduce la rentabilidad de los bonos del Tesoro (es decir, el tipo de interés pagado por el estado) al proporcionar un aumento de la demanda. Financiar estas operaciones de la misma manera esencial que los préstamos con descuento a sus bancos miembros. La diferencia es sencillamente que estas compras constituyen préstamos con descuento realizados al estado.

La Fed puede *fingir* que tiene dinero dentro de su cámara acorazada imprimir solamente lo que resulte necesario para las liquidaciones. Esto crea la ilusión de que la inflación monetaria es resultado de los préstamos. Pero en realidad es enteramente el resultado de la potestad de la Fed de comprar dinero con descuento, y en virtud de esto financiar los préstamos. Cuando un banco miembro requiere dinero, se lo puede comprar a la Fed por medio de bonos del Tesoro. Cuando la reserva de dinero real de la Fed resulta insuficiente, sencillamente realiza una "retirada" a cargo del contribuyente al hacer pedidos de dinero a la imprenta.

Reference

[1] https://www.stlouisfed.org/open-vault/2019/august/open-market-operations-monetary-policy-tools-explained

[2] https://wiki.mises.org/wiki/Money_substitutes

[3] https://fred.stlouisfed.org/series/TREAST

La Fed le paga al Tesoro los siguientes importes por los billetes de dólares:

Denominación	Precio
1$	5,5 céntimos
2$	5,5 céntimos
5$	11,4 céntimos
10$	11,1 céntimos
20$	11,5 céntimos
50$	11,5 céntimos
100$	14,2 céntimos

Si hubiera costado 5,5 céntimos imprimir un billete de 1$ en 1915, imprimirlo ahora costaría unos $1,40. Cuando el coste de imprimir un billete alcanza su valor nominal, ha completado la transición de dinero fiduciario a dinero mercancía[1]. En ese momento, su valor de señoreaje es nulo. A medida que continúa la devaluación, los billetes de ese importe deja de producirse. Resulta informativo observar los bancos centrales involucrados en la hiperinflación[2], puesto que el dinero alcanza su coste de impresión a lo largo de periodos mucho más cortos, y las monedas tienden a desaparecer por completo. La emisión de billetes de mayor importe permite que el dinero siga siendo fiduciario a medida que se abandona el dinero mercancía. El dólar de Zimbabue[3] alcanzó billetes con un importe individual de 100.000.000.000.000 unidades antes de que se abandonara completamente en favor de las divisas extranjeras.

Reference

[1] https://es.wikipedia.org/wiki/Dinero_mercanc%C3%ADa

[2] https://es.wikipedia.org/wiki/Hiperinflaci%C3%B3n_en_Venezuela

[3] https://es.wikipedia.org/wiki/D%C3%B3lar_zimbabuense

Sin esta capacidad de crear dinero fiduciario, la Fed sería incapaz de liquidar cuentas, al igual que cualquier otro banco, si hubiera una reserva suficiente (incluyendo lo que se pudiera pedir prestado) para cubrir las retiradas de efectivo y los impagos. Hasta que el banco miembro tenga que realizar la liquidación en dinero, como es el caso de una retirada de efectivo en cajeros automáticos[1], ventanillas de bancos[2] o bancos no miembros y otras instituciones, no existe ninguna necesidad de mover el dinero en sí, ni de imprimirlo.

Pero si la capacidad de primero por debajo del coste, la Fed estaría sujeta a la suspensión de pagos al igual que cualquier otro banco.

La cantidad total de dólares estadounidenses en circulación[3] se denomina "M0". Esto incluye toda la moneda tangible ("efectivo en cámaras acorazadas") más los balances bancarios intangibles en las cuentas de la Reserva Federal. Estas dos formas se consideran "obligaciones"[4] intercambiables (dinero) de la Fed. Las obligaciones intangibles son dinero contabilizado pero aún no impreso.

En la medida en que se reduce la oferta de préstamos por parte de los bancos miembros, por ejemplo porque la Fed suba los tipos de interés, las obligaciones de la Fed se pueden destruir con el efecto opuesto al de su impresión. Si bien la Fed ha producido una contracción de la M0[5] de casi un 20% en los cuatro años posteriores su máximo de 2015, esto supone un coste para los ingresos fiscales. La Fed se pone la máscara de organización

Reference

[1] https://es.wikipedia.org/wiki/Cajero_autom%C3%A1tico

[2] https://en.wikipedia.org/wiki/Bank_teller

[3] https://en.wikipedia.org/wiki/Money_supply#United_States

[4] https://en.wikipedia.org/wiki/Money_supply#Money_creation_by_commercial_banks

[5] https://tradingeconomics.com/united-states/money-supply-m0

sin ánimo de lucro, remitiendo cada año sus ingresos netos procedentes de sus préstamos al Tesoro estadounidense[1].

> La Reserva Federal aumentó el objetivo de los tipos de los fondos federales siete veces entre diciembre de 2015 y junio de 2018. Esto tiene implicaciones para la trayectoria del déficit y la deuda federales en dos sentidos:
>
> * directamente a través de los pagos de intereses netos
> * indirectamente a través de los importes remitidos anualmente por la Fed al Departamento del Tesoro de los Estados Unidos
>
> Las remesas anuales al Tesoro son esencialmente los ingresos restantes de la Fed después de los gastos operativos. Por ley, estos ingresos adicionales tienen que ser transferidos al Tesoro.
>
> Los ingresos enviados al tesoro marcaron un máximo de 97.700 millones de dólares en 2015 y han estado reduciéndose de manera constante desde entonces. En enero, la Fed envió 80.200 millones de dólares al Tesoro.
>
> *Banco de la Reserva Federal de St. Louis*

Estos "ingresos restantes de la Fed" es lo que se gana, después de los gastos operativos, mediante préstamos de dinero impreso por el Tesoro estadounidense a su coste nominal, garantizado por su protección del monopolio[2] de hacerlo. El resultado neto es que el Tesoro imprime dinero nuevo y luego reobtiene el dinero ganado como intereses sobre ese dinero impreso. Según se muestra anteriormente, el Tesoro también pide prestado dinero a tipos descontados indirectamente financiados por la Fed, a través de la emisión de títulos del Tesoro. **Si bien el dinero no se imprime y luego se deposita directamente en el Tesoro, el resultado es el mismo.**

Reference

[1] https://www.stlouisfed.org/on-the-economy/2018/september/fed-payments-treasury-rising-interest-rates

[2] https://es.wikipedia.org/wiki/Falsificaci%C3%B3n

El dinero monopolístico[1] no se crea *ex nihilo* mediante contabilidad bancaria fraudulenta. Se crea por parte del estado literalmente a partir de vaqueros azules usados[2].

La transición a una "sociedad sin efectivo"[3] implica que los bancos centrales conservarían la manera existente de contabilizar el dinero fiduciario aún no impreso, y sencillamente realizarían todas las liquidaciones internamente. Esto eliminará los costes de impresión y de transporte para liquidaciones, y garantiza una censurabilidad total. Un ejemplo de Fedcoin[4], como la e-Krona[5] experimental, se exigiría para que las personas operen electrónicamente dinero estatal. Bitcoin sirve para la misma finalidad, pero sin el control estatal ni sobre su emisión (minado) ni sobre su confirmación. Por estos motivos, no se puede esperar que Bitcoin actúe como la divisa de reserva[6] (dinero) para la banca estatal, ya que necesariamente seguiría la misma trayectoria que el fallido patrón oro[7]. La propuesta de valor[8] de Bitcoin es evitar el dinero estatal.

Reference

[1] Capítulo: Taxonomía del dinero

[2] https://www.washingtonpost.com/news/wonk/wp/2013/12/16/how-tight-jeans-almost-ruined-americas-money

[3] https://www.nytimes.com/2018/11/21/business/sweden-cashless-society.html

[4] Capítulo: Objetivos del Fedcoin

[5] https://www.riksbank.se/en-gb/payments--cash/e-krona

[6] Capítulo: Falacia de la Divisa de Reserva

[7] https://es.wikipedia.org/wiki/Patr%C3%B3n_oro

[8] Capítulo: Propuesta de Valor

MINERÍA

Falacia del Monopolio de ASIC

Existe una teoría que afirma que el precio de los ASIC[1] de Bitcoin está controlado por un cártel[2] de mineras, lo que crea una ventaja desproporcionada para los socios mineros del cártel.

No existe ninguna diferencia económica entre un cártel y una organización individual. Cambiar el tamaño de la organización es un resultado del libre mercado observable cuando el capital busca economías de escala[3] óptimas. Si los socios reciben ASICs a un precio que produce un rendimiento sobre el capital por debajo del mercado, esto equivale a una subvención interna entre socios. Lo mismo es cierto referido a un precio que produzca un rendimiento sobre el capital por encima del de mercado, siendo la subvención en sentido opuesto en este caso. Por consiguiente, no hay ninguna ventaja neta de ese tipo de descuentos entre socios.

La producción se establece generalmente a un nivel que pretende producir una rentabilidad porcentual[4] máxima del capital. La única manera económicamente racional de que un productor aumente el precio es limitar la producción por debajo de ese óptimo. De lo contrario, un precio superior implica un inventario no vendido, lo cual redunda en menores rentabilidades netas. Esto implica que la producción tiene que ser restringida por el cártel con la finalidad de elevar el precio unitario[5] para los no socios.

Reference

[1] https://es.wikipedia.org/wiki/Circuito_integrado_de_aplicaci%C3%B3n_espec%C3%ADfica

[2] https://mises.org/library/man-economy-and-state-power-and-market/html/p/1059

[3] https://es.wikipedia.org/wiki/Econom%C3%ADa_de_escala

[4] https://es.wikipedia.org/wiki/Tasa_de_retorno

[5] https://en.wikipedia.org/wiki/Unit_price

Evitar la producción deja una oportunidad a otros productores para obtener clientes con una menor utilidad marginal[1] para el producto, ya que esos clientes, de lo contrario, no serían atendidos. Así, la competición rebaja el precio hasta que se despeja el mercado. Un mercado libre busca el precio de liquidación que produzca el rendimiento global del capital (interés). Un precio corriente por encima de este nivel aumenta la producción y por debajo, reduce la producción. Es la preferencia temporal[2] la que determina el tipo de interés.

A no ser que la producción esté sujeta desproporcionadamente a fuerzas contrarias al mercado, tales como la fiscalidad o las subvenciones, cada cual disfruta de la misma oportunidad de recaudar capital y competir en la producción.

Si nos urge competencia, esto implica que los retornos en esta línea de negocio son al menos consistentes con los retornos promedio del mercado. La fiscalidad y las subvenciones causan distorsiones regionales, pero no eliminan la competencia. **En otras palabras, el precio monopolístico sólo se puede lograr por la concesión estatal del poder monopolístico.**

Una teoría relacionada afirma que comprar ASICs a este cártel aumenta su potencia de hash. Esto es inválido sobre la base de la explicación anterior del establecimiento monopolístico de los precios. El capital del productor buscará el mismo retorno en cualquier línea de negocio o inversión. No existe ningún motivo para creer que el retorno será desproporcionado en los ASICs.

Una teoría relacionada afirma que el algoritmo de prueba de trabajo del Bitcoin produce una presión pro-compartición de recursos[3], como consecuencia de la supuesta cartelización. Si las personas verdaderamente creyeran que los ASICs tienen un precio

Reference

[1] https://es.wikipedia.org/wiki/Utilidad_marginal

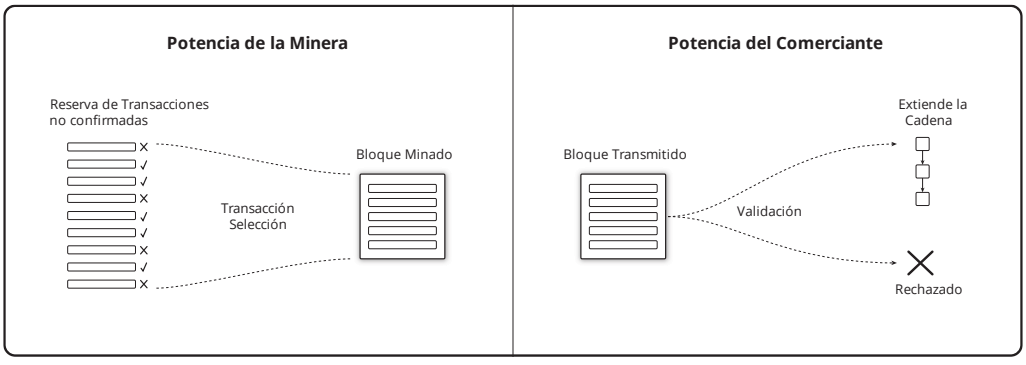
[2] https://en.wikipedia.org/wiki/Time_preference

[3] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

excesivo, la respuesta racional consiste en recaudar capital y producir ASICs. Pero, en cualquier caso, las fuerzas favorables y contrarias al mercado (estatales) controlan en exclusiva la producción de los chips y, por tanto, no constituyen una presión pro-compartición de recursos basada en un protocolo.

Falacia del Equilibrio de Poder

El poder en Bitcoin reside en las mineras y en los comerciantes. Sin embargo, estos dos poderes no están "equilibrados" entre sí, como si estuvieran bloqueados por una suerte de sistema de controles y contrapesos[1]. El poder de las mineras es ortogonal[2] al poder de los comerciantes. Las mineras controlan la selección de las transacciones, los comerciantes controlan la validez, y ninguno puede controlar al otro. Resulta poco sorprendente que en la descripción[3] original y en la implementación original, estos roles fueran combinados.



El poder no es lo mismo que la influencia. Los comerciantes pueden influir en las mineras al no comprar el servicio. De manera análoga, las mineras pueden influir en los comerciantes al no producirlo. Estas elecciones se manifiestan como divisiones o paradas. Sin embargo, la naturaleza del poder es que puede ignorar la influencia (y a menudo la ignora). El estado tiene poder; puede aplicar la coacción y la cooptación al tiempo que ignora las influencias. Los comerciantes y las mineras *juntos* tienen el poder

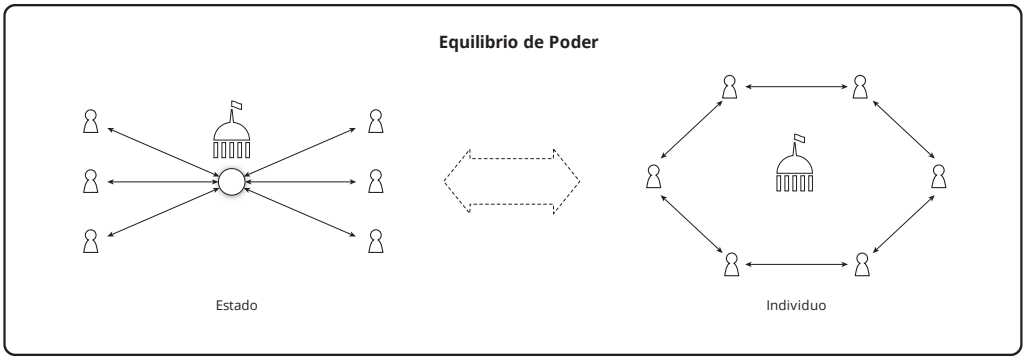
Reference

[1] https://es.wikipedia.org/wiki/Separaci%C3%B3n_de_poderes

[2] https://es.wikipedia.org/wiki/Ortogonalidad_(matem%C3%A1ticas)

[3] https://bitcoin.org/bitcoin.pdf

de defenderse[1] contra estas agresiones, pero ninguna puede hacerlo sin el apoyo de la otra.



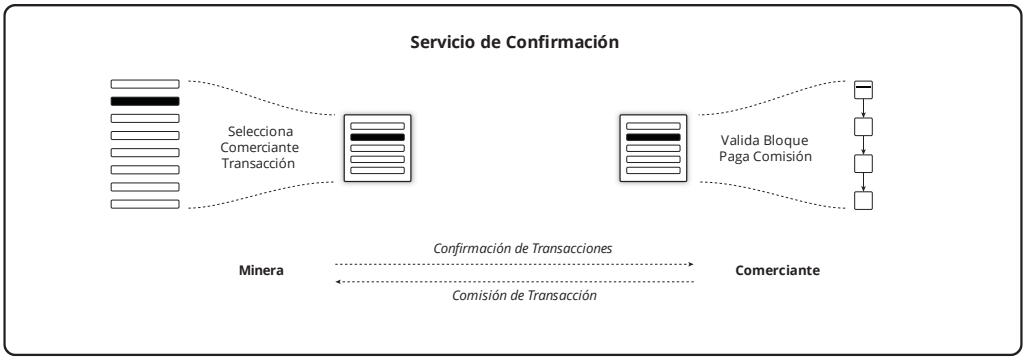
El equilibrio de poder en Bitcoin es entre los *individuos* y el Estado. Incluso los estados crean sistemas que intentan[2] aislar sus dineros del control político. Bitcoin no es distinto en ese sentido, incorporando el axioma de resistencia[3]. Los individuos pueden ser mineras y pueden ser comerciantes. Con una amplia distribución de estas actividades, se hace difícil para los agentes estatales censurar este mercado. **La idea de que las mineras y los comerciantes se encuentran en una posición enfrentada es no entender el modelo de seguridad de Bitcoin.**

Reference

[1] Capítulo: Principio de la Compartición de Riesgos

[2] https://www.federalreserve.gov/aboutthefed/bios/board/default.htm

[3] Capítulo: Axioma de resistencia



Los comerciantes compran un servicio a las mineras y, por tanto, ambos están desarrollando intercambios. Los comerciantes adquieren los servicios de minería que satisfacen sus reglas por una comisión satisfactoria. Son libres de separarse mediante una división de moneda y las mineras son libres de no minar en absoluto, o de seleccionar transacciones particulares por cualquier motivo que quieran. Los intercambios no son entre adversarios ni son asimétricos; son voluntarios y mutuamente beneficiosos, con todas las tensiones resueltas en el precio.

No comprender esto lleva a la gente a pensar que la minería se puede realizar con una compartición de recursos centralizada siempre que los comerciantes no estén centralizados en la validación, ya que la economía puede controlar el comportamiento de la minería, haciendo que el sistema sea seguro. Esta creencia es incorrecta pero desafortunadamente la gente está sacando esta conclusión[1] inválida por eventos recientes. Una falacia estrechamente relacionada[2] es que una bifurcación dura realizada por los comerciantes con prueba de trabajo puede controlar el comportamiento de las mineras.

Reference

[1] https://www.coindesk.com/uasf-revisited-will-bitcoins-user-revolt-leave-lasting-legacy

[2] Capítulo: Falacia de la Prueba de Trabajo

Falacia de la Minería de Producto Residual

Existe una teoría que afirma que, en la medida en que la minería de Bitcoin puede consumir un producto residual[1] de la producción de energía que fuera necesario y no comercializable de ninguna otra manera, como gas natural sin utilizar[2], hay implícita una reducción en el consumo de energía comercializable.

Dado un nuevo mercado de productos residuales, no aprovecharse del supuesto menor precio representa un coste de oportunidad[3] para cada minera. La competición por el producto residual aumenta su precio, lo cual termina por llevarlo a un nivel en el que se elimina su ventaja neta. En el ínterin, esto representa una oportunidad[4] de beneficios en la minería.

Paradójicamente[5], los costes reducidos producen como resultado un consumo proporcionalmente mayor. El coste disminuido de la minería tiene que producir como resultado un incremento en la minería, de manera que su coste regrese al nivel de la recompensa. Por tanto, el producto residual anteriormente "consumido" como desecho aumenta la tasa de hash de la minería hasta que se consume el mismo coste en la minería. El consumo neto de energía en minería realmente aumenta por el menor precio.

Y, sin embargo, al monetizar un recurso residual, el suministro de energía total comercializable aumenta sin que haya un aumento en su coste de producción. Y en la minería disminuye la demanda del suministro de energía comercializable de otro modo. Esto implica un menor precio de mercado de la energía.

Reference

[1] https://es.wikipedia.org/wiki/Basura

[2] https://es.wikipedia.org/wiki/Quemado_en_antorcha

[3] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[4] https://bitcoinist.com/bitcoin-mining-waste-oil-industry

[5] Capítulo: Paradoja de la Eficiencia

La correspondiente expansión de la producción generalmente puede ser el resultado de un menor precio de mercado de la energía. Esta estabilidad de precios[1] es una característica general de todos los productos. **Por consiguiente, no se puede suponer una reducción consiguiente en el consumo total de energía a causa de la minería con productos residuales**, lo que invalida la teoría. Sin embargo, sí hay implícito un aumento global de la riqueza por una mayor producción al mismo coste o la misma producción a un menor coste.

Reference

[1] Capítulo: Propiedad de Estabilidad

Falacia de la Causación

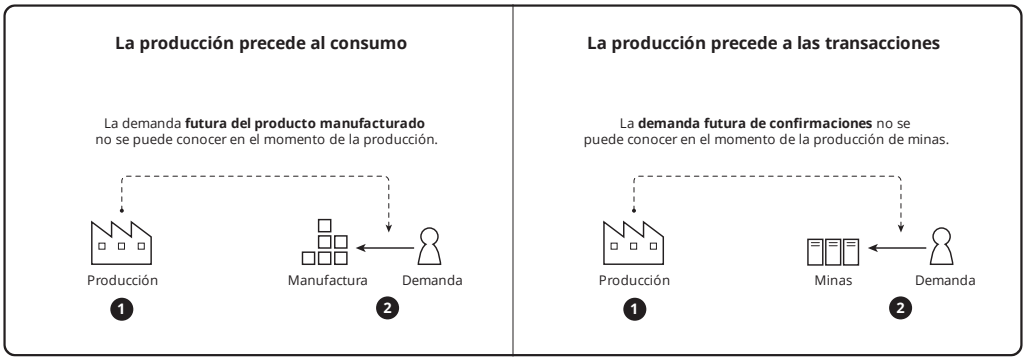
Existe una teoría en el sentido de que la minería "sigue" al precio, o más específicamente, el valor de la recompensa. La implicación es que la minería está sometida al precio, y no afecta de ninguna manera a la utilidad de la moneda.

Considérese la minera que responda solamente a los valores históricos de recompensa. Esta persona no puede ser la primera minera, porque la recompensa carece de valores históricos. No se puede establecer ningún precio porque no se han producido intercambios. La minera podría haber oído que un número de unidades no confirmadas han comprado una pizza, pero quizá esas mismas unidades hayan sido gastadas por duplicado. Debe anticiparse a un cierto nivel de rentabilidad futura sobre el capital que no se puede conocer hasta que o bien se materialice o no lo haga. Esa es la naturaleza del riesgo empresarial. El riesgo debe asumirse antes de que pueda existir el producto. Uno podría creer que el riesgo se puede trasladar al consumidor, con pedidos por anticipado. Pero en ese momento el consumidor se habrá convertido en emprendedor, proporcionando el capital para la producción y asumiendo el riesgo correspondiente.

Ciertamente es posible que una minera responda solamente a valores históricos de recompensa una vez que se haya establecido un historial gracias al riesgo asumido por otros. ¿Pero cuál es el periodo de tiempo y el método de promediado que predice los valores de recompensa futuros? La capacidad exclusiva de predecir los precios de cambio proporcionaría riquezas ilimitadas a la minera. Si pudiera realizarse con carácter general, el precio nunca cambiaría, ya que todos los cambios potenciales se descontarían con la primera acuñación. Por tanto, o bien el precio cambia de manera impredecible, o no cambia en absoluto. En otras palabras, cada minera se enfrenta a la misma situación que la primera. No existen precios históricos que puedan predecir precios futuros.

Asumiendo con carácter general una rentabilidad media de mercado sobre el capital minero, un fallo de estimación del valor de recompensa, tanto por exceso como por defecto, implican pérdidas en relación con el coste del capital. Dada la naturaleza de la

competición, los beneficios y las pérdidas (por encima y por debajo de las rentabilidades de mercado sobre el capital, respectivamente) experimentan una presión existencial negativa constante. En otras palabras, el mercado trata de eliminar esos errores. Pero dada la naturaleza impredecible del precio, nunca puede llegar a hacerlo. La producción nunca persigue a la demanda que existe, que es inherentemente histórica; siempre persigue la demanda que anticipa. **La producción sigue tratando de adivinar el consumo futuro y, al hacerlo, crea la oportunidad de consumo.**



Las mineras intercambian su capital por unidades de bitcoin. Al hacerlo, constituyen una fracción de la demanda total de bitcoin. Y, sin embargo, las mineras no establecen el precio de manera independiente. Su demanda particular no tiene más impacto en el precio que el de una persona no minera con el mismo nivel de demanda.

Uno podría decir que las mineras convergen a una rentabilidad de mercado al anticipar los *máximos* valores posibles de las comisiones. Pero los comerciantes convergen de manera similar a una rentabilidad de mercado sobre el capital minero al perseguir el *mínimo* valor posible de las comisiones. Sin embargo, las mineras deben anticipar la demanda total y arriesgarse a minar antes de que pueda haber utilidad alguna. Así que, en la medida en que haya alguna simetría, la minería precede a las transacciones, de la misma manera que toda producción debe preceder a su consumo. Asumir lo contrario confunde la dirección que persigue un mercado con la manera en que lo hace.

Falacia de la Minería Desacoplada

Existe una teoría en el sentido de que la seguridad[1] se incrementa al desacoplar la recompensa respecto de la selección de transacciones en la minería con *pooling*. La teoría sostiene que, al compartir solamente la recompensa, el control sobre la selección de las transacciones se traslada a las mineras con menos potencia de hash. Esto implica una reducción en el descuento de varianza[2] y, por consiguiente, un aumento en la competitividad[3] de las minas más pequeñas. Puesto que las minas más pequeñas presumiblemente puedan operar de manera más encubierta que las más grandes, esto a su vez implica que se incrementa la resistencia[4] a la censura.

La teoría no reconoce que el control sobre la selección de transacciones sigue siendo del gestor del pool y, por consiguiente, es inválida. La única ventaja es la reducción de la varianza, pero esto solo se consigue con el recibo de pago. Puesto que el pago es discrecional, se puede imponer cualquier condición. Tales condiciones pueden incluir la censura y la identidad. El recurso de los miembros es dejar el *pool* por otro, al igual que sucede con el pool emparejado. Por tanto, los *pools* desemparejados y los *pools* emparejados están sujetos por igual a la cooptación.

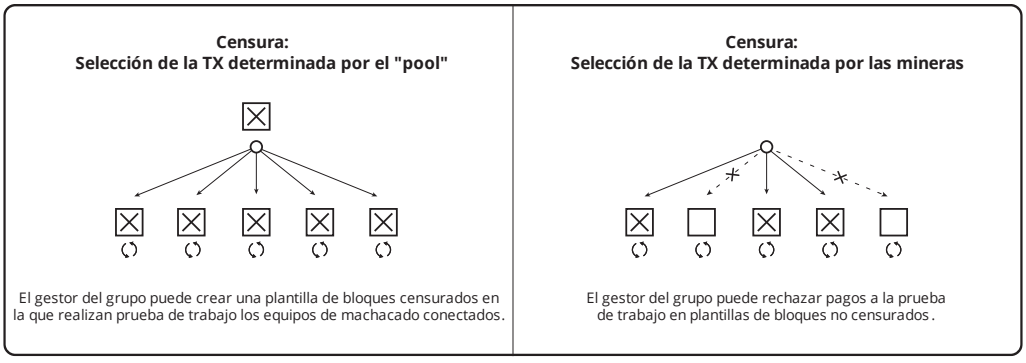
Reference

[1] Capítulo: Modelo de Seguridad Cualitativa

[2] Capítulo: Deficiencia del Descuento de Varianza

[3] Capítulo: Propiedad de resistencia a la censura

[4] Capítulo: Axioma de resistencia



Existe una teoría relacionada que afirma que la transparencia de un *pool* desemparejado es mayor que la de un *pool* emparejado, lo que facilita la vida de los miembros a *pools* que no censuren y, por consiguiente, limita la dominancia de los *pools* que censuren. Aceptando generosamente las suposiciones de una mayor transparencia y de las mineras independientes en contra de su interés propio financiero, aún nos queda el hecho de la cooptación. El estado todavía puede reservarse para sí mismo la capacidad de operar con las ventajas financieras de la compartición de recursos[1] y la teoría es, por consiguiente, inválida.

Esta falacia es parecida a la Falacia del Repetidor[2] en la que toda la ventaja financiera depende de mineras por lo demás independientes que concedan el control de esa ventaja a una persona individual.

Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[2] Capítulo: Falacia del Repetidor

Principio del Coste Dedicado

Los costes innecesarios en que incurran las mineras no contribuyen nada ni a la resistencia al gasto por duplicado ni a la resistencia a la censura[1]. Tales costes constituyen un auténtico desperdicio que representa meramente la ineficiencia de una minera dada. Por ejemplo, no contribuye a la seguridad que una minera con máquinas configuradas incorrectamente gaste una gran cantidad de energía al tiempo que es incapaz de ganar una recompensa por la configuración incorrecta. Cualquier coste que no se requiera estrictamente para la generación óptima de potencia de hash no constituye un coste necesario. Una configuración incorrecta por parte de una minera no representa un coste para otra.

Existe una teoría en el sentido de que la prueba de trabajo (PoW) se puede hacer más eficiente energéticamente[2] introduciendo costes no dedicados en la función de minería. Un ejemplo de esto es el descubrimiento de números primos[3]. La razón de incorporar tales costes es que los descubrimientos resultantes tienen un valor comercializable presumible. De lo contrario, objetivamente no habría ningún valor en incorporarlos.

Por analogía, las fábricas de cerveza pueden vender sus productos secundarios de grano a los granjeros. Esto mejora su eficiencia al reducir el coste. Así que, en la medida en que el producto secundario resultante sea valioso, su producción no genera un coste neto. Y, sin embargo, el coste neto necesario debe aumentar hasta el nivel de la recompensa, como consecuencia de la competición. Por consiguiente, el mismo resultado se obtendría con una PoW básica que consumiera el valor completo de la recompensa y operaciones independientes que consumieran energía y generaran los productos comercializables. **Cualquier coste dedicado a la producción de valor comercializable de manera**

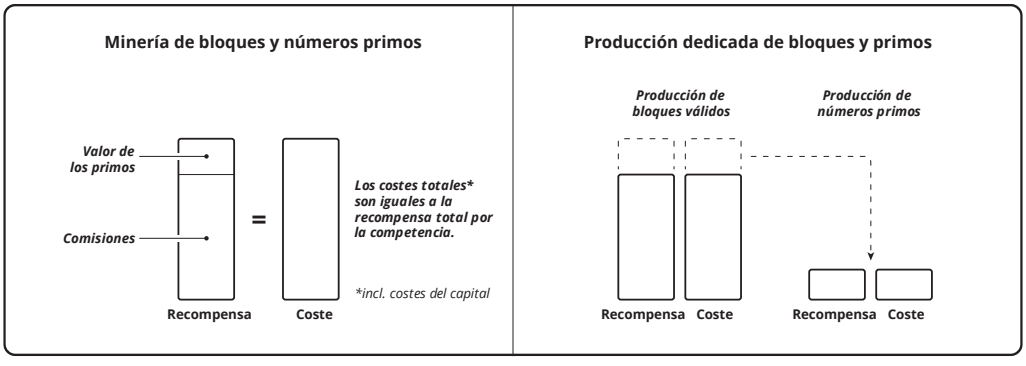
Reference

[1] Capítulo: Propiedad de resistencia a la censura

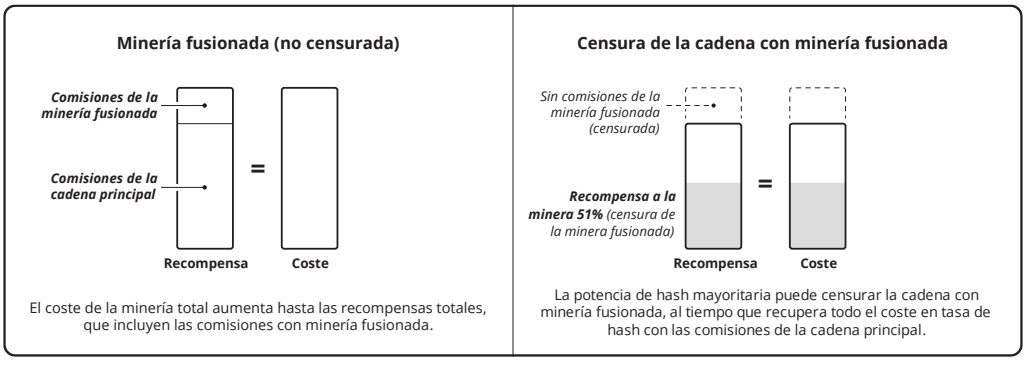
[2] Capítulo: Paradoja de la Eficiencia

[3] http://primecoin.io

independiente se puede compensar vendiendo ese producto secundario. Por consiguiente, la teoría es inválida.



La minería fusionada[1] se implementa típicamente para resolver el problema de sacar adelante una nueva moneda durante la etapa vulnerable de una baja tasa de hash. Este diseño no reconoce que la tasa de hash no dedicada a la nueva moneda no contribuye a su seguridad. Puesto que el coste íntegro de la tasa de hash se puede recuperar vendiéndola en una cadena, no tiene coste censurar la(s) otra(s) cadena(s) minadas mediante minería fusionada.



Reference

[1] https://eprint.iacr.org/2017/791.pdf

Paradoja de la Eficiencia

La minería de Bitcoin en general no se puede hacer más eficiente en términos de coste real. Dado que todos los costes son asimilables a energía, esto se podría reformular como: Bitcoin no se puede hacer más eficiente energéticamente. Paradójicamente[1], no importa qué mejora tecnológica se introduzca, el coste de confirmar una transacción seguirá siendo el importe de la recompensa por esa confirmación.

Esta aparente contradicción surge del hecho de que la recompensa determina el coste en última instancia. Un aumento en la tasa de hash por el mismo coste produce un incremento en la dificultad para mantener el periodo de bloque, aumentando el coste de manera correspondiente. La minería de Bitcoin siempre debe consumir en costes el importe de su recompensa actual.

Reference

[1] https://es.wikipedia.org/wiki/Paradoja

Falacia del Bloque Vacío

Existe una teoría en el sentido de que el minado de bloques vacíos constituye un ataque. La teoría no requiere que los bloques sean minados en una rama débil en un intento de permitir gastos por duplicado, ni especifica a qué persona se dirige el ataque.

Considérese lo siguiente:

- El término "ataque" implica robo. El artículo (*whitepaper*) que propuso Bitcoin, por ejemplo, utiliza el término exclusivamente para describir intentos de gastos por duplicado.
- Una recompensa está compuesta por comisiones por las transacciones y una subvención para el bloque. La minera que renuncia a comisiones de transacción por no incluir transacciones no se ve recompensada por ellas.
- La potencia de hash de la minera contribuye proporcionalmente a la seguridad de la red. La subvención constituye una compensación por esa seguridad durante la fase inflacionista. El propósito de la inflación es distribuir unidades racionalmente. La distribución racional se realiza específicamente a cambio de la potencia de hash, no de la inclusión de transacciones.
- La confirmación de transacciones no está asegurada. Las comisiones son el incentivo para la confirmación. La falta de confirmación implica objetivamente una comisión insuficiente.
- El minado de bloques vacíos es enteramente consistente con las reglas de consenso y no se puede evitar razonablemente con una nueva regla.

Además, si el 10% de la potencia de hash mina bloques vacíos, entonces las confirmaciones requerirán un 10% más de tiempo en promedio. Sin embargo, si una minera retira el 10% de la potencia total de hash, las confirmaciones también requerirán un 10% más de tiempo en promedio, hasta el próximo ajuste de dificultad. Por consiguiente, minar un bloque vacío resulta indistinguible de no minarlo.

Vale la pena explorar el origen de la falacia. Debido a la Propiedad de Suma Nula[1], podría haber una suposición de que minar un bloque vacío quita "injustamente" la oportunidad de que se confirmen transacciones.

Una minera dedica capital a la minería, produciendo potencia de hash. Dejando de lado los efectos del *pooling*[2], la minera recibe una subvención en proporción a la tasa de hash. Sin este trabajo, otras mineras producirían el mismo número medio de bloques a una dificultad proporcionalmente menor. En otras palabras, los ataques *reales* saldrían proporcionalmente más baratos. Por tanto, a pesar de no recibir recompensa por incluir transacciones, la minera de bloques vacíos está asegurando transacciones confirmadas anteriormente.

Dado que el coste marginal[3] de incluir una transacción se encuentra necesariamente por debajo de los niveles medios de las comisiones, la minera de bloques vacíos está incurriendo en un coste de oportunidad[4]. Esto equivale a que la minera subvenciona la seguridad de la cadena.

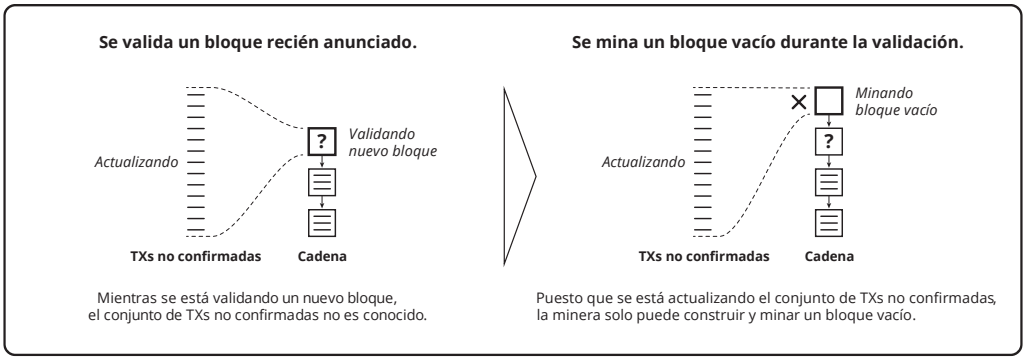
Reference

[1] Capítulo: Propiedad de la Suma Nula

[2] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[3] https://es.wikipedia.org/wiki/Coste_marginal

[4] https://es.wikipedia.org/wiki/Coste_de_oportunidad



Si bien esto parece económicamente irracional, puede deberse al coste de oportunidad de esperar a un nuevo candidato que no esté vacío después de un anuncio. **En la medida en que reduzca los costes de las mineras, el minado de bloques vacíos no puede tener impacto en las comisiones ni en la tasa de confirmaciones.** Por consiguiente, la teoría es inválida.

Si bien una minera dada podría considerar ventajoso minar bloques vacíos, está dentro del poder de cualquier otra persona hacer lo contrario. En última instancia es el aprovechamiento de esta oportunidad competitiva y en interés propio lo que asegura la moneda ante ataques reales.

Falacia del Agotamiento de la Energía

Existe una teoría que dice que la prueba de trabajo podría agotar toda la energía disponible a las personas. La PoW convierte la energía en una barrera contra gastos por duplicado monótona creciente[1] para cualquier transacción dada. Esto es comparable a la energía consumida para proteger cualquier tipo de dinero respecto de falsificaciones (por parte de su propio emisor o por otros).

La finalidad de cualquier medida de seguridad es generar un coste necesario para superar la medida, es decir, una barrera financiera. Bitcoin crea su barrera contra gastos por duplicado obligando al atacante a reemplazar la rama de la transacción objetivo por otra con un trabajo probabilísticamente mayor. Curiosamente, ese reemplazo aumenta la barrera para atacantes sucesivos. **La energía consumida no es importante de manera independiente, la barrera levantada constituye la carga financiera necesaria para el atacante.**

La barrera de seguridad (S) de un bloque es el producto del coste de hash unitario (C), la tasa de hash (H), y el periodo (T).

```
S = C * H * T
```

El ajuste varía la tasa de hash con el fin de mantener un periodo constante para una seguridad y un coste de hash dados.

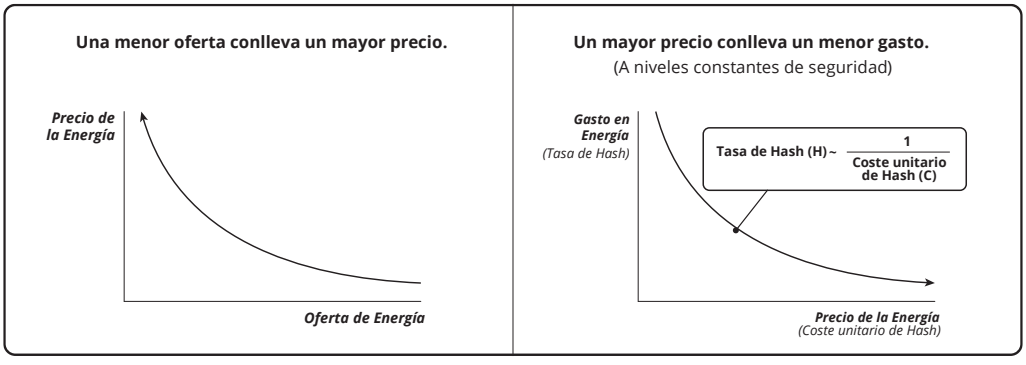
```
T = S / (C * H)
```

Reference

[1] https://es.wikipedia.org/wiki/Funci%C3%B3n_mon%C3%B3tona

Un periodo constante implica que la tasa de hash es inversamente proporcional al coste de una seguridad dada.

```
H ~ S / C
```



A medida que el suministro de energía se reduce, su precio tiene que aumentar, lo cual reduce la cantidad consumida para un nivel de seguridad dado. Por consiguiente, la energía no puede agotarse con la minería y la teoría es inválida.

Falacia del Almacenamiento de la Energía

Existe una teoría que afirma que el valor de la energía consumida mediante la prueba de trabajo se convierte al valor de la moneda, "almacenando" en efecto la energía para su consumo posterior. Suponiendo que la energía y la moneda tengan valor para algunas personas en algún momento futuro, pueden ser intercambiadas de nuevo.

No obstante, esto constituye una metáfora desafortunada en el mejor de los casos. Las mineras intercambian energía por unidades. Sin embargo, *todos* los comerciantes que aceptan unidades de la moneda intercambian algo por ella, y *todas las cosas* ofrecidas a cambio representan demanda. La teoría yerra en la implicación de que el valor de energía consumido en la minería resulta único por su contribución al valor. **Aparte de por la magnitud, una fuente de demanda no puede ser con carácter general un factor más determinante del valor que otra fuente**. Por consiguiente, la teoría es inválida.

Además, constituye un error similar afirmar que el dinero[1] es un almacén de valor[2]. El dinero es un almacén de dinero. Solamente los objetos pueden almacenarse de verdad. El valor del dinero se deriva enteramente el valor que, para las personas que lo intercambien, tenga aquello por lo que pueda ser intercambiado. Puesto que el valor es subjetivo[3], es una preferencia humana, sujeta a cambios constantes e impredecibles, y no puede ser almacenado.

Reference

[1] Capítulo: Taxonomía del dinero

[2] https://en.m.wikipedia.org/wiki/Store_of_value

[3] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

Falacia del Desperdicio de Energía

Existe una teoría que dice que la prueba de trabajo desperdicia energía. Esto implica que el nivel de seguridad proporcionado es mayor del necesario, o que se puede proporcionar el mismo nivel de seguridad mediante otra prueba externalizada a un menor coste de energía. Una prueba *internalizada*, específicamente la prueba de participación[1], constituye un modelo de seguridad diferente que no es seguro desde el punto de vista criptodinámico[2], y no se considera aquí.

La potencia de hash total es una función de la recompensa, que es una función de las comisiones, que son determinadas por el mercado de las confirmaciones. Si una persona considera que la potencia de hash actual resulta insuficiente para asegurar intercambios a un determinado valor respecto de gastos por duplicado, entonces aumenta la profundidad requerida. Además, según se muestra en Propiedad del Umbral de Utilidad[3], las transacciones con valor insuficiente para incluso la seguridad de una confirmación única quedan, por precio, fuera de la cadena.

Estos límites de seguridad superior e inferior dependen del coste de confirmación y, por consiguiente, son independientes de la técnica de prueba. **No hay un nivel necesario de seguridad, solamente una profundidad de confirmación subjetiva y una utilidad mínima.**

La seguridad de confirmación aumenta con el coste de generar cada bloque. El gasto por duplicado de una transacción requiere que su rama sea reemplazada por otra con un coste probabilísticamente mayor. Por tanto, el coste energético solo puede ser reducido

Reference

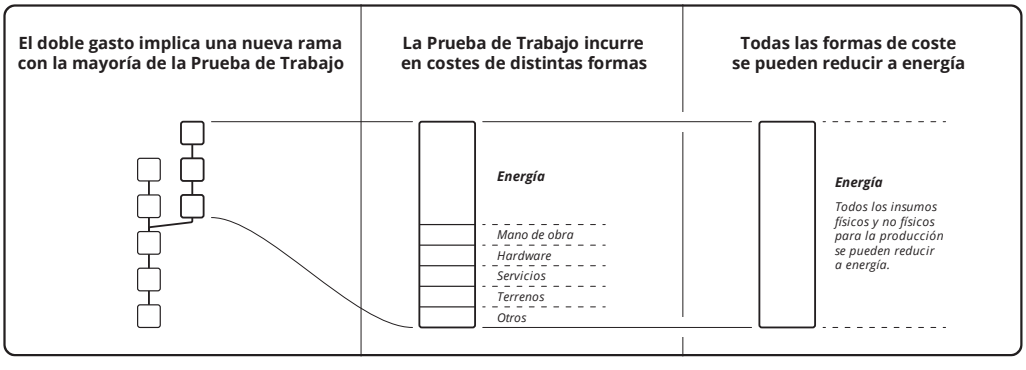
[1] https://es.wikipedia.org/wiki/Prueba_de_participaci%C3%B3n

[2] Capítulo: Falacia de la Prueba de Participación

[3] Capítulo: Propiedad del Umbral de Utilidad

gastando el mismo coste medio para un tiempo de confirmación dado, pero con un menor componente de energía.

El trabajo incurre en varias formas de costes, incluyendo la mano de obra, el *hardware*, los servicios, el terreno, etc. Cualquier otra prueba externalizada consume estos mismos recursos, aunque potencialmente en distinta proporción. La cuestión de la reducción del coste energético se reduce, por tanto, a si se puede sustituir un componente energético del coste de una prueba por un componente de distinto recurso con el mismo coste. Sin embargo, el coste del recurso sustituto incluye todos sus costes de producción, que deben ser asimilables a la energía. Por consiguiente, la teoría es inválida.



Además, asegurar cualquier moneda genera un coste para los comerciantes. Por consiguiente, su propia utilización por sí misma lleva implícito que se la prefiere a las alternativas. Esto implica que las alternativas son más costosas en última instancia. Dado que todos los costes son asimilables a energía, se deduce que el dinero[1] utilizado es el más eficiente energéticamente.

Reference

[1] Capítulo: Taxonomía del dinero

Falacia de la Recuperación de las Comisiones

Existe una teoría en el sentido de que las mineras obtienen una ventaja financiera sobre las demás mineras al minar sus propias transacciones y "recuperar" sus propias comisiones.

La teoría ignora el coste de oportunidad[1] de minar espacio en bloques sin recibir pago a cambio. El pago de una comisión *de cualquier importe* a uno mismo no constituye un evento financiero. No recaudar una comisión es un coste real por el importe que se ha dejado de ganar, ya que el coste de minar esa porción del bloque no se ve compensada. **La comisión real pagada por la minera es la oportunidad que deja pasar.**

Existe una teoría relacionada que afirma que se puede engañar a las herramientas de estimación de comisiones para que recomienden unas comisiones mayores de las exigidas. Según se muestra en la Falacia de las Comisiones Aparte[2], esto presupone una relación entre las comisiones históricas y futuras que no existe, y que todas las comisiones están visibles en la cadena, lo cual no es el caso.

Reference

[1] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[2] Capítulo: Falacia de las Comisiones Aparte

Falacia de la Reducción a la Mitad

Las reglas de consenso de Bitcoin producen una tasa predecible de inflación monetaria. Esta tasa se reduce periódicamente en un punto llamado *halving* (en español, "reducción a la mitad"). Existen varias funciones de escalón[1] en Bitcoin. La reducción a la mitad o *halving* se produce cada 210.000 bloques fuertes; el ajuste de la dificultad, cada 2.016 bloques fuertes; y la organización de la cadena, aproximadamente cada 10 minutos. Los valores numéricos que controlan esos intervalos son arbitrarios y, sin embargo, la discontinuidad resulta necesaria a causa de los intervalos discretos exigidos para la prueba de trabajo. Existe una teoría que dice que el *halving* crea un abismo financiero para las mineras que podría producir una parada perpetua. La teoría se basa en la confluencia de dos funciones de escalón (el *halving* y la dificultad), lo que hace que el periodo de otra (organización) se expanda vertiginosamente por la reducción coincidente en beneficios de las mineras.

La teoría supone que el ajuste de dificultad restablece en cero los beneficios financieros[2] medios de las mineras, dejando que solamente sobrevivan la mitad superior de las mineras (por rentabilidad), lo que termina por reducir la minería a unas pocas mineras. En otras palabras, el ajuste de dificultad se considera una presión de *pooling*[3] positiva. Sin embargo, no existe ningún motivo para creer que el ajuste reduzca a cero los beneficios de *ninguna* minera. La consecuencia de esta presuposición no es que habrá *pocas* mineras, sino que no habrá *ninguna*, por la mera causa del ajuste de dificultad. El ajuste en realidad no hace nada que regule los beneficios de las mineras, solamente controla el periodo de organización. Sin ajustes, los beneficios no se verían afectados mientras que el periodo de organización y, por consiguiente, la varianza responderían a una tasa de hash total. La

Reference

[1] https://es.wikipedia.org/wiki/Funci%C3%B3n_escalonada

[2] http://www.investopedia.com/terms/e/economicprofit.asp

[3] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

preferencia temporal[1], que dicta la rentabilidad de mercado sobre el capital, regula los beneficios de las mineras al igual que lo hace en cualquier mercado.

Considérese el caso de que no cambie el precio. En este caso, no existe ningún motivo para esperar un cambio en la tasa de hash total, no hay ajustes en la dificultad, y podemos concluir que la mina promedio genera la rentabilidad de mercado sobre el capital. En otras palabras, cualquier número de mineras independientes puede competir indefinidamente (en ausencia de presiones de *pooling* reales).

Considérese también que los cambios de precio, los ajustes de dificultad, y las fluctuaciones de las recompensas afectan todas ellas a la rentabilidad de las mineras de la misma manera. Por consiguiente, un ajuste de dificultad y/o *halving* no es más importante para una minera que una fluctuación comparable en el precio, y muestra una mayor predecibilidad.

La teoría también contempla que la recompensa podría ser insuficiente para compensar a las mineras por la dificultad inmediatamente después de un *halving*. Por consiguiente, podrían optar por reducir la tasa de hash, ampliar los tiempos de confirmación hasta que suban las comisiones, suba el precio y/o la dificultad se ajuste a la baja. No obstante, las comisiones y el precio se determinan en un mercado y ciertamente pueden subir a cualquier nivel que las personas estén dispuestas a pagar.

No hay manera de saber qué niveles soportará el mercado, pero el precio sigue teniendo un impacto mucho mayor que los eventos de *halving*. Los eventos de *halving* más grandes se han producido sin ninguna perturbación. Dado que los *halvings* sucesivos producirán el equivalente de una reducción de precios exponencialmente *menor*, no hay motivo para creer que los eventos futuros serán más interesantes que los pasados.

Reference

[1] https://en.wikipedia.org/wiki/Time_preference

Falacia de la Minería Impotente

Existe una teoría que afirma que las mineras no tienen ningún poder. Esta falacia es distinta de la Falacia de la Prueba de Trabajo[1], estrechamente relacionada. La teoría descansa en la suposición de que las mineras están sujetas a presiones económicas que excluyen de antemano los ataques eficaces sostenidos. Esta teoría lleva a personas a creer que la minería se puede realizar con un *pooling* intenso en tanto los comerciantes no estén centralizados, ya que la economía puede controlar el comportamiento de la minería, haciendo que el sistema sea seguro. La consecuencia de esta teoría inválida es la complacencia en relación con la inseguridad causada por la compartición de recursos.

La teoría sostiene que si la potencia de hash mayoritaria gasta por duplicado, entonces los comerciantes necesariamente aumentarán los requisitos de profundidad de confirmación, aumentando el coste de los ataques sucesivos. En algún punto se logra un equilibrio en el que unas profundidades mayores se consideren suficientes para el cambio. Dado que esto excluiría de antemano los gastos por duplicado, sostener el ataque no conllevaría ninguna ventaja. La teoría acepta que los ataques pueden producirse, pero no con suficiente frecuencia para reducir sustancialmente la utilidad.

La teoría también sostiene que una minera no puede evitar seleccionar las transacciones de mayores comisiones puesto que esto reduce la recompensa relativa, enriqueciendo a otras mineras. Se presupone que esto producirá una pérdida de potencia mayoritaria y, por consiguiente, la incapacidad de continuar. Este aspecto de la teoría implica que las mineras no pueden censurar eficazmente.

La teoría también considera que la minería egoísta por parte de la potencia de hash mayoritaria es viable, pero en ausencia de gastos por duplicado y censura, no existe ninguna consecuencia adversa para la economía. En este caso, la mayoría sencillamente

Reference

[1] Capítulo: Falacia de la Prueba de Trabajo

se convierte en la única minera, ya que los demás son incapaces de conservar las recompensas. A pesar de la falta de competencia, se mantienen la tasa de hash y los niveles de comisiones por la *posibilidad* de competencia, siempre próxima.

No obstante, las mineras y los comerciantes son socios comerciales, que desarrollan voluntariamente una actividad que redunda en beneficio mutuo. Según se exploró en la Falacia del Equilibrio de Poder[1], ninguno de ambos puede controlar al otro y el precio constituye la resolución de todas las preferencias. Esto parecería apoyar la teoría, sin embargo, **la teoría no aborda la amenaza**, y constituye una cortina de humo[2]. Bitcoin está diseñado para defenderse de las fuerzas *no de mercado*, específicamente el estado. Las fuerzas de mercado nunca son una amenaza para el propio mercado.

La puesta en común de potencia de hash como recurso eviscera la seguridad, ya que los estados sencillamente pueden cooptarla. Pero los estados también pueden construir sus propias minas a tal efecto. Por consiguiente, Bitcoin requiere tanto una potencia de hash significativa como *también* la distribución de esa potencia entre las personas dispuestas y capaces de asumir el riesgo de controles estatales[3].

El estado es un agente económicamente racional. La inflación es beneficiosa para el emisor. El amplio uso del Bitcoin evitaría que los estados recaudaran eficazmente el impuesto de la inflación[4]. Por consiguiente, cabe esperar ataques estatales, y ataques análogos son comunes[5]. En la práctica resulta inevitable que los estados subvencionen ataques, pero incluso la posibilidad de que lo hagan invalida la teoría.

Reference

[1] Capítulo: Falacia del Equilibrio de Poder

[2] https://es.wikipedia.org/wiki/Red_herring

[3] Capítulo: Principio de la Compartición de Riesgos

[4] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[5] https://en.wikipedia.org/wiki/Foreign_exchange_controls

Modelo de Negocio de las Mineras

Las mineras juegan a un juego de suma nula[1] dentro de una economía de suma positiva[2]. Compiten entre sí, no con la economía. El aumento de la utilidad es el reflejo de una suma positiva y una consecuencia natural de los intercambios.

Se ha argumentado que los bloques minados en un periodo de subida de precios producen rentabilidades desproporcionadas para las mineras, al menos hasta el ajuste de dificultad. Esta idea está basada en la incapacidad habitual para comprender que los precios de mercado no son predecibles[3]. Las apuestas sobre cambios de precios son especulativas. No existe ningún motivo para suponer que la especulación del Bitcoin sea ni más ni menos eficaz que cualquier otra. En la medida en que una subida de precio puede ser predicha con carácter general por las mineras, la competencia la predice, lo que invalida la idea de cualquier rentabilidad desproporcionada inherente.

La inversión en minería de Bitcoin, por otro lado, se basa en la relación predecible entre los beneficios y la competencia a lo largo del tiempo. Esa relación predice que el promedio de toda la minería se aproxima al tipo de interés de mercado. Como con todos los mercados, los periodos más breves son impredecibles en precio y los periodos más largos se aproximan a las rentabilidades de mercado. En última instancia, la preferencia temporal[4] controla la tasa de mercado para la rentabilidad de las inversiones.

¿Entonces cómo logra rentabilidades desproporcionadas una minera? No se puede hacer con acuerdos de comisiones aparte[5]. Solamente hay una manera de lograr una rentabilidad superior al tipo de mercado, que consiste en tener un coste de la potencia de

Reference

[1] https://es.wikipedia.org/wiki/Juego_de_suma_cero

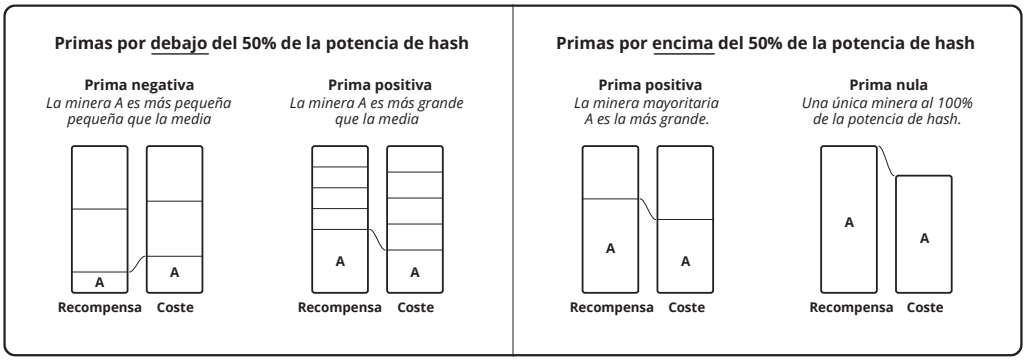
[2] https://es.wikipedia.org/wiki/Juego_ganar_ganar

[3] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_caos

[4] https://en.wikipedia.org/wiki/Time_preference

[5] Capítulo: Falacia de las Comisiones Aparte

hash inferior al medio para la moneda. Esto se logra aprovechando presiones de *pooling*[1] o por medio de una eficiencia operativa superior. Debido a la propiedad de suma nula[2], estas se compensan con tipos de rentabilidad menores a las del mercado por parte de otras mineras. Por consiguiente, la prima disminuye para una minera honesta por encima del 50% de potencia de hash, hasta cero al 100%.



Sin embargo, otras mineras terminarán por abandonar en tanto su capital persigue rentabilidades de mercado. Esto dejaría una minera, sujeta a las rentabilidades del mercado. En otras palabras, lograr rentabilidades desproporcionadas requiere otros de los que capturar esas rentabilidades. La rentabilidad más elevada que se puede sostener es función del máximo coste de oportunidad que otros están dispuestos a sostener. Este es función de la utilidad de recompensa diferencial, según se debate en Paradoja del Nivel de Amenaza[3].

Al limitar los dividendos[4] a las tasas de rentabilidad del mercado y reinvertir todas las recompensas restantes, una minera puede mantener una potencia de hash constante y, por consiguiente, obtener rentabilidades de mercado sobre una base de capital

Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[2] Capítulo: Propiedad de la Suma Nula

[3] Capítulo: Paradoja del Nivel de Amenaza

[4] https://es.wikipedia.org/wiki/Dividendo

proporcional a la capitalización del Bitcoin. Reinvertir los dividendos aumenta la potencia de hash y la liquidación la reduce. Los equipos de machacado se liquidan desconectando cada dispositivo cuando pasa a ser un productor neto negativo, o descontando[1] esos retornos futuros vendiendo el dispositivo.

El tipo de rentabilidad sobre el capital de la minería depende exclusivamente de la preferencia temporal. La relación entre la economía y las mineras se explora adicionalmente en Falacia del Equilibrio de Poder[2].

Reference

[1] https://en.wikipedia.org/wiki/Present_value

[2] Capítulo: Falacia del Equilibrio de Poder

Riesgo de Presiones Pro-Compartición de Recursos

La presión pro-compartición de recursos, o presión de *pooling*, es el conjunto de incentivos financieros para la agregación de la tasa de hash, específicamente:

- Prima de Proximidad[1]
- Descuento de Varianza[2]
- Variación de Mercado
- Distorsión de Mercado
- Economías de Escala[3]

La latencia y la varianza son inevitables. En realidad, las reglas de consenso crean esos dos primeros incentivos financieros. La variación es una consecuencia del cambiante precio de mercado de los recursos mineros. La distorsión es una consecuencia de los cambiantes costes no de mercado, incluidos la fiscalidad, la regulación, la subvención, y las patentes; la fuerza contra la que Bitcoin tiene la finalidad de resistir[4]. En un entorno de amenaza elevada, las economías de escala podrían pasar a ser negativas por el coste asociado a una mayor visibilidad[5] pero, por lo demás, podrán ser positivas.

Existen varias manifestaciones de la compartición de recursos. Una es geográfica; en ella, unas mineras independientes pasan a estar más próximas físicamente. Otra es cooperativa; en este caso, las mineras previamente independientes unen fuerzas y ubican conjuntamente el trabajo de machacado. Otra es virtual; en ella, las mineras se convierten

Reference

[1] Capítulo: Fallo Lógico de la Prima de Proximidad

[2] Capítulo: Deficiencia del Descuento de Varianza

[3] https://es.wikipedia.org/wiki/Econom%C3%ADa_de_escala

[4] Capítulo: Axioma de resistencia

[5] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/

en machacadoras y agregan tasa de hash a una única minera remota. Otra consiste en utilizar repetidores[1], que agregan potencia de hash de las mineras. Otra es el flujo de capitales, puesto que la mayor tasa de hash asociada a una mayor utilización de capital constituye una forma de ubicación conjunta.

Dada una presión positiva perpetua, la selección de transacciones estará reducida eventualmente al control de una persona. Es posible que este ya sea el caso. El riesgo para Bitcoin es que una persona sea la única defensa[2] de la utilidad, haciendo inevitable una cooptación exitosa. Este riesgo no puede ser mitigado[3] por la economía.

La presión pro-compartición de recursos es una analogía en Bitcoin del sistema de la Reserva Federal de los Estados Unidos[4]. El sistema fue diseñado[5] para facilitar la fiscalidad por medio de la devaluación[6] de un tipo de dinero de mercado. Ofrecía apoyo[7] estatal para un sustituto[8] monetario a cambio de dinero de mercado[9]. Esta combinación fue diseñada para crear una presión que recaudara dinero de mercado en la autoridad central. Una vez que esta recaudación fue suficiente, el estado se dejó de fingimientos y sencillamente se incautó[10] de todo el dinero de mercado que quedaba. Todos los estados tienen sistemas parecidos y cooperan[11] para defenderlos.

Reference

[1] Capítulo: Falacia del Repetidor

[2] Capítulo: Principio de la Compartición de Riesgos

[3] Capítulo: Falacia del Equilibrio de Poder

[4] https://www.federalreserve.gov

[5] Capítulo: Principio de la Banca Estatal

[6] https://es.wikipedia.org/wiki/Envilecimiento_de_la_moneda

[7] https://es.wikipedia.org/wiki/Curso_legal

[8] https://es.wikipedia.org/wiki/Billetes_de_d%C3%B3lar_estadounidense

[9] Capítulo: Taxonomía del dinero

[10] https://es.wikipedia.org/wiki/Orden_Ejecutiva_6102

[11] https://es.wikipedia.org/wiki/Fondo_Monetario_Internacional

Esto no implica que la minería sea adversa al Bitcoin. Siguiendo la analogía, la banca libre[1] no se opone al oro. La minería constituye una parte necesaria del Bitcoin. La compartición de recursos representa un riesgo, aunque la presión pro-compartición de recursos no la crean las mineras sino deficiencias en el propio Bitcoin.

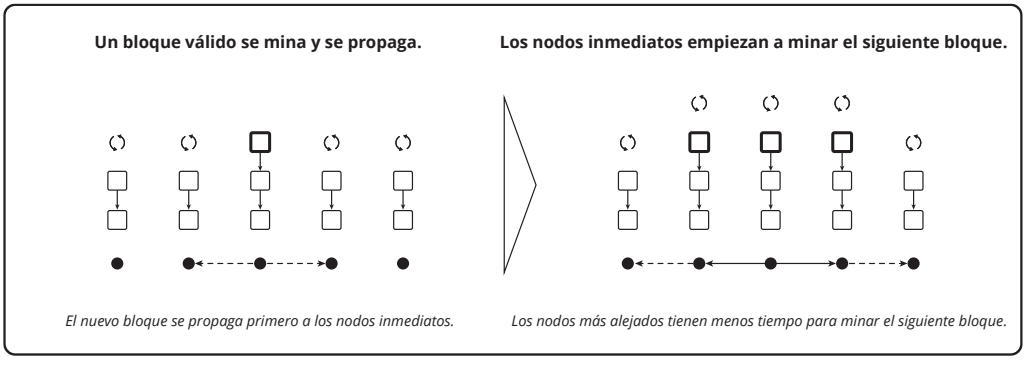
Reference

[1] https://es.wikipedia.org/wiki/Banca_libre

Fallo Lógico de la Prima de Proximidad

La latencia es el tiempo exigido para la comunicación. La información se mueve a una velocidad no mayor a la velocidad de la luz[1] y, por consiguiente, no se puede eliminar la latencia.

Las diferentes distancias entre las mineras implica que los anuncios serán conocidos por unos antes que por otros. Mientras una minera siga sin ser consciente de un anuncio, estará desperdiciando el capital machacándose con un candidato débil. A medida que pasan más tiempo, pasa a ser exponencialmente menos probable que la minera sea recompensada por el candidato. Las mineras, por consiguiente, compiten por ver los anuncios antes que las demás mineras, puesto que esto reduce el coste de oportunidad[2].



Si dispersáramos las mineras con igual tasa de hash a puntos equidistantes alrededor de la tierra, experimentarían la misma latencia promedio. Y, sin embargo, debido a la ventaja financiera de una reducción en latencia, tenderían a acercarse unas a otras. Las mineras obtienen una prima en los retornos por la agregación.

Reference

[1] https://es.wikipedia.org/wiki/Velocidad_de_la_luz

[2] https://es.wikipedia.org/wiki/Coste_de_oportunidad

Esta presión pro-compartición de recursos[1] basada en la proximidad es consecuencia de la ordenación lineal de bloques requerida por las reglas de consenso. **Bitcoin prescribe una ordenación en la que el ganador se lleva todo, lo cual produce un coste de oportunidad dispar.** El descuento por varianza[2] es la otra presión pro-compartición de recursos causada por el consenso.

La defensa[3] que Bitcoin *tiene la intención* de levantar es la defensa del mercado contra las fuerzas anti-mercado (estatales). Para hacer esto, la potencia de hash tiene que distribuirse ampliamente entre las personas de manera que pase a ser difícil de cooptar. Sin embargo, las presiones pro-compartición de recursos inherentes en el consenso actúan en contra de este objetivo. Por consiguiente, esta característica se apunta como deficiencia, aunque no se ha descubierto ninguna manera de eliminar esta deficiencia.

Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

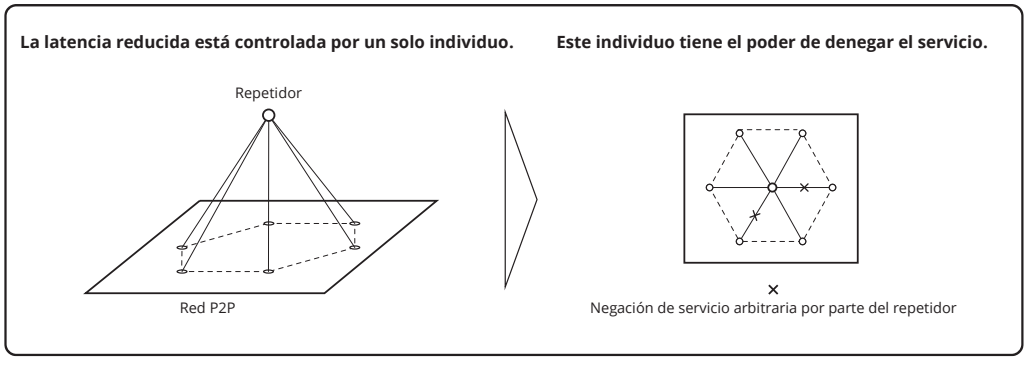
[2] Capítulo: Deficiencia del Descuento de Varianza

[3] Capítulo: Axioma de resistencia

Falacia del Repetidor

La red entre pares disemina bloques y transacciones no confirmadas. El protocolo en sí permite que los nodos se protejan ante la negación del servicio. Por consiguiente, esta comunicación no requiere de ninguna identidad. Esta protección es la manera que tiene la red de evitar la necesidad de permisos para participar.

Sin embargo, esta protección incurre en un coste en términos de latencia en los anuncios, y debido a la ventaja de la proximidad[1], una menor latencia se traduce en una mayor potencia de hash aparente. Por consiguiente, las mineras compiten por una reducción en la latencia. Una forma de reducir la latencia es la compartición de recursos, otra consiste en utilizar una red de diseminación más eficiente. Dado que la compartición de recursos entrega poder al gestor, presumiblemente la segunda opción resulte preferible.



Una forma de mejorar la diseminación es *optimizar* la red entre pares (*Peer-to-Peer*). La otra es unirse a una red distinta, llamada repetidor, que tenga una latencia menor por la eliminación de las protección contra negaciones del servicio, por ejemplo[2]:

Reference

[1] Capítulo: Fallo Lógico de la Prima de Proximidad

[2] http://bitcoinfibre.org

> El formato de mensaje cmpctblock fue diseñado para garantizar que se adaptara bien a un mecanismo de repetidor basado en UDP-FEC. La única diferencia reside en que lo enviamos a través de UDP con FED... De esta manera, los saltos adicionales no introducen más latencia. Tristemente, a causa de la naturaleza de la codificación FEC, no podemos saber si los paquetes individuales forman parte de un bloque legítimo, o de algún bloque, y así solamente permiten esta optimización entre nodos operados por el mismo grupo.
>
> *bitcoinfibre.org*

El repetidor acepta la comunicación desde un conjunto de mineras a través del protocolo *peer-to-peer* u otro protocolo. El repetidor está compuesto por un conjunto de máquinas bajo el control del operador del repetidor. Comunica los anuncios dentro de su red interna[1] y, eventualmente, a las mineras adheridas.

La observación de seguridad importante es que la comunicación dentro del repetidor está bajo el control del operador del repetidor. Al retirar las protecciones contra negaciones del servicio, el control central resulta *necesario* para el sistema. El operador del repetidor puede retrasar ciertos bloques sobre la base de la minera, la región, la señal, el impago, etc. Un operador de repetidor vende una latencia reducida y, por consiguiente, está dentro del negocio de la minería. Desde un punto de vista de la seguridad, da igual que el servicio se ofrezca o no gratuitamente. De manera análoga, las mineras podrían ofrecer a las machacadoras una reducción gratuita de la latencia y la varianza.

Los repetidores son agregaciones de mineras y las mineras son agregaciones de machacadoras. Cuanto mayor sea la agregación de la potencia de hash, más rentable es la mina, y el repetidor. Uno podría considerar que las machacadoras son libres de dejar las minas y que las mineras son libres de dejar los repetidores, y naturalmente es posible que una machacadora opere su propia mina y su propio repetidor. Pero las agregaciones más

Reference

[1] https://bitcoinmagazine.com/articles/blockstream-satellite-broadcasting-bitcoin-space

grandes son más rentables, por lo cual dejar el repetidor o la mina de mayor tamaño aumenta el coste relativo[1].

Una teoría sostiene que los repetidores reducen la presión pro-compartición de recursos. Esto constituye un error. **La reducción en la compartición de recursos causada por un repetidor no desaparece sino que se transfiere al repetidor como un aumento de la compartición de recursos.** Las estadísticas de los repetidores típicamente no se presentan junto con las estadísticas de minado, lo que enmascara la transferencia de poder. Esto puede llevar a la gente a pensar que la minería tiene una compartición de recursos menos intensa de la que realmente se da.

Reference

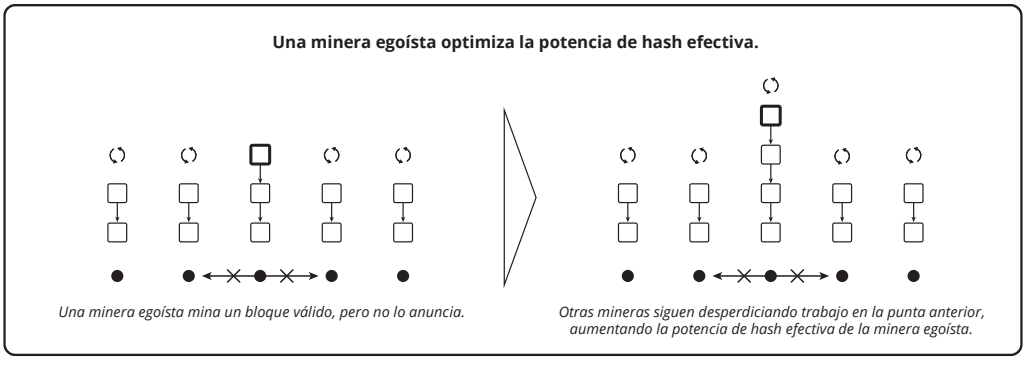
[1] Capítulo: Propiedad de la Suma Nula

Falacia de la Minería Egoísta

La expresión minería egoísta se refiere a la *optimización* de la minería. Sin embargo, un artículo académico[1] contextualiza la optimización de la siguiente manera:

> La sabiduría convencional afirma que el protocolo de minado es compatible con los incentivos y seguro ante la colusión de grupos minoritarios, es decir, que incentiva que las mineras sigan el protocolo según se prescribe. Mostramos que el protocolo de minado de Bitcoin no es compatible con los incentivos.
>
> *Ittay Eyal y Emin Gün Sirer: La mayoría no basta*

Esta afirmación supone un "protocolo de minado de Bitcoin prescrito" que excluye de antemano la retención, lo cual constituye un hombre de paja[2]. Las reglas de consenso de Bitcoin guardan silencio necesariamente en lo que respecta a los tiempos de los anuncios.



> Presentamos un ataque con el que las mineras en colusión obtienen unos ingresos mayores que su cuota justa.

Reference

[1] https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

[2] https://es.wikipedia.org/wiki/Falacia_del_hombre_de_paja

Esta afirmación supone un concepto de "cuota justa" ajeno a Bitcoin, otro hombre de paja. Una minera recibe una recompensa sobre la base de los bloques que alcanzan la madurez, no como proporción de una tasa de hash real.

Estos hombres de paja se atribuyen explícitamente a la "sabiduría convencional". En otras palabras, el artículo las utiliza para mostrar que la sabiduría convencional es incorrecta. Sin embargo, el artículo yerra al declarar incondicionalmente que esta *violación del protocolo* supuestamente *injusta* constituye un ataque:

> Esta ataque puede tener consecuencias significativas para Bitcoin: Las mineras racionales prefieren unirse a las mineras egoístas, y el grupo en colusión aumentará de tamaño hasta hacerse mayoritario. En ese momento, el sistema de Bitcoin deja de ser una divisa descentralizada.

Esa es la fuente de la falacia. No es un ataque que la sabiduría convencional sea incorrecta, es un error de la supuesta sabiduría convencional. La minería egoísta implica que Bitcoin exhibe presión pro-compartición de recursos[1] sobre la base de la latencia, aunque esto es una deficiencia bien establecida[2]. Todas las presiones pro-compartición de recursos tienden a reducir el número de mineras, lo que expone a Bitcoin a ataques.

Las optimizaciones no son ataques. La compartición de recursos aumenta las *oportunidades* de los ataques, pero las oportunidades no se deben confundir con las acciones. El término "ataque" implica robo. De hecho, el artículo que propuso[3] Bitcoin utiliza el término solamente para describir los intentos de gastos por duplicado.

Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[2] Capítulo: Fallo Lógico de la Prima de Proximidad

[3] https://bitcoin.org/bitcoin.pdf

Falacia de las Comisiones Aparte

Existe una teoría que afirma que las comisiones por transacciones que se pagan externamente representan un incentivo individual que produce un efecto contrario a la seguridad del sistema (incompatible con los incentivos[1]). La teoría sostiene que un comerciante que le paga a una minera "fuera de la cadena" para confirmar las transacciones del comerciante impide que las transacciones de otros comerciantes sean confirmadas, o que aumenta el coste de esas confirmaciones, dando ventaja a los que acepten tales comisiones.

Un impacto de este tipo de esquemas es que no se puede determinar una tasa promedio *histórica* de las comisiones por medio del análisis de la cadena. La tasa aparente sería menor que la tasa de mercado. Esto, por supuesto, podría llevar a que los que realicen gastos subestimen la comisión suficiente. Sin embargo, no hay ningún aspecto del Bitcoin que exija que las comisiones futuras igualen un promedio de las comisiones pasadas. La estimación necesariamente realiza compensaciones, como ignorar las transacciones “gratuitas” en los bloques completos o utilizar la desviación típica[2] para identificar las muestras atípicas. Pero la estimación de comisiones es solo eso, estimación. Los niveles actuales de comisiones están controlados por la competencia.

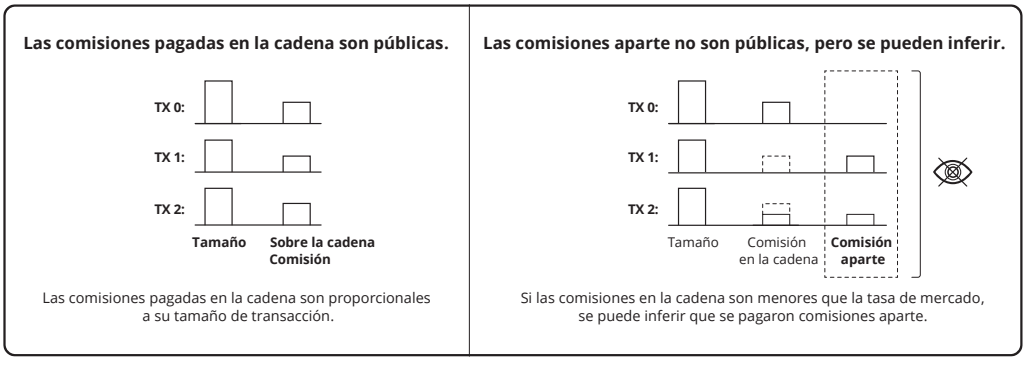
Otro impacto es que los diferentes niveles de comisiones relativas puedan destacar ciertas transacciones como asociadas a tales esquemas. Esto puede contribuir a contaminar la transacción del comerciante y/o la base monetaria de la minera. Pero dado que este esquema ha sido elegido por los creadores de estas transacciones, no hay ninguna pérdida de privacidad.

Reference

[1] https://en.wikipedia.org/wiki/Incentive_compatibility

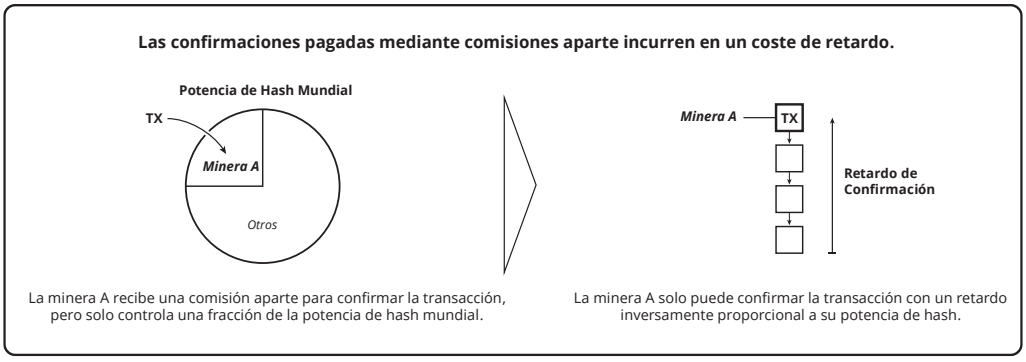
[2] https://es.wikipedia.org/wiki/Desviaci%C3%B3n_t%C3%ADpica

No hay ningún impacto en las tasas de las comisiones de mercado ni en la capacidad de que otros obtengan confirmaciones. Si el esquema se desvía de las tasas de mercado, entonces o bien la minera o el comerciante están aceptando una pérdida innecesaria. No es distinto al caso de que la minera confirme transacciones con comisiones en la cadena por debajo de las de mercado o el caso de que el comerciante sobrestime las comisiones en la cadena, respectivamente. En cualquier caso, no habría ningún perjuicio para la seguridad del sistema incluso si todas las comisiones se pagaran fuera de la cadena.



Bitcoin proporciona un mecanismo de comisiones en la cadena de manera que una transacción pueda compensar a *cualquier* minera sin utilizar su identidad. Es un aspecto práctico que preserva la privacidad. **Si las mineras y los comerciantes prefieren debilitar su propia privacidad realizando tareas adicionales, no hay ninguna base para considerar esto poco deseable.** Por consiguiente, esta teoría es inválida.

Además, el comerciante tiene que aceptar un tiempo de confirmación retardado inversamente proporcional a la potencia de hash de la minera. La comisión aparte se ofrece a la tasa de mercado puesto que, de lo contrario, la minera incurrirá en un coste de oportunidad.



Existe una teoría que afirma que los esquemas de comisiones aparte constituyen una presión pro-compartición de recursos[1]. Si las comisiones pagadas son consistentes con el mercado, no puede haber ningún efecto sobre la compartición de recursos. Las comisiones por encima de mercado constituyen una subvención estatal, ya que tenemos que tratar la subvención como no racional económicamente. Las comisiones por debajo de mercado son un impuesto, ya que tenemos que tratar las pérdidas como involuntarias. Son distorsiones como cualquier otro impuesto/subvención estatal y, por consiguiente, no son exclusivas de las comisiones aparte. Por consiguiente, la existencia de comisiones aparte no crea una nueva presión pro-compartición de recursos más allá de lo que existe con las comisiones en la cadena, y la teoría, por tanto, es inválida.

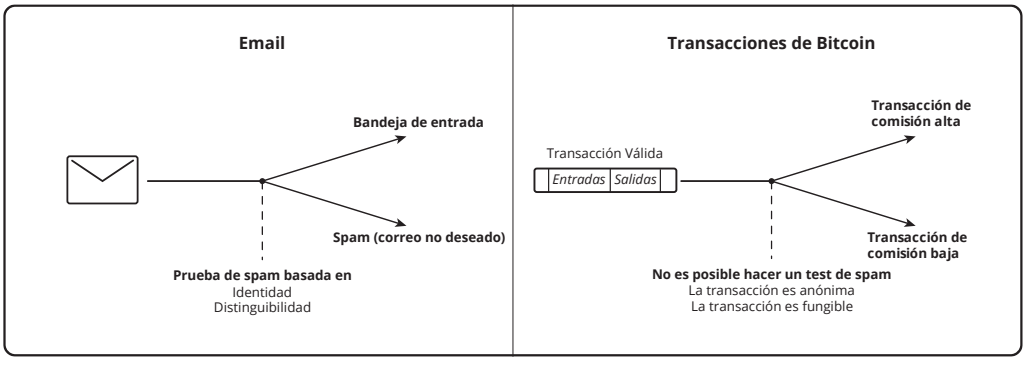
Reference

[1] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

Spam como denominación poco apropiada

El término spam[1] en informática se refería originariamente a las publicaciones cruzadas excesivas en Usenet y posteriormente se convirtió en un sinónimo de los correos electrónicos no deseados. Si bien no existe una clara distinción entre los correos electrónicos deseados y los no deseados, los mensajes transmiten la identidad, no son fungibles, y no transmiten un pago para su procesamiento por el destinatario. En comparación, las transacciones de Bitcoin son necesariamente anónimas[2], fungibles y transmiten pagos para su procesamiento.

Si bien la detección del *spam* en correos electrónicos es un proceso subjetivo, es necesario por la falta de pagos a procesar. Esto proceso se ve facilitado por la identidad y por la falta de fungibilidad. Por el contrario, gracias al anonimato y al objetivo de fungibilidad, no existe ninguna prueba posible para decidir la legitimidad de una transacción, y gracias al pago no hay ninguna necesidad de ella. En otras palabras, **todas las transacciones válidas son igualmente legítimas**, y esto no expone a los nodos a negaciones del servicio. Un nombre adecuado para una transacción con una comisión baja es "transacción a comisión baja".



Reference

[1] https://en.m.wikipedia.org/wiki/History_of_email_spam

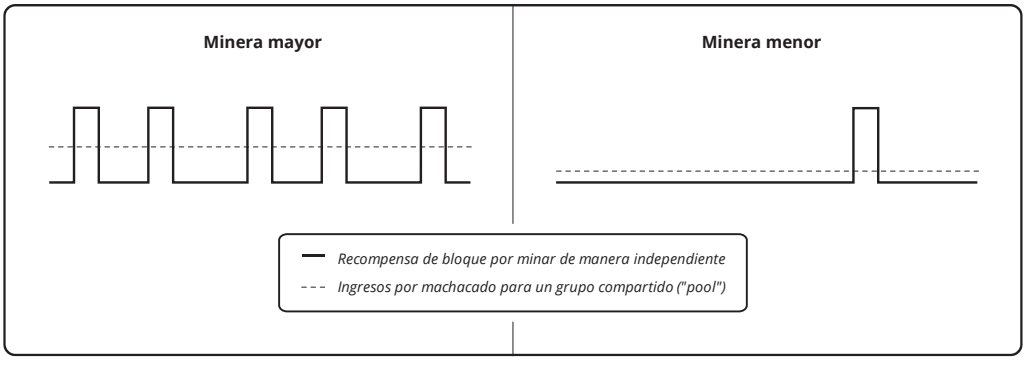
[2] Capítulo: Principio de la Compartición de Riesgos

El envío de un alto volumen de transacciones redundantes constituye un problema típico de negación del servicio que es independiente de la comisión de las transacciones y puede ser llevado a cabo por cualquier persona, no solo quien realice un gasto. Las transacciones no redundantes que incorporan gastos en conflicto entre sí no suponen un riesgo de negación del servicio, puesto que o bien son rechazadas como inválidas o son aceptadas gracias a un aumento suficiente de la comisión.

Deficiencia del Descuento de Varianza

La varianza es la frecuencia variante con que se logra una recompensa. La varianza es inherente a la naturaleza probabilística de la minería y no puede ser eliminada.

Por cuestión de consenso, una potencia de hash distinta entre mineras implica que las recompensas serán obtenidas por unas con más frecuencia que por otras. Con un 10% de tasa de hash, uno podría esperar ser recompensado 10 veces más frecuentemente que con un 1%. Los resultados reales son impredecibles y pueden variar significativamente. Pero aquí basta en ambos casos con suponer que haya proporcionalidad. En este ejemplo, una minera recibe una recompensa cada 100 minutos y la otra cada 1000 minutos. Suponiendo recompensas idénticas por bloque, la magnitud de la recompensa también es proporcional a la potencia de hash.



Considérese entonces que una minera diminuta podría tener que esperar durante años antes de una recompensa. También existe la posibilidad de que una mina se configure mal y no pueda tener éxito nunca. A pesar de ser recompensada proporcionalmente, una minera más pequeña se enfrenta a una deficiencia en relación con la minera más grande. Debe mejorar su flujo de liquidez[1] para recibir una fracción de la recompensa más

Reference

[1] https://en.wikipedia.org/wiki/Operating_cash_flow

frecuentemente. Por estos motivos, las mineras descuentan rentabilidad a cambio de una menor varianza. Las mineras más pequeñas convertirán sus minas en machacadoras y pagarán a una minera agregante por una varianza menor. Evitar esta agregación es la justificación que hay detrás de P2Pool[1], pero puesto que la reducción de la varianza distribuida es menor eficiente, domina la compartición de recursos.

Esta presión pro-compartición de recursos[2] basada en la varianza es una consecuencia de la dificultad singular que exigen las reglas de consenso. **Las mineras pequeñas tienen que competir a una dificultad alta a pesar de una potencia de hash baja, lo cual magnifica la varianza inherente.** La prima de proximidad[3] es la otra presión pro-compartición de recursos causada por el consenso.

La defensa[4] que Bitcoin *tiene la intención* de levantar es la defensa del mercado contra las fuerzas anti-mercado (estatales). Para hacer esto, la potencia de hash tiene que distribuirse ampliamente entre las personas de manera que pase a ser difícil de cooptar. Sin embargo, las presiones pro-compartición de recursos inherentes en el consenso actúan en contra de este objetivo. Por consiguiente, esta característica se apunta como deficiencia, aunque no se ha descubierto ninguna manera de eliminar esta deficiencia.

Reference

[1] https://en.bitcoin.it/wiki/P2Pool

[2] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[3] Capítulo: Fallo Lógico de la Prima de Proximidad

[4] Capítulo: Axioma de resistencia

Propiedad de la Suma Nula

La minería de Bitcoin es un juego de suma nula[1]. En promedio, la cadena crece un bloque cada 10 minutos, controlando su minera toda la recompensa. Las mineras compiten por lograr esta recompensa y, aparte de las presiones pro-compartición de recursos[2], cada una de ellas promedia un número de recompensas proporcional a la tasa de hash. La diferencia entre el coste de una minera y esta recompensa a lo largo del tiempo es el interés sobre el capital invertido en la mina.

Hay dos aspectos de la propiedad de suma nula:

- Durante el periodo de tiempo entre las organizaciones, una minera gana una recompensa y las demás mineras no ganan ninguna recompensa. Ni el precio, ni la tasa de hash, ni la dificultad, ni la inflación, ni las comisiones, ni ninguna otra cosa tienen ningún efecto sobre esta propiedad.
- La magnitud de las recompensas, ya sea en unidades de moneda o precio de cambio, no tiene ningún efecto en la tasa de retorno sobre el capital.

La minería de Bitcoin idealizada constituye un sistema cerrado[3]. El retorno sobre el capital varía en relación con las otras minas, a causa de las deficiencias del protocolo que constituyen la prima de proximidad[4] y el descuento por varianza[5], así como por las economías de escala[6] y la eficiencia de la operadora. **Sin embargo, porque estas solo impactan al coste relativo de la tasa de hash, se ve afectada la proporcionalidad de las tasas de retorno, no los retornos totales.**

Reference

[1] https://es.wikipedia.org/wiki/Juego_de_suma_cero

[2] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

[3] https://es.wikipedia.org/wiki/Sistema_cerrado

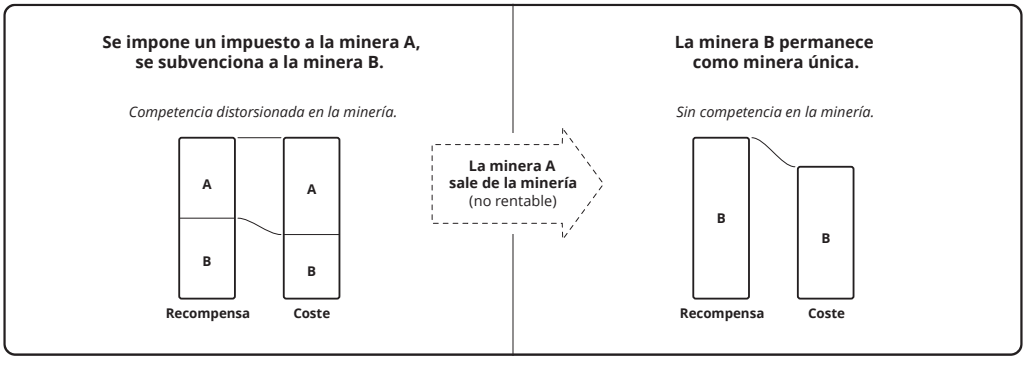
[4] Capítulo: Fallo Lógico de la Prima de Proximidad

[5] Capítulo: Deficiencia del Descuento de Varianza

[6] https://es.wikipedia.org/wiki/Econom%C3%ADa_de_escala

El Bitcoin real no constituye un sistema cerrado. Las presiones pro-compartición de recursos de mercado y anti-mercado de variación y distorsión (respectivamente) son externas. Fundamentalmente, Bitcoin existe para defender los mercados, enfrentando necesariamente a la distorsión contra la variación (o falta de ella).

Cuando se aplica una distorsión a una minera en este sistema de suma nula, todas las demás mineras se ven afectadas. Por ejemplo, una subvención[1] (no confundir con una subvención de consenso) a una minera actúa como un impuesto a todas las demás, y un impuesto a una minera actúa como una subvención a todas las demás. La minera subvencionada opera a un coste menor para la misma tasa de hash, o tiene una mayor tasa de hash efectiva (es decir, potencia de hash) por el mismo coste. La minera sujeta al impuesto opera a un coste mayor para la misma tasa de hash, o tiene una menor tasa de hash efectiva por el mismo coste.



Quien subsidia no espera ningún retorno sobre el capital, de lo contrario se consideraría inversor(a). La inversión es una fuerza de mercado mediante la cual la minera paga un precio de mercado por el capital. Con una mayor tasa de retorno efectiva, la minera subvencionada atrae más capital que otras mineras, y sigue aumentándose su potencia

Reference

[1] https://es.wikipedia.org/wiki/Subsidio

de hash hasta que haya una minera con potencia de hash mayoritaria. El objetivo de quien subsidia es, en última instancia, el *control* sobre la mina subvencionada.

Un impuesto sobre la minería tiene el efecto de mover la potencia de hash a minas no sujetas a impuestos, más allá del alcance de la autoridad fiscal, ya que el capital persigue rendimientos de mercado. Si se aplica ampliamente, esto puede darle a la autoridad el control o medio de su propia explotación minera. En otras palabras, la autoridad puede suprimir la competencia. Esto también se puede lograr mediante un impuesto del 100%, en virtud del cual la autoridad coopte las minas. El efecto es el mismo, se expulsa del negocio a la minera sujeta a impuesto, y el dinero recaudado con el impuesto se destina al control.

Las consecuencias de la minería de suma nula con presión pro-compartición de recursos inherente se exploran en Paradoja del Nivel de Amenaza[1].

Reference

[1] Capítulo: Paradoja del Nivel de Amenaza

ALTERNATIVAS

Etiquetas indicativas de Bitcoin

Desde su comienzo, Bitcoin ha desafiado las definiciones claras[1]. Esto es consecuencia de la utilización del término, muy sobresaturado. El término fue acuñado por Satoshi en Bitcoin: A Peer-to-Peer Electronic Cash System[2] ("Bitcoin: Un sistema de efectivo electrónico entre iguales") como etiqueta indicativa de los conceptos esenciales. Posteriormente fue utilizado para la implementación del prototipo, una cadena (historial) de transacciones confirmadas, un conjunto de reglas de consenso que limitan una cadena, una unidad de la moneda, y una comunidad de personas de límites borrosos.

Si bien solamente hay un conjunto de conceptos, cada uno de los demás contextos tiene cualquier número de variaciones posibles consistentes con ellos. Existen muchas implementaciones (del prototipo y de lo demás), las reglas de consenso han divergido (en el prototipo y en las demás implementaciones), el historial es dinámico y arbitrario (incluso el bloque de génesis codificado en el prototipo podría haber sido distinto sin consecuencias), y cada moneda manifiesta un conjunto independiente de unidades y está apoyada por su propio conjunto de adeptos.

Por estos motivos, Bitcoin se utiliza en la presente obra como etiqueta indicativa de los Principios Criptodinámicos[3]. Se hace referencia a las implementaciones por sus marcas[4], como "Bitcoin Core"[5] o "Libbitcoin"[6]; se hace referencia a las cadenas por los símbolos de *trading* en uso habitual, como "BTC" y "LTC"; se hace referencia a las reglas de consenso de una cadena dada en el contexto de su símbolo de *trading*, como "reglas de consenso

Reference

[1] http://gavinandresen.ninja/a-definition-of-bitcoin

[2] https://bitcoin.org/bitcoin.pdf

[3] Capítulo: Principios Criptodinámicos

[4] Capítulo: Arrogación de marca

[5] https://bitcoin.org/en/bitcoin-core

[6] https://libbitcoin.info

LTC"; una unidad de moneda se denomina con la minúscula del símbolo de *trading*, como "btc" o "ltc" (un refinamiento de la convención ambigua de utilizar "bitcoin" en minúscula para referirse a una unidad de "BTC"); y las comunidades se denominan o bien como "comunidad Bitcoin" (con carácter general) o "comunidad BTC" (con carácter específico).

Si bien los maximalistas[1] podrían rechazar el uso de "Bitcoin" como etiqueta indicativa de concepto, asociándola por el contrario con un historial, **el término fue acuñado en relación con un conjunto de principios y sigue siendo aplicable a estos.** Además, existen múltiples ejemplos de cadenas independientes que se adhieren a esos principios, haciendo que resulte ambigua la etiqueta indicativa sobre la base del historial. A causa de esta ambigüedad, la gente ha adoptado naturalmente la convención de referirse a los historiales sin ambigüedad por medio de los símbolos de *trading*.

Reference

[1] Capítulo: Definición de maximalismo

Falacia de la Cadena de Bloques

Existe una teoría en el sentido de que la propiedad poseída se puede asegurar mediante un registro de derechos reclamables inmutable, protegiéndolo tanto de la pérdida del derecho reclamable como del riesgo de custodia[1].

Puesto que un derecho reclamable no es en sí mismo la propiedad, el control de la propiedad descansa en el custodio contra el cual se realiza la reclamación. Un custodio tiene la capacidad de entregar o retener la propiedad y es, por consiguiente, un tercero de confianza[2]. La abolición de un derecho reclamable realizada por su custodio siempre se ve mitigada por una firma del custodio, criptográfica o de otro tipo, dejándose a su propietario la ejecución del derecho.

La teoría afirma que el registro inmutable de derechos reclamables proporciona seguridad contra la pérdida del derecho reclamable por su propietario, ya que nadie más estaría interesado en que lo perdiera. Sin embargo, para reclamar el derecho reclamable su propietario tiene que mostrarle al custodio una prueba de que es el propietario. Esto requiere que el propietario no pierda el secreto que demuestra que es el propietario. Por consiguiente, la seguridad del derecho reclamable contra pérdidas no se ve mitigada en absoluto, solamente cambia de forma. Por lo tanto, la teoría es inválida sobre la base de la prevención de pérdidas.

Guardar una referencia fuerte al derecho reclamable puede reducir el tamaño, y por consiguiente el coste, de su almacenamiento inmutable. El derecho reclamable podrá estar en forma de un contrato humano o máquina, y se hará referencia al mismo como hash unidireccional[3]. En cualquier caso, se exigen la validación y la ejecución del contrato

Reference

[1] Capítulo: Principio de Riesgo de Custodia

[2] https://en.wikipedia.org/wiki/Trusted_third_party

[3] https://es.wikipedia.org/wiki/Funci%C3%B3n_hash_criptogr%C3%A1fica

para que se transfiera la propiedad por parte del custodio. Por consiguiente, un derecho reclamable contractual referenciado aumenta el riesgo de pérdida con datos adicionales, el contrato.

Según se muestra en Principio de Compartición de Riesgos[1], las personas siempre forman la base de la seguridad. Las personas pueden actuar colectivamente para proteger la inmutabilidad de un dinero, y, por consiguiente, los datos de derechos reclamables asociados al control del dinero.

Sin embargo, un custodio es un tercero en el que se confía. Los derechos reclamables inmutables no mitigan en ningún caso los ataques directos contra un custodio o por parte de un custodio. Cuando el custodio es el estado o está sujeto a su control, el derecho reclamable no ofrece ninguna garantía[2] contra la posibilidad de que la autoridad estatal sustituya a la propiedad demostrada de cualquier derecho reclamable. Por consiguiente, la teoría también es inválida sobre la base del incumplimiento de custodia.

Bitcoin como dinero[3] no está sujeto a custodia. Sus unidades no representan un activo mantenido por un tercero en el que se confía. El dinero se intercambia directamente entre el cliente y el comerciante. En este sentido, *todos los comerciantes* son custodios del valor de Bitcoin. **La falacia de la cadena de bloques surge de una idea equivocada del modelo de seguridad de Bitcoin, que atribuye la seguridad a su tecnología en vez de a su distribución de comerciantes.** El término "tecnología de cadena de bloques" refuerza este error, llevando implícito que es principalmente la estructura de los datos de Bitcoin lo que lo asegura.

Reference

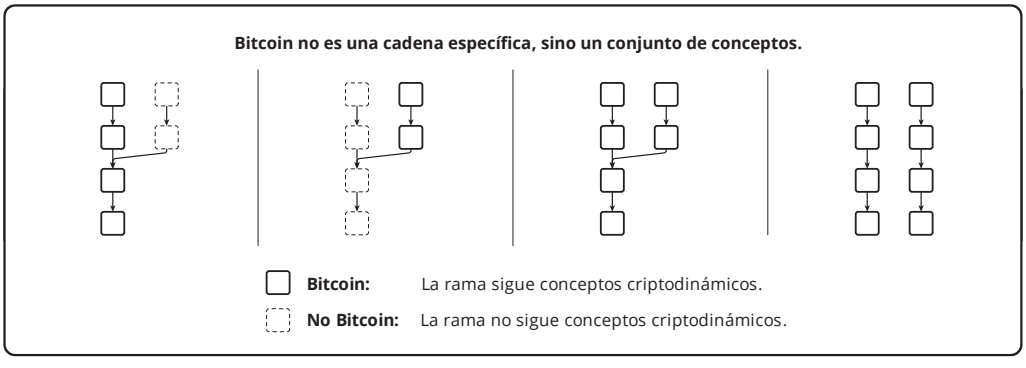
[1] Capítulo: Principio de la Compartición de Riesgos

[2] https://es.wikipedia.org/wiki/Orden_Ejecutiva_6102

[3] Capítulo: Taxonomía del dinero

Arrogación de marca

Bitcoin es un conjunto de conceptos esenciales[1], no una cadena. Ninguna persona puede controlar los conceptos. Las personas lo utilizarán para describir una o más cadenas y divisiones según vayan evolucionando. Esto sucede con todos los tipos de dinero[2], incluido el oro y el petróleo que se comercian con diferentes purezas y calidades.



Esto es consistente con la declaración de Bitcoin[3], ya que vincula un conjunto de conceptos, no un conjunto de reglas, protocolos, o implementaciones. **Las personas con capital invertido tienen un deseo inherente de que se asocie con la marca, pero no existe nada parecido a un derecho "legítimo" a tal asociación.**

Reference

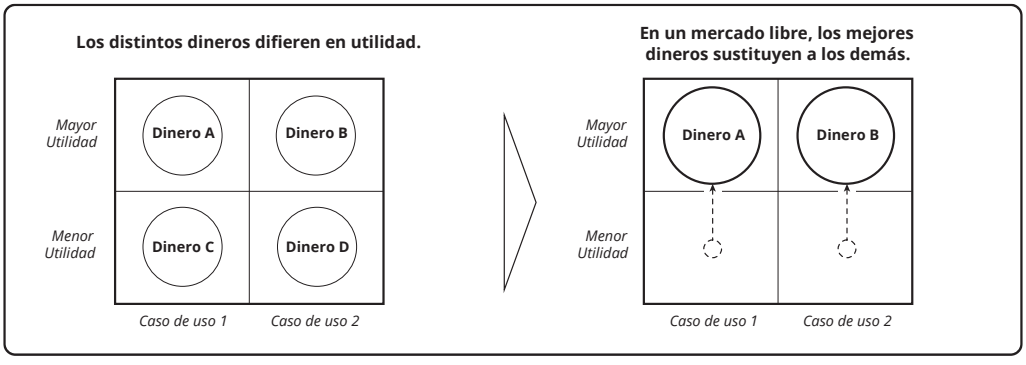
[1] Capítulo: Principios Criptodinámicos

[2] Capítulo: Taxonomía del dinero

[3] https://bitcoin.org/bitcoin.pdf

Principio de Consolidación

La necesidad de cambiar una moneda con el fin de realizar intercambios con comerciantes de otra constituye un coste. Este coste debe ser no nulo incluso si se automatiza, ya que se tiene que consumir espacio y/o tiempo. Por tanto, una moneda siempre es "mejor" (mayor utilidad) que dos, en la medida en que la moneda resultante no pase a estar sujeta a comisiones, según implica el umbral de utilidad[1].



Podemos suponer razonablemente que dos tipos de dinero[2] distintos no pueden tener una utilidad idéntica a perpetuidad. La Ley de Thiers[3] trata las consecuencias de un mejor tipo de dinero en ausencia de controles estatales. A partir de esto, concluimos necesariamente que **el mejor de los dos tipos de dinero terminará por sustituir al otro** en ausencia de controles estatales. A medida que esto ocurra, crecerá la utilidad de la moneda superviviente de manera opuesta a lo detallado en el Principio de Fragmentación[4].

Reference

[1] Capítulo: Propiedad del Umbral de Utilidad

[2] Capítulo: Taxonomía del dinero

[3] https://es.wikipedia.org/wiki/Ley_de_Gresham#Reverso_de_la_ley_de_Gresham_(ley_de_Thiers)

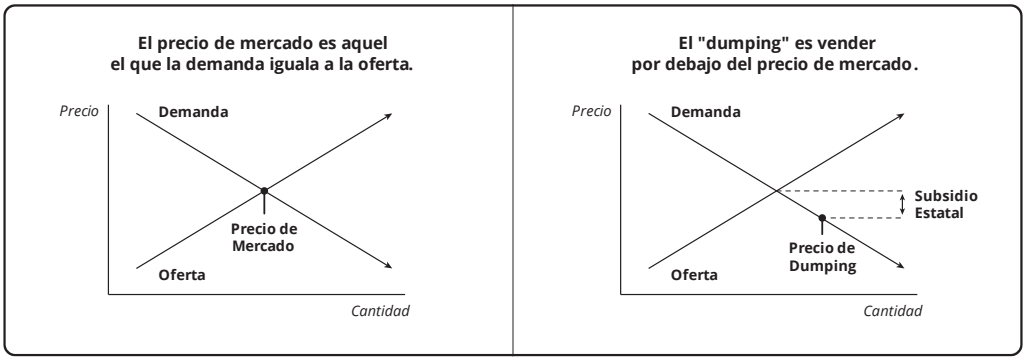
[4] Capítulo: Principio de Fragmentación

Esto no implica que no se puedan crear nuevas monedas ni que no puedan existir durante un periodo significativo. Implica que existe una presión de mercado hacia una única moneda. Un mejor tipo de dinero en una situación puede no ser un tipo de dinero mejor, o tan siquiera útil, en otra.

Por ejemplo, el oro no constituye un tipo de dinero útil para la transferencia electrónica y el bitcoin no resulta muy útil sin una red. Un tipo de dinero sustituye a otro en los escenarios en los que aquel es mejor.

Falacia del *Dumping*

Existe una teoría que afirma que vender unidades de un lado de una moneda dividida por unidades del otro reduce la utilidad relativa de la moneda "vendida". Sin embargo, cada parte está vendiendo (y comprando). Como intercambio, la acción es simétrica y, por consiguiente, la teoría es inválida.



Existe una teoría relacionada que dice que cambiar unidades de un lado de una moneda dividida constituye un *dumping*[1] de esa moneda, lo cual reduce su utilidad. **La teoría sencillamente representa de manera incorrecta el concepto de dumping.** El *dumping* es una subvención[2] estatal (no confundir con la subvención de Bitcoin) de un producto vendido en otro estado. Es un arancel aplicado sobre los contribuyentes del estado que subvenciona, aplicado típicamente con la finalidad de establecer cuota de mercado para el producto. En el caso en el que la demanda resulte elástica[3], la subvención aumenta el volumen de ventas del producto reduciendo el precio en relación con el precio de mercado que habría en otro caso. El menor precio aumenta la demanda al capturar compradores con una menor utilidad marginal[4] por el producto, hasta que el mercado se despeje. Al

Reference

[1] https://es.wikipedia.org/wiki/Dumping

[2] https://es.wikipedia.org/wiki/Subsidio

[3] https://es.wikipedia.org/wiki/Elasticidad_precio_de_la_demanda

[4] https://es.wikipedia.org/wiki/Utilidad_marginal

contrario que el *dumping*, los intercambios a precio de mercado no reducen el precio porque no están subvencionados.

Finalmente, existe una teoría relacionada que afirma que la reducción en el atesoramiento[1] generalmente reduce los precios de cambio de la propiedad atesorada. Esto es cierto[2]; sin embargo, una transferencia no es una reducción de los niveles de atesoramiento a no ser que el comprador de la propiedad atesorada posteriormente la atesore menos que el vendedor. Constituye un error suponer que este sea el caso.

Reference

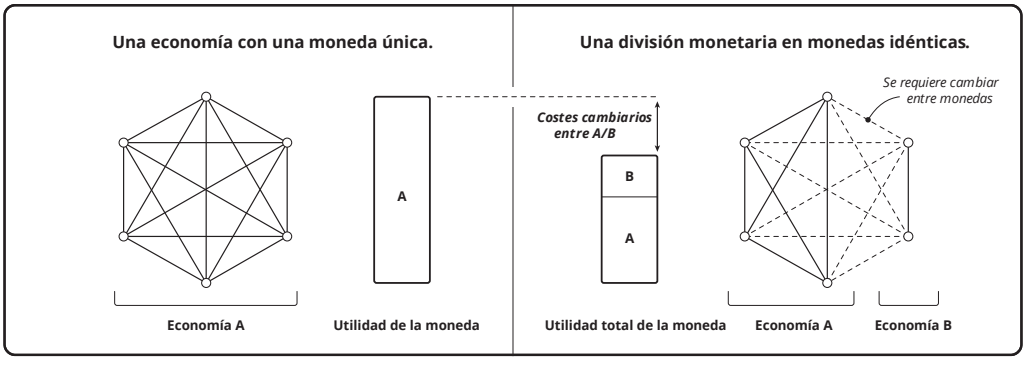
[1] https://en.m.wikipedia.org/wiki/Hoarding_(economics)

[2] https://mises.org/blog/problem-hoarding

Principio de Fragmentación

La utilidad de un dinero[1] se deriva directamente de su capacidad para facilitar los intercambios, en contraposición con el trueque[2]. Si no es aceptado por *ningún* comerciante, entonces objetivamente no tiene utilidad monetaria. Cuantos más bienes y servicios[3] (considerando también la ubicación) puedan ser adquiridos con un tipo de dinero en un momento dado, más probable resulta que ese tipo de dinero represente una mayor utilidad para cualquier persona dada.

Una división implica que cero comerciantes o más han dejado de aceptar la moneda original y que cero o más han empezado a aceptar la moneda dividida. Una división "limpia" es un escenario hipotético en el que no hay solapamiento en la aceptación de las dos monedas entre comerciantes, y no hay ningún cambio en el conjunto de comerciantes. Una división limpia produce dos economías del conjunto original de comerciantes.



Reference

[1] Capítulo: Taxonomía del dinero

[2] https://es.wikipedia.org/wiki/Trueque

[3] https://es.wikipedia.org/wiki/Bienes_y_servicios

Si suponemos que las monedas son idénticas aparte del hecho de la división, el Principio de Consolidación[1] implica que la utilidad de las monedas combinadas es la misma que la utilidad de la original menos el coste cambiario. Este escenario se puede ampliar para incluir el solapamiento de los comerciantes. Esto no tiene efectos en la utilidad de la moneda, ya que solo traslada del comprador al vendedor la incidencia del coste cambiario.

Un aumento o una disminución en el número de comerciantes que acepte cualquiera de las monedas constituye una ganancia o pérdida neta, respectivamente, de la utilidad combinada, ya que lleva implícito que se retire o añada un coste cambiario entre monedas. En otras palabras, el efecto es proporcional a cada una de las monedas en la división. Este factor se relaciona con las características particulares de una división dada, no con la división en general.

Por consiguiente, una división produce tanto un desplazamiento como una reducción de la utilidad, en proporción a los tamaños relativos de las economías resultantes. La Falacia del Efecto de Red[2] explica por qué la reducción no es de naturaleza cuadrática, como a veces se supone.

Si bien puede parecer que en el desplazamiento alguien ha "capturado" valor de la moneda original, ese valor en realidad "salió" para formar la moneda dividida. En otras palabras, los comerciantes son dueños del valor que proporcionan a un tipo de dinero. Los propietarios tienen una influencia independiente sobre el poder adquisitivo, sobre la base de su nivel de atesoramiento[3]. Sin embargo, esto afecta al precio unitario, no a la utilidad.

Reference

[1] Capítulo: Principio de Consolidación

[2] Capítulo: Falacia del Efecto de Red

[3] Capítulo: Falacia del *Dumping*

En el momento de la división, una unidad original pasa a ser dos unidades, cada una con una utilidad reducida y proporcional en relación con la original. Con una protección contra repeticiones de movimientos[1], cada una de ellas se puede gastar sin coste adicional. De lo contrario, la necesidad de autoprotección descuenta[2] unidades de la(s) cadena(s) no protegida(s).

Este análisis también es aplicable a nuevas monedas. La diferencia en el caso de una nueva moneda es que las unidades de la (otra) moneda original no se pueden gastar en la nueva cadena. Por consiguiente, la nueva moneda se enfrenta a la dificultad de adjudicar unidades, lo cual requiere trabajo y, por consiguiente, tiempo. Las divisiones sacan adelante[3] este proceso subdividiendo la utilidad de una cadena existente, en la medida en que sus comerciantes estén dispuestos a hacerlo.

Reference

[1] Capítulo: Falacia de la Protección contra Repeticiones de Movimientos

[2] https://es.wikipedia.org/wiki/Valor_actual_neto

[3] https://es.wikipedia.org/wiki/Bootstrapping_(inform%C3%A1tica)

Falacia de la Pureza Genética

Existe una teoría de que una moneda es más fuerte cuando toda validación se realiza con una implementación común. Según esta teoría, la complejidad de la implementación de las reglas de consenso implica que es probable que las múltiples implementaciones diverjan, lo que produce una división de cadena inadvertida. La división implica pérdidas financieras por parte de personas en el lado más débil. Además de la divergencia, una implementación única corre con el riesgo de una parada mundial de la red. La amenaza de pérdidas financieras implica una menor utilidad y, por consiguiente, menor seguridad del sistema.

Sobre la base de la presunción de una alta complejidad, cada actualización al "cliente verdadero único" produce la misma probabilidad de divergencia. De manera parecida, la dependencia respecto de librerías actualizadas independientemente tiene el mismo efecto. En otras palabras, *no es posible que haya solamente una implementación*. En el caso de la implementación inicial de Bitcoin, tanto la actualización del cliente[1] como la actualización de una dependencia externa[2] han producido divisiones de cadena no intencionadas y pérdidas financieras significativas[3]. Además, las deficiencias del día cero[4] en esta implementación se han publicado sin previo aviso[5] y podrían haber producido una parada mundial.

Una única implementación produciría una debilidad directamente análoga a la de una especie viva con uniformidad genética. En el caso de una única implementación, las

Reference

[1] https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

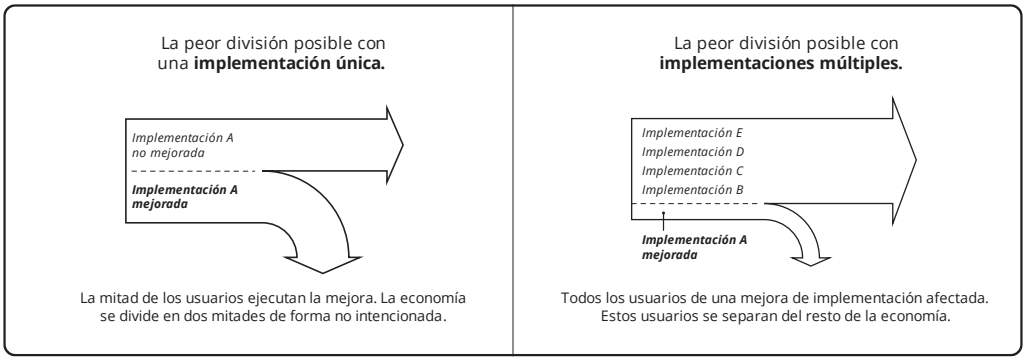
[2] https://github.com/bitcoin/bips/blob/master/bip-0066.mediawiki

[3] https://cointelegraph.com/news/miners-lost-over-50000-from-the-bitcoin-hardfork-last-weekend

[4] https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero

[5] https://www.reddit.com/r/btc/comments/6z827o/chris_jeffrey_jj_discloses_bitcoin_attack_vector/

actualizaciones tanto internas como externas penetran la economía de manera rápida y profunda. El impacto financiero de una división, por consiguiente, resulta más significativo que el causado por una implementación desplegada con menor difusión. En un escenario con diez implementaciones, cada una de las cuales apoye una fracción uniforme de la economía, habría un riesgo para el 10% de la economía como mucho para cualquier actualización dada, mientras que la actualización de una implementación única desplegada universalmente alcanza el riesgo máximo de división del 50%. Por lo tanto, la teoría no solamente es inválida sino que expresa lo contrario del comportamiento real.



Falacia de la Minería Híbrida

Existe una teoría que dice que una combinación de la minería con prueba de trabajo (PoW) y prueba de participación (PoS) ofrece un mayor nivel de seguridad del sistema que la PoW. La teoría implica que una mayoría de los propietarios de monedas pueden mitigar las "malas conductas" de las mineras PoW.

En ausencia de una minera con potencia de hash mayoritaria, no hay nada que mitigar. Por tanto, la teoría se basa en la premisa de aumentar el coste de un régimen de censura. Esto descansa en la suposición no defendible de que las mineras PoW no son también mineras PoS.

El coste de la minería híbrida son los costes combinados de trabajo y participación, incluido el coste de capital. El retorno sobre la inversión minera necesariamente es igual al coste de capital, como consecuencia de la competencia. Puesto que la minería es rentable, el coste de capital no contribuye a la seguridad. **Lograr una participación mayoritaria no es más costoso que lograr una potencia de hash mayoritaria.** Por consiguiente, la teoría es inválida.

Dado un modelo en virtud del cual un participante mayoritario pueda evitar la confirmación de bloques PoW que por lo demás fueran válidos, una vez se logra una mayoría el censor no puede ser destronado[1]. Un sistema de este tipo es fundamentalmente una moneda PoS, sin resistencia a la censura[2], y el aspecto de PoW no proporciona ninguna seguridad adicional.

Reference

[1] Capítulo: Falacia de la Prueba de Participación

[2] Capítulo: Propiedad de resistencia a la censura

Definición de maximalismo

El maximalismo es un esfuerzo de relaciones públicas para desalentar la formación de sustitutos para una moneda dada. En la medida en que tenga éxito, puede beneficiar a los propietarios al restringir la oferta y, por consiguiente, elevando el precio. Sin embargo, en tanto las personas no encuentran sustitutos[1] próximos, la actividad se mueve a sustitutos más distantes. En el caso de pagos electrónicos, esto generalmente son formas de dinero estatal.

El maximalismo es distinto de la conciencia de criptomierdas[2] en que se caracteriza por promover un Bitcoin por encima de todos los demás. Los promotores a menudo expresan la teoría contradictoria de que ninguna otra moneda podría ser competitiva respecto de su moneda preferida. Si este fuera el caso, no habría ningún motivo para abogar por una única moneda.

Reference

[1] Capítulo: Principio de Sustitución

[2] Capítulo: Definición de Criptomierda

Falacia del Efecto de Red

Existe una teoría que afirma que la utilidad creada por una economía varía con el cuadrado del número de sus comerciantes, suponiendo que cada comerciante ofrezca el mismo valor de bienes o servicios a la venta en una moneda. La teoría es una aplicación de la Ley de Metcalfe[1].

Esto implica que una división uniforme de la economía reduce la utilidad combinada a la mitad. Por ejemplo, si 1 red de 20 comerciantes tiene una utilidad de 400, entonces 2 redes de 10 de estos comerciantes tienen una utilidad de 200.

Sin embargo, la capacidad de cambiar las unidades de una moneda por otra hace que la utilidad de las dos economías se combine en una economía híbrida. A causa del coste de conversión[2], **la moneda híbrida tiene una menor utilidad de la que tendría una sola, pero esto no puede ser comparable con la pérdida completa de una de las dos salvo que el coste de conversión sea ilimitado.** Por consiguiente, la teoría es inválida.

Reference

[1] https://es.wikipedia.org/wiki/Ley_de_Metcalfe

[2] Capítulo: Principio de Consolidación

Falacia de la Prueba de Coste

En un mercado (libre) competitivo, la minería de Bitcoin consume en coste para la minera lo que crea en valor para la minera, tanto en la emisión de nuevas unidades como en el servicio de confirmación. Este es el caso independientemente de que una recompensa por bloque minado refleje el retorno total de la minera o no lo haga.

La cantidad de cálculos realizados en la minería se refleja probabilísticamente en la dificultad del bloque. Estos cálculos se denominan trabajo. Un encabezamiento de bloque válido es una prueba probabilística de que se realizó este trabajo. Esta es la base del término "prueba de trabajo".

La cantidad de energía consumida en la producción de bloques no es demostrable, ni específica ni probabilísticamente. La eficiencia energética varía. Un encabezamiento de bloque no refleja la "prueba de energía" consumida. Esas afirmaciones son aproximaciones.

El retorno de una minera en la producción de un bloque no se ve reflejado totalmente en el bloque. El minado de las transacciones propias de uno implica comisiones no necesariamente reflejadas en el bloque, como es el caso general de las comisiones aparte[1]. Una minera puede introducir transacciones con comisiones arbitrariamente altas o bajas. La recompensa de bloque no representa una "prueba de recompensa". Esas afirmaciones son suposiciones.

En un mercado libre, el retorno sobre el minado es el valor de su recompensa, independientemente de que ese importe esté reflejado o no en el bloque, y las comisiones obtenidas están determinadas por la demanda de realizar transacciones. Esto es consecuencia de la competencia. Así pues, en este caso es correcto considerar un

Reference

[1] Capítulo: Falacia de las Comisiones Aparte

encabezamiento de bloque válido como “prueba de coste”; sin embargo, el importe del coste sigue siendo desconocido. Todo lo que se sabe es que la minera obtuvo una rentabilidad porcentual de mercado sobre el capital.

Sin embargo, en el caso del monopolio[1] estatal, el precio no se controla mediante la competencia. Un monopolio puede cobrar cualquier precio que soporte el mercado. El coste de hacer valer el monopolio lo paga el contribuyente. La prima de precio es otro impuesto, pagado por el consumidor. El valor del impuesto se transfiere al monopolio.

En el caso de censura del Bitcoin patrocinada por el estado, tanto la ejecución como la prima de precio (comisión) existen como impuestos en forma de monopolio. El nivel de comisiones puede superar el tipo de mercado, y su ejecución está subvencionada mediante impuestos. La minería monopolística puede producir un señoreaje[2] al igual que cualquier dinero monopolístico. El encabezamiento de bloque sigue proporcionando una prueba de trabajo, pero ha dejado de proporcionar una prueba del coste de mercado.

De la misma manera, la existencia de una unidad válida de dinero monopolístico[3] proporciona una prueba suficiente de un coste de producción real, pero no proporciona ninguna prueba de que el emisor no obtuviera una prima monopolística sobre este coste. Existe una teoría que afirma que el coste de producción de Bitcoin es “no falsificable”, siendo el señoreaje de dinero estatal una “falsificación de costes”. Según se ha mostrado, el **Bitcoin también está sujeto al señoreaje**, lo que invalida la teoría.

Reference

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/pp/1054

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] Capítulo: Taxonomía del dinero

Todos los bienes tienen un coste de producción real. El monopolio existe para aumentar el precio por encima del coste. Si bien Bitcoin es resistente a la censura[1], la eficacia de la resistencia no está garantizada[2].

Reference

[1] Capítulo: Propiedad de resistencia a la censura

[2] Capítulo: Axioma de resistencia

Fachada de Prueba de Memoria

Se ha propuesto[1] que una prueba de memoria (PoM) puede reemplazar una fracción del coste energético de la prueba de trabajo (PoW) con hardware, incluso recurriendo a dispositivos de memoria existentes. Como se muestra en Falacia del Desperdicio de Energía[2], un nivel constante de seguridad requiere un gasto corriente constante. Por consiguiente, un sistema de este tipo requeriría un nivel comparable de consumo de hardware que compensara cualquier reducción en el coste energético. **En otras palabras, el consumo total de energía no se puede reducir, solo se puede transferir a la fabricación y operación del hardware y a su eliminación como residuos.**

En diciembre de 2017, el coste anualizado estimado de energía consumida en la minería del Bitcoin era de 1.628 millones de dólares, sobre la base de las aproximaciones de 32,56 teravatios-hora consumidos a un promedio de 0,05 dólares por kilovatio-hora de energía. En ese momento, este nivel de coste equivalía al consumo de 32.560.000 memorias de terabyte a un promedio de 50$ por unidad. La utilización de la memoria existente desaprovechada reduce el coste unitario y, por consiguiente, aumenta comparativamente el requisito de tamaño.

Vale la pena considerar el comportamiento económico de un sistema teórico en el que la PoM viene determinada por una reserva fija existente (exenta de coste) de memoria sin caducidad ni costes operativos. Puesto que el coste de la minería es cero, las recompensas fluyen sin coste alguno en proporción a la memoria (asumiendo que no hay presiones pro-compartición de recursos[3]). Cualquier aumento en la comisión media aumenta esta recompensa de la memoria. El capital invertido es cero y, por consiguiente, el tipo de interés es infinito a perpetuidad. A pesar de este incentivo ilimitado, la suposición de

Reference

[1] https://eprint.iacr.org/2017/893.pdf

[2] Capítulo: Falacia del Desperdicio de Energía

[3] Capítulo: Riesgo de Presiones Pro-Compartición de Recursos

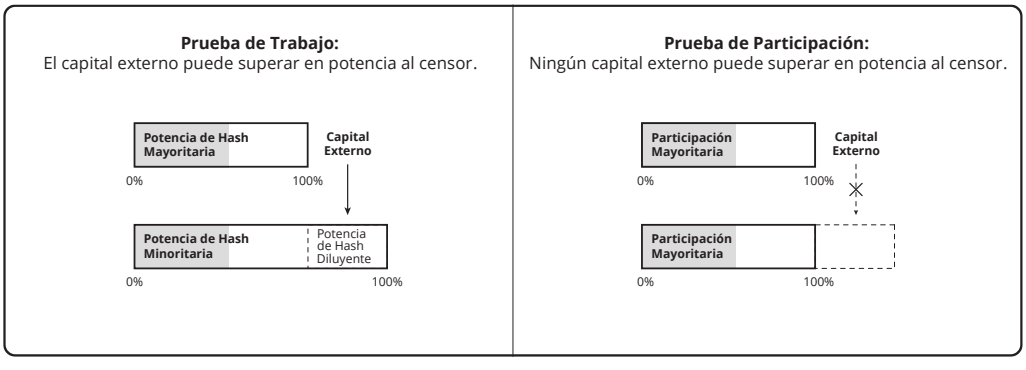
expansión nula excluye de antemano la competencia. Pero, puesto que la prueba se externaliza, no se puede restringir realmente la competencia. En un sistema real, la fabricación de hardware se amplía a perpetuidad para un nivel dado de comisiones, y esta expansión se acelera con los aumentos en el nivel de comisiones.

La prueba de memoria es igual a la prueba de trabajo en términos de consumo de recursos y no hay motivo para suponer una menor componente energética de ese coste. El hardware actúa como una batería de pruebas, lo cual representa energía consumida de manera demostrable en su fabricación. Esto constituye una fachada análoga al coche eléctrico de "cero emisiones".

Falacia de la Prueba de Participación

La seguridad de la confirmación requiere que una persona ordene las transacciones. Bitcoin asigna periódicamente esta autoridad a la minera que produce la mayor prueba de trabajo. Todas las formas de trabajo se reducen necesariamente[1] al consumo de energía[2]. Resulta esencial[3] que tal prueba sea independiente del historial de la cadena. Podemos referirnos a esto como prueba "externa".

La otra única fuente de autoridad para dar órdenes, por consiguiente, depende del historial de la cadena, fuente que podríamos denominar "interna". Existe una teoría que dice que la prueba de participación (PoS) constituye una alternativa comparable a la prueba de trabajo (PoW) en términos de la seguridad de las confirmaciones. Es verdad que tanto PoS como PoW delegan el control de las órdenes de transacción a una persona que controle la mayor reserva de cierto capital.



La diferencia reside en el carácter desplegable del capital. PoW excluye el capital que no pueda ser convertido en trabajo, mientras que el PoS excluye el capital que no pueda

Reference

[1] Capítulo: Fachada de Prueba de Memoria

[2] Capítulo: Falacia del Desperdicio de Energía

[3] Capítulo: Propiedad de resistencia a la censura

adquirir unidades de la moneda. Esta diferencia tiene consecuencias significativas para la seguridad.

En el Principio de los Otros Medios[1], se muestra que la resistencia a la censura depende de que las personas paguen a las mineras para superar en potencia al censor. **Superar la censura no es posible en un sistema PoS, ya que el censor ha adquirido una participación mayoritaria y no puede ser destronado.** Por consiguiente, los sistemas PoS no son resistentes a la censura y la teoría, por tanto, es inválida.

Reference

[1] Capítulo: Principio de los Otros Medios

Falacia de la Protección contra Repeticiones de Movimientos

Existe una teoría que afirma que la protección contra repeticiones de movimientos aplicada en una cadena dividida aumenta la utilidad relativa de la cadena original. La protección contra repeticiones de movimientos es una regla diseñada en relación con otra cadena y con un comportamiento direccional. La protección hace que las transacciones de la cadena protegida sean inválidas en la otra.

Incluso sin esa protección, es posible que un propietario gaste de tal forma que se evite la repetición de movimientos en un sentido o el otro, aunque de esta manera se incurre en una comisión y/o coste de complejidad. Una división puede reducir, pero no eliminar, este coste en uno o los dos sentidos al activar reglas que los gastos puedan utilizar selectivamente. Esto se llama opción de inclusión, en contraste a la protección obligatoria contra repeticiones de movimientos. La protección contra repeticiones de movimientos en virtud de una opción de inclusión reduce pero no elimina el coste, mientras que la protección obligatoria puede eliminar el coste.

La repetición de un gasto en otra cadena no es dilutiva[1]. La salida común se puede gastar en cada una de las cadenas con o sin repetición de movimientos. **La única distinción proporcionada por la protección es que los gastos siempre pueden ser distintos en cada cadena sin coste adicional para la persona que gasta.** La oferta en cada cadena no se ve afectada por la protección.

Es un error curioso pensar que una cadena puede absorber de alguna manera las transacciones de otra en una división. Todas las salidas del segmento común se pueden

Reference

[1] https://es.wikipedia.org/wiki/Diluci%C3%B3n_de_capital

gastar en ambas cadenas. La protección contra repeticiones de movimientos solamente reduce el coste de gastarlas en la cadena protegida.

Uno podría suponer que la falta de protección reduce la probabilidad de que un propietario gaste en la cadena no protegida, limitándose así la oferta y aumentando el precio de cambio. Sin embargo, esto supone que la demanda no se ve afectada por lo que equivale a un aumento en el coste de realizar intercambios. Si el propietario no realiza intercambios por el mayor coste de hacerlos, entonces la utilidad de la moneda no aumenta sino que disminuye.

El coste de autoprotección equivale a un demoraje[1] único que persiste hasta que se aplica la protección a las unidades desprotegidas, intencionadamente o no. Este costo es un descuento[2] a la utilidad de una cadena desprotegida respecto de la misma cadena hipotética con protección. Esto implica una utilidad *mayor* de una cadena protegida, respecto de una cadena desprotegida asociada por división, de lo que sería el caso de otro modo. Por consiguiente, la teoría es inválida.

Reference

[1] https://es.wikipedia.org/wiki/Demora_(transporte_mar%C3%ADtimo)

[2] https://es.wikipedia.org/wiki/Valor_actual_neto

Definición de Criptomierda

Una criptomierda (en inglés, *shitcoin*) es cualquier sistema que no sea seguro desde un punto de vista criptodinámico[1] pero pretenda capturar la propuesta de valor[2] de Bitcoin.

Se presume que las criptomierdas son estafas, aunque sigue siendo posible que quienes las propongan tengan buenas intenciones pero ignoren los principios criptodinámicos. A modo de ejemplo, las tecnologías con prueba de participación[3] son criptomierdas.

Si bien puede haber implementaciones de Bitcoin que sean más seguras que otras, esto son cuestiones de grado. Ningún Bitcoin se puede demostrar que sea totalmente seguro[4]. Por tanto, el término no se aplica razonablemente a ningún Bitcoin. A modo de ejemplo, las tecnologías con prueba de memoria[5] podrían no ser criptomierdas (a pesar de que no cumplan objetivos fundamentales).

Reference

[1] Capítulo: Principios Criptodinámicos

[2] Capítulo: Propuesta de Valor

[3] Capítulo: Falacia de la Prueba de Participación

[4] Capítulo: Axioma de resistencia

[5] Capítulo: Fachada de Prueba de Memoria

Falacia de la Expansión del Crédito por División

Existe una teoría que afirma que un aumento de las unidades monetarias, como es el caso de una división o una nueva moneda, crea crédito. Esto es un error presumiblemente consecuencia de suponer que la expansión del crédito[1] impulsada por la expansión monetaria estatal es una fuerza del mercado. Esta suposición no tiene en cuenta que el dinero de mercado[2] no puede producir señoreaje[3].

El señoreaje es un impuesto. Las unidades monetarias creadas no representan un capital nuevo sino, por el contrario, la dilución por parte del estado de las unidades existentes, lo cual transfiere la propiedad del capital que representan al soberano. A medida que este capital se emplea en subvencionar los préstamos concedidos por el cártel de la banca estatal[4], como dinero descontado[5] y seguros[6], se reduce el coste del capital para los clientes del banco.

Esta llamada expansión del crédito no es sencillamente el resultado de la banca fraccional como fuerza de mercado; es la consecuencia de que el estado favorezca a los deudores a costa de los ahorradores. En un mercado libre de la banca, los bancos son sencillamente *fondos de inversión*. Los inversores obtienen de media un retorno de mercado sobre el capital y sufren el riesgo de hacerlo. En la banca estatal, el riesgo, y por consiguiente el capital, se reasignan según objetivos políticos.

Reference

[1] Capítulo: Falacia de la Expansión del Crédito

[2] Capítulo: Taxonomía del dinero

[3] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[4] Capítulo: Principio de la Banca Estatal

[5] https://www.frbdiscountwindow.org

[6] https://www.fdic.gov/resources/deposit-insurance

La expansión del crédito del mercado es un aumento en la concesión de préstamos de capital, en contraposición a su atesoramiento. Los mayores tipos de los préstamos son consecuencia de una preferencia temporal[1] reducida, y reducen el coste del capital. Es imposible mostrar que la creación de una división o de una nueva moneda (o cualquier otra cosa) reduzca la preferencia temporal. Por consiguiente, es un error suponer que esas creaciones aumenten la disponibilidad del capital o reduzcan su coste.

Reference

[1] https://en.wikipedia.org/wiki/Time_preference

Dilema del Especulador de Divisiones

Cuando surge una división, el propietario de una moneda original se enfrenta a la decisión de elegir si retener o vender unidades de las cadenas original y fruto de la división.

Según se discutió en la Falacia del *Dumping*[1], no existe ninguna manera de desalentar la existencia de una cadena u la otra por el intercambio o el atesoramiento[2] de unidades de alguna de ambas. Por consiguiente, consideramos que esta elección es estrictamente una cuestión de cómo maximizar el valor de las tenencias existentes después de una división.

Dada una posición anterior a la división, un propietario se ve impactado por el mayor coste de la conversión de unidades, y por la protección contra repetición de movimientos[3] si es aplicable. Estos son futuros costes inevitables de los intercambios que reducen el valor actual neto[4] de las unidades. Por consiguiente, estos factores no son relevantes para la cuestión.

Las consideraciones restantes *suponen* que las monedas combinadas aumentarán de precio a lo largo del periodo de tiempo contemplado.

Bajo las suposiciones del Principio de Consolidación[5], dos monedas similares terminarán por consolidarse, reduciéndose a cero el valor de una de ellas a lo largo del tiempo. Si resulta que uno sabe cuál será, es racional venderla y comprar la otra. Sin embargo, puesto que uno podría *no* saber qué moneda sobrevivirá, existe una posibilidad de que en la operación de intercambio se vendiera la moneda que tiene éxito por la que fracase,

Reference

[1] Capítulo: Falacia del *Dumping*

[2] https://en.m.wikipedia.org/wiki/Hoarding_(economics)

[3] Capítulo: Falacia de la Protección contra Repeticiones de Movimientos

[4] https://es.wikipedia.org/wiki/Valor_actual_neto

[5] Capítulo: Principio de Consolidación

sacrificando *todo* el valor contenido en las unidades originales. **Sin conocimiento del futuro, vender todo o parte de una por la otra aumenta la recompensa potencial en proporción al incremento del riesgo.** Por consiguiente, es igual de racional atesorar ambas, lo cual preserva las suposiciones que existían antes de la división.

Finalmente, cabría enfatizar que podrían fallar ambas cadenas, consolidándose el valor en una cadena independiente, mercancía, o dinero *estatal*. Este tema solo pretende proporcionar un marco de decisión racional sobre la base de suposiciones que podrían no llegar a cumplirse.

ECONOMÍA

Falacia de la Expansión del Crédito

La expansión del crédito es la multiplicación del crédito contra el dinero[1] como consecuencia de los préstamos. Cuando se emite un préstamo, tanto el prestamista como el tomador del préstamo parecen ser titulares del mismo dinero. A causa de la naturaleza inflacionista[2] aparente de la expansión del crédito, habitualmente se trata como un efecto adverso sobre las personas propietarias del dinero. Puesto que los bancos son los prestamistas más visibles, este efecto a menudo se atribuye a la propia banca. Existe una teoría que afirma que Bitcoin puede eliminar los efectos de la banca de reserva fraccionaria[3] y, por consiguiente, eliminar la expansión del crédito.

El ahorro abarca el atesoramiento y la inversión. El atesoramiento implica una depreciación[4] continua, que es consumo real. La inversión son préstamos a la producción, e implica que no hay depreciación ya que los productos tienen que existir antes de que puedan depreciarse. La inversión incluye tanto los contratos de deuda como los de capital social ya que la distinción es estrictamente financiera, y no tiene ninguna importancia económica[5].

Reference

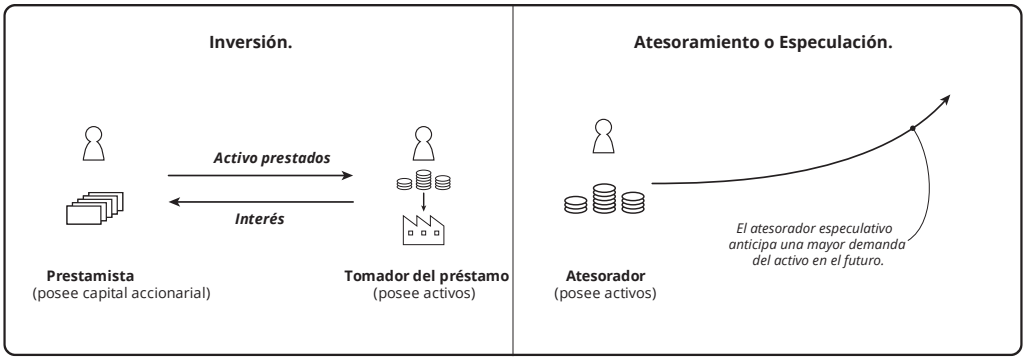
[1] Capítulo: Taxonomía del dinero

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] https://es.wikipedia.org/wiki/Banca_de_reserva_fraccional

[4] Capítulo: Principio de Depreciación

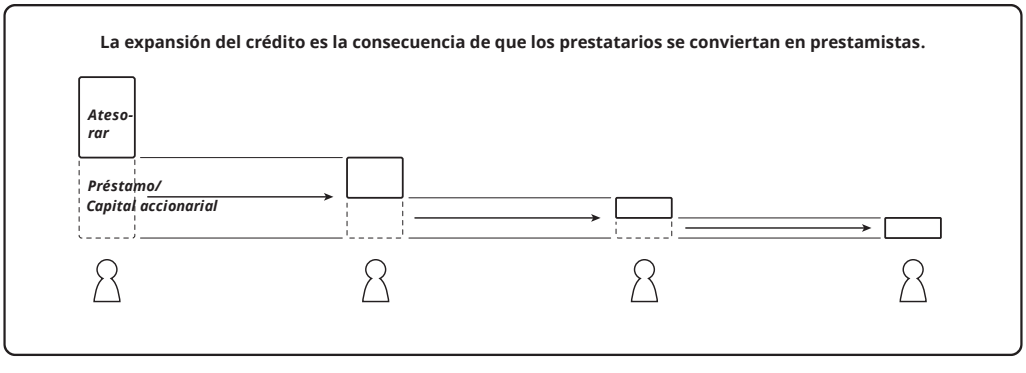
[5] https://mises.org/library/man-economy-and-state-power-and-market/html/p/996



La distinción entre el atesoramiento y la inversión resulta esencial para comprender la expansión del crédito. El dinero atesorado se encuentra bajo el control de su propietario, ya sea en una cámara acorazada, enterrado en el patio, o guardado debajo del colchón.

Esto es inherente al significado de propiedad. El prestamista del dinero no es el propietario del dinero, aunque un préstamo se considere ahorro.

Un prestamista requiere liquidez para operar, y por tanto tiene que atesorar una cierta fracción del ahorro. Cuando se crea un préstamo, el tomador del préstamo posee el importe prestado. El tomador del préstamo también requiere liquidez y de esta forma atesora una cierta fracción del préstamo. El resto del préstamo necesariamente se invierte. Esto implica que el tomador del préstamo se ha convertido en prestamista. El proceso continúa hasta que todo el capital que existe se haya atesorado.



El importe atesorado a veces se denomina como la "reserva" del propietario, pero en sentido correcto es el tesoro del propietario, una fracción del ahorro total del propietario. Este uso de la palabra reserva no debe confundirse con su uso en el contexto monetario estatal de la divisa de reserva[1] (es decir, las reservas cambiarias[2]). La expresión "banca de reserva fraccional" hace referencia a la proporción del tesoro del banco respecto del crédito que ha emitido (cuentas dinerarias).

La cantidad total de dólares estadounidenses en circulación[3] se denomina "M0". Esto incluye toda la moneda tangible ("efectivo en cámaras acorazadas") más los balances bancarios intangibles en las cuentas de la Reserva Federal. Estas dos formas se consideran obligaciones de la Reserva Federal[4] intercambiables. Las obligaciones intangibles son dinero contabilizado pero aún no impreso[5]. Según informa la Fed[6], el total de dólares estadounidenses es:

Dólares	Importe (2019)
Tangibles	1.738.984.000.000$
Intangibles	1.535.857.000.000$
Dinero total (M0)	3.274.841.000.000$

M0 más todo el dinero de cuentas bancarias se denomina "M3". Esto ya no lo publica la Fed, pero se estima[7] en 17.682.335.000.000 $. El importe total de créditos extendidos en dólares estadounidenses se puede estimar a partir de la suma de las cuentas[8] dinerarias

Reference

[1] Capítulo: Falacia de la Divisa de Reserva

[2] https://en.wikipedia.org/wiki/Foreign-exchange_reserves

[3] https://en.wikipedia.org/wiki/Money_supply#United_States

[4] https://en.wikipedia.org/wiki/Money_supply#Money_creation_by_commercial_banks

[5] Capítulo: Principio de la Banca Estatal

[6] https://www.federalreserve.gov/releases/h3/current/default.htm

[7] https://fred.stlouisfed.org/series/MABMM301USM189S

[8] https://es.wikipedia.org/wiki/Cuenta_bancaria

denominadas en dólares, los bonos[1], las acciones de sociedades anónimas[2] y las acciones de sociedades limitadas[3].

Crédito en dólares	Importe (2019)
Banco (M3-M0)	14.407.494.000.000$
Bono	41.000.000.000.000$
Acciones de sociedades anónimas	32.891.169.631.125$
Acciones de sociedades limitadas	6.426.333.525.358$

A partir de la tabla:

- La relación total del dinero respecto del crédito es de ~3,46%, una expansión del crédito de 29,9 veces el dinero.
- Las reservas[4] bancarias de 1.400.949.000.000 $ indican una ratio de reserva bancaria de ~11,11% contra el crédito bancario, o bien una expansión del crédito de 9,0 veces el dinero. Esto está levemente por encima del ratio de reserva exigida[5], que no supera el 10%[6].
- La reserva del dinero restante (es decir, excluyendo las reservas bancarias) en relación con los mercados de bonos y acciones (esto es, la ratio de M0 menos reservas bancarias respecto de la suma de bonos y capital social) es de ~2,08%, o bien una expansión del crédito de 48,0 veces el dinero.

Reference

[1] https://www.forbes.com/sites/kevinmcpartland/2018/10/11/understanding-us-bond-market/
[2] https://data.worldbank.org/indicator/cm.mkt.lcap.cd
[3] https://www.quora.com/What-is-the-estimated-total-value-of-all-US-private-companies
[4] https://www.federalreserve.gov/releases/h3/current/default.htm
[5] https://es.wikipedia.org/wiki/Coeficiente_de_caja
[6] https://es.wikipedia.org/wiki/Coeficiente_de_caja#Estados_Unidos

Eliminar la expansión del crédito requiere eliminar el crédito y, por consiguiente, la producción. Todo crédito está sujeto a impagos. Sin embargo, la teoría sostiene que el crédito bancario es distinto al presuponerse que está "exento de riesgo". Esta presunción surge del hecho de que los contribuyentes aseguran[1] el crédito. Esto no es consecuencia de la banca sino de la intervención estatal en la banca. En la medida en que la presunción se atribuya a la banca libre[2], la teoría es inválida. Todas las clases de negocio están sujetas a impagos y, haciéndolo así, la banca libre elimina este percepción incorrecta.

La distinción entre un fondo del mercado monetario[3] (MMF) y una cuenta del mercado monetario[4] (MMA) es informativa. Ambos están destinados a mantener una equivalencia uno a uno con el dinero, sin embargo, ambos se descuentan del dinero debido a los costes de liquidación[5] y riesgo (por ejemplo, algunas personas solo aceptan dinero, rechazando los costes más altos de las transacciones con tarjetas de crédito[6] y cheques[7]). La diferencia (aparte de la garantía del contribuyente del último) se encuentra en el tratamiento del riesgo de inversiones y de una reserva insuficiente.

En el caso de un MMF, el fracaso de la inversión se refleja en el precio unitario. Si bien el fondo trata de mantener un valor liquidativo[8] (VL) que permita intercambiar una unidad del fondo por otra del dinero, una caída suficiente del VL se reflejará en el precio unitario. En el caso de un MMA, esas pérdidas son absorbidas por reservas dinerarias. Si existe una reserva insuficiente, bien por un nivel inesperado de retiradas o por las pérdidas de la inversión, el MMA fracasa. El fracaso de un MMA se manifiesta como pánico bancario[9], en

Reference

[1] https://www.fdic.gov
[2] https://es.wikipedia.org/wiki/Banca_libre
[3] https://en.wikipedia.org/wiki/Money_market_fund
[4] https://en.wikipedia.org/wiki/Money_market_account
[5] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)
[6] https://es.wikipedia.org/wiki/Tarjeta_de_cr%C3%A9dito
[7] https://es.wikipedia.org/wiki/Cheque
[8] https://en.wikipedia.org/wiki/Net_asset_value
[9] https://es.wikipedia.org/wiki/P%C3%A1nico_bancario

el que algunas personas reciben el reembolso y otras no. El VL insuficiente de un MMF se manifiesta como una caída uniforme en el precio unitario.

La ventaja del MMA es que sus unidades son más fungibles[1], aunque sigan estando descontadas respecto del dinero. La ventaja del MMF es que las pérdidas se distribuyen uniformemente. No es, por tanto, sorprendente que los MMAs estén típicamente asegurados por el contribuyente, estén más estrechamente regulados por el estado, y se contabilicen como crédito bancario. Es raro que un MMF "pierda la paridad"[2] pero por supuesto puede pasar y pasa. Las quiebras bancarias también suceden pero están encubiertas por la garantía del contribuyente.

El crédito bancario no es verdaderamente fungible. Esto se puede ver en el uso diario de las tarjetas de crédito y los cheques. Existe un riesgo asociado sustancial de incapacidad de liquidar pagos con ellos. Si bien este riesgo se atribuye generalmente al titular de la cuenta (por ejemplo, en el caso de un MMA), esto no supone ninguna diferencia para la persona que acepta el crédito. Por tanto, uno podría imaginar que la aceptación de las tarjetas de crédito y los cheques contra MMFs se trate de manera análoga. El crédito circularía como equivalente a dinero si bien se distribuiría el riesgo más uniformemente entre aquellos que se benefician de su retorno sobre la inversión. La banca libre tiene la opción de adoptar cualquiera de ambos modelos en la medida en que la gente lo desee, pero en cualquier caso el crédito se expandirá contra dinero, existirá el riesgo, y existirán sustitutivos dinerarios[3].

La decisión de atesorar vs. invertir[4] se basa estrictamente en la preferencia temporal[5] de cada persona. La preferencia temporal no se puede deducir de ninguna condición. Es, tal

Reference

[1] https://es.wikipedia.org/wiki/Bien_fungible

[2] https://www.investopedia.com/articles/mutualfund/08/money-market-break-buck.asp

[3] https://wiki.mises.org/wiki/Money_substitutes

[4] Capítulo: Relación de ahorro

[5] https://en.wikipedia.org/wiki/Time_preference

y como implica su nombre, una preferencia humana. Las preferencias humanas cambian y, por tanto, también lo hace la preferencia temporal. La preferencia temporal determina el tipo de interés económico que también se puede considerar coste del capital. Un aumento en el coste del capital que resulte de aumentar la preferencia temporal hace que el crédito disponible se contraiga, y una disminución tiene el efecto contrario. Con una preferencia temporal infinita, todo el capital se atesoraría para el consumo, finalizando toda la producción.

No importa que un prestamista se denomine "banco" o no, toda inversión implica el mismo comportamiento. Si los bancos operaran con un atesoramiento del 100% no serían prestamistas. Esto no implica ninguna reducción en la concesión de préstamos, ya que la tasa de concesión de préstamos[1] la determina exclusivamente la preferencia temporal. El Bitcoin se puede prestar y no hace nada para limitar la expansión del crédito. Por consiguiente, la teoría es inválida.

Eliminar la expansión del crédito es equivalente a la condición de una preferencia temporal infinita, un tipo de interés infinito, que no haya capital disponible para la producción, y que no haya productos disponibles para el consumo. En los estados en los que el crédito está limitado o prohibido por la norma legal (leyes de usura[2]), la inversión se mueve a los instrumentos accionariales, préstamos a tipos de usura[3], o el fin de la producción.

Reference

[1] Capítulo: Falacia del Dinero Imprestable

[2] https://es.wikipedia.org/wiki/Usura

[3] https://en.wikipedia.org/wiki/Loan_shark

Principio de Depreciación

La propiedad de un producto se mueve del productor al consumidor (o productor) y, sin embargo, ni la producción ni el consumo[1] tienen lugar en ese momento. El productor atesora el producto antes de los intercambios y el consumidor lo atesora posteriormente. El producto existe y termina por ser intercambiado entre personas. Los términos "productor" y "consumidor" son nombres de los *objetivos* (producción y ocio) de los dos agentes económicos principales. El productor *tiene la intención* de crear capital (hacer que se aprecie), mientras que el consumidor intenta destruirlo (depreciarlo). Un productor que solo posee no produce y un consumidor que no posee no consume. Pero lo atesorado por el productor (inventario) deprecia el producto igual que lo atesorado por el consumidor.

El uso habitual del término "consumo" confunde el interés y la depreciación[2]. La venta de un producto representa intereses para el inversor, no la depreciación del producto. La depreciación de un producto es el consumo *real*, y representa o bien la extracción del servicio para su propietario[3] (utilidad), o bien su desperdicio[4]. El desperdicio es la depreciación que para el propietario carece de valor. Solo su destrucción refleja un consumo real, al igual que solo su creación refleja una producción real. Solamente la *acción* tiene importancia económica, el nombre de un rol dado no la tiene. Los rendimientos netos de una venta del productor al consumidor son intereses, incluso si están capitalizados a través de reinversiones.

La riqueza, definida como capital acumulado, es la suma de productos. Todos los productos siempre están atesorados y depreciándose. La producción crea productos,

Reference

[1] Capítulo: Producción y consumo

[2] https://en.wikipedia.org/wiki/Depreciation_(economics)

[3] https://mises.org/library/man-economy-and-state-power-and-market/html/p/974

[4] https://es.wikipedia.org/wiki/Basura

siendo los intereses tanto el coste como el rendimiento de los mismos. El precio de un producto es la suma de los intereses generados sobre la inversión y el coste de todos los productos consumidos en su producción. Cualquier producto incorporado a un nuevo componente de producto se deprecia totalmente como producto independiente y se aprecia dentro del nuevo producto. Puesto que la suma de los costes de producción es igual al principal de la inversión[1], el aumento neto en los productos es sencillamente el interés.

La tasa de crecimiento en la riqueza es la diferencia entre el tipo de interés y la tasa de depreciación.

```
tasa-crecimiento = tipo-interés - tasa-depreciación
```

Los siguientes ejemplos demuestran el efecto de la depreciación sobre el crecimiento:

```
tasa-crecimiento = tipo-interés - tasa-depreciación
5% = 10% - 5%
-10% = 10% - 20%
```

La tasa de depreciación siempre es positiva, ya que toda propiedad se deprecia.

```
tasa-depreciación > 0
tipo-interés - tasa-crecimiento = tasa-depreciación
tipo-interés - tasa-crecimiento > 0
tipo-interés > tasa-crecimiento
```

Toda propiedad exhibe una depreciación, lo que implica que el interés económico siempre es mayor que el crecimiento económico.

Reference

[1] https://en.wikipedia.org/wiki/Bond_(finance)#Principal

El tipo de interés económico se puede observar a lo largo del tiempo como el rendimiento sobre el capital invertido.[1]

> Los inversores esperan rendimientos del 10,2%, y los *millennials* tienen la esperanza de rendimientos aún mayores.
>
> *Schroders: Global Investor Study*

El tipo de depreciación se puede deducir a partir del interés observado y las tasas de crecimiento del capital.[2]

> El crecimiento global en 2019 se ha rebajado al 2,6 por ciento, [...] lo que refleja una inversión y un comercio internacional más débiles de lo esperado a principios de año. Se prevé que el crecimiento crezca gradualmente hasta el 2,8 por ciento para 2021.
>
> *Banco Mundial: Perspectivas Económicas Globales*

En este caso, un tipo de interés del 10,2% se ve compensado con una depreciación del 7,6% para obtener un crecimiento del 2,6%.

```
tasa-depreciación = tipo-interés - tasa-crecimiento tasa-depreciación
10,2% - 2,6% = 7,6%
```

Esto es consistente con las estimaciones de depreciación del capital. Si bien los edificios y la maquinaria tienen tasas bajas de depreciación, los vehículos, los equipos de oficina y los alimentos (por ejemplo) tienen tasas mucho mayores.[3]

> Para el periodo 1960-2000, las tres estimaciones para maquinaria y equipos son del 5,61%, 5,42%, y 5,68%. Para los edificios, las estimaciones son del 3,36%, 3,43%, y 3,43%.
>
> *OECD: Estimación de las Tasas de Depreciación*

Reference

[1] https://www.schroders.com/en/insights/global-investor-study/investors-expect-returns-of-10.2-with-millennials-hoping-for-more

[2] https://www.worldbank.org/en/publication/global-economic-prospects

[3] https://www.oecd.org/sdd/productivity-stats/35409605.pdf

En la medida en que el dinero[1] presente valor de uso[2], se deprecia como cualquier bien[3]. El dinero fiduciario, como el Bitcoin o el dólar estadounidense, se presupone que no tiene valor de uso. Un dinero puro no presenta ningún crecimiento debido al coste de oportunidad[4] de los intereses a los que se renuncia. En otras palabras, los intereses son la adquisición de valor en el tiempo y la depreciación del dinero incluye la no adquisición de ese valor.

```
tasa-crecimiento-dinero-puro = tipo-interés - tipo-interés
9% - 9% = 0%
```

Todo el valor del dinero actual también se deprecia a causa del demoraje[5] monetario (sobrestadía).

```
tasa-crecimiento-dinero-mercancía = tasa-crecimiento-dinero-puro - tasa-
sobrestadía
0% - 1% = -1%
```

Las tasas de crecimiento del dinero inflacionista[6] y deflacionista se muestran en Falacia del Dinero Imprestable[7].

Reference

[1] Capítulo: Taxonomía del dinero

[2] https://es.wikipedia.org/wiki/Valor_de_uso

[3] https://es.wikipedia.org/wiki/Bien_econ%C3%B3mico

[4] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[5] https://es.wikipedia.org/wiki/Sobrestad%C3%ADa_(divisa)

[6] https://en.wikipedia.org/wiki/Monetary_inflation

[7] Capítulo: Falacia del Dinero Imprestable

Principio de Expresión

Las acciones humanas no deben confundirse con bienes. No distinguir entre ambos, al nivel más fundamental, conlleva errores de consecuencias significativas[1]. Las acciones son preferencias fundamentalmente humanas expresadas a través de los bienes, que son los objetos de esa expresión. Sin expresión, una preferencia es un mero pensamiento y un bien no proporciona ningún servicio. La Cataláctica[2] se ocupa de las preferencias expresadas, específicamente la producción[3], los intercambios, y el consumo[4].

El espíritu humano es el agente (la persona). Tiene preferencias que expresa motivando al cuerpo que controla (posee). Este cuerpo es su propiedad, un bien. Cuando su cuerpo se ha depreciado totalmente (está muerto), el espíritu deja de ser un agente. No es necesario contemplar espíritus incorpóreos, ya que no implica ninguna acción.

La Cataláctica no se ocupa de los conceptos legales, teológicos o éticos de la humanidad. El Test de Turing[5] es un criterio suficiente para la definición de humanidad. La distinción cataláctica es la formación de las preferencias, con independencia de cualquier otro agente. Una persona en este sentido es un decisor, en oposición a un seguidor de reglas. Una máquina es un bien que expresa las preferencias de una persona. Una persona expresa sus preferencias motivando su máquina.

Un espíritu no puede ser propiedad, y un cuerpo es la propiedad de su espíritu. Solamente el espíritu controla el cuerpo, donde el control define la relación de propiedad. Cuando el

Reference

[1] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor-trabajo

[2] https://es.wikipedia.org/wiki/Catalaxia

[3] Capítulo: Producción y consumo

[4] Capítulo: Principio de Depreciación

[5] https://es.wikipedia.org/wiki/Prueba_de_Turing

espíritu se ve obligado a actuar por la agresión[1] de otro agente, la preferencia no es independiente. La preferencia expresada (acción) es la del agresor.

La Cataláctica solo considera las consecuencias de los agentes independientes. Cuando una persona sufre un robo, se expresa la preferencia del ladrón, no la suya propia. Cuando una persona paga un impuesto, se presume que está expresando la preferencia de otra persona, ya que el impuesto es involuntario por naturaleza. La esclavitud implica la expresión de las preferencias del esclavista, no las del esclavo. La sustitución de la preferencia de uno por la de otro es un intercambio involuntario (robo).

A veces se argumenta que el tiempo es valioso porque la vida es temporal. Esta no es la base de la preferencia temporal[2]. La impermanencia de una persona carece de consecuencias a efectos de la Cataláctica. Una persona podría vivir para siempre y, sin embargo, seguirá presuponiéndose que presenta una preferencia por tener los bienes antes y no por tenerlos después. Una vida infinita no implica la ausencia de deseo de consumir.

La acción es la expresión de la preferencia humana a través de los bienes. Los procesos dirigidos por los humanos son acción, los procesos dirigidos por máquinas son bienes. En otras palabras, la producción/mano de obra[3], los intercambios/robos, y el ocio/desperdicio son acciones, mientras que las webs, las líneas de montaje y los automóviles son bienes.

Reference

[1] https://es.wikipedia.org/wiki/Principio_de_no_agresi%C3%B3n

[2] Capítulo: Falacia de la Preferencia Temporal

[3] Capítulo: Mano de obra y ocio

Falacia de la Reserva Plena

Existe una teoría que afirma que la banca de reserva fraccionaria[1] es un fraude que permite a los bancos crear dinero[2] "de la nada"[3]. La teoría implica que una banca honesta tiene que ser de reserva plena[4].

Esta teoría pende de la definición de la palabra "banco". Rothbard[5] escribe el argumento anterior en *Man, Economy, and State*[6], pero limita explícitamente su definición de un banco[7] al de un "almacén" de dinero:

> Cuando un hombre deposita bienes en un almacén, se le da un recibo y paga al propietario del almacén un cierto importe por el servicio de almacenamiento. Sigue teniendo la titularidad de la propiedad; el propietario del almacén sencillamente la guarda por él. Cuando se presenta el recibo del almacén, el propietario está obligado a devolver el bien depositado. Un almacén especializado en dinero se conoce como "banco".
>
> *Murray Rothbard: Man, Economy, and State*

Los bancos sí que ofrecen este servicio de almacén, con el nombre de cajas de seguridad[8]. Pero los bancos no se definen en un sentido tan estrecho. Generalmente también ofrecen cuentas remuneradas con interés, como cuentas de ahorro[9] y depósitos a plazo fijo[10].

Reference

[1] https://es.wikipedia.org/wiki/Banca_de_reserva_fraccional

[2] Capítulo: Taxonomía del dinero

[3] Capítulo: Falacia de la Nada

[4] https://es.wikipedia.org/wiki/Banca_de_reserva_100_%25

[5] https://es.wikipedia.org/wiki/Murray_Rothbard

[6] https://mises.org/library/man-economy-and-state-power-and-market/html

[7] https://mises.org/library/man-economy-and-state-power-and-market/html/pp/1086

[8] https://es.wikipedia.org/wiki/Caja_de_seguridad

[9] https://es.wikipedia.org/wiki/Cuenta_de_ahorro

[10] https://es.wikipedia.org/wiki/Dep%C3%B3sito_a_plazo_fijo

Rothbard utiliza la expectativa de interés para diferenciar el almacenamiento de dinero y el préstamo del mismo:

> El almacén recibe la propiedad de otra persona y la utiliza para sus propios fines de lucro. No es prestado, ya que no se paga interés por la utilización del dinero.

En otras palabras, su requerimiento de reserva plena no es aplicable a las cuentas remuneradas con intereses. Sin embargo, se olvida de apuntar que los intereses obtenidos con el dinero representado mediante depósitos pueden compensar legítimamente las comisiones de cuenta necesarias por lo demás.

Los bancos a menudo ofrecen cuentas de depósito a demanda[1] (por ejemplo, cheques) sin intereses. Que haya una rentabilidad positiva en la cuenta no es la demarcación que separe el almacenamiento y los préstamos, ni siquiera siguiendo su propia definición. Cuando una cuenta bancaria rente un 5% con una comisión del 6%, no hay ninguna diferencia respecto de una rentabilidad del 0% con una comisión del 1%. La diferencia es el acuerdo contractual entre el depositante y el banco.

> Puesto que es conveniente transferir papel a cambio en vez de llevar oro, los almacenes de dinero (o bancos) que se ganen la confianza del público verán que pocas personas rescatan sus certificados.

Los certificados que representan dinero almacenado son dinero representativo[2], una forma de sustitutivo dinerario[3]. En los Estados Unidos, los bancos estatales[4] y otros

Reference

[1] https://es.wikipedia.org/wiki/Cuenta_corriente_(banca)

[2] https://es.wikipedia.org/wiki/Dinero_representativo

[3] https://wiki.mises.org/wiki/Money_substitutes

[4] https://en.wikipedia.org/wiki/State_bank

emitieron antiguamente tales certificados. Estos terminaron por ser reemplazados por certificados de oro[1] y certificados de plata[2] emitidos por el banco central[3].

> Los bancos estarán sujetos, en particular, a la tentación de cometer fraude y emitir certificados pseudo-dinerarios que circulen junto con certificados dinerarios genuinos como sustitutos de dinero aceptables. Que el dinero sea un bien homogéneo significa que a las personas no les importa que el dinero que rescaten sea el dinero original que depositaron. Esto hace que los fraudes bancarios sean más fáciles de lograr.

En la medida en que los certificados del banco central representaban todo el dinero almacenado (por ejemplo, oro y plata), terminaron por seguir el rumbo descrito por Rothbard.

A medida que la suma de certificados se hizo demasiado grande para soportar la canjeabilidad, fueron abolidos y se obligó[4] a las personas a convertirlos a dinero fiduciario. Estos fraudes a gran escala sucedieron en vida de Rothbard y de su precursor von Mises[5], y fueron perpetrados por el estado y los bancos centrales bajo la protección de la norma legal (esto es, el estado).

La teoría no limita su condena de la banca al fraude del almacenamiento (cajas de seguridad), sino que la extiende al préstamo honesto de depósitos por los bancos con carácter general, incluyendo el depósito bajo demanda, las cuentas de ahorro y a menudo los depósitos a plazo fijo. Por consiguiente, la teoría es inválida. Además, implica una condena a la concesión de préstamos y a la inversión con carácter general. Tal y como apunta[6] el propio Rothbard, los préstamos no son distintos de la inversión:

Reference

[1] https://es.wikipedia.org/wiki/Certificado_de_oro

[2] https://en.wikipedia.org/wiki/Silver_certificate

[3] https://es.wikipedia.org/wiki/Banco_central

[4] https://en.wikipedia.org/wiki/Gold_Reserve_Act

[5] https://es.wikipedia.org/wiki/Ludwig_von_Mises

[6] https://mises.org/library/man-economy-and-state-power-and-market/html/p/996

> Que el capital ahorrado se canalice a inversiones por medio de acciones o por medio de préstamos es poco importante. La única diferencia reside en los aspectos técnicos legales. De hecho, incluso la diferencia legal entre el acreedor y el propietario es despreciable.

Todos los préstamos se originan a partir del capital acumulado de una persona, ya esté depositado en un banco o no. No hay ninguna fuente de préstamos distinta de los ahorros depositados. Existe una teoría relacionada[1] que afirma que las personas son demasiado poco inteligentes para comprender las condiciones contractuales del depósito.

> Huerta de Soto considera la posibilidad "de que un cierto grupo de clientes bancarios (o, a efectos del argumento, todos ellos) celebren un contrato de depósito siendo conscientes de que, y aceptando plenamente que, los bancos invertirán (o prestarán, etc.) una gran proporción del dinero que depositen". En este caso, argumenta Huerta de Soto, "la supuesta autorización de los depositantes carece de validez legal" porque pocos legos en la materia comprenden la inestabilidad inherente a la banca de reserva fraccional: creen que su depósito está garantizado, lo cual Huerta de Soto considera un error conceptual (casi universal).
>
> *Wikipedia: Jesús Huerta de Soto*

Sin embargo, los que defienden este argumento se creen capaces de comprenderlo. Por consiguiente, la teoría es inválida. Dada la no agresión[2] como distinción moral, todo individuo tiene el derecho de celebrar contratos con otro de manera voluntaria. El delito estaría en hurtarles este derecho. Las referencias a los "no bancarizados" generalmente asumen que un gran número de personas no tiene "acceso" a los servicios bancarios. En general, este no es el caso; la banca está disponible ampliamente por todo el mundo. Se trata de las personas que comprenden los riesgos[3] y eligen no asumirlos.

Una teoría relacionada es que los sustitutos de dinero cotizan al mismo valor que el dinero, lo cual representaría un fraude. En la medida en que los sustitutos de dinero (por

Reference

[1] https://es.wikipedia.org/wiki/Jes%C3%BAs_Huerta_de_Soto#Ciclo_econ%C3%B3mico_austriaco_y_banca_de_reserva_completa

[2] https://es.wikipedia.org/wiki/Principio_de_no_agresi%C3%B3n

[3] https://www.reuters.com/article/zimbabwe-crisis-cbank/zimbabwe-c-bank-says-raided-private-bank-accounts-idUSLK23553320090420

ejemplo, cuentas de depósito) estén aseguradas por el contribuyente[1], el descuento respecto del dinero que sustituyen es menor. Sin embargo, incluso si se garantiza completamente, es un error asumir que cotizan con el mismo valor que el dinero. Los sustitutos de dinero se manifiestan como cuentas de depósito y generalmente se utilizan en transacciones electrónicas. Liquidar[2] cuentas dinerarias incurre en costes de tiempo, dinero y riesgo. El fraude en tarjetas de crédito y cheques está extendido[3], y este coste aflora en todas las comisiones de transacciones y cuentas. La liquidación puede llevar días[4], cuando no meses[5]. Los comerciantes necesariamente descuentan los sustitutivos dinerarios[6] respecto del dinero. Incluso la transferencia electrónica directa entre bancos incurre en un coste de liquidación sustancial[7]:

> A los bancos se les cobra una comisión bruta de transferencia de 0,82$ por cada transacción; no obstante, existe un esquema de descuentos de tres niveles, lo cual hace que las comisiones de transacción reales cuesten entre 0,034$ y 0,82$ por transacción, en función del volumen de operaciones.
>
> *Wikipedia: Fedwire*

Por ello muchos negocios solo aceptan efectivo, otros no aceptan cheques, otros cobran un extra para compensar el descuento, y por ello hay comisiones de cajero[8], etc. Por consiguiente, la observación de que los sustitutivos dinerarios no se descuentan viene refutada por una montaña de evidencia que señala lo contrario. Y aún más importante: este descuento es demostrablemente necesario, lo que invalida la teoría.

Reference

[1] https://www.fdic.gov/

[2] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)

[3] https://en.wikipedia.org/wiki/Credit_card_fraud

[4] https://en.wikipedia.org/wiki/Cheque_clearing

[5] https://es.wikipedia.org/wiki/Chargeback_(Contracargo)

[6] https://en.wikipedia.org/wiki/Merchant_account#Discount_rates

[7] https://en.wikipedia.org/wiki/Fedwire

[8] https://es.wikipedia.org/wiki/Comisiones_por_el_uso_de_cajeros_autom%C3%A1ticos

Una teoría relacionada es que los préstamos bancarios crean la inflación de precios[1] como consecuencia de la expansión del crédito[2]. Dado que los préstamos y el dinero han evolucionado juntos necesariamente, nunca hay un momento en el que la expansión del crédito en sí cambie el nivel de los sustitutivos dinerarios. Esto exige o bien una expansión de la oferta de dinero[3], o una reducción en la preferencia temporal[4], reflejada como tasa económica de interés. La expansión del crédito es estrictamente una función de estos dos factores, no los préstamos en sí. Por consiguiente, la teoría es inválida.

Una teoría relacionada es que los bancos pueden prestar legítimamente solamente "su propio" dinero. Todo el capital prestado son ahorros de alguien. Si cualquiera puede operar un banco (esto es, pedir prestado contra sus propios ahorros y prestárselo a otros), esto es una distinción sin diferencia. Agregar ahorros con otras personas (es decir, mediante depósitos bancarios) no genera ninguna distinción significativa. Por consiguiente, la teoría es inválida.

Una teoría relacionada es que los bancos pueden prestar legítimamente solamente contra depósitos a plazo. No existe ninguna distinción económica entre un depósito a plazo y un depósito bajo demanda, ya que ambos implican reserva fraccional. La naturaleza del depósito, incluso del depósito en caja fuerte, implica que se exigen tiempo y otras limitaciones (p. ej. identificación) para su retirada. Incluso las cuentas de cheques y ahorros garantizadas por los contribuyentes son efectivamente depósitos a plazo[5]:

Reference

[1] https://es.wikipedia.org/wiki/Inflaci%C3%B3n

[2] Capítulo: Falacia de la Expansión del Crédito

[3] https://es.wikipedia.org/wiki/Miner%C3%ADa_del_oro

[4] Capítulo: Falacia de la Preferencia Temporal

[5] https://www.chase.com/content/dam/chasecom/en/checking/documents/deposit_account_agreement.pdf

> Para todas las cuentas de ahorros y todas las cuentas personales de cheques con interés remunerado, nos reservamos el derecho de requerir un preaviso de retirada por escrito de siete días.
>
> *Chase Bank: Contrato de Depósito*

El riesgo de impago y la expansión del crédito permanecen a pesar de hacer corresponder los vencimientos. Por consiguiente, la teoría es inválida. El único depósito bajo demanda auténtico es no hacer ningún depósito en absoluto (dinero), y, por supuesto, las personas tienen esta opción y la del depósito a plazo en la medida en que lo prefieren.

Una teoría relacionada es que los bancos pueden prestar legítimamente solamente contra depósitos totalmente garantizados. Sin embargo, el único retorno libre de riesgo[1] auténtico es el retorno nulo. Ese es el motivo por el que los contribuyentes garantizan los préstamos (es decir, porque les obligan). La garantía total es equivalente económicamente a que no haya ningún tipo de préstamos, lo que hace que la teoría entre en contradicción y, por consiguiente, sea inválida.

Una teoría relacionada es que incluso la banca libre[2] tiene una capacidad inherente para crear dinero "de la nada"[3]. Y, sin embargo, si esto es cierto, entonces cualquiera puede hacerlo, ya que la banca libre no confiere poderes especiales sobre las personas que se autodenominan bancos. Si el dinero se puede crear sin coste alguno, no puede ser propiedad. Por consiguiente, la teoría es inválida. Incluso el dinero fiduciario estatal incurre en un coste de producción[4], un coste de mantener su monopolio sobre la producción[5], y un coste político[6] de inflación monetaria[7]. La banca libre, por ejemplo con

Reference

[1] Capítulo: Falacia de la Rentabilidad Exenta de Riesgo
[2] https://es.wikipedia.org/wiki/Banca_libre
[3] Capítulo: Falacia de la Nada
[4] https://www.federalreserve.gov/faqs/currency_12771.htm
[5] https://es.wikipedia.org/wiki/Falsificaci%C3%B3n
[6] https://es.wikipedia.org/wiki/Crisis_en_Venezuela
[7] https://en.wikipedia.org/wiki/Monetary_inflation

el oro o con Bitcoin, no disfruta del privilegio del señoreaje[1], a causa de la naturaleza de la competencia.

Finalmente, a menudo resulta que las personas que defienden los préstamos con reserva completa son las mismas personas que defienden preferencias temporales más débiles. Esto es una contradicción directa, ya que lo primero implica una preferencia temporal infinita.

Reference

[1] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

Principio de Inflación

Se presupone[1] que un dinero[2] cambia en poder adquisitivo[3] en proporción a la demanda de bienes que representa. En otras palabras, con el doble de cantidad de dinero, cada unidad de ese dinero cotizará a la mitad de su anterior cantidad de bienes, ya que el aumento en los bienes implica una menor demanda de ellos. Se trata de una relación proporcional[4] entre la inflación monetaria[5] y la inflación de precios[6] (o la deflación). Esta relación dineraria[7] es una expresión de la ley de la oferta y la demanda[8].

- El dinero de mercado con oferta creciente, como el oro y el Bitcoin *temprano*, consume el mismo valor en bienes a medida que crea nuevas unidades – incluido el coste de oportunidad[9] del capital invertido al hacerlo. Por tanto, no produce ningún cambio en proporcionalidad y, por consiguiente, no produce ninguna inflación de precios.
- El dinero monopolístico no está sujeto a la producción competitiva, lo que permite que su productor obtenga una prima monopolística[10] en el precio de las nuevas unidades. Por tanto, aumenta la proporción del dinero respecto de los bienes, lo cual produce inflación de precios como resultado.

Reference

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/p/1107
[2] Capítulo: Taxonomía del dinero
[3] https://es.wikipedia.org/wiki/Poder_adquisitivo
[4] https://es.wikipedia.org/wiki/Proporcionalidad
[5] https://en.wikipedia.org/wiki/Monetary_inflation
[6] https://es.wikipedia.org/wiki/Inflaci%C3%B3n
[7] https://mises.org/library/human-action-0/html/pp/778
[8] https://es.wikipedia.org/wiki/Oferta_y_demanda
[9] https://es.wikipedia.org/wiki/Coste_de_oportunidad
[10] https://mises.org/library/man-economy-and-state-power-and-market/html/pp/1054

- El dinero de mercado con oferta fija, como el Bitcoin tardío, no crea unidades. Por tanto, la proporción del dinero respecto de los bienes disminuye con el crecimiento económico, lo cual produce deflación de precios[1] como resultado.

La proporcionalidad se refiere a los bienes "representados" por un dinero. Si solamente existiera un dinero, sería una relación directa a todos los bienes. Sin embargo, debe abordarse la relación en el caso de que haya múltiples dineros. Los bienes representados por un dinero son aquellos por los que se puede intercambiar. En otras palabras, la relación implica demanda de bienes en el dinero.

No obstante, la demanda no permanece constante en el caso de una decisión de minar. La nueva demanda de bienes se crea con el hecho de minar. La minera tiene que consumir bienes de "representación" al producir el dinero. El nuevo dinero se ve compensado por completo con el aumento de demanda representado por los bienes consumidos y el coste de oportunidad (es decir, menos bienes nuevos) de emplearlos en la minería. Por consiguiente, la proporcionalidad se preserva en el caso de múltiples dineros también. **El crecimiento económico no es inflacionista en precios en un mercado libre.**

Ampliando la teoría cuantitativa del dinero[2] copernicana[3], Richard Cantillon[4] formuló una teoría ahora conocida como el Efecto Cantillon[5]. La teoría es válida cuando se aplica a los dineros monopolísticos, pero no es relevante para el dinero de mercado – un hecho que parece habérseles escapado a los economistas desde Cantillon. La base de las distorsiones explicadas por Cantillon es el señoreaje[6], no la producción de dinero. La

Reference

[1] https://es.wikipedia.org/wiki/Deflaci%C3%B3n
[2] https://es.wikipedia.org/wiki/Teor%C3%ADa_cuantitativa_del_dinero
[3] https://es.wikipedia.org/wiki/Nicol%C3%A1s_Cop%C3%A9rnico
[4] https://es.wikipedia.org/wiki/Richard_Cantillon
[5] https://es.wikipedia.org/wiki/Richard_Cantillon#Teor%C3%ADa_monetaria
[6] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

producción de mercado del dinero, al igual que la producción de mercado de las cosas, no solo es neutra en efectos reales[1] sino también es neutra en precio.

En *Human Action (La acción humana)*[2], Ludwig von Mises[3], como sus predecesores, intenta demostrar[4] la validez del Efecto Cantillon para *cualquier* dinero.

> Los cambios en la oferta de dinero tienen que alterar necesariamente la disposición de los bienes vendibles poseídos por diversos individuos y empresas. La cantidad de dinero disponible en todo el sistema de mercado no puede aumentar o disminuir sin aumentar o disminuir primero las cantidades de efectivo poseídas por ciertos miembros individuales.
>
> *Ludwig von Mises: Human Action (La acción humana)*

Esta afirmación asegura que el nuevo dinero afecta primero las cantidades de efectivo poseídas existentes. Sin embargo, este no es el caso del dinero de mercado. Su creación *reduce los bienes poseídos* al tiempo que *aumenta las cantidades de dinero poseídas*. La mayor demanda de dinero se compensa con su mayor oferta de manera concurrente y proporcional. La reducción de bienes no se puede ignorar en la evaluación de la relación de dinero. La afirmación confunde el dinero de mercado con el dinero monopolístico, ya que este último no consume su valor en bienes mediante la producción. En la medida en que los bienes se consumen en esencialmente la misma ubicación en que se produce el dinero, y al mismo tiempo, ni siquiera se implica una distribución no uniforme de la relación de dinero. Este error persiste a pesar del reconocimiento explícito de que la minería consume en bienes el valor que produce en dinero nuevo.

Reference

[1] https://es.wikipedia.org/wiki/Neutralidad_del_dinero

[2] https://mises.org/library/human-action-0/html

[3] https://es.wikipedia.org/wiki/Ludwig_von_Mises

[4] https://mises.org/library/human-action-0/html/pp/778

> Que los propietarios de minas de oro confíen en ingresos anuales continuos por su producción de oro no cancela el efecto del oro recién minado sobre los precios. Los propietarios de las minas toman del mercado, a cambio del oro producido, los bienes y servicios requeridos para su minería [...]. Si no hubieran producido esta cantidad de oro, los precios no se habrían visto afectados por ella.

Tomada literalmente, la última frase es una tautología[1] (la ausencia de creación implica la ausencia de efecto de precio por la creación). Por el contexto queda claro que Mises quiere decir que, si no se hubiera producido el oro, los precios no habrían experimentado cambio alguno. Y, sin embargo, sin un cambio en la oferta de dinero, si los bienes hubieran sido consumidos en otra producción[2], el crecimiento económico implícito *reduciría* los precios; y si los bienes hubieran sido consumidos en ocio[3], la contracción económica implícita *aumentaría* los precios. En otras palabras, la conclusión anterior se invierte perfectamente. La relación de dinero se *preserva* por la producción de dinero y cambiaría por la falta de esta. Este error infecta posteriormente a las teorías dependientes.

> En contra de este razonamiento, primero de todo uno tiene que observar que, dentro de una economía que progresa y en la que las cifras de población estén aumentando y se perfeccione la división del trabajo y su corolario, la especialización industrial, prevalece en ella una tendencia hacia un aumento en la demanda de dinero. Aparecen en escena personas adicionales y quieren poseer cantidades en efectivo. El alcance de la autosuficiencia económica, esto es, de la producción para las necesidades propias del hogar, encoge y las personas se hacen más dependientes del mercado; esto, a grandes rasgos, [pág. 415] les impulsa a aumentar la cantidad de efectivo que poseen.

En otras palabras, el crecimiento económico por sí solo cambia la relación del dinero – una contradicción directa de la afirmación anterior.

Reference

[1] https://es.wikipedia.org/wiki/Tautolog%C3%ADa

[2] Capítulo: Producción y consumo

[3] Capítulo: Mano de obra y ocio

Así, la tendencia al crecimiento de los precios que emana de lo que se llama la producción de oro "normal" encuentra una tendencia de rebaja de precios que emana de la mayor demanda de poseer efectivo. Sin embargo, estas dos tendencias opuestas no se neutralizan. Los dos procesos siguen su propio curso, ambos son resultado de la dislocación de las condiciones sociales existentes, que enriquece a algunas personas y empobrece a otras. Ambos afectan a los precios de diversos bienes en distintas fechas y en distinto grado. Es cierto que el aumento en los precios de algunas materias primas causado por uno de esos procesos puede verse finalmente compensado por la caída causada por el otro proceso. Puede suceder que al final algunos o muchos precios regresen a su nivel anterior. Pero este resultado final no es el resultado de una ausencia de movimientos provocada por los cambios en la relación de dinero. Es más bien el resultado del efecto conjunto de la coincidencia de dos procesos independientes el uno del otro.

Esto constituye una refutación de la idea de la creación de dinero como un "estímulo"[1] al crecimiento, lo cual es correcto. Sin embargo, supone incorrectamente que la demanda de dinero y la creación de dinero son procesos independientes. Son explícitamente dependientes según se expresa en la relación dineraria y la ley de la oferta y la demanda que refleja. El efecto de interacciones no relacionadas se invierte perfectamente en este argumento, ya que solo puede enmascarar la relación dineraria. El estímulo es una inversión de la causa y el efecto, adecuadamente refutado; no obstante, es un error aceptar la relación dineraria y rechazarla.

El error subyacente de la inflación, como el del teorema de la regresión[2], puede surgir de un deseo comprensible de explicar los efectos adversos[3] del dinero monopolístico. Sin embargo, en el sistema puramente racional de la catalάctica[4], cualquier error en la deducción produce una inconsistencia, lo cual resulta evidente en este caso. El dinero de mercado está sujeto a la inflación monetaria, pero no produce ninguna inflación de precios. El dinero monopolístico está sujeto a inflación monetaria de manera parecida, pero produce inflación de precios – solamente a causa del monopolio sobre la producción.

Reference

[1] https://en.wikipedia.org/wiki/Stimulus_(economics)

[2] Capítulo: Falacia de la Regresión

[3] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[4] https://es.wikipedia.org/wiki/Catalaxia

Mises generaliza excesivamente al afirmar que *toda* inflación monetaria es inflacionista en precios.

> Los precios también aumentan de la misma manera si [...] la demanda de dinero cae por una tendencia general hacia una disminución del efectivo poseído. El dinero gastado adicionalmente por un "desatesoramiento" de este tipo provoca una tendencia hacia precios mayores de la misma manera que fluyen de las minas de oro [...]. Por el contrario, los precios caen cuando la oferta de dinero cae [cuando] la demanda de dinero aumenta (por ejemplo, a través de una tendencia hacia el "atesoramiento", hacia mantener mayores balances de efectivo).

Todo el dinero siempre está poseído por alguien. Bajo la anterior suposición de que no se crea dinero, un mayor "balance de efectivo" para una persona implica un menor balance para otra. Un mayor atesoramiento de dinero implica solamente una menor demanda presente de bienes en relación con la demanda futura anticipada. Un menor atesoramiento implica solamente una mayor demanda presente de bienes. No es como si el dinero se hubiera vuelto a coser en la tierra. No existe ningún coste de "desatesoramiento" (utilizar el dinero en intercambios), así que hacerlo es distinto de que el dinero "fluya de las minas de oro".

Un nivel generalmente aumentado de atesoramiento da la *impresión* de una mayor riqueza, pero es ilusoria. Para que sea de valor para las personas, el dinero tiene que ser intercambiado por bienes; llegados a este punto, la ilusión se evapora. Al contrario que la minería, el efecto del desatesoramiento no es uniforme. El primero en hacerlo obtiene el mayor valor de cambio; y el último, el menor. La estrategia especulativa[1] de "*pump and dump*[2]" (endilgar y desechar) se basa en explotar esta falta de uniformidad. La riqueza se transfiere, no se crea.

Reference

[1] Capítulo: Consumo especulativo

[2] https://es.wikipedia.org/wiki/Pump_and_dump

Además, un aumento en el atesoramiento implica una mayor preferencia temporal[1], que es el ratio del capital atesorado respecto del capital prestado (ratio de capital[2]), reflejado en el tipo de interés. Esto constituye un coste temporal mayor, no un mayor valor de capital. Existen la misma cantidad de bienes (riqueza) en el momento en el que aumenta el atesoramiento. Sin embargo, este aumento reduce proporcionalmente la producción, a causa del mayor coste de capital. Esto crea una reducción *permanente* y multiplicativa en la riqueza, ya que el tiempo perdido en la producción nunca se recupera, ni siquiera con un desatesoramiento posterior. Si se atesorara todo el dinero durante una década (suponiendo que no se produjera una vuelta al trueque), las personas podrían desatesorar solamente para constatar que su dinero ha perdido un valor significativo a causa de la vertiginosa reducción en la cantidad de bienes.

Independientemente del crecimiento económico (o su contracción), un cambio en la demanda de un dinero de mercado implica un cambio proporcional en la demanda de, o la oferta de, bienes intercambiados por el dinero, al contrario que respecto de otro dinero o del trueque. La oferta de bienes es el nivel al cual se acepta el dinero en un intercambio por ellos. Un dinero presenta valor monetario solamente en su capacidad de ser intercambiado directa o indirectamente por cosas de valor de uso[3], según implica directamente la propia relación dineraria. El valor de un dinero se deriva de las personas dispuestas a aceptarlo en intercambios (es decir, la economía). Dada la fungibilidad[4] del dinero, venderle el dinero[5] a otra persona no implica ningún cambio para esta aceptación.

En la medida en que afecta al dinero mercancía, este principio asume que la cantidad de bienes requerida para producir el dinero permanece constante. Por consiguiente, el precio de los bienes en el dinero se mantiene constante por la relación de dinero. Sin

Reference

[1] Capítulo: Falacia de la Preferencia Temporal

[2] Capítulo: Relación de ahorro

[3] https://es.wikipedia.org/wiki/Valor_de_uso

[4] https://es.wikipedia.org/wiki/Bien_fungible

[5] Capítulo: Falacia del *Dumping*

embargo, cuando el valor de los bienes requeridos para producir un dinero mercancía aumenta o disminuye, esto implica respectivamente una disminución o aumento de precios en ese dinero. Por consiguiente, independientemente de la demanda, la relación de dinero la controla la tasa de cambio en los factores de producción necesarios. Estos cambios se presuponen impredecibles, ya que de lo contrario ya están incorporados en el precio. Por consiguiente, esto constituye un error especulativo.

Mano de obra y ocio

La mano de obra y el ocio son acciones humanas[1] complementarias que afectan a la producción y el consumo[2] de bienes económicos[3]. La mano de obra es el proceso de consumo para producir un bien económico (producción). El ocio es el proceso de consumo que no produce un bien económico. El consumo sin utilidad es el proceso de desperdicio[4]. Según Murray Rothbard[5], en su *Man, Economy and State*[6]:

> el trabajo siempre involucra la renuncia al ocio, un bien deseable
>
> *Murray Rothbard: Man, Economy and State*

Este sutil error implica que tanto el trabajo como el ocio son bienes económicos. Y, sin embargo, solamente las acciones crean o consumen bienes[7]. El trabajo (producción de bienes económicos) y el ocio (producción de bienes no económicos) son acciones humanas que crean y consumen bienes a lo largo del tiempo. En el sentido más básico, la producción implica el consumo del cuerpo del agente, mientras que el consumo implica su producción.

Reference

[1] https://en.wikipedia.org/wiki/Action_axiom

[2] Capítulo: Producción y consumo

[3] https://es.wikipedia.org/wiki/Bienes_y_servicios

[4] https://es.wikipedia.org/wiki/Basura

[5] https://es.wikipedia.org/wiki/Murray_Rothbard

[6] https://mises.org/library/man-economy-and-state-power-and-market/html/p/926

[7] Capítulo: Principio de Expresión

Cada hora, invertirá su esfuerzo en producir el bien cuyo producto marginal sea el mayor en su escala de valores. Si tiene que renunciar a una hora de trabajo, renunciará a una unidad de ese bien cuya utilidad marginal sea la menor en su escala de valores. En cada momento equilibrará la utilidad del producto en su escala de valores contra la utilidad negativa de trabajar más. Sabemos que la utilidad marginal de los bienes producidos mediante esfuerzo de un hombre declinará a medida que aumente su inversión de esfuerzo. Por otro lado, con cada nueva inversión de esfuerzo, la utilidad negativa marginal del esfuerzo sigue aumentando. Por consiguiente, un hombre invertirá su trabajo en tanto la utilidad marginal del rendimiento supera la utilidad negativa marginal del esfuerzo del trabajo. Un hombre dejará de trabajar cuando la utilidad negativa marginal del trabajo sea mayor que la utilidad marginal de los bienes aumentados proporcionados por el esfuerzo.

Entonces, a medida que aumente su consumo de ocio, la utilidad marginal del ocio declinará, mientras que la utilidad marginal de los bienes a los que ha renunciado aumenta, hasta que finalmente la utilidad de los productos marginales a los que renunciar pasa a ser mayor que la utilidad marginal del ocio, y el agente reanudará el trabajo de nuevo.

Este análisis de las leyes del esfuerzo de trabajo ha sido deducido de las implicaciones del axioma de la acción y la suposición del ocio como un bien de los consumidores.

No es ni correcto ni necesario asumir que el ocio es un bien, ni implicar al hacerlo que el trabajo es un anti-bien. De la misma manera, no es necesario construir el artificio de la utilidad negativa. El valor es sencillamente una preferencia por la utilidad mayor frente a la utilidad menor. Tanto el trabajo como el ocio producen bienes de utilidad (positiva).

Es la preferencia temporal[1] lo que implica que la utilidad del ocio es mayor que la utilidad del trabajo. Considerando correctamente el cuerpo de una persona como propiedad, la "preferencia de ocio" se deduce directamente de la preferencia temporal. Como implica la cita anterior, esto es resultado de un intercambio de tiempo sin el cuerpo de uno (tiempo de trabajo) por la cantidad de intereses que compensa el valor que uno atribuye al tiempo con su cuerpo (tiempo de ocio).

El tiempo, el espacio y los bienes son los factores de toda producción, mientras que el trabajo es el proceso de producción. **Trabajo/ocio y producción son nombres distintos para la misma acción humana.** El acto de producir es trabajo u ocio; el acto de trabajar o

Reference

[1] Capítulo: Falacia de la Preferencia Temporal

estar ocioso es la producción. El Banco Puro[1] proporciona el modelo de toda la producción. Este ciclo es evidente claramente en el caso del autoempleo, que es solamente el ejemplo de la producción. En el caso de un asalariado existen dos productores, el empleado y el empleador.

Un empleado asalariado puro obtiene capital prestado y mediante él realiza intercambios por alimentos, educación y equipos requeridos para un trabajo. Una fracción de su capital es atesorada y el resto es prestado al empleador. El empleador paga al empleado los intereses (salario) del plazo de este préstamo. El empleado recupera su principal depreciado y el salario al final del trabajo.

La tarifa salarial compensa tanto la preferencia temporal por la cantidad prestada (tipo de interés nominal) y la depreciación del principal durante el plazo del préstamo. La cantidad de principal e intereses, menos la depreciación de la fracción reservada, se devuelve al acreedor del empleado. En el caso en el que su inversión de capital se tome prestada de su propio atesoramiento, el empleado es su propio acreedor. El retorno luego se atesora o se reinvierte en el trabajo futuro (o no).

Un empleador y empleado auténticos obtienen una tasa de interés de mercado. El tipo de interés del empleado es su salario menos su gasto de producción. El tipo de interés del empleador es el precio obtenido por el producto del trabajo a lo largo del tiempo de su producción menos el gasto de producción. El gasto de producción del empleador es el consumo de su capital prestado, reservado[2] a lo largo de ese tiempo, al igual que para el empleado. La cantidad en la que los intereses superan la depreciación es el aumento de riqueza[3] para ambas partes.

Reference

[1] Capítulo: Banco Puro

[2] Capítulo: Principio de Reserva

[3] Capítulo: Principio de Depreciación

El tipo de interés obtenido por ambas clases de producción es el mismo. La diferencia en cantidades devueltas es estrictamente una función de la cantidad de capital invertido, ya sea en la producción individual (empleado) o en la administración de la producción colectiva (empleador). La valoración máxima del ocio de una persona se puede inferir a partir de la tarifa salarial que acepta, descontando[1] el principal implicado utilizándose el tipo de interés de mercado.

```
tarifa-salarial = tarifa-ocio * (1 + tipo-interés + tasa-depreciación-del-
cuerpo)
```

El empleado intercambia tiempo de ocio por tiempo de trabajo en la medida en que valore la cantidad de intereses más que el valor que atribuya al tiempo de ocio. La preferencia por el ocio es una reformulación de la preferencia temporal, en la que el propio cuerpo de uno es el bien económico que se presta para la producción a cambio de intereses.

La riqueza dineraria generalmente es menor a una edad temprana, lo que implica una mayor preferencia temporal dineraria. Con el tiempo, se acumula la riqueza y disminuye la preferencia temporal. Pero lo contrario es cierto en relación con la preferencia por el ocio. El dinero y el cuerpo de uno no son la misma propiedad, y generalmente no son intercambiables. A una edad temprana, uno tiene la preferencia más baja por el ocio. A medida que el cuerpo de uno se deprecia con la edad, la cantidad de este declina a pesar de la riqueza dineraria, aumentando la preferencia por el ocio. Esto podría terminar por requerir un tipo de interés mayor que el de mercado para compensar la preferencia, lo cual produce la jubilación como resultado. La preferencia temporal dineraria y la preferencia por el ocio afectan la una a la otra ya que tienden a moverse en sentido contrario. En la medida en que el objetivo del ocio es aumentar la riqueza, menos riqueza disminuye la preferencia temporal del ocio, y más riqueza la aumenta. Esto también podría producir la jubilación como resultado.

Reference

[1] https://en.m.wikipedia.org/wiki/Present_value

Producción y consumo

La producción y el consumo son las acciones humanas[1] complementarias de producir y consumir bienes económicos[2]. Los roles humanos de productor y consumidor no deben confundirse[3] con los actos de producción y consumo. Un rol se refiere a la intención, no a la acción. Todos los productores consumen y todos los consumidores producen. El consumo que produce un bien económico es producción, de lo contrario es el proceso de ocio[4] o desperdicio[5].

El Banco Puro[6] proporciona el modelo de toda la producción. Un productor puro tiene capital prestado, consumiéndolo en la creación de un producto. La fracción consumida en cualquier momento ha sido prestada a la producción. La fracción no consumida en cualquier momento ha sido reservada[7] para tener liquidez. El nuevo producto se vende, obteniéndose intereses en la fracción consumida, devueltos como dividendo[8]. La cantidad de reserva es el mismo gasto productivo necesario que la reserva de liquidez del Banco Puro. **La reserva solo se repuebla con más capital tomado como préstamo, incluida la reinversión de dividendos/beneficios.**

Un productor de verdad convierte el tiempo y el capital en intereses, al precio de mercado del producto producido, al igual que un banco de verdad obtiene intereses al precio de mercado. El banco solamente está obteniendo los intereses de otro productor al ser un

Reference

[1] https://en.wikipedia.org/wiki/Action_axiom
[2] https://es.wikipedia.org/wiki/Bienes_y_servicios
[3] Capítulo: Principio de Depreciación
[4] Capítulo: Mano de obra y ocio
[5] https://es.wikipedia.org/wiki/Basura
[6] Capítulo: Banco Puro
[7] Capítulo: Definición de reserva
[8] https://es.wikipedia.org/wiki/Dividendo

inversor suyo. Esto muestra la equivalencia fundamental de realizar un préstamo como deuda y capital accionarial, independientemente de las distinciones *legales* (fiscalidad).

Un consumidor puro atesora capital sin prestar ningún capital a la producción. Todo el capital se presta o se reserva. Para una reserva del 100% no hay ningún interés, ninguna rentabilidad, y terminará por depreciarse por completo. En ese caso, el capital prestado se considera un regalo (caridad[1]). Además, un consumidor de verdad está sujeto a la fiscalidad y a las subvenciones, lo cual aumenta y disminuye, respectivamente, la tasa de depreciación de la cantidad atesorada.

Reference

[1] https://es.wikipedia.org/wiki/Beneficencia

Banco Puro

El concepto de un Banco Puro puede resultar útil para demostrar el comportamiento al realizar préstamos con carácter general.

Un Banco Puro proporciona solamente los siguientes servicios:

- Pide prestado dinero (deuda para con los acreedores).
- Presta dinero (saldo para con los deudores).
- Atesora dinero (reserva).

Las diferencias sustanciales respecto de un banco de verdad son:

- ausencia de intervención estatal (banca libre)
- ausencia de costes de operación (perfectamente eficiente)

El banco es propiedad de sus acreedores en proporción a su saldo, como es el caso de cualquier empresa. Hay grandes bancos que existen y son propiedades de los titulares de sus cuentas, como USAA[1] y Vanguard[2]; por tanto, esta no constituye una diferencia con respecto a un banco de verdad. Ni un Banco Puro ni un banco de verdad tienen "capital propio" para prestar, ya que todo el capital se ha pedido prestado a inversores de una manera u otra. El objetivo de los acreedores es maximizar su rentabilidad porcentual. El objetivo de los deudores es minimizar su interés devengado como gasto.

Las cuentas de acreedores son sustitutivos dinerarios[3]. Este aspecto distingue al banco de un fondo de inversión. El sustitutivo dinerario puede ser o bien un depósito a demanda[4]

Reference

[1] https://www.usaa.com

[2] https://investor.vanguard.com

[3] https://wiki.mises.org/wiki/Money_substitutes

[4] https://en.wikipedia.org/wiki/Demand_deposit

o bien un mercado monetario[1]. La diferencia es la asignación de una reserva insuficiente (rentabilidad porcentual negativa), siendo en el primer caso "el primero que llega se lo lleva"[2] y en el segundo "perder la paridad"[3].

La ausencia de intervención estatal es el concepto común de banca libre[4], en la que no existe ningún control legislativo[5], seguros estatales[6], capital con descuento[7], ni señoreaje[8]. El banco utiliza dinero mercancía[9] salvo que se especifique lo contrario, lo cual simplifica los cálculos al eliminar[10] la necesidad de compensar la inflación de precios[11] o la deflación de precios[12].

La eficiencia perfecta difiere de un banco de verdad solamente en la rentabilidad porcentual, ya que no se consume nada en su funcionamiento. Todas las ganancias son consecuencia de la preferencia temporal[13]. Se supone un interés uniforme, ya que el arbitraje[14] de tipos constituye un gasto. El demoraje monetario (sobrestadía)[15] es el gasto de guardar el dinero. La proporción del gasto (incluida la sobrestadía) es de 1 para el Banco Puro.

Reference

[1] https://en.wikipedia.org/wiki/Money_market_fund
[2] https://es.wikipedia.org/wiki/P%C3%A1nico_bancario
[3] https://en.wikipedia.org/wiki/Money_market_fund#Breaking_the_buck
[4] https://es.wikipedia.org/wiki/Banca_libre
[5] https://es.wikipedia.org/wiki/Junta_de_la_Reserva_Federal
[6] https://www.fdic.gov
[7] https://en.wikipedia.org/wiki/Discount_window
[8] https://es.wikipedia.org/wiki/Se%C3%B1oreaje
[9] Capítulo: Taxonomía del dinero
[10] Capítulo: Principio de Inflación
[11] https://es.wikipedia.org/wiki/Inflaci%C3%B3n
[12] https://es.wikipedia.org/wiki/Deflaci%C3%B3n
[13] Capítulo: Falacia de la Preferencia Temporal
[14] https://es.wikipedia.org/wiki/Arbitraje_(econom%C3%ADa)
[15] https://es.wikipedia.org/wiki/Sobrestad%C3%ADa_(divisa)

El capital reservado[1] es el dinero en el que el saldo y la deuda se compensan[2] (vencimiento[3] cero). La depreciación[4] es el coste de oportunidad[5] de no ser prestado, también conocido como "cash drag". Las relaciones entre intereses suponen un único periodo de capitalización[6] con la tasa de interés durante ese periodo. Esta simplificación en la presentación no tiene consecuencias para las relaciones implícitas.

Dada la definición precedente de un Banco Puro, las siguientes relaciones son absolutas.

```
reservado = tomado_en_préstamo - prestado
sobrestadía = tasa_sobrestadía * reservado
depreciación = tipo_interés * reservado
interés = tipo_interés * prestado
retorno = ratio_gasto * intereses
```

Para el Banco Puro, el ratio de reserva[7] determina completamente el ratio de capital[8], el ratio de deuda[9], y el ratio de ahorro.

Ratio de reserva

```
ratio_reserva = reservado / tomado_prestado
ratio_reserva = (tomado_prestado - prestado) / tomado_prestado
```

Reference

[1] Capítulo: Definición de reserva

[2] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)

[3] https://en.wikipedia.org/wiki/Maturity_(finance)

[4] Capítulo: Principio de Depreciación

[5] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[6] https://es.wikipedia.org/wiki/Inter%C3%A9s_compuesto

[7] https://es.wikipedia.org/wiki/Coeficiente_de_caja

[8] https://es.wikipedia.org/wiki/Requerimiento_de_capital

[9] https://en.wikipedia.org/wiki/Debt_ratio

Ratio de capital

```
ratio_capital = reservado / prestado
ratio_capital = (tomado_prestado - prestado) / prestado
```

Ratio de deuda

```
ratio_deuda = tomado_prestado / reservado
ratio_deuda = tomado_prestado / (tomado_prestado - prestado)
```

Ratio de ahorro

```
ratio_ahorro = prestado / reservado
ratio_ahorro = prestado / (tomado_prestado - prestado)
```

Balance

El Banco Puro no tiene pasivos, solo capital accionarial.

activos bancarios	capital accionarial
prestado + reservado	tomado_prestado

Rentabilidad porcentual

La rentabilidad porcentual para el acreedor es también función del tipo de interés. La rentabilidad porcentual del acreedor es menor que el tipo de interés del deudor a causa del *cash drag*, el gasto necesario de la retirada bajo demanda. Para reducir este gasto,

típicamente se incluyen límites temporales en los contratos de los bancos de verdad[1]. Por ejemplo, por ley cualquier retirada de dinero en una cuenta bancaria estadounidense remunerada con intereses se puede retrasar siete días. El acreedor solo puede eliminar el *cash drag*[2] invirtiendo directamente (esto es, sin garantías de liquidación).

```
rentabilidad_porcentual = tipo-interés * prestado / tomado_prestado
```

Según se demostró en Relación de Ahorro[3], los ratios de capital individuales determinan totalmente el tipo de interés del mercado. Cuando consideramos que cada persona opera como un banco puro, queda claro que el ratio de capital determina el tipo de interés. Un ratio de capital del 0% para todas las personas implica que el capital es gratuito y no tiene rendimientos. A medida que crecen los ratios de capital, van creciendo los tipos de interés. En atesoramiento total, el coste del capital es "infinito" – no se puede obtener ninguno para la producción.

La presuposición de la relación dineraria[4] es que el precio es proporcional al ratio de la demanda respecto de la oferta. Pero, según se demostró en Relación de Ahorro, la oferta y la demanda de capital existen en una relación de suma nula. Un aumento en el atesoramiento implica la correspondiente disminución en préstamos, y lo contrario implica un aumento. Por consiguiente, ni el ratio de capital ni el tipo de interés son lineales en relación con el cambio en la cantidad atesorada (o prestada). Esto ha llevado a buscar una "proporción aúrea"[5]. Y, sin embargo, dada la subjetividad del valor, esto en definitiva constituye un ejercicio fútil.

Reference

[1] https://www.chase.com/content/dam/chasecom/en/checking/documents/deposit_account_agreement.pdf

[2] https://www.investopedia.com/terms/p/performance_drag.asp

[3] Capítulo: Relación de ahorro

[4] Capítulo: Principio de Inflación

[5] https://es.wikipedia.org/wiki/Regla_de_oro_del_ahorro

No obstante, los ratios de capital determinan totalmente el tipo de interés. Puesto que las personas individualmente tratan de obtener una proporción aúrea sobre la base de sus propias preferencias, se obtiene como resultado el tipo de interés de mercado. Sustituir el ratio de capital por el tipo de interés demuestra el efecto de reserva en el Banco Puro, bajo la suposición adicional de que todo el mundo opera como Banco Puro y con el mismo ratio de capital. El ratio de capital incluye la depreciación de los bienes presentes, lo cual para el dinero es sobrestadía. La sobrestadía del Banco Puro es de 1, por lo cual desaparece.

```
rentabilidad_porcentual = (reservado * ratio_sobrestadía / prestado) *
(prestado / tomado_prestado)
rentabilidad_porcentual = (reservado / tomado_prestado) * ratio_sobrestadía
rentabilidad_porcentual = reservado / tomado_prestado
```

La rentabilidad porcentual sobre la inversión en el Banco Puro pasa a ser el ratio de reserva. Esto no implica que un Banco Puro individual pueda establecer su propia rentabilidad estableciendo su ratio de capital. Refleja meramente que el ratio de capital de mercado determina el rendimiento sobre el capital. Si *todos los prestamistas* doblaran su ratio de capital presente, sus rendimientos necesariamente se duplicarían, ya que el coste del capital y, por consiguiente, su rendimiento, se doblarían.

Bancos de verdad

Los ratios de capital independientes de todas las personas, sobre la base de su preferencia temporal individual, determinan el tipo de interés de mercado. La sustitución anterior del ratio de capital propio del banco como tipo de interés parece implicar que el banco está estableciendo el tipo de interés. Sin embargo, esto está inherente en el concepto de la preferencia temporal. Un banco puede establecer cualquier nivel de intereses que prefiera. No existe ninguna suposición por parte de los bancos de verdad en el sentido de que el mercado la aceptará, por lo cual se suponen intereses de mercado y, por consiguiente, rendimientos de mercado.

```
rentabilidad_porcentual_mercado = tipo_interés_mercado * (prestado /
tomado_prestado)
rentabilidad_porcentual_mercado = ratio_capital_mercado * (prestado /
tomado_prestado)
```

La Banca Libre también difiere del Banco Puro en los gastos de funcionamiento, que reducen directamente la rentabilidad porcentual.

```
rentabilidad_porcentual_banca_libre = rentabilidad_porcentual_mercado *
ratio_gastos
```

La banca de verdad solo difiere de la banca libre en la fiscalidad (incluidos los gastos por normas regulatorias), la cual reduce directamente la rentabilidad porcentual.

```
rentabilidad_porcentual_bancos_de_verdad =
rentabilidad_porcentual_banca_libre * ratio_gastos_fiscales
```

La Banca Central (estatal) solamente difiere del banco de verdad en la subvención de los contribuyentes (incluidas las cantidades tomadas como préstamos descontados), lo cual aumenta directamente la rentabilidad porcentual.

```
rentabilidad_porcentual_central = rentabilidad_bancos_de_verdad *
ratio_ingresos_por_subvención
```

Cuando la fiscalidad incluye el señoreaje del dinero bancario, se tiene que aplicar la Ecuación de Fisher[1] anterior para pasar el tipo de interés de un tipo nominal a un tipo real. No hay implícito ningún otro cambio aparte de la fiscalidad, que se contabiliza mediante el banco de verdad anteriormente indicado. Esta fiscalidad es generalmente la

Reference

[1] https://es.wikipedia.org/wiki/Ecuaci%C3%B3n_Fisher

fuente de la subvención, que se contabiliza mediante el Banco Central anteriormente indicado.

Toda persona, o compañía de personas (empresa), es un banco de verdad, y el estado es un Banco Central. Un banco de verdad produce el servicio de la inversión líquida, un bien económico[1]. El coste de producirlo es la depreciación de su reserva. Este es el modelo de toda la producción.

Reference

[1] https://es.wikipedia.org/wiki/Bien_econ%C3%B3mico

Relación de ahorro

La preferencia temporal[1] es la suposición cataláctica[2] de la preferencia humana por los bienes presentes antes que por los bienes futuros. Está bien establecido que la preferencia temporal se refleja en el tipo de interés. Según Murray Rothbard[3], en su *Man, Economy and State*[4]:

> El nivel del tipo de interés puro es determinado por el mercado para el intercambio de bienes presentes por bienes futuros, un mercado que, según veremos, impregna muchas partes del sistema económico. [...] Así, si, en el mercado temporal, 100 onzas de oro se intercambian por la expectativa de obtener 105 onzas de oro dentro de un año, entonces el tipo de interés es de aproximadamente un 5 por ciento anual. Este es el tipo de descuento temporal del dinero futuro respecto del presente. [...] El tipo de interés puro será entonces la tasa corriente de descuento temporal, el ratio del precio de los bienes presentes respecto del de los bienes futuros.
>
> *Murray Rothbard: Man, Economy and State*

No obstante, es el ratio de capital[5] individual lo que *determina* el tipo de interés. El ratio de interés es el del precio del bien futuro respecto del precio del bien presente. Es la prima en el precio de mercado exigida para compensarle a un propietario el tiempo sin su bien – o el precio del tiempo. Como sucede con todos los precios, está determinado enteramente por las preferencias individuales, en este caso por la preferencia temporal, expresada[6] en intercambios individuales.

La preferencia temporal de un individuo se puede representar como el ratio del precio de su cantidad atesorada respecto de su cantidad prestada a otros. En conjunto, estas cantidades constituyen sus ahorros. Al intercambiar por su valor futuro una fracción de

Reference

[1] Capítulo: Falacia de la Preferencia Temporal

[2] https://es.wikipedia.org/wiki/Catalaxia

[3] https://es.wikipedia.org/wiki/Murray_Rothbard

[4] https://mises.org/library/man-economy-and-state-power-and-market/html/p/989

[5] https://es.wikipedia.org/wiki/Requerimiento_de_capital

[6] Capítulo: Principio de Expresión

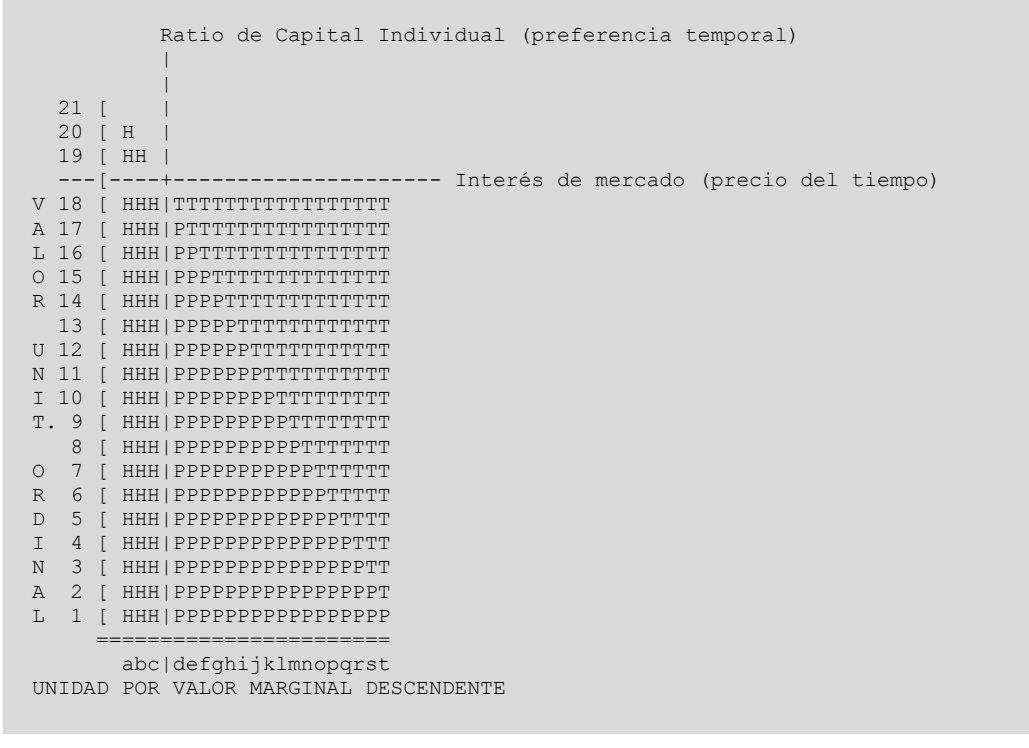
su cantidad atesorada, uno expresa que su cantidad futura vale más para uno que la cantidad en el presente. Por el contrario, no hacerlo expresa la valoración opuesta.

Una cantidad atesorada es la oportunidad de invertir (prestar) y una inversión es la oportunidad de consumir. La una se intercambia por la otra hasta que no se obtenga ningún aumento adicional de valor por seguir haciéndolo. Al invertir, uno valora la cantidad futura más que la cantidad presente no invertida. Al no invertir, uno valora la cantidad presente no invertida más que la cantidad futura. Si no fuera este el caso, habría un nivel de inversión menor o mayor, respectivamente. Esta valoración, que se manifiesta en un intercambio, es la expresión de la preferencia temporal de uno.

> Quizá se hayan cometido más falacias en las discusiones relativas al tipo de interés que al tratar cualquier otro aspecto de la economía. A la Economía le llevó mucho tiempo comprender la importancia crucial de la preferencia temporal a la hora de determinar el tipo de interés puro; a los economistas les llevó aún más tiempo comprender que la preferencia temporal es el único factor determinante. La renuencia a aceptar una interpretación causal monística ha azotado a la Economía hasta el día de hoy.

El *individuo* no controla el tipo de interés de mercado. El individuo controla su ratio de capital dado el tipo de interés de mercado. El ratio de capital es cómo *se expresa* la preferencia temporal individual. El tipo de interés es cómo el mercado *integra en los precios* esas preferencias.

El siguiente diagrama de barras verticales proporciona un ejemplo de los ahorros de un individuo.



Cada incremento ordinal representa un incremento de valor marginal. Los símbolos H, P, y T representan incrementos de valor de Atesoramiento (del inglés *Hoard*), Presente y Tiempo, respectivamente. El valor atesorado es el valor presente de una unidad no prestada. El valor presente es el de una unidad prestada si no hubiera sido prestada. El valor del tiempo es el valor neto esperado (principal + intereses) de la unidad prestada a lo largo de un periodo de tiempo al tipo de interés de mercado de ese periodo.

Cada barra vertical en el eje horizontal representa una unidad monetaria; no obstante, cada unidad tiene un valor marginal distinto para el propietario, como consecuencia de la utilidad marginal[1]. Este valor se expresa en el eje vertical como altura de la barra. Uno

Reference

[1] https://es.wikipedia.org/wiki/Utilidad_marginal

no debería confundir el valor con el precio. El valor de cada unidad poseída aumenta a medida que disminuye la cantidad atesorada y, por consiguiente, el valor neto del mismo tipo de interés (precio del dinero[1]) disminuye a medida que aumenta el atesoramiento, hasta volverse negativo (cuando ya no se presta más).

La preferencia temporal del individuo se demuestra mediante su valoración entre las unidades marginales "c" (la siguiente unidad que puede ser prestada) y "d" (la última unidad prestada). El valor presente[2] del primero es mayor de lo que se puede compensar con su valor temporal[3] potencial, por lo que no se presta. El valor presente del último no lo es, por lo que se presta. Si el tipo de interés de mercado aumenta de tal manera que el aumento del retorno por prestar "c" supera el incremento de valor cardinal de "b" (esto es, la celda "b19" de la tabla), entonces se prestará "c". Si el tipo de interés de mercado cae de tal manera que la disminución en el retorno sobre "d" supera "c18", entonces se liquidará el préstamo de "d".

Los ahorros totales son 20 unidades (unidades "a" hasta "t"). El atesoramiento total es de 3 unidades ("a" hasta "c"). El préstamo total es de 17 unidades ("d" hasta "t"). El ratio de capital del individuo es, por consiguiente, de 3/17 (~17,65%), representado en la tabla como una línea vertical entre las unidades "c" y "d". El coste de oportunidad[4] del atesoramiento es de 3 unidades x el tipo de interés del mercado. El retorno sobre el préstamo es de 17 unidades x el tipo de interés de mercado.

Es importante observar que, puesto que el valor es subjetivo[5], en este contexto solo tiene sentido la valoración que haga el individuo del importe de los intereses. El tipo de interés de mercado eleva su valoración ordinal de las unidades prestadas a entre "18" y "19". Por

Reference

[1] Capítulo: Taxonomía del dinero

[2] https://en.wikipedia.org/wiki/Present_value

[3] https://es.wikipedia.org/wiki/Valor_tiempo_del_dinero

[4] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[5] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

consiguiente, la tabla representa el interés del mercado como una línea horizontal entre esos incrementos.

Solamente la elección entre prestar y no prestar expresa una preferencia temporal. La depreciación tiene lugar en lo que se atesora, no en lo que se presta. Según se muestra en el Principio de Depreciación[1], el atesoramiento es consumo. La percepción habitual de que un intercambio de "productor" a "consumidor" constituye un consumo es un claro error. Uno puede disminuir su tasa de depreciación y, de esta manera, hacer que su atesoramiento dure más tiempo, **pero para que se refleje como preferencia temporal uno tiene que cambiar la tasa a la que realiza préstamos a otros.**

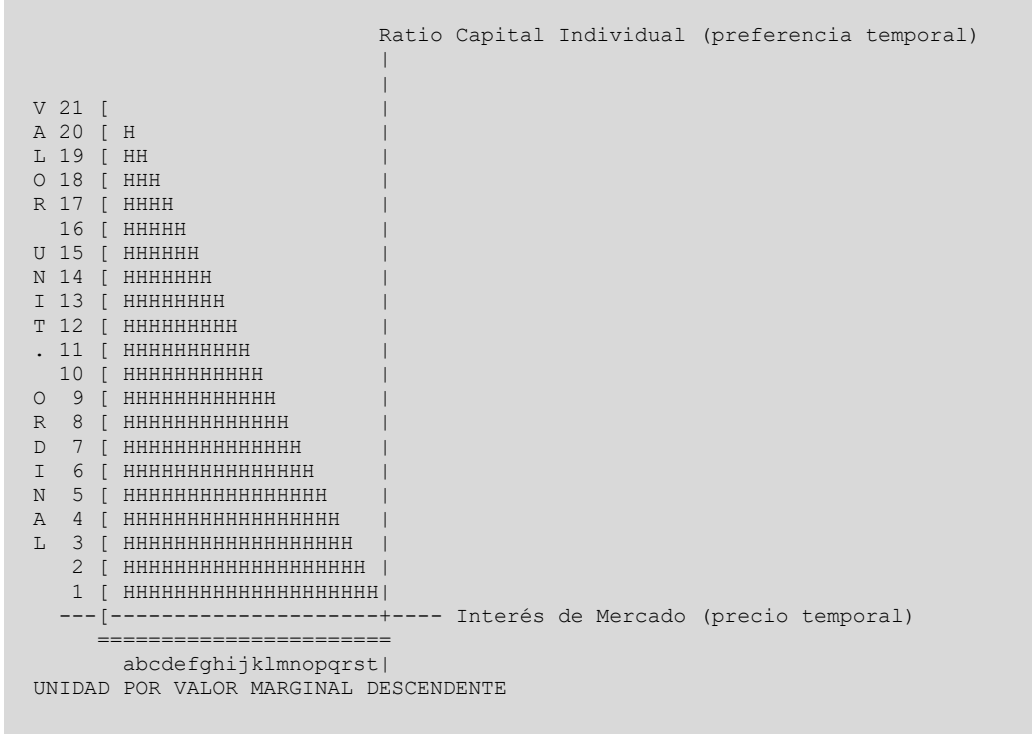
Reference

[1] Capítulo: Principio de Depreciación

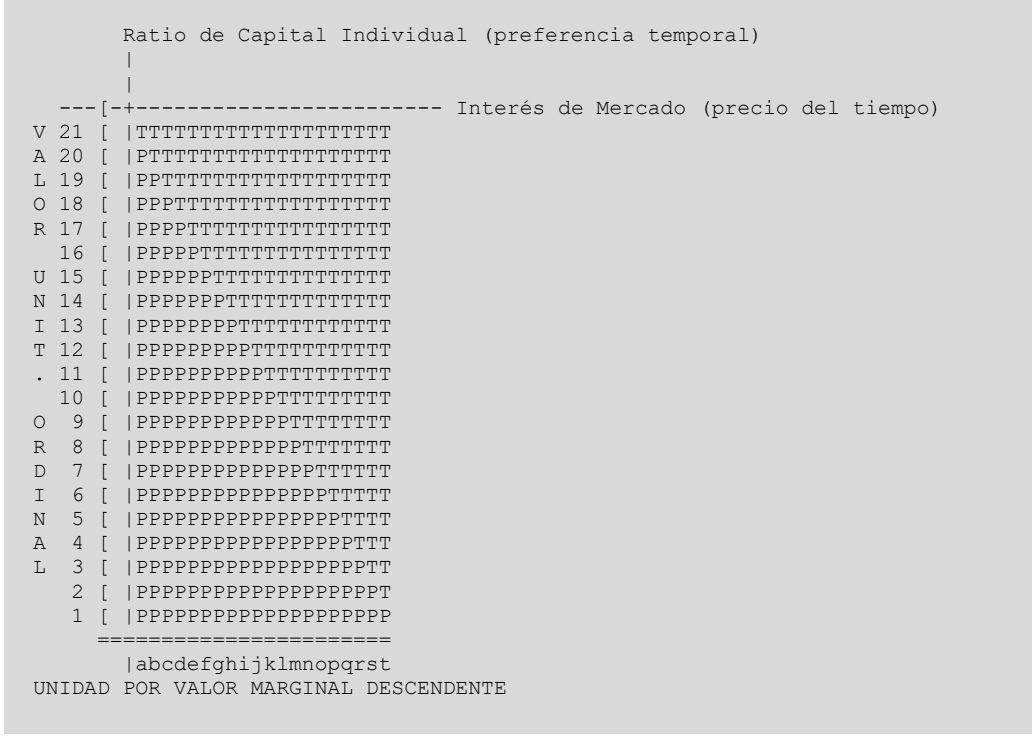
Obsérvese que, en relación con el diagrama anterior, una disminución en el tipo de interés por el valor del 18º incremento ordinal implica que se presta una unidad menos.

```
           Ratio de Capital Individual (preferencia temporal)
          |
          |
  21 [    |
  20 [ H  |
  19 [ HH |
  ---[----+---------------------- Interés de mercado (precio del tiempo)
V 18 [ HHH|TTTTTTTTTTTTTTTTT
A 17 [ HHH|PTTTTTTTTTTTTTTTT
L 16 [ HHH|PPTTTTTTTTTTTTTTT
O 15 [ HHH|PPPTTTTTTTTTTTTTT
R 14 [ HHH|PPPPTTTTTTTTTTTTT
  13 [ HHH|PPPPPTTTTTTTTTTTT
U 12 [ HHH|PPPPPPTTTTTTTTTTT
N 11 [ HHH|PPPPPPPTTTTTTTTTT
I 10 [ HHH|PPPPPPPPTTTTTTTTT
T.  9 [ HHH|PPPPPPPPPTTTTTTTT
    8 [ HHH|PPPPPPPPPPTTTTTTT
O   7 [ HHH|PPPPPPPPPPPTTTTTT
R   6 [ HHH|PPPPPPPPPPPPTTTTT
D   5 [ HHH|PPPPPPPPPPPPPTTTT
I   4 [ HHH|PPPPPPPPPPPPPPTTT
N   3 [ HHH|PPPPPPPPPPPPPPPTT
A   2 [ HHH|PPPPPPPPPPPPPPPPT
L   1 [ HHH|PPPPPPPPPPPPPPPPP
      ======================
        abc|defghijklmnopqrst
UNIDAD POR VALOR MARGINAL DESCENDENTE
```

Esto se cumple en cada incremento hasta el nivel de interés en el que el individuo no presta.



De manera análoga, esta relación se mantiene hasta el punto en el que el individuo presta todo su capital.



Consumo especulativo

La catalláctica[1] define dos categorías de empleo del capital: el consumo y la producción. Los productos son producidos y consumidos. La producción, o la creación de productos, requiere tiempo y, por consiguiente, capital ahorrado (inversión). El consumo también requiere tiempo y, por consiguiente, capital ahorrado (atesorado).

La energía humana se puede destinar al ocio o al trabajo[2], siendo la depreciación de la energía humana almacenada un factor (coste) de producción. En cualquiera de los dos casos, la conversión de esta energía potencial[3] a trabajo[4] es un consumo de capital almacenado. El trabajo puede producir alimentos y la persona puede comérselos inmediatamente. Esto constituye una economía de subsistencia[5] absoluta, en la que el único ahorro es la energía potencial almacenada en el cuerpo de uno. El producto del trabajo, del tiempo y de los factores concedidos por la naturaleza[6] se consume continuamente, ya sea en la producción (p. ej. recolectando frutos salvajes) o el ocio (p. ej. dormir). Esto a menudo se denomina vivir "al día". La propiedad ahorrada en este proceso es el propio cuerpo de la persona. Un niño comienza su vida con la energía potencial que le ha donado su madre.

El ahorro es, por consiguiente, la única fuente tanto de la producción como del ocio. Entonces surge la pregunta: ¿a qué se aplica el ahorro? Incluso en el caso de la comida que se ha digerido, permanece la pregunta. El capital aplicado a la producción se intercambia por la titularidad de lo que termine por producirse. La titularidad de un bien futuro se llama una "inversión de ahorros" (o, sencillamente, "inversión"). El capital no aplicado a

Reference

[1] https://es.wikipedia.org/wiki/Catalaxia

[2] https://mises.org/library/man-economy-and-state-power-and-market/html/p/926

[3] https://es.wikipedia.org/wiki/Energ%C3%ADa_potencial

[4] https://en.wikipedia.org/wiki/Potential_energy#Work_and_potential_energy

[5] https://es.wikipedia.org/wiki/Econom%C3%ADa_de_subsistencia

[6] https://mises.org/library/man-economy-and-state-power-and-market/html/p/939

la producción se llama un "atesoramiento de ahorros" (o, sencillamente, "atesoramiento"). El ahorro es la suma del capital atesorado *y* del capital invertido que tiene uno. El proceso de aplicar el capital atesorado a la inversión o al ocio se llama "desatesoramiento"[1].

> Después de vender sus servicios, obtiene su ingreso dinerario a partir de la producción, aumentando así sus existencias de dinero. Luego asigna su ingreso entre el consumo y la inversión de ahorro, y estamos asumiendo que no hay ningún atesoramiento ni desatesoramiento.
>
> *Murray Rothbard: Man, Economy and State*

La cataláctica versa sobre la *acción* humana, rechazando explícitamente el análisis de los *pensamientos* humanos. Los pensamientos son subjetivos, se expresan objetivamente solamente en la acción de un intercambio. Este principio se encarna en la teoría del valor subjetivo[2]. Como factor necesario tanto de la producción como del ocio, *se asume* que el tiempo tiene valor objetivo. No existe ninguna expresión de si el ahorro de uno va a ser utilizado en la producción o en el ocio hasta que se desatesora. Uno puede preferir el ahorro a la producción, pero luego se puede quedar dormido y consumir el ahorro en ocio. De manera análoga, uno puede preferir las manzanas con carácter general, pero intercambiar una manzana por una naranja. La única expresión objetiva de una preferencia es un intercambio, incluido el intercambio de ahorros por su consumo mediante producción u ocio. Puesto que no se aplica a la producción, el capital atesorado se llama "improductivo", al igual que una persona que no se dedicada a la producción.

El atesoramiento es una consecuencia necesaria de la incertidumbre. A medida que aumenta la incertidumbre, las personas tienden a aumentar su nivel de atesoramiento, ya sea limitando el ocio o la producción. Esto hace que su capital atesorado pueda ser aplicada a cualquiera de ambos en el futuro. Y, sin embargo, el capital improductivo incurre en costes de tiempo. El tiempo es objetivamente valioso. La oportunidad de

Reference

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/p/992

[2] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

utilizar el capital en producción ha sido intercambiada por una mayor certidumbre. Este es el coste de oportunidad[1] de la certidumbre, un gasto. Tanto los usos productivos como los improductivos del capital intercambian oportunidad por certidumbre. Lo atesorado se denomina "liquidez" y es necesario solamente por el hecho de la incertidumbre[2].

Según se mostró en Relación de ahorro[3], la ratio del ahorro atesorado respecto del invertido es expresión de la preferencia temporal[4] humana. Como pasa con todas las valoraciones, la de la certidumbre respecto del coste de oportunidad es subjetiva. Si bien el tiempo tiene una utilidad objetiva (esto es, más tiempo vale más que menos), el valor sigue siendo relativo y subjetivo. Y, sin embargo, como sucede con todas las valoraciones, la consecuencia es un precio objetivo del capital a lo largo del tiempo, expresado mediante intercambios y denominado el tipo de interés. El interés es tanto el retorno del capital como el coste del capital. El coste de oportunidad es la pérdida de ganancia productiva que surge de atesorar capital, medida mediante el tipo de interés.

Un atesoramiento representa la valoración subjetiva de que vale más a lo largo del tiempo que el coste de oportunidad que representa a lo largo de ese tiempo. Esto se llama "especulación". Es la expresión de una preferencia por poseer un bien en vez de deshacerse de él, con su coste medido mediante el interés al que se renuncia. La oportunidad de invertir a lo largo del tiempo lo atesorado se pierde para siempre. En otras palabras, el acto de no invertir capital es el consumo de capital. Con todo el capital atesorado, no hay producción de nuevo capital y todo el capital terminará por consumirse.

Cómo "se justifica" la especulación no es relevante para esta distinción, ya que el valor es subjetivo. Y, sin embargo, es necesario cierto nivel de atesoramiento por el hecho de la

Reference

[1] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[2] https://mises.org/wire/problem-hoarding

[3] Capítulo: Relación de ahorro

[4] Capítulo: Falacia de la Preferencia Temporal

incertidumbre (esto es, del futuro). Una preferencia por el capital en el presente, en vez de por más en el futuro, se expresa siempre en forma de atesoramiento. Uno ciertamente puede atesorar a un nivel que va más allá de la liquidez que pretende compensar la incertidumbre. Por ejemplo, uno podría atesorar por el entretenimiento de los juegos de azar[1]. El coste de oportunidad en este caso es un gasto de entretenimiento. Uno puede atesorar buscando el mejor momento para una venta[2]. En este caso, el coste de oportunidad se llama "cash drag". No importa que la persona anticipe una ganancia neta o la consiga, el atesoramiento necesariamente representa un gasto – porque el tiempo tiene valor.

Sin embargo, la preferencia temporal a veces se malinterpreta como una relación entre el consumo y el ahorro. Esto se describe a menudo de forma poco rigurosa como "consumo diferido" o "gratificación postergada". Sin embargo, según se ha mostrado, el atesoramiento es un consumo. El consumo no ha sido diferido; la gratificación no ha sido postergada. Compensar la incertidumbre es una gratificación (tranquilidad mental), el entretenimiento es gratificación (actividad de ocio), la ganancia potencial si se logra actuar en el momento óptimo en el mercado es gratificación (anticipación de un mejor precio). Todos estos consumen capital. La distinción realizada por el concepto de la preferencia temporal se encuentra en el intercambio del capital a lo largo del tiempo a cambio de intereses. Una especulación no hace ese intercambio.

Toda la propiedad (ahorro) de una persona está o bien atesorada o invertida. El atesoramiento erosiona esa propiedad a lo largo del tiempo. Los coches se desgastan, los alimentos se convierten en energía, los muebles se desgastan, el capital decae. El dinero no es diferente, decae si se atesora por su coste de acarreo[3] y su coste de oportunidad. El valor presente[4] del dinero siempre se descuenta contra su valor futuro. Esto se describe

Reference

[1] https://es.wikipedia.org/wiki/Juegos_de_azar
[2] https://en.wikipedia.org/wiki/Market_timing
[3] https://en.wikipedia.org/wiki/Cost_of_carry
[4] https://en.wikipedia.org/wiki/Present_value

como el "valor temporal del dinero". Al gastar el valor futuro, el atesoramiento de dinero se desprecia realmente por el importe del descuento a lo largo del tiempo atesorado.

Según se muestra en Principio de Depreciación[1], el acto de adquirir bienes no es consumo. No existe ningún consumo real salvo en la medida en que se deprecia la propiedad. Por consiguiente, no existe ninguna distinción entre retrasar la adquisición de bienes y comprarlos. Se trata de un mero intercambio de un tipo de propiedad por otra, ambas sujetas a depreciación. La preferencia temporal no es una distinción entre el consumo y el ahorro, es una distinción entre el atesoramiento y la inversión.

El emprendimiento necesariamente conlleva especulación e inversión. Se requiere capital para la producción, y el emprendedor está especulando en el precio de lo que se va a producir. Esta especulación sobre un bien futuro es el efecto secundario inevitable de producir productos que no tienen un precio establecido. Por consiguiente, el emprendimiento es "producción especulativa", mientras que la depreciación de un bien presente es "consumo especulativo". Dado que cualquier estimación de precio futuro está sujeta a error, toda inversión tiene carácter emprendedor en cierta medida. La inversión es producción especulativa y el atesoramiento es el consumo especulativo. Esto es evidente dado que, con todo el capital atesorado, no hay producción.

La discusión anterior diferencia entre el empleo productivo del capital y el consuntivo, en el contexto de una sola persona. En aras de la simplicidad, hemos discutido solamente el consumo de ocio (esto es, de lo atesorado por un consumidor), evitando el consumo productivo (esto es, de lo atesorado por un productor). Si bien una sola persona puede ser tanto consumidora como productora, un productor también tiene que consumir en la producción. Así, puesto que los términos han quedado sobrecargados, resulta más fácil pensar en la inversión de una persona como si fuera en el negocio de producción de otra persona.

Reference

[1] Capítulo: Principio de Depreciación

El *objetivo* de una persona es el ocio, mientras que el de un negocio es la producción. Los dos objetivos son de naturaleza consumidora; no obstante, el consumo en el contexto de un negocio es para la producción, no para el ocio. Al igual que cualquier persona, un negocio tiene que determinar su ratio de atesoramiento respecto de inversión, sobre la base de la preferencia temporal. Las inversiones de un negocio no pueden ser en su propia producción, al igual que las de una persona no pueden ser en su propio ocio, ya que cada una de ellas sería circular. Un negocio adquiere activos y los deprecia a lo largo del tiempo. Si bien estos se denominan a menudo como inversiones, un negocio no se paga intereses a sí mismo. Estos activos son capital atesorado en el proceso de consumo, para el objetivo de la producción. Su capital restante se invierte en otros negocios, como fondos de inversión o cuentas bancarias remuneradas con intereses. A medida que cada persona y negocio atesora una fracción[1] de su capital e invierte el resto, el crédito expande[2] el dinero[3] en función de la preferencia temporal.

La idea de que una persona sea tanto consumidor como productor plantea la cuestión categórica del trabajo. Si bien todas las personas tienen que consumir, la mayoría también son productores. Una persona involucrada en un trabajo asalariado es un productor. Un asalariado[4] invierte capital en su persona (por ejemplo, educación, reputación, alimentos) e invierte tiempo sin su capital humano cuando su persona está alejada de su objetivo de ocio. El salario y los beneficios asociados son su retorno sobre la inversión. A causa de la competencia laboral, este retorno busca el nivel de intereses sobre su valor comercializable a lo largo del tiempo de trabajo.

La especulación es una consecuencia necesaria del error inherente tanto en el consumo como en la inversión. El atesoramiento es consuntivo y la inversión es productiva. El concepto económico de preferencia temporal es específicamente la distinción entre el

Reference

[1] Capítulo: Falacia de la Reserva Plena

[2] Capítulo: Falacia de la Expansión del Crédito

[3] Capítulo: Taxonomía del dinero

[4] https://en.wikipedia.org/wiki/Salaryman

atesoramiento y la inversión. Esto resulta evidente en la relación de identidad entre la preferencia temporal y el interés económico. **Una proporción mayor del atesoramiento respecto de la inversión refleja una mayor preferencia temporal e implica una menor producción.**

Principio de la Inflación Subjetiva

La inflación de precios del mercado es totalmente consecuencia de preferencias personales y, por consiguiente, no se puede deducir de ninguna otra cosa.

- Los precios de los bienes se determinan subjetivamente. (Teoría Subjetiva del Valor[1])
- La preferencia temporal determina la expansión[2] del crédito respecto del dinero. (Axioma de la Preferencia Temporal[3])
- La creación de dinero[4] no es inflacionista a efecto de precios. (Principio de Inflación[5])

Esto podría obtenerse de manera más sencilla a partir de la definición del mercado libre como enteramente consecuencia de las preferencias personales.

Reference

[1] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

[2] Capítulo: Falacia de la Expansión del Crédito

[3] Capítulo: Falacia de la Preferencia Temporal

[4] Capítulo: Taxonomía del dinero

[5] Capítulo: Principio de Inflación

Falacia de la Preferencia Temporal

Existe una teoría que afirma que una menor preferencia temporal[1] es mejor que una mayor, ya que redunda en una mayor producción y, por consiguiente, una mayor riqueza. Esto constituye una inversión de causa y efecto.

La preferencia temporal es el axioma[2] económico que afirma que las personas preferimos un "bien presente" al mismo "bien futuro". Al estar en conflicto con el valor subjetivo[3], esta idea no puede ser demostrada. El tiempo resulta único en el sentido de que se asume que tiene un valor inherente. Esta presuposición está justificada en las observaciones de que las personas tenemos un tiempo limitado y de que es un factor necesario para toda producción.

El valor deriva de la percepción humana de utilidad. Una persona que intercambia un coche por un caballo valora objetivamente la utilidad de poseer el caballo más que el coche. Esto no implica nada acerca de por qué uno es más valioso para la persona que el otro, ni siquiera en presencia del intercambio. El valor que se le da a un bien anteponiéndolo a otro es una preferencia[4]. No se puede demostrar que una persona expresará una preferencia por bien alguno, ni siquiera por su propia vida. El motivo de una preferencia no es demostrable dentro de la teoría económica racional[5], con una excepción – el efecto de la riqueza en la preferencia temporal.

La disminución de la utilidad marginal[6] implica que cada unidad adicional de un bien acumulado por una persona tiene una menor utilidad para la persona que la unidad

Reference

[1] https://en.m.wikipedia.org/wiki/Time_preference
[2] https://es.wikipedia.org/wiki/Axioma
[3] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo
[4] https://es.wikipedia.org/wiki/Preferencia#Preferencias_en_econom%C3%ADa
[5] https://es.wikipedia.org/wiki/Catalaxia
[6] https://es.wikipedia.org/wiki/Utilidad_marginal

anterior. Esto implica que, para un tipo de interés dado, aumentar la riqueza implica una mayor disposición a hacer préstamos. Esta es la expresión de una preferencia temporal que va disminuyendo, y se refleja por consiguiente en un tipo de interés que va disminuyendo a causa de la mayor oferta de capital que compite por los préstamos.

El tipo de interés económico es un mero reflejo de la preferencia temporal. Si bien cualquier cosa puede afectar a la preferencia temporal de una persona, solo un cambio de riqueza implica un cambio necesario. Un mayor tipo de interés implica una mayor disposición a hacer préstamos por parte de una persona con una preferencia temporal dada. Sin embargo, sería irracional suponer que unos tipos de interés mayores aumentan la preferencia temporal. Es un error parecido asumir que una persona será más rica si reduce su preferencia temporal. En ambos casos se está produciendo una inversión de causa y efecto. Por consiguiente, la teoría es inválida.

Una preferencia temporal infinita implica la ausencia de préstamos y, por consiguiente, la ausencia de producción. Una preferencia temporal nula implica la ausencia de consumo de aquello que se produzca. Puesto que la producción solamente existe para satisfacer el consumo que termine por haber, una preferencia temporal nula también implica la ausencia de producción, puesto que no hay ningún valor atribuible al consumo de productos. Por tanto, la más baja de las preferencias temporales no es inherentemente más productiva. Por consiguiente, la teoría es inválida. La preferencia temporal es un equilibrio entre el consumo y la producción.

La riqueza de una persona aumenta solamente en la medida en que sea más capaz de satisfacer sus preferencias, incluidas las de consumo presente y diferido. Los estados emplean estímulos monetarios[1] y fiscales en un intento de aumentar el consumo o la producción, respectivamente. No obstante, esto tiene un coste: la fiscalidad. El resultado es el traslado de las decisiones de asignación de capital del mercado al estado, lo que tiene

Reference

[1] https://en.m.wikipedia.org/wiki/Stimulus_(economics)

como resultado el desperdicio de capital en productos no consumidos (exceso de oferta) o no disponibles (escasez). Esto implica que las personas son menos capaces de *satisfacer* sus preferencias. Sin embargo, no implica ningún cambio en las preferencias que tienen, salvo en la medida en que la fiscalidad disminuya su riqueza o los subsidios la aumenten.

La economía no hace juicios de valor, infiere su necesaria consecuencia. La teoría presupone una moralidad, que se puede asumir pero que tiene que ser objetiva. La agresión diferencia el mercado de las intervenciones en el mercado, como las del estado. Sin embargo, incluso si uno acepta la no agresión[1] como la frontera de lo moral, no existe ninguna distinción moral entre una preferencia temporal mayor y una menor. No hay ninguna proporción de consumo respecto de la producción que implique agresión alguna, sigue siendo subjetiva a pesar de verse afectada por la riqueza. Por consiguiente, la teoría es inválida.

Puede resultar ilustrativo considerar la subjetividad del valor en términos de preferencia sexual.

```
{ X, Y }
{ X->X, Y->Y }
{ X->X|Y, Y->X|Y }
{ X->Y, Y->X }
```

Uno podría considerar la lista ordenada por una mayor producción (es decir, producir más humanos). Muchos estados intentan reducir la expresión de la preferencia sexual al conjunto { X->Y, Y->X }. Tanto la criminalización[2] directa de la expresión como el incentivo financiero[3] explícito a la misma se emplean para tal finalidad. Esto tiene un

Reference

[1] https://es.wikipedia.org/wiki/Principio_de_no_agresi%C3%B3n

[2] https://es.m.wikipedia.org/wiki/Legislaci%C3%B3n_sobre_derechos_LGBT_en_el_mundo

[3] https://en.m.wikipedia.org/wiki/Marriage_promotion

impacto discernible en la expresión de la preferencia sexual pero no se puede decir que tenga ningún impacto en la preferencia en sí.

De manera análoga, debería estar claro que un aumento de la producción no es objetivamente bueno. Que la gente haga lo que prefiera es el bien moral, asumiendo de nuevo el principio moral de la no agresión. Incluso si suponemos que las personas prefieren la continuidad de la especie[1], esto no implica nada a efectos de las preferencias sexuales individuales.

Una teoría relacionada dice que las personas pueden demostrar una menor preferencia temporal atesorando más bitcoin. Un nivel incrementado de atesoramiento a costa de préstamos implica una *mayor* preferencia temporal. Un nivel incrementado de atesoramiento a costa del consumo parece implicar una menor preferencia temporal, puesto que el consumo parece retrasarse. Sin embargo, un atesoramiento representa solamente la liquidez requerida para el consumo.

En tanto juego de azar[2], cualquier especulación es un consumo del coste de "jugar", costeado con la liquidez que requiera. Este coste es, como mínimo, el coste de oportunidad[3] de no prestar la cantidad (esto es, el interés). A pesar de que el juego, como todo consumo, requiere tiempo, la preferencia expresada es jugar al juego, no capturar el valor temporal. Por tanto, esta teoría también es inválida.

Existe una teoría relacionada que afirma que la preferencia temporal se expresa a través del consumo diferido – cuando una persona acumula ahorros en vez de consumir esos ahorros. Según se demostró en Consumo Especulativo[4], esto representa de manera

Reference

[1] https://futurism.com/in-order-to-ensure-human-survival-we-must-become-a-multi-planetary-species

[2] https://es.wikipedia.org/wiki/Juegos_de_azar

[3] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[4] Capítulo: Consumo especulativo

incorrecta todo ahorro como inversión implícita. El ahorro es un término general que abarca tanto el atesoramiento como la inversión de una persona.

El ahorro es la *fuente* de toda inversión, pero solo la inversión real expresa una preferencia temporal. Lo atesorado ciertamente puede cambiar de valor comercializable. **Pero considerar un mayor atesoramiento como expresión de una menor preferencia temporal es una interpretación errónea coloquial y común del significado económico del término.** Esto invierte su significado, lo que lleva a conclusiones como que el atesoramiento total expresa una preferencia temporal nula. Y, sin embargo, con atesoramiento total los tipos de interés son infinitos, y un interés infinito refleja una preferencia temporal infinita. Esta contradicción directa evidencia que el significado del término preferencia temporal se ha invertido, invalidando la teoría.

DINERO

Tautología del Coleccionable

Intentando aplicar el Teorema de Regresión[1] a Bitcoin, uno podría postular que Bitcoin comenzó como un "coleccionable", surgiendo del interés de los teóricos monetarios. El coleccionable obtuvo un valor de uso[2] original a causa de sus preferencias personales. Entonces fue intercambiado en trueque[3] como consecuencia de este valor, pasando a ser un medio de cambio[4] sobre la base de la memoria del valor de trueque.

Esto parece consistente con el teorema[5], que argumenta que todo dinero[6] *debe* originarse a partir de una mercancía[7] que obtenga valor de trueque y luego valor de cambio monetario. Y, sin embargo, si el valor de la materia prima pudiera surgir de su potencial como dinero, entonces el teorema es tautológico[8], implicando nada más que "el dinero es dinero".

> Ahora bien, el teorema de regresión pretende interpretar la primera emergencia de una demanda monetaria de un bien que anteriormente hubiera sido demandado exclusivamente para fines industriales, influida por el valor de cambio que se le asignara en ese momento por cuenta de sus servicios no monetarios exclusivamente.
>
> *Ludwig von Mises: Human Action (La acción humana)*

El postulado se aprovecha de la ambigüedad coloquial en la palabra "materia prima", a pesar de la referencia explícita al valor de uso "industrial" en el propio teorema. **Si**

Reference

[1] Capítulo: Falacia de la Regresión

[2] https://es.wikipedia.org/wiki/Valor_de_uso

[3] https://es.wikipedia.org/wiki/Trueque

[4] https://en.m.wikipedia.org/wiki/Medium_of_exchange

[5] https://mises.org/library/human-action-0/html/pp/778

[6] Capítulo: Taxonomía del dinero

[7] https://es.wikipedia.org/wiki/Mercanc%C3%ADa_(econom%C3%ADa)

[8] https://es.wikipedia.org/wiki/Tautolog%C3%ADa

cualquier cosa puede ser una materia prima, entonces el Teorema de Regresión implicaría, al contrario de lo que afirma, que cualquier cosa puede ser dinero.

> En economía, una "commodity" (traducido habitualmente como mercancía) es un bien o servicio económico que tiene una fungibilidad plena o sustancial: esto es, el mercado trata ejemplares del bien como equivalentes o prácticamente equivalentes sin considerar quién los ha producido. [...]
>
> La mayoría de las "commodities" son materias primas, recursos básicos, productos agrícolas o de la minería, como mineral hierro, azúcar, o granos como el arroz o el trigo. Las "commodities" también pueden ser productos no especializados producidos en masa como productos químicos o memorias informáticas.
>
> *Wikipedia: Commodity*

El Teorema de la Regresión utiliza "commodity" (dinero mercancía) para distinguir el dinero de algo que no tiene valor de uso original. Si lo que pretende decir es que *cualquier cosa* es una "commodity", es una tautología; y de lo contrario, este postulado es una tergiversación del teorema.

Falacia del Bucle de la Deuda

Existe una teoría que afirma que no hay dinero[1] real en los sistemas estatales modernos de moneda[2]. En vez de esto, lo que se conoce habitualmente como dinero "fiduciario" es realmente un sustitutivo dinerario[3] (por ejemplo, un derecho a dinero que sea reclamable y se puede hacer valer legalmente). Un sustituto de dinero es una obligación para rescatar el sustituto obteniendo el dinero tomado prestado que representa, por lo que incluso con fines de definición esto presenta un problema: la base del término "bucle". La teoría se basa en la observación de que el estado tanto emite la moneda como la acepta, lo que implica una obligación de hacerlo, por ejemplo en la cancelación de deuda con el estado (por ejemplo, los impuestos). Por consiguiente, al emitirlo, el derecho reclamable es un crédito contra futuras liquidaciones de impuestos, etc. (es decir, el dinero real).

Y, sin embargo, los sustitutivos dinerarios son derechos reclamables a una cantidad definida de dinero[4], ya que de lo contrario no son fungibles. El importe de deuda fiscal representado por un billete de 100$, en pago de 100$ de impuestos, se define en términos de sí mismo (esto es, el error lógico del razonamiento circular[5]). La cantidad que este compensa es lo que el estado esté dispuesto a intercambiar por él. Este sería el caso para cualquier dinero, incluidas 100 onzas de oro o 100 unidades de dinero fiduciario. **El dinero no representa ninguna cantidad de otro bien, representa aquello por lo cual se pueda intercambiar.**

El estado no incurre en ninguna deuda al declarar que aceptará un dinero, ya sea oro o dinero fiduciario. De manera análoga, un negocio que declare que aceptará un dinero

Reference

[1] Capítulo: Taxonomía del dinero

[2] https://es.wikipedia.org/wiki/Moneda_(divisa)

[3] https://wiki.mises.org/wiki/Money_substitutes

[4] https://wiki.mises.org/wiki/Money_substitutes#Nature

[5] https://es.wikipedia.org/wiki/Razonamiento_circular

concreto no incurre en ninguna deuda al hacerlo. La deuda del dinero representativo[1] (una forma de sustitutivo dinerario), como un certificado de oro[2], se expresa en el intercambio del oro por el derecho reclamable a oro que tiene el poseedor del certificado. La emisión del dinero no cambia este hecho. El estado o un negocio ciertamente pueden emitir oro en intercambios sin que el oro se considere una deuda. El dinero fiduciario estatal disfruta de una protección monopolística[3] sobre la emisión, lo que le garantiza al estado un beneficio[4] al hacerlo. Pero esto no es relevante para la cuestión de si el dinero fiduciario es dinero o es deuda.

Ningún dinero tiene valor intrínseco. El dinero fiduciario se distingue del dinero mercancía, como el oro, solamente en la presunción de no tener valor de uso[5]. Pero dado que el valor es subjetivo[6], esta no supone una distinción sustancial. Ni siquiera una distinción real, ya que el papel moneda puede quemarse para obtener calor. Si el estado minara, acuñara y aceptara oro o bitcóin, la teoría tendría que considerar unidades de oro y deuda de bitcóin bajo los mismos criterios que aplica al dinero fiduciario.

La teoría representa una falta de comprensión de la naturaleza de los sustitutivos dinerarios. Un derecho reclamable no puede ser un derecho a sí mismo. En tal escenario, el derecho reclamable se compensaría[7] consigo mismo. En otras palabras, si 100$ fuera un derecho reclamable a 100$ de algo, poseer el derecho reclamable satisface su propia reclamación. No sería un derecho reclamable en absoluto, sería dinero. Por consiguiente, la teoría es inválida.

Reference

[1] https://es.wikipedia.org/wiki/Dinero_representativo

[2] https://es.wikipedia.org/wiki/Certificado_de_oro

[3] https://es.wikipedia.org/wiki/Falsificaci%C3%B3n

[4] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[5] https://es.wikipedia.org/wiki/Valor_de_uso

[6] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

[7] https://es.wikipedia.org/wiki/Compensaci%C3%B3n_(finanzas)

La transición desde derecho reclamable hasta dinero fiduciario sucede cuando el dinero representativo es derogado por su emisor. El dólar estadounidense fue monetizado en 1934[1] cuando se canceló su canjeabilidad. Se obligó a las personas a intercambiar dólares canjeables por dólares no canjeables. En la medida en que los dólares anteriormente canjeables permanecen en circulación, como es el caso de muchos, son convertidos cuando los encuentra la Reserva Federal[2]. La retención de la frase "Federal Reserve Note" (que en inglés hace referencia a su carácter de pagaré) en el dólar no canjeable constituye un anacronismo.

Todo el dinero implica sustitutivos dinerarios, como consecuencia de los préstamos[3]. Podemos clasificar cuatro escenarios hipotéticos de los sustitutivos dinerarios en términos de regresión de la deuda, donde cada etapa en la regresión es un pagaré[4].

- Sin regresión (dinero)
- Regresión sencilla (dinero representativo)
- Regresión finita (sustitutivo dinerario)
- Regresión infinita (dinero imposible)

Un pagaré puede ser un derecho reclamable de otro tipo de derecho reclamable, pero no de sí mismo (esto es, cualquier cosa por la que pueda ser intercambiado). De lo contrario, no hay ninguna regresión real y el supuesto derecho reclamable *es* dinero. Esto es cierto en el caso en el que el derecho reclamable sea totalmente circular directa o indirectamente, según implica el término "bucle", ya que el pagaré se compensa a sí mismo. Así pues, el término "bucle de deuda" es sencillamente otra descripción de

Reference

[1] https://en.wikipedia.org/wiki/Gold_Reserve_Act

[2] https://es.wikipedia.org/wiki/Junta_de_la_Reserva_Federal

[3] Capítulo: Falacia de la Expansión del Crédito

[4] https://es.wikipedia.org/wiki/Pagar%C3%A9

"dinero". Los ejemplos incluyen oro, Bitcoin, y el dólar estadounidense no canjeable (moderno).

Un derecho reclamable directo (regresión sencilla) de dinero es un dinero representativo, aunque este término se reserva generalmente para un pagaré tangible que represente un dinero mercancía[1]. El pagaré representa dinero directamente. El dólar estadounidense canjeable era un dinero representativo.

Un derecho reclamable indirecto representa cualquier progresión finita de derechos reclamables frente a otros. Cuando se compensan todos los derechos reclamables, el dinero lo detenta su legítimo propietario con todos los derechos reclamables liquidados, y cualquier derecho reclamable circular totalmente compensado recíprocamente[2]. Obsérvese que si los derechos reclamables son totalmente circulares no hay nada que compensar (esto es, el derecho reclamable es dinero).

Una regresión infinita de derechos reclamables no puede existir[3]. Considérese un pagaré hipotético emitido por el tesoro estatal con canjeabilidad en términos de compensar una obligación fiscal estatal.

- 1$ compensa la obligación fiscal sobre 10$ de ingresos.
- 10$ compensa la obligación fiscal sobre 100$ de ingresos.
- 100$ compensa la obligación fiscal sobre 1000$ de ingresos.
- Y así en adelante...

Si bien el pagaré no se representa a sí mismo, su regresión es infinita. Un derecho reclamable solo se puede reclamar contra un número finito de otros derechos

Reference

[1] https://es.wikipedia.org/wiki/Dinero_mercanc%C3%ADa

[2] https://en.wikipedia.org/wiki/Set-off_(law)#Close_out_netting

[3] https://en.wikipedia.org/wiki/Turtles_all_the_way_down

reclamables. En este caso, cualquier instrumento de este tipo no es en realidad un billete y solamente podría intercambiarse como dinero.

Falacia del Dinero Ideal

Se ha propuesto[1] que la existencia de un "índice de valores" internacional apolítico (esto es, objetivo) tendrá como resultado que las personas obliguen a los estados a utilizar el índice como "objetivo de valor" para sus dineros, eliminando así la inflación de precios[2]. También se ha sugerido que Bitcoin es un índice de este tipo y precipitará este escenario.

La fuerza de presión prevista es la opción de abandonar ciertos dineros estatales en favor de otros. El movimiento va de los dineros de inflación más alta a los de inflación más baja, sobre la base de su comparación con el índice. La consecuencia es que los estados tendrán que utilizar cada vez más el índice como objetivo para sus tasas individuales de inflación de precios. Este resultado es que los dineros estatales se acerquen "asintóticamente" a la condición de Dinero Ideal[3] representada por el índice.

El Dinero Ideal es un dinero estatal con una tasa nula de inflación de precios:

> ...no existe una tasa ideal de inflación que debiera ser seleccionada y elegida como objetivo sino más bien que el concepto ideal necesariamente sería el de una tasa nula para lo que se llama inflación.
>
> *John F. Nash Jr.: Dinero Ideal y Dinero Asintóticamente Ideal*

La expresión de la teoría es tanto variada como limitada (se deja la prueba al lector). Sin embargo, el resumen anterior expresa todos los elementos esenciales. Dadas estas limitaciones, puede resultar de ayuda comenzar con suposiciones generosas. Supongamos que un dinero puede expresar un valor objetivo (véase la teoría subjetiva del valor[4]), que Bitcoin es un dinero de este tipo, y que las personas generalmente tienen la

Reference

[1] http://sites.stat.psu.edu/~gjb6/nash/money.pdf

[2] https://es.wikipedia.org/wiki/Inflaci%C3%B3n

[3] https://en.wikipedia.org/wiki/Ideal_money

[4] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

capacidad de comparar el valor de Bitcoin con el de otros dineros estatales importantes. Supongamos también que, a pesar de la contradicción aparente, las personas generalmente utilizarán Bitcoin en intercambios (la fuente del índice) *y* preferirán utilizar dineros estatales (una premisa necesaria).

Si también asumimos que las personas están libres de las leyes relativas al curso legal de monedas[1], y que su utilización de divisas competidoras logra obligar a los estados a utilizar Bitcoin como "objetivo de valor", se eliminará el señoreaje[2]. Sin embargo, según se demuestra en Principio de Estabilidad[3], la finalidad del dinero estatal (fiduciario[4]) es recaudar el señoreaje, que constituye un impuesto. En otras palabras, el Dinero Ideal es un sistema de recaudación de impuestos que no recauda ningún impuesto. Si se aceptan las suposiciones anteriores, el Dinero Ideal es la obsolescencia del dinero estatal. **La propuesta no considera el motivo por el cual existía inicialmente el dinero fiduciario.**

Reconsidérense ahora las suposiciones. El dinero fiduciario requiere que existan leyes relativas al curso legal de monedas y, por tanto, la Ley de Gresham[5] (plasmada por primera vez por Nicole Oresme[6] en *De origine, natura, jure et mutationibus monetarum*, aprox. en 1360) siempre rige sobre el dinero fiduciario:

Reference

[1] https://es.wikipedia.org/wiki/Curso_legal

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] Capítulo: Propiedad de Estabilidad

[4] https://es.wikipedia.org/wiki/Dinero_por_decreto

[5] https://es.wikipedia.org/wiki/Ley_de_Gresham

[6] https://es.wikipedia.org/wiki/Nicol%C3%A1s_Oresme

> Estos ejemplos muestran que, en ausencia de leyes eficaces relativas al curso legal de monedas, la Ley de Gresham funciona en sentido contrario. Si se les da a elegir qué dinero aceptar, las personas operarán con el dinero que creen que vaya a tener el mayor valor a largo plazo. Sin embargo, si no se les da a elegir, y si se les exige aceptar todo dinero, de buena o mala calidad, tenderán a mantener en su posición el dinero de mayor valor percibido, y transferirán el dinero de mala calidad a otras personas. En resumen, en ausencia de leyes relativas al curso legal, el vendedor no aceptará nada más que dinero de cierto valor (dinero de buena calidad), mientras que la existencia de leyes relativas al curso legal hará que el comprador ofrezca solamente el dinero con el menor valor como materia prima (dinero de mala calidad) ya que el acreedor tiene que aceptar ese dinero por su valor nominal.
>
> *Wikipedia: Ley de Gresham*

La propuesta asume incorrectamente que rige la Ley de Thiers[1]. Si este fuera el caso, la gente no utilizaría dinero fiduciario. También ignora la existencia de controles cambiarios[2] que existen específicamente para prevenir la fuga de capitales[3]. Tales controles se refuerzan a medida que se acelera la fuga de capitales, con el fin de preservar los ingresos fiscales. Finalmente, tales controles limitan sustancialmente el descubrimiento de precios en el índice, haciendo que resulte menos útil que la referencia concebida.

La propuesta no ofrece ninguna explicación racional por la que las personas pasaran a poder moverse entre dineros estatales en presencia de dichos controles. Supone que las personas reconocerán mejor el impuesto, por la presencia del índice y su capacidad de hacer comparaciones con él, y, por consiguiente, controlará más eficazmente el apetito fiscal del estado. Dado el uso prácticamente universal del oro como un índice comparativamente objetivo antes de la evolución del dinero fiduciario mundial, no está claro cómo llegó a establecerse el dinero fiduciario si podemos asumir que las personas van a reaccionar ante él de esa manera.

Reference

[1] https://es.wikipedia.org/wiki/Ley_de_Gresham#Reverso_de_la_ley_de_Gresham_(ley_de_Thiers)

[2] https://en.wikipedia.org/wiki/Foreign_exchange_controls

[3] https://es.wikipedia.org/wiki/Fuga_de_capitales

Existe el argumento de que Bitcoin es un índice objetivos mientras que el oro no lo es. Esto se basa en la oferta inflacionaria del oro, en contraste con la oferta fija de Bitcoin. Esto supone que la inflación monetaria implica un dinero inestable mientras que la oferta fija implica un dinero estable. Según se muestra en Propiedad de Estabilidad, los dos dineros son estables. El argumento no reconoce que el valor, indicado por el índice, es una consecuencia tanto de la oferta como de la demanda. La demanda de oro se estabiliza con la inflación y la demanda de Bitcoin se estabiliza con las comisiones.

Por consiguiente, la teoría es inválida. O bien el dinero fiduciario dejará de existir o recaudará el impuesto. Los estados solo renunciarán a este impuesto bajo una presión extrema y, en tales casos, solo brevemente. Si acaso, el "dinero ideal" será el Bitcoin, y no se intercambiará libremente con los dineros estatales (en la medida en que estos sigan existiendo).

Principio de Inflación

Las reglas de consenso de Bitcoin crean un periodo de inflación monetaria[1]. Existe una teoría que afirma que esto hace que el dinero pierda poder adquisitivo[2]. Según se muestra en Principio de Inflación[3], **el aumenta de oferta de un dinero de mercado no implica ningún cambio en su poder adquisitivo**. Por consiguiente, la teoría es inválida.

Que Bitcoin no sea inflacionista en precios implica que los propietarios no "subvencionan" la minería. El capital consumido por las mineras es el suyo propio (inversión), el dinero creado es su propio producto, y el rendimiento sobre la inversión (intereses) es una consecuencia del aumento en la demanda que proporcionan ellas mismas – compensando el coste de oportunidad[4] de desplegar su propio capital a lo largo del tiempo.

Reference

[1] https://en.wikipedia.org/wiki/Monetary_inflation

[2] https://es.wikipedia.org/wiki/Poder_adquisitivo

[3] Capítulo: Principio de Inflación

[4] https://es.wikipedia.org/wiki/Coste_de_oportunidad

Taxonomía del dinero

El dinero fiduciario no tiene valor de uso[1]. Tiene utilidad como dinero solamente en la medida en que las personas estén dispuestas a recibirlo en intercambios. Estas personas pueden incluir, y a menudo incluyen, un estado emisor, aunque esto no constituye una característica distintiva. El nombre proviene de que existe como dinero por decreto[2] ("dixitque Deus fiat lux et facta est lux"). No obstante, una declaración de este tipo tampoco constituye una característica distintiva. **El dinero fiduciario es sencillamente dinero sin valor de uso.** Al dinero con valor de uso se le denomina dinero mercancía[3].

Si bien el valor es subjetivo[4], lo que hace imposible determinar en la práctica su valor de uso, la clasificación en sí está clara. El dinero de papel se puede quemar como calefacción, pero esto típicamente no se considera un valor de uso sustancial. El Bitcoin puede ser utilizado para aplicar marcas temporales[5], pero tampoco esto se considera típicamente como valor de uso sustancial. El oro, la plata, el cobre, y otras acuñaciones se considera generalmente que no tienen un valor de uso sustancial. Cuando el valor nominal de un dinero mercancía pasa a ser menor que su valor como materia prima, se ha convertido en una materia prima[6] y se funde o se atesora[7].

Reference

[1] https://es.wikipedia.org/wiki/Valor_de_uso

[3] https://es.wikipedia.org/wiki/Dinero_mercanc%C3%ADa

[4] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

[5] https://es.wikipedia.org/wiki/Sellado_de_tiempo_confiable

[6] https://es.wikipedia.org/wiki/Bol%C3%ADvar_(moneda)#Bol%C3%ADvar_Fuerte_(VEF)_(2008_-_2018)

[7] https://es.wikipedia.org/wiki/Ley_de_Gresham

Un sustitutivo dinerario[1] es un derecho reclamable contractual[2] a una determinada cantidad de dinero, rescatable bajo demanda. Por tanto, un sustitutivo dinerario representa un "bien futuro" mientras que el dinero es un "bien presente". El dinero fiduciario no es un sustitutivo dinerario[3] porque no es rescatable por ninguna cantidad definida de dinero, es el dinero en sí. La deuda a menudo se tituliza[4] y es garantizada por el prestamista como sustitutivo dinerario, conocido como billete[5]. Puesto que el valor es subjetivo, tampoco es posible distinguir si lo que valora una persona es el rescate, o el derecho reclamable en sí, pero generalmente se asume que lo que se valora es el rescate, no el documento en el que se consigna. Cuando se abole un sustitutivo dinerario pero sigue utilizándose en intercambios, se ha completado su transición a dinero fiduciario[6].

El dinero representativo[7] a menudo se malinterpreta como un bien presente, pero puesto que es un derecho reclamable (a aquello que representa), constituye un sustitutivo dinerario. El dólar estadounidense respaldado por el oro fue un sustitutivo dinerario y el dólar estadounidense moderno es dinero fiduciario. Los dólares estadounidenses basados en cuentas son sustitutivos dinerarios electrónicos[8], al igual que todas las cuentas custodiadas de Bitcoin y los intercambios en operaciones no confirmadas. Se trata de promesas a rescatar en dólares o bitcóins, respectivamente.

Los dólares que uno puede sujetar en una mano son dinero fiduciario, al igual que los bitcóins que uno puede gastar con las claves privadas de uno. Por tanto, el término "dinero fiduciario" por sí solo no distingue al dólar del bitcóin. *Sin embargo, esta distinción*

Reference

[1] https://wiki.mises.org/wiki/Money_substitutes

[2] https://financial-dictionary.thefreedictionary.com/Contractual+Claim

[3] Capítulo: Falacia del Bucle de la Deuda

[4] https://es.wikipedia.org/wiki/Titulizaci%C3%B3n

[5] https://es.wikipedia.org/wiki/Papel_moneda

[6] https://es.wikipedia.org/wiki/Certificado_de_oro

[7] https://es.wikipedia.org/wiki/Dinero_representativo

[8] https://www.investopedia.com/terms/e/electronic-money.asp

nunca hizo falta antes de que existiera el Bitcoin. Se presuponía que los dineros de mercado sin valor de uso no eran posibles[1]. Sin embargo, existe una diferencia sustancial entre esos dos tipos de dinero, ninguno de los cuales tiene valor de uso. Esto sugiere la necesidad de un nuevo término que los diferencie.

El dólar (como todo dinero fiduciario estatal) se diferencia del Bitcoin en que depende de la protección del monopolio[2] de su producción. Es esta prohibición de competencia en el mercado lo que permite que el estado limite la oferta y, por consiguiente, extraiga el señoreaje[3].

> El monopolio es una concesión de un privilegio especial por el Estado, que reserva una cierta área de producción a un individuo o grupo particular
>
> *Murray Rothbard: Man, Economy and State*

El monopolio sobre la producción del dinero fiduciario estatal se crea mediante una norma legal contra la falsificación[4]. Una unidad del dinero se considera inválida salvo que la produzca un agente autorizado[5] del estado. Esto constituye una diferencia respecto de Bitcoin, ya que se produce mediante la competencia en el mercado y la falsificación queda excluida en virtud del acuerdo establecido en un libro contable público. El dinero protegido de la falsificación mediante norma legal puede entonces recibir la denominación razonable de "dinero monopolístico" (no confundir con Dinero del Monopoly[6]); y el Bitcoin, la de "dinero de mercado". Cuando el valor nominal del dinero fiduciario se reduce a su coste de producción, se ha convertido en dinero de mercado[7].

Reference

[1] Capítulo: Falacia de la Regresión

[2] https://mises.org/library/man-economy-and-state-power-and-market/html/pp/1054

[3] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[4] https://es.wikipedia.org/wiki/Dinero_falsificado

[5] https://www.moneyfactory.gov

[6] https://monopoly.fandom.com/wiki/Monopoly_Money

[7] https://es.wikipedia.org/wiki/D%C3%B3lar_zimbabuense

El dinero mercancía también es un dinero de mercado, ya que no se basa en un privilegio monopolístico que restrinja su oferta. Si la oferta del dinero mercancía es demasiado grande, deja de ser un dinero útil por su falta de portabilidad. La diferencia entre el dinero mercancía y el Bitcoin se obtiene a partir de los principios criptodinámicos[1]. La oferta de dinero mercancía se controla a través de la competencia de mercado que la proporciona, como consecuencia de su demanda en el mercado. No es un dinero fiduciario dada la presuposición del valor de uso.

Tanto el dinero como los sustitutivos dinerarios son moneda[2]. A veces al dinero se le denomina dinero básico. Todos los dineros están sujetos al préstamo y, por consiguiente, necesariamente a la expansión del crédito[3] (es decir, la expansión en sustitutivos dinerarios) y su correspondiente reserva fraccionaria[4].

Reference

[1] Capítulo: Principios Criptodinámicos

[2] https://es.wikipedia.org/wiki/Moneda_(divisa)

[3] Capítulo: Falacia de la Expansión del Crédito

[4] Capítulo: Definición de reserva

La siguiente tabla ofrece ejemplos para cada una de las clasificaciones antes mencionadas.

- moneda
    - dinero [*presente*]
        - materia prima [*valor de uso*]

            monopolio

            Moneda de dólar estadounidense

            mercado

            Lingotes
        - dinero fiduciario [*sin valor de uso*]

            monopolio

            Billete de dólar estadounidense

            mercado

            Bitcoin
    - sustitutivo dinerario [*futuro*]
        - electrónico [*intangible*]

            cuenta

            Visa
        - representativo [*tangible*]

            papel moneda

            Certificado de Plata de los Estados Unidos

Falacia de la Regresión

El Teorema de la Regresión[1] se basa en la suposición de que las primeras personas en valorar algo como dinero[2] tienen que hacerlo sobre la base de un recuerdo de su anterior valor de uso[3], obteniendo la cosa eventualmente utilidad en el trueque[4] y, finalmente, valor monetario[5].

> Ningún bien puede ser empleado para la función de medio de cambio que, al principio de su uso para este propósito, no tuviera valor de cambio a cuenta de otros empleos.
>
> *Ludwig von Mises: Human Action (La acción humana)*

Nótese que la teoría no es un mero intento de explicar el origen del concepto de dinero, sino de *cualquier cosa que pueda ser un dinero*. En otras palabras, si un bien no sigue esta progresión, no es dinero.

El teorema contradice la teoría subjetiva del valor[6] en la que se basa. El valor es subjetivo, lo cual implica que puede estar basado en cualquier cosa, incluso si objetivamente esa base parece irracional.

El teorema no logra completar su regresión al no explicar cómo una persona llega a valorar algo por su utilidad original. Uno tiene que suponer (no recordar) que algo será útil si nadie ha intentado utilizarlo nunca. La suposición de utilidad es la primera

Reference

[1] https://wiki.mises.org/wiki/Regression_theorem
[2] Capítulo: Taxonomía del dinero
[3] https://es.wikipedia.org/wiki/Valor_de_uso
[4] https://es.wikipedia.org/wiki/Trueque
[5] https://mises.org/library/human-action-0/html/pp/778
[6] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo

valoración, la cual sigue siendo subjetiva. La primera valoración de una cosa, como todas las que vengan después, puede deberse a cualquier motivo, incluido su uso como dinero[1].

Dado un concepto preexistente de dinero, se ha sugerido[2] que anticipar que algo es dinero es suficiente para satisfacer el teorema. En otras palabras, el dinero no necesita seguir la progresión en la práctica real. En este caso, dado un concepto preexistente de dinero, cualquier cosa puede empezar siendo dinero. Esta interpretación hace que el teorema sea una tautología: cualquier cosa que las personas valoren como dinero puede ser dinero. En otras palabras, se reduce al primer valor subjetivo.

El teorema en realidad está basado en la observación *empírica* de la evolución monetaria. Y, sin embargo, la teoría económica[3] racional en la que se basa, y el teorema en sí, rechazan explícitamente el empiricismo.

> Todos estos enunciados implícitos en el teorema de la regresión se enuncian apodícticamente como implicados en el apriorismo de la praxeología. Así tiene que suceder. Nadie puede lograr construir un caso hipotético en el que las cosas fueran a ocurrir de manera diferente.

Uno de los muchos problemas que se tiene con la economía empírica es que las observaciones nuevas pueden invalidar las conclusiones anteriores. Bitcoin lo ha hecho con este teorema que pretendía no ser empírico. Se puede observar claramente que Satoshi pretendía crear un dinero[4], para que fuera utilizado primero como dinero.

La idea es una *teoría* empírica razonable acerca de la evolución del concepto de dinero, pero inválida como *teorema* racional que distinga lo que es dinero de lo que no es dinero. El dinero se distingue por ciertos comportamientos expresados por las personas.

Reference

[1] Capítulo: Tautología del Coleccionable

[2] https://mises.org/library/cryptocurrencies-and-wider-regression-theorem

[3] https://es.wikipedia.org/wiki/Catalaxia

[4] https://bitcoin.org/bitcoin.pdf

Concluir que algo constituye un dinero consiste en observar esos comportamientos, un método estrictamente empírico.

Definición de reserva

Una reserva es el capital que posee una persona. Es capital presente, en oposición al capital invertido. El capital presente se deprecia[1] y, por tanto, representa un coste continuo para su propietario. La proporción del capital reservado respecto del invertido constituye un reflejo[2] de la preferencia temporal[3] del propietario.

El capital de reserva que se tiene la intención de utilizar para la liquidación[4] de deudas es el medio de liquidación. Por ejemplo, cuando el oro es el medio de liquidación, el oro es el capital de reserva. Una promesa de oro, como un certificado de oro[5], es un préstamo y, por tanto, no es una reserva para con la deuda. Si la deuda se puede liquidar con certificados de oro, entonces la posesión de los certificados constituye una reserva.

Si bien pudiera parecer que mantener un certificado como reserva para con una deuda de certificados contradice la definición de reserva como capital presente, no lo hace. En tanto medio de liquidación, el certificado en sí no es más que un papel para la persona que lo mantiene en reserva. Las condiciones que lleva asociadas serán transferidas al emisor del certificado. La persona que lo mantiene en reserva no experimenta costes ni ganancias por liquidar el certificado. Su coste de liquidación es solamente una consecuencia de transferir el papel a su acreedor.

La reserva a menudo se confunde con hacer corresponder los vencimientos[6]. La gestión de vencimientos[7] dispares en préstamos y tipos de interés dispares es una estrategia de

Reference

[1] Capítulo: Principio de Depreciación

[2] Capítulo: Relación de ahorro

[3] Capítulo: Falacia de la Preferencia Temporal

[4] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)

[5] https://es.wikipedia.org/wiki/Certificado_de_oro

[6] https://en.m.wikipedia.org/wiki/Asset%E2%80%93liability_mismatch

[7] https://en.m.wikipedia.org/wiki/Maturity_(finance)

gestión del riesgo. Si bien la reserva de capital también constituye una estrategia de gestión del riesgo, **lo que distingue a una reserva es que el capital reservado es "presente", teniendo un periodo de vencimiento de cero.**

Falacia de la Rentabilidad Exenta de Riesgo

El concepto hipotético de una tasa de rendimiento exenta de riesgo[1] es el tipo de interés económico con una devolución garantizada del principal del préstamo. Existe una teoría de que Bitcoin permite que esto exista en la práctica real al hacer valer la devolución del principal. Un corolario a la teoría es que esta capacidad puede limitar la expansión del crédito[2] con carácter general.

La teoría requiere un convenio[3] de tiempo fijo demostrable sobre las unidades de moneda prestadas por el prestamista. El convenio asegura que el prestamista no puede gastar las unidades hasta el vencimiento[4] del préstamo y que la propiedad de las unidades regresa al prestamista en ese momento. El prestamista intercambia con un prestatario estas unidades gravadas a cambio de intereses. El coste de oportunidad[5] impuesto por el convenio al prestamista se compensa con este interés.

Sin embargo, las unidades no proporcionan ningún valor monetario al tomador del préstamo. El control completo de las unidades regresa al prestamista de manera demostrable, lo cual deja sin nada en ese momento a cualquier persona que las haya aceptado. **Este valor nulo se imputa necesariamente a cada intercambio previo al vencimiento y, por tanto, al préstamo en sí, lo cual invalida la teoría.**

Existe una teoría relacionada que afirma que el coste de oportunidad del prestamista puede ser utilizado para representar un gasto demostrable, al igual que sucede con la prueba de trabajo. Esto puede ser utilizada de manera análoga al hashcash[6] como forma

Reference

[1] https://es.wikipedia.org/wiki/Tasa_de_inter%C3%A9s_libre_de_riesgo

[2] Capítulo: Falacia de la Expansión del Crédito

[3] https://en.wikipedia.org/wiki/Covenant_(law)

[4] https://en.wikipedia.org/wiki/Maturity_(finance)

[5] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[6] https://es.wikipedia.org/wiki/Hashcash

de mitigar la negación de servicio[1]. Es cierto, no obstante, que es un gasto y que se puede lograr gastando (incluso destruyendo) unidades. Al igual que con la prueba de trabajo, es un intercambio de coste demostrable del capital por unidades. Por tanto, no constituye un préstamo (es decir, no devenga ningún interés), lo cual invalida la teoría.

Existe una teoría relacionada que dice que las unidades pueden ser utilizadas por el tomador del préstamo para, en cambio, hacer un seguimiento de un activo de valor perpetuo. Dado que el seguimiento expira al vencimiento, esta teoría es inválida por el mismo motivo. Existe una teoría relacionada que dice que las unidades prestadas pueden ser utilizadas para hacer un seguimiento de un activo a plazo fijo que expira al vencimiento del préstamo (por ejemplo, una entrada al teatro). Esto es verdad; no obstante, el coste del seguimiento, para cualquier duración, se limita en BTC a 1 unidad por la regla del consenso del polvo. Por tanto, el coste de oportunidad se limita a 1 unidad más al menos una comisión de transacción por establecer el préstamo.

La utilidad para el tomador del préstamo es la reducción del coste de seguimiento a lo largo del plazo del préstamo. A un tipo de interés del 10% y una expiración más allá de aproximadamente 7,2 años[2], se vuelve más barato gastar 1 unidad que pedirla prestada. En cambio, gastando directamente 1 sola unidad, se puede hacer un seguimiento del activo de manera perpetua.

Si bien el escenario final es económicamente racional, no se puede describir con exactitud como un préstamo ya que la unidad no puede ser intercambiada ni destruida por el llamado tomador del préstamo. Sería más adecuado referirnos a esto como un "alquiler" de la unidad, aunque sea solo para distinguirla de los préstamos de verdad.

Reference

[1] https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[2] https://en.wikipedia.org/wiki/Rule_of_72

A pesar de esto, se puede obtener teóricamente un rendimiento por el alquiler de 1 unidad, hasta el límite económico impuesto por el tipo de interés (p. ej. ~7,2 años al 10%). Y, sin embargo, la comisión requerida para que esto fuera económicamente racional debe ser de 0 unidades, ya que se exige la transacción que establece el alquiler, si no es cuando se utiliza la unidad propia de uno para el seguimiento. Así, en el caso en el que la demanda de transacciones supere la oferta fija de confirmaciones, este escenario no es económicamente racional. Esta relación se mantiene en cualquier nivel de polvo de monedas obligatorio por encima de cero en la medida en que el polvo sea una tarifa insuficiente para financiar la confirmación.

Falacia de la Nada

Existe una teoría que afirma que la banca de reserva fraccionaria[1] proporciona inherentemente a los bancos la capacidad de crear el dinero sin ningún coste sustancial. La teoría no depende del privilegio estatal del señoreaje[2]. Se considera una consecuencia de las prácticas contables de la banca libre[3]. A menudo se denomina a esto crear dinero *ex nihilo* o "de la nada"[4].

> Al contrario de lo que muchos libros de texto siguen sugiriendo, los bancos no aceptan depósitos de dinero existente de los ahorradores y se lo prestan a los tomadores de préstamos: crean crédito y dinero ex nihilo – extendiendo un préstamo al tomador del préstamo y abonándoselo simultáneamente en la cuenta dineraria del tomador del préstamo.
>
> *Lord Turner, Secretario de la Autoridad de Servicios Financieros del Reino Unido hasta su abolición en marzo de 2013*
> *Conferencia de la Escuela de Economía de Estocolmo sobre: "Hacia un sistema financiero sostenible" 12 de septiembre de 2013*

Los adeptos describen dos visiones opuestas de la creación del dinero. El entendimiento tradicional es ingenuo respecto de su visión más práctica, como lo implica Lord Turner. La teoría afirma que la banca inherentemente crea no solo el crédito, sino también el dinero.

Visión ingenua

El dinero es creado por mineras con un coste sustancial, puede ser vendido a personas, y terminar siendo prestado a personas. Esta teoría sostiene que el prestador solo está prestando dinero que posee. Por tanto, el prestador está funcionando a reserva plena[5] y

Reference

[1] https://es.wikipedia.org/wiki/Banca_de_reserva_fraccional

[2] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[3] https://es.wikipedia.org/wiki/Banca_libre

[4] https://cdn.evbuc.com/eventlogos/67785745/turner.pdf

[5] Capítulo: Falacia de la Reserva Plena

no puede involucrarse en prácticas de reserva fraccional, que se consideran fraudulentas. En tanto que prestador honesto, solamente es capaz de emitir derechos reclamables (dinero representativo[1]) contra el dinero en posesión suya, lo que impide la expansión del crédito[2] y, por tanto, la inflación de precios[3] persistente.

Visión práctica

Los sustitutivos dinerarios son creados por los bancos, sin ningún coste sustancial, como consecuencia de los préstamos de reserva fraccional. La oferta de estos sustitutivos se expande con cada préstamo, contrayéndose solamente a medida que se van liquidando[4] los préstamos. Dada la ausencia implícita de restricciones sobre la expansión del crédito, la deuda total crece sin límite, creando una inflación de precios persistente.

En un mercado libre, las personas pueden realizar las mismas operaciones que los bancos sin llamarse necesariamente bancos a sí mismos. Por consiguiente, la distinción entre estas dos posibilidades tiene que estar basada en la ofuscación del supuesto fraude. La teoría sostiene que esta ofuscación se logra utilizando un truco contable que no es comprendido por muchos. Así pues, investiguemos la diferencia. Cualquier dinero bastará en esta investigación de los sustitutivos dinerarios[5] creados en cada uno de los dos casos, incluido el oro, el Bitcoin o el dinero monopolístico[6].

En la visión ingenua, el prestamista potencial ha ahorrado tanto la liquidez requerida para el consumo personal (atesoramiento) como la cantidad dedicada a la obtención de intereses (inversión). En este escenario, todo préstamo se origina a partir de los ahorros,

Reference

[1] https://es.wikipedia.org/wiki/Dinero_representativo
[2] Capítulo: Falacia de la Expansión del Crédito
[3] https://es.wikipedia.org/wiki/Inflaci%C3%B3n
[4] https://es.wikipedia.org/wiki/Compensaci%C3%B3n_(finanzas)
[5] https://wiki.mises.org/wiki/Money_substitutes
[6] Capítulo: Taxonomía del dinero

como el oro acumulado del bateo[1]. Los ahorros incluyen la suma de la cantidad atesorada (dinero) y la cantidad en que el crédito supera a la deuda: ahorros = dinero + (crédito - deuda). El dinero es el oro y los créditos son sustitutivos dinerarios:

	Ahorros	Dinero	Crédito	Deuda
Persona	100 oz	100 oz		

En esta visión de los préstamos personales, la Persona entrega 81 oz de oro al Tomador del préstamo. El Tomador acepta una obligación de devolver el préstamo a la Persona con intereses al vencimiento del préstamo[2]. Para simplificar la contabilidad, asumiremos un interés cero y no se contabilizará el riesgo de no devolución (es decir, no habrá descuentos por él):

	Ahorros	Dinero	Crédito	Deuda
Persona	100 oz	19 oz	81 oz	
Tomador del préstamo		81 oz		81 oz

La Persona realmente ha prestado a su propia empresa (por ejemplo, un negocio de préstamos) una fracción de sus ahorros, que se contabiliza a continuación. Supongamos que la Persona atesora el 10% de sus ahorros para la liquidez requerida para el consumo a corto plazo y su Negocio atesora el 10% por la misma razón:

Reference

[1] https://es.wikipedia.org/wiki/Bateo_de_oro

[2] https://en.wikipedia.org/wiki/Maturity_(finance)

	Ahorros	Dinero	Crédito	Deuda
Persona	100 oz	10 oz	90 oz	
Negocio		9 oz	81 oz	90 oz
Tomador del préstamo		81 oz		81 oz

El negocio de la Persona está funcionando con un 10% de reserva, ya que el 90% de su dinero depositado está en riesgo de impago. Proyectar esto en la visión ingenua de la banca solo requiere renombrar el "Prestamista" como "Depositante" y "Negocio" a "Banco". No hay ninguna necesidad de suponer que son individuos distintos:

	Ahorros	Dinero	Crédito	Deuda
Depositante	100 oz	10 oz	90 oz	
Banco		9 oz	81 oz	90 oz
Tomador del préstamo		81 oz		81 oz

Al contabilizar adecuadamente que la Persona tiene dinero en riesgo (es decir, que es un depositante), podemos ver que todos los préstamos tienen una reserva fraccionada. Hay dos préstamos en este escenario reservados al 10%, lo que resulta en sustitutos monetarios (crédito) del 171% del dinero. Dado el supuesto de preferencia temporal uniforme, el Prestatario prestará el 90% de sus ahorros, al igual que todos los prestatarios posteriores. Suponiendo un préstamo práctico mínimo de 1 oz, después de 43 préstamos, la expansión del crédito termina en 8.903 veces la cantidad de dinero.

Donde r es el nivel uniforme de reserva individual y m es la cantidad de dinero, la cantidad total de crédito c para cualquier número de préstamos n viene dada por la siguiente **¡Error! Referencia de hipervínculo no válida.**:

```
c = ∑(n=1..n)[m * (1 - r)^n] =
(m * (r - 1) ((1 - r)^n - 1))/r =
(100oz * (10% - 1) ((1 - 10%)^43 - 1))/10% = 890.3oz
```

El ratio de reserva[1] rr viene dado por la ratio del dinero respecto del crédito:

```
rr = m/c = 100oz/890.3oz = ~11.23%
```

El multiplicador de dinero[2] viene dado por la inversa del ratio de reserva:

```
1/rr = 1/(100oz/890.3oz) = 8.903
```

Es solo porque un solo dólar se considera la unidad prestable más pequeña que la serie está limitada a 43 iteraciones. Una función continua produce un multiplicador monetario de 9 al 10% de atesoramiento.

La iteración produce la siguiente tabla:

Reference

[1] https://es.wikipedia.org/wiki/Coeficiente_de_caja

[2] https://es.wikipedia.org/wiki/Multiplicador_monetario

Préstamo	Atesorado	Prestado	Crédito
1	10,00	90,00	90,00
2	19,00	81,00	171,00
3	27,10	72,90	243,90
4	34,39	65,61	309,51
5	40,95	59,05	368,56
6	46,86	53,14	421,70
7	52,17	47,83	469,53
8	56,95	43,05	512,58
9	61,26	38,74	551,32
10	65,13	34,87	586,19
11	68,62	31,38	617,57
12	71,76	28,24	645,81
13	74,58	25,42	671,23
14	77,12	22,88	694,11
15	79,41	20,59	714,70
16	81,47	18,53	733,23
17	83,32	16,68	749,91
18	84,99	15,01	764,91
19	86,49	13,51	778,42
20	87,84	12,16	790,58

21	89,06	10,94	801,52
22	90,15	9,85	811,37
23	91,14	8,86	820,23
24	92,02	7,98	828,21
25	92,82	7,18	835,39
26	93,54	6,46	841,85
27	94,19	5,81	847,67
28	94,77	5,23	852,90
29	95,29	4,71	857,61
30	95,76	4,24	861,85
31	96,18	3,82	865,66
32	96,57	3,43	869,10
33	96,91	3,09	872,19
34	97,22	2,78	874,97
35	97,50	2,50	877,47
36	97,75	2,25	879,72
37	97,97	2,03	881,75
38	98,18	1,82	883,58
39	98,36	1,64	885,22
40	98,52	1,48	886,70
41	98,67	1,33	888,03

42	98,80	1,20	889,22
43	98,92	1,08	890,30

Obsérvese que, en expansión completa, para que cualquier persona gaste de su cantidad atesorada al tiempo que mantiene su preferencia temporal, debe liquidarse un préstamo para compensar el gasto. El proceso de liquidación mueve el dinero del antiguo prestatario a su prestamista y cancela la letra. La persona que recibe el dinero gastado debe prestarlo para satisfacer su preferencia de tiempo, y así sucesivamente.

No es posible una mayor expansión sin un aumento en la cantidad de dinero o una reducción general en la preferencia temporal. Un aumento en el dinero aumenta la cantidad absoluta de crédito y una reducción en la preferencia temporal aumenta la proporción de crédito con respecto al dinero. Dado que el dinero y el crédito evolucionan juntos, nunca hay un aumento real en los sustitutivos dinerarios aparte de estos cambios.

En la práctica típica de la contabilidad bancaria, el Banco no entrega el dinero. Por el contrario, crea asientos contables en un proceso denominado "creación del crédito". Crea asientos de libro contable[1] que se compensan recíprocamente para los ingresos del Depositante y el préstamo ("crédito" y "deuda"); y, para sí mismo, asientos en el balance[2] que se compensan ("activo" y "pasivo"). En el momento de emitirse el préstamo, las cuentas son las siguientes:

Reference

[1] https://es.wikipedia.org/wiki/Libro_mayor

[2] https://es.wikipedia.org/wiki/Balance_general

	Ahorros	Dinero	Crédito	Deuda	Activo	Pasivo
Depositante	100 oz	10 oz	90 oz		100 oz	
Banco		90 oz	81 oz	171 oz	171 oz	171 oz
Tomador del préstamo			81 oz	81 oz	81 oz	81 oz

Así es como tienden a terminar las explicaciones de la teoría[1]. Las cuentas que se compensan tanto del Banco como del Prestatario tienen saldo, pero el Prestatario tiene 81 onzas de oro para gastar y el Banco no ha tenido que entregar nada de oro al Prestatario. Todavía hay solo 100 oz de dinero, pero el Prestatario tiene 81 oz en sustitutivo dinerario y el Banco tiene 81 oz más en activos. La teoría proclama que Bank ha creado así no solo crédito, sino también *dinero*. Obsérvese que todo sigue equilibrado y todas las cuentas se pueden liquidar, aparentemente validando la teoría expuesta por Lord Turner, de que "... crean crédito y dinero ex nihilo, otorgando un préstamo al prestatario y abonando simultáneamente un saldo en la cuenta dineraria del prestatario".

Esto, sin embargo, no demuestra ningún gasto real ni del crédito de préstamo ni del activo bancario. Llevemos esto un poco más lejos, asumiendo que el Prestatario borra su cuenta y, por lo tanto, los correspondientes asientos bancarios de activos y pasivos del Banco.

Reference

[1] https://www.sciencedirect.com/science/article/pii/S1057521915001477

	Ahorros	Dinero	Crédito	Deuda	Activo	Pasivo
Depositante	100 oz	10 oz	90 oz		100 oz	
Banco		9 oz	81 oz	90 oz	90 oz	90 oz
Tomador del préstamo		81 oz		81 oz	81 oz	81 oz

Obsérvese que esto es idéntico al resultado de la visión ingenua. **No existe ninguna diferencia entre estas visiones supuestamente en conflicto en torno a la creación del dinero**, lo que invalida la teoría. Esto resuelve el debate de siglos[1], que comenzó aparentemente entre Platón[2] y Aristóteles[3], acerca de si el dinero se basa en la minería o en el crédito. Las teorías son idénticas, ya que el dinero y el crédito son una dualidad[4].

> Según Joseph Schumpeter, el primer defensor conocido de una teoría crediticia del dinero fue Platón. Schumpeter describe el metalismo como la otra de las "dos teorías fundamentales del dinero", diciendo que el primer defensor del metalismo fue Aristóteles.

Los partidarios de las dos teorías mantienen un diálogo de sordos[5]. El Bitcoin, como dinero fiduciario (esto es, dinero sin valor de uso[6]) sin apoyo estatal[7], finalmente ha hecho que sean observables tanto los errores lógicos del metalismo[8], que trató de

Reference

[1] https://en.wikipedia.org/wiki/Credit_theory_of_money#Scholarship

[2] https://es.wikipedia.org/wiki/Plat%C3%B3n

[3] https://es.wikipedia.org/wiki/Arist%C3%B3teles

[4] https://dle.rae.es/dualidad?m=form

[5] https://dle.rae.es/di%C3%A1logo

[6] https://es.wikipedia.org/wiki/Valor_de_uso

[7] Capítulo: Propuesta de Valor

[8] https://en.m.wikipedia.org/wiki/Metallism

demostrar[1] la necesidad del valor de uso para el dinero, como el cartalismo[2], que trató de demostrar[3] la necesidad de apoyo estatal para el dinero fiduciario.

Recuérdese que cada préstamo tiene una reserva del 10%, por lo que el Banco puede prestar hasta 8.903 veces la cantidad de dinero en reserva, o 890,3 oz en sustitutivo dinerario contra 100 oz de dinero reservado. Si el Banco reserva cada préstamo al 0%, la expansión del crédito sería infinita. Sin embargo, esto implica preferencia temporal nula, o la idea de que el tiempo no tiene valor, lo que implica que todo el dinero se presta indefinidamente. En el caso del Banco, la reserva del 0% implica que no hay liquidez para satisfacer ninguna retirada de dinero (es decir, suspensión de pagos inmediata). Sin embargo, dada la preferencia temporal nula, nunca podría haber retiradas de dinero, lo que hace que el escenario sea irrelevante. La expansión del crédito es necesariamente finita.

Así que revisemos el escenario en el que el Banco crea crédito con reserva negativa (es decir, de la nada), esta vez considerando el gasto. Por ejemplo, sobre los depósitos de 0 oz, el Banco tiene la intención de emitir un préstamo de 1000 oz. En lugar de depender del dinero reservado para liquidar eventualmente el préstamo, el Banco "crea dinero" en su balance. Luego, el Banco aumenta las cuentas de crédito y deuda del Prestatario, lo que representa el dinero prestado y la obligación de pagar, respectivamente:

Reference

[1] Capítulo: Falacia de la Regresión

[2] https://es.wikipedia.org/wiki/Chartalismo

[3] Capítulo: Falacia del Bucle de la Deuda

	Ahorros	Dinero	Crédito	Deuda	Activo	Pasivo
Banco			1000 oz	1000 oz	1000 oz	1000 oz
Tomador del préstamo			1000 oz	1000 oz	1000 oz	1000 oz

Cuando el Prestatario intercambia 1 oz (de su cuenta de crédito) para un coche, su cuenta de crédito se reduce en 1 oz y la del Comerciante aumenta en 1 oz. Obsérvese que el Prestatario ahora le debe 1 oz al Banco, adelantado por el contrato de préstamo.

	Ahorros	Dinero	Crédito	Deuda	Activo	Pasivo
Banco			1000 oz	1000 oz	1000 oz	1000 oz
Tomador del préstamo	-1 oz		999 oz	1000 oz	999 oz	1000 oz
Comerciante	1 oz		1 oz		1 oz	

Todo pinta bien hasta que el Comerciante intenta retirar dinero de su cuenta. En ese momento, el Banco ha suspendido pagos y el Comerciante no ha recibido su pago. Si la cuenta del Comerciante está en otro banco, el pago fracasa en cuanto los dos bancos tratan de liquidar cuentas. Con una hipotética reserva negativa, las cuentas se equilibran de la siguiente manera, lo que indica la desaparición del Banco[1] (dinero negativo):

Reference

[1] https://en.wikipedia.org/wiki/Bank_failure

	Ahorros	Dinero	Crédito	Deuda	Activo	Pasivo
Banco	-1 oz	-1 oz	1000 oz	999 oz	999 oz	999 oz
Tomador del préstamo			999 oz	1000 oz	999 oz	1000 oz
Comerciante	1 oz	1 oz			1 oz	

El dinero se tiene que mover realmente[1] pasando del control del Banco al Comerciante o al banco del Comerciante, lo cual no es posible. Un ejemplo más sencillo es el fracaso de cualquier intento del Prestatario de retirar[2] dinero de su cuenta. El Banco puede crear tanto sustitutivo dinerario como desee, pero la reserva negativa es sencillamente una promesa vacía[3]. En este ejemplo, el Banco ha creado 1000 oz de promesas que no puede cumplir.

No reconocer estos principios probablemente es consecuencia de no tener en cuenta el proceso de liquidación[4]. Esto probablemente viene de no reconocer la inherente *dualidad del dinero y del crédito*, ya que el primero siempre tiene que existir para liquidar las reclamaciones implicadas por el segundo. Esto probablemente viene del hábito de referirnos al dinero (p. ej. oro) en los mismos términos que a los sustitutivos dinerarios (p. ej. saldos de oro).

Los asientos compensatorios de activos y pasivos sirvieron solo para contabilizar los préstamos emitidos y pendientes, que son la base del balance general del Banco. Del mismo modo, el Banco no creó los asientos compensatorios de crédito y deuda para ocultar la creación fraudulenta de dinero. El Banco creó estas cuentas por dos razones:

Reference

[1] https://www.brinks.com/en/public/brinks/logistics

[2] https://es.wikipedia.org/wiki/Cajero_autom%C3%A1tico

[3] https://en.wiktionary.org/wiki/empty_promise

[4] https://www.youtube.com/watch?v=IzE038REw2k

- Evitar la transferencia física solo para volver a depositar el dinero en el Banco.
- Fomentar que se volviera a depositar en el Banco en lugar de un competidor (o el tesoro del Prestatario).

Cuando el Banco tiene reservas insuficientes para satisfacer las retiradas, ya sea debido a préstamos en mora o un pánico bancario[1], solo tiene dos opciones, la suspensión de pagos o pedir prestado. Para evitar lo primero, existe la banca central[2] para proporcionar lo segundo. Ese es el significado del término "prestamista de última instancia"[3]. El Principio de la Banca Estatal[4] proporciona una explicación detallada de esta fuente real de inflación monetaria[5].

En resumen, se ha demostrado que:

- Los Bancos no tienen la capacidad de crear dinero.
- La reserva fraccionaria es inherente a los préstamos.
- La fracción de la reserva es expresión de la preferencia temporal.
- La reserva nula elimina cualquier posibilidad de poder liquidar cuentas.
- No existe ninguna distinción entre las teorías ingenua y práctica de la creación del dinero.

Reference

[1] https://es.wikipedia.org/wiki/P%C3%A1nico_bancario

[2] https://es.wikipedia.org/wiki/Banco_central

[3] https://es.wikipedia.org/wiki/Prestamista_de_%C3%BAltima_instancia

[4] Capítulo: Principio de la Banca Estatal

[5] https://en.wikipedia.org/wiki/Monetary_inflation

Falacia del Dinero Imprestable

La Ecuación de Fisher[1] se tiene que utilizar para combinar una tasa de crecimiento en un dinero a su vez sujeto a la inflación[2], ya que la depreciación tiene lugar en el dinero futuro. Esto ajusta el tipo de interés nominal para obtener el tipo de interés real. La presentación se simplifica utilizando ratios en vez de tasas. Según se muestra en Principio de Depreciación[3], la tasa de crecimiento del dinero mercancía es del 0%, o una ratio de crecimiento del 100%.

El dinero monopolístico[4] exhibe depreciación a causa del señoreaje[5].

```
ratio-crecimiento-dinero-monopolístico = ratio-crecimiento-dinero-mercancía
/ ratio-señoreaje
100% / 103% = ~97%
```

La oferta fija de dinero puede apreciarse por la deflación de precios[6]

```
ratio-crecimiento-dinero-oferta-fija = ratio-crecimiento-dinero-mercancía /
ratio-inflación
100% / 97% = ~103%
```

Un dinero de oferta fija se supone que cambia de poder adquisitivo[7] en proporción a los productos que representa (esto es, demanda). En otras palabras, con el doble de la

Reference

[1] https://es.wikipedia.org/wiki/Ecuaci%C3%B3n_Fisher

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] Capítulo: Principio de Depreciación

[4] Capítulo: Taxonomía del dinero

[5] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[6] https://es.wikipedia.org/wiki/Deflaci%C3%B3n

[7] Capítulo: Principio de Inflación

cantidad de productos, cada unidad del dinero se intercambiará por el doble de su anterior cantidad de productos.

```
poder_adquisitivo_este_año = poder_adquisitivo_año_pasado *
ratio_crecimiento_anual
100 * 103% = 103
```

La presuposición de la deflación de precios del dinero de oferta fija descansa en la suposición de un crecimiento económico positivo. En el caso de una contracción económica, el dinero presenta inflación de precios[1]. El caso de crecimiento económico (riqueza en aumento) implica que los intereses superan la depreciación. Tanto los intereses como la depreciación siempre tienen que ser positivos tal y como implica la preferencia temporal[2].

```
ratio_intereses > ratio_depreciación > 100%
ratio_intereses / ratio_crecimiento = ratio_depreciación
ratio_intereses / ratio_crecimiento > 100%
ratio_intereses > ratio_crecimiento
```

La contracción económica (riqueza en disminución) implica una mayor tasa de intereses, tal y como implica la teoría de la utilidad marginal[3], hasta que se restaure el crecimiento positivo. Por tanto, la contracción es una condición autocorrectiva.

```
ratio_depreciación > ratio_intereses > 100%
ratio_intereses / ratio_crecimiento = ratio_depreciación
ratio_intereses / ratio_crecimiento > 100%
ratio_intereses > ratio_crecimiento
```

Obsérvese que, en los dos casos de crecimiento económico y contracción, los intereses deben superar el crecimiento, ya que la concesión de préstamos es la única fuente de

Reference

[1] https://es.wikipedia.org/wiki/Inflaci%C3%B3n

[2] Capítulo: Falacia de la Preferencia Temporal

[3] https://es.wikipedia.org/wiki/Utilidad_marginal

crecimiento. Dado que el crecimiento es la única base de la deflación en un dinero deflacionista, atesorar el dinero representa una depreciación monetaria (consumo).

Existe una teoría que afirma que es económicamente irracional prestar un dinero deflacionista. **Según se ha mostrado, es racional prestar cualquier dinero, incluido uno deflacionista, lo que invalida la teoría.** Cualquier comportamiento contrario implica una condición puramente especulativa[1], que no se apoya en que la oferta sea fija.

Reference

[1] Capítulo: Consumo especulativo

PRECIO

Falacia Lunar

Existe una teoría que afirma que atesorar bitcoin garantiza un beneficio perpetuo. La teoría está basada en las siguientes leyes económicas.

- Un dinero es mejor que dos (Ley de Metcalfe[1])
- El mejor dinero desplaza a otros dineros (Ley de Thiers[2])
- Para una oferta fija, el precio aumenta con la demanda (Ley de la Oferta y la Demanda[3])
- El aumento potencial de la demanda es ilimitado (los intercambios son una suma positiva)

El atesoramiento es puramente especulativo, con todos los retornos constituyendo beneficios o pérdidas. El dinero no se presta a otro por intereses y, por tanto, siempre está disponible para intercambios, una ventaja que compensa los intereses a los que se renuncia.

Un corolario a la teoría es que no se requiere ninguna inversión en la producción para beneficiarse de esta. Se requiere capital para toda producción. Los prestamistas (inversores) cobran intereses a cambio del tiempo sin su capital. **La producción es la fuente de los intercambios y, por tanto, toda actividad económica es consecuencia de la inversión.** Se define un atesoramiento por su falta de consumo en la producción. Si todas las personas atesoraran su capital, no habría nada que intercambiar y, por tanto, no habría demanda de dinero.

Reference

[1] https://es.wikipedia.org/wiki/Ley_de_Metcalfe

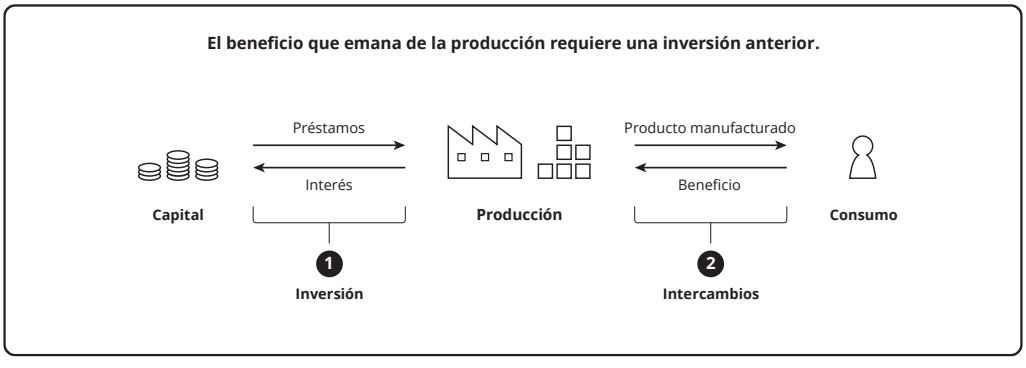
[2] https://es.wikipedia.org/wiki/Ley_de_Gresham#Reverso_de_la_ley_de_Gresham_(ley_de_Thiers)

[3] https://es.wikipedia.org/wiki/Oferta_y_demanda

Parece que la teoría es irracional, lo que apoya la idea de que Bitcoin es, en efecto, Dinero Mágico de Internet[1]. Cuando una teoría produce una contradicción, la teoría es deficiente. Un dinero de mercado de oferta fija[2] solo puede aumentar en poder adquisitivo a causa de:

1. crecimiento económico – que crea más demanda para utilizar el dinero a cambio
2. monetización – que las personas transfieran demanda desde otro dinero

Y, sin embargo, el crecimiento económico es estrictamente consecuencia de la inversión. El crecimiento es necesariamente[3] menos que el retorno sobre la inversión (intereses), y el atesoramiento completo no es ninguna inversión en absoluto. Y, por supuesto, la monetización tiene un límite. Por último, la teoría no reconoce la propiedad de estabilidad[4] del Bitcoin. Por estos motivos, la teoría es inválida.



Reference

[1] https://medium.com/@paulbars/magic-internet-money-how-a-reddit-ad-made-bitcoin-hit-1000-and-inspired-south-parks-art-b414ec7a5598

[2] Capítulo: Taxonomía del dinero

[3] Capítulo: Principio de Depreciación

[4] Capítulo: Propiedad de Estabilidad

Estimación de Precios

La potencial capitalización y, por consiguiente, el precio unitario del Bitcoin, se estiman de diversas maneras. Un enfoque habitual es imaginar que el Bitcoin sustituya todo el dinero estatal[1] o incluso el producto mundial bruto[2]. Otros enfoques que utilizan modelos de precios históricos[3] para predecir precios futuros son económicamente irracionales[4] y, por consiguiente, no se consideran aquí. La presuposición de Bitcoin como divisa de reserva[5] mundial se desestima por los motivos discutidos en Falacia de la Divisa de Reserva[6]. Los efectos del atesoramiento especulativo sobre el precio no se consideran, sobre la base de la prueba catalláctica[7] de que la especulación no es un factor determinante del precio[8].

Dado que el Bitcoin es dinero[9] y no crédito, el enfoque "dinerario" es una suposición de partida más racional. No obstante, sin una comprensión clara de la distinción esencial entre dinero y crédito, este enfoque a menudo presenta deficiencias lógicas en la práctica. Según se demuestra en Falacia de la Expansión del Crédito[10], el Bitcoin no puede limitar la expansión del crédito. Si eliminara la expansión del crédito (hipotéticamente), no habría ninguna producción de ningún tipo y no valdría nada. La suposición de partida más racional respecto de la expansión del crédito es que el Bitcoin se reserva al mismo ritmo que otros dineros. La tasa de la expansión crediticia está impulsada por la

Reference

[1] https://www.fool.com/investing/2017/05/25/could-the-price-of-bitcoin-go-to-1-million.aspx

[2] https://en.wikipedia.org/wiki/Gross_world_product

[3] https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

[4] Capítulo: Falacia de la Razón Existencias-Flujo

[5] Capítulo: Principio de Reserva

[6] Capítulo: Falacia de la Divisa de Reserva

[7] https://es.wikipedia.org/wiki/Catalaxia

[8] https://mises.org/library/man-economy-and-state-power-and-market/html/p/949

[9] Capítulo: Taxonomía del dinero

[10] Capítulo: Falacia de la Expansión del Crédito

preferencia temporal[1] humana solamente, por lo que esta es una suposición de que la producción será, por tanto, consistente con las normas históricas.

Consideremos cinco posibles opciones para la sustitución del "dinero" por Bitcoin:

- Dinero tangible.
- Dinero base (M0).
- Crédito bancario (M3-M0).
- Todo el crédito (bancario, deudas, capital accionarial).
- Producto bruto.

Utilizar solamente el dinero tangible ("efectivo en cámaras acorazadas") es un enfoque irracional. El dinero que se contabiliza como equivalente monetario también debe incluirse si se va a considerar el dinero tangible, ya que son de la misma oferta. Los bancos centrales[2] imprimen y acuñan dinero tangible cuando es necesario, contra una base de "obligaciones" para hacerlo, y todo el crédito en el dinero se expande contra esta base. Este concepto se discute en Principio de la Banca Estatal[3]. Utilizar crédito también es un enfoque irracional, puesto que el Bitcoin no es crédito. Como dinero, se utiliza para liquidar[4] obligaciones crediticias. Este concepto se discute en Falacia del Bucle de la Deuda[5]. Así que, por supuesto, utilizar cualquier combinación de dinero y crédito (como M1, M2 o M3[6], ya que estos incluyen M0) es irracional por el mismo razonamiento. De manera análoga, es injustificable utilizar el producto bruto en sustitución, ya que no es ni dinero ni crédito.

Reference

[1] Capítulo: Falacia de la Preferencia Temporal

[2] https://es.wikipedia.org/wiki/Banco_central

[3] Capítulo: Principio de la Banca Estatal

[4] https://es.wikipedia.org/wiki/Liquidaci%C3%B3n_(finanzas)

[5] Capítulo: Falacia del Bucle de la Deuda

[6] https://en.wikipedia.org/wiki/Money_supply#United_States

Sin embargo, con fines comparativos, estimemos cada una de las cinco opciones enumeradas anteriormente. Los valores básicos para la siguiente tabla son cantidades en dólar estadounidense tomadas prestadas de la Falacia de la Expansión del Crédito. Estos se expanden por una estimación del tamaño relativo[1] de la economía mundial por capitalización del mercado accionarial. El mercado estadounidense es aproximadamente el 40% de los mercados globales. Por consiguiente, estos valores superan las cifras estadounidenses en un factor de 1/40%. Esto favorece la simplicidad sobre la precisión, ya que el único objetivo es demostrar un método racional de estimación. La cantidad de Bitcoin asumida es de 18.952.500, dado un 95% minado (~10 años en el futuro) y un 5% perdido (p. ej. Satoshi perdió las claves privadas).

Las valoraciones se basan en los números de 2019 aunque la inflación de Bitcoin se basa en 2029. Esto implica que los valores deberían ser mayores sobre la base de la presunción de crecimiento económico e inflación monetaria[2] del dólar estadounidense. Esto último se puede eliminar considerando esto como una proyección de dólares constantes de 2019. Asumiendo un crecimiento económico[3] real anual del 2% compuesto durante 10 años, los valores de 2029 se han incrementado un ~22%.

Reference

[1] https://seekingalpha.com/article/4202768-u-s-percent-world-stock-market-cap-tops-40-percent

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] https://es.wikipedia.org/wiki/Crecimiento_econ%C3%B3mico

Sustituto	Tamaño (2019)	USD/BTC (2029)
Dinero tangible	4.347.460.000.000$	279.852$
Dinero base	8.187.102.500.000$	527.016$
Crédito bancario	36.018.735.000.000$	2.318.578$
Todo el crédito	236.812.492.891.206$	15.243.965$
Producto bruto	80.270.000.000.000$	5.167.097$

La estimación de la sustitución dineraria de base mundial es de 527.016$. La determinación del valor actual neto[1] requiere una estimación del coste de capital. Utilizando un valor conservador del 7,2% de intereses implica[2] un coste de oportunidad[3] del 100% de la especulación a lo largo de un plazo de ~10 años, o un precio presente de 263.508$.

Ahora consideramos la suposición principal, la de sustitución de todo el dinero. El Bitcoin no ofrece ninguna garantía[4] contra la prohibición estatal de su uso en intercambios. Bajo la suposición de que los estados tratan de retener el señoreaje[5] y la censura, podríamos multiplicar por la fracción del mercado negro mundial, que se estima[6] en ~28% del mercado mundial. La estimación del dinero base incluye *toda* la actividad de mercado en ese dinero (las estimaciones de crédito no la incluyen). A un 100% de sustitución para el comercio estimado del mercado negro, el precio es de 73.782$.

Reference

[1] https://es.wikipedia.org/wiki/Valor_actual_neto

[2] https://en.m.wikipedia.org/wiki/Rule_of_72

[3] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[4] Capítulo: Principio de Ausencia de Permisos

[5] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[6] https://voxeu.org/index.php?q=node/7964

Sin embargo, dada la suposición de que los dineros estatales sean de uso exclusivo en el mercado legal no podemos suponer que el 100% de la actividad del mercado negro sea en Bitcoin. No existe ninguna base obvia para estimar esta proporción, pero **el precio de 2019 de ~10.000$ implica una adopción de ~7,4% en el mercado negro proyectada para 2029.**

Esta estimación no tiene en cuenta la propiedad de estabilidad[1] del Bitcoin. Es posible que los intercambios se vean forzados a pasar a sustitutivos monetarios[2] antes de que se pueda alcanzar la adopción futura que implican las proyecciones actuales.

Reference

[1] Capítulo: Propiedad de Estabilidad

[2] Capítulo: Principio de Sustitución

Falacia de la Escasez

Como concepto *absoluto*, la escasez[1] económica de un recurso implica solamente que no está disponible en oferta ilimitada. Además, si ninguna persona demanda incluso un recurso escaso, no tiene valor. Un recurso escaso bajo demanda es propiedad. No se implica ningún grado de dificultad en producir el recurso.

La escasez también podría referirse a la disponibilidad *relativa* de alguna propiedad. Para una oferta dada, aumentar la demanda implica una disponibilidad menor (mayor escasez). Sin embargo, el aumento de la demanda tiende a aumentar la producción y, por lo tanto, la disponibilidad. De manera similar, para una demanda dada, aumentar la oferta implica aumentar la disponibilidad (disminuir la escasez). Sin embargo, el aumento de la oferta tiende a disminuir la producción y, por lo tanto, la disponibilidad. Estas retroalimentaciones negativas estabilizan la disponibilidad y, en consecuencia, el precio.

Una sola moneda tiene una oferta fija[2]. Existe la teoría de que la oferta fija de Bitcoin es la fuente de su valor. Al igual que con Bitcoin, hay una oferta fija de Mona Lisa[3], solo una es posible. La teoría implica que esta es la fuente de valor de la famosa obra de arte. Sin embargo, existen innumerables obras de arte únicas sin demanda y, por lo tanto, sin valor. **El Bitcoin no puede aumentar de valor solo por la escasez absoluta.** Al contrario, necesariamente se vuelve más escaso a medida que se valora más. La prevalencia no es una propiedad monetaria importante salvo en lo que respecta a la portabilidad y la divisibilidad.

Reference

[1] https://es.wikipedia.org/wiki/Escasez

[2] Capítulo: Principio de Inflación

[3] https://es.wikipedia.org/wiki/La_Gioconda

Un aspecto de la teoría es que la oferta fija de Bitcoin es la fuente de su utilidad porque garantiza que no aumente su disponibilidad. Sin embargo, esto requiere una demanda que no disminuya. El Bitcoin es único en el ámbito de las propiedades en que el coste de transferirlo aumente inherentemente con la demanda de transferencias. Esto crea efectivamente la misma retroalimentación negativa de la demanda[1] vista en propiedades sin oferta fija.

Al contrario que la Mona Lisa, también está sujeta a una sustitución efectiva[2]. Dado que no está garantizada la no disminución de la demanda, la teoría es inválida. Como resulta habitual en las falacias económicas, el error viene en parte de considerar solamente un lado de la relación oferta-demanda.

Otra causa del error es una mala interpretación del comportamiento del dinero mercancía. Debido a su menor prevalencia en la superficie de la Tierra, el oro se ha mantenido más portátil[3] en escenarios habituales que los materiales más prevalentes como el hierro y la sal. Sin embargo, la portabilidad del dinero electrónico[4] es independiente del número de unidades existentes. Aparte de una divisibilidad suficiente, el número total de unidades de Bitcoin es completamente arbitrario y, por lo tanto, no está relacionado con su utilidad.

Otra causa del error es una mala interpretación del comportamiento de los dineros estatales. A través de las leyes contra la falsificación[5], el estado controla la oferta de su dinero restringiendo la competencia. Por lo tanto, puede recaudar un impuesto de inflación[6] al expandir la oferta sin consumir tanto capital en la producción, lo que

Reference

[1] Capítulo: Propiedad de Estabilidad

[2] Capítulo: Principio de Sustitución

[3] https://en.m.wikipedia.org/wiki/Money#Properties

[4] Capítulo: Taxonomía del dinero

[5] https://es.wikipedia.org/wiki/Dinero_falsificado

[6] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

aumenta la relación entre dinero y capital. Sin una competencia restringida, la oferta se expandiría a través de las fuerzas del mercado, en respuesta a la demanda, eliminando el impuesto. En otras palabras, el dinero se comportaría como una mercancía prevalente, con poca portabilidad (al menos hasta que sea remunerado por el estado). La mala portabilidad es a menudo una consecuencia real de la hiperinflación.

La escasez es una función tanto de la oferta como de la demanda y, por lo tanto, no puede ser inherente a un dinero, incluso con una oferta fija. Tanto el dinero mercancía como el Bitcoin eliminan el impuesto de la inflación, aunque el dinero mercancía está sujeto a la retroalimentación negativa de la inflación monetaria y el Bitcoin está sujeto a la retroalimentación negativa de la presión de las comisiones.

Propiedad de Estabilidad

El valor es subjetivo[1] y, por consiguiente, el carácter constante de los precios es una ficción económica. Los precios de cambio de un dinero vienen determinados por su oferta y demanda[2], a su vez afectada por los calendarios de demanda de todas las personas para todos los productos. La estabilidad de un dinero no es una tendencia hacia un precio constante en todas las demás cosas, es una relación de amortiguación[3] entre la demanda del dinero y su oferta.

Podemos organizar los dineros por sus ofertas en tres categorías:

- Oferta de mercado (dinero mercancía[4] y Bitcoin temprano)
- Oferta monopolística (monopolio[5])
- Oferta fija (Bitcoin[6] tardío)

En cualquier dinero, la destrucción de unidades reduce la oferta y, por consiguiente, aumenta el valor de las restantes. Puesto que no hay ningún incentivo financiero a favor de tener pérdidas, no tiene impacto en la estabilidad.

La oferta de dinero de mercado aumenta por el incentivo financiero de producir más[7] cuando se espera que el precio iguale o supere el coste de producción (incluido el coste del capital). Según se muestra en Principio de Inflación[8], la relación entre la oferta y la

Reference

[1] https://es.wikipedia.org/wiki/Teor%C3%ADa_del_valor_subjetivo
[2] https://es.wikipedia.org/wiki/Oferta_y_demanda
[3] https://es.wikipedia.org/wiki/Amortiguamiento
[4] https://es.wikipedia.org/wiki/Dinero_mercanc%C3%ADa
[5] Capítulo: Taxonomía del dinero
[6] https://es.wikipedia.org/wiki/Bitcoin
[7] https://es.wikipedia.org/wiki/Miner%C3%ADa_del_oro
[8] Capítulo: Principio de Inflación

demanda (el precio) es estable a pesar de que la oferta no sea fija. La competencia garantiza que la producción del dinero de mercado esté controlada por la demanda. La retroalimentación de la disminución de la demanda como consecuencia del aumento de la oferta reduce el incentivo de la producción, lo que garantiza la estabilidad.

Como dinero de mercado, el aumento de la oferta de Bitcoin no tiene ningún efecto sobre el precio. Y, sin embargo, puesto que el crecimiento de su oferta está prefijado, su estabilidad se basa en cambios en la demanda. Al contrario que el dinero basado en materias primas, el coste de producir Bitcoin aumenta y disminuye según la demanda del mismo. Puesto que el precio es la relación entre la oferta y la demanda, esto tiene el mismo efecto. El propósito de la inflación monetaria del Bitcoin es distribuir racionalmente las unidades y, por tanto, termina por ser desactivada.

La oferta de dinero monopolístico aumenta arbitrariamente (o está sujeta a impuestos como sobrestadía[1]) por el soberano[2] a causa de la recompensa financiera del señoreaje[3].

Cuando la inflación monetaria monopolística es predecible, se puede capitalizar, lo que descuenta el rendimiento del señoreaje. Por tanto, los cambios en la oferta a menudo no se publican[4]. Debido a la protección del monopolio[5] estatal (es decir, producirlo supone el delito de la falsificación de moneda), la competencia no puede limitar eficazmente los rendimientos. El beneficio soberano resultante (impuesto) es la recompensa del señoreaje y el motivo del dinero monopolístico[6]. La protección del monopolio es la única diferencia económica entre el dinero basado en materias primas y el dinero

Reference

[1] https://es.wikipedia.org/wiki/Sobrestad%C3%ADa_(divisa)

[2] https://es.wikipedia.org/wiki/Soberan%C3%ADa

[3] https://es.wikipedia.org/wiki/Se%C3%B1oreaje

[4] https://www.reuters.com/article/us-venezuela-economy/crisis-hit-venezuela-halts-publication-of-another-major-indicator-idUSKBN16S1YF

[5] https://es.wikipedia.org/wiki/Monopolio_p%C3%BAblico

[6] Capítulo: Principio de Reserva

monopolístico. El aumento de la oferta causado por el señoreaje se ve mitigado exclusivamente por el malestar político, ya que la gente se resiste a la consiguiente disminución de valor. Este malestar se manifiesta inicialmente como fuga de capitales[1], que se contrarresta mediante controles cambiarios[2].

Como dinero de oferta fija, el Bitcoin tardío permanece estable. A medida que las comisiones aumentan necesariamente con la demanda, el umbral de utilidad[3] elimina la demanda de transacciones de valor inferior al umbral. De manera más general, el nivel de comisiones aumenta al punto en el que los sustitutos monetarios[4] son más eficaces en costes para una transacción de un valor dado. **Por consiguiente, la estabilidad es el resultado de limitar la demanda directamente, al contrario de basarse en un aumento de la oferta para hacerlo.** La estabilidad implica que el precio está limitado, pero puede aumentar con una mayor capacidad de carga[5] efectiva de transacciones de la moneda y con una mayor utilidad en relación con los sustitutivos.

Reference

[1] https://es.wikipedia.org/wiki/Fuga_de_capitales

[2] https://en.wikipedia.org/wiki/Foreign_exchange_controls

[3] Capítulo: Propiedad del Umbral de Utilidad

[4] Capítulo: Principio de Sustitución

[5] Capítulo: Principio de Escalabilidad

Falacia de la Razón Existencias-Flujo

La Razón Existencias-Flujo[1] (en inglés, *Stock-to-Flow*) describe históricamente la relación entre el capital y los ingresos, lo que permite que se estime un nivel futuro de capital a partir de un nivel esperado de ingresos. Posteriormente, este concepto elemental fue aplicado a la oferta de dinero con carácter general.

La razón existencias-flujo es una medida del tiempo. Dada una razón mayor, las existencias aumentarán más lentamente. Existe una teoría que afirma que el dinero con una mayor razón existencias-flujo inherente sufrirá proporcionalmente una menor inflación monetaria[2] que un dinero con una razón menor. La teoría sostiene que la mayor razón implica un tipo de dinero "más duro", definido como inherentemente más resistente a los efectos de la inflación monetaria.

La teoría no considera el origen de las velocidades de flujo. Supone necesariamente que la velocidad de producción es sencillamente una propiedad de la sustancia. Pero la producción de cualquier cosa tiene lugar cuando el precio anticipado hace que la producción sea rentable. Un mayor potencial de beneficios produce una mayor competencia, acelerando el aumento de la oferta. Que haya más gente haciendo excavaciones para encontrar oro aumenta su flujo.

En otras palabras, el flujo es una función de la demanda. La anticipación de pérdidas tiene como consecuencia que no haya ninguna producción en absoluto. Esta falta de flujo *no es inherente a la sustancia* sino una consecuencia de la *falta de demanda*. Dado que tanto la oferta como la demanda determinan el flujo, la teoría es inválida. Este error,

Reference

[1] https://en.m.wikipedia.org/wiki/Stock_and_flow

[2] https://en.m.wikipedia.org/wiki/Monetary_inflation

comprendido desde hace mucho tiempo[1], no es un aspecto del concepto elemental de la razón existencias-flujo, sino de su aplicación incorrecta.

Dada la legislación contra falsificaciones, se restringe la competencia para producir dinero estatal, lo que permite el control de la oferta por el estado, independientemente de las fuerzas del mercado. Como sucede con otros tipos de dinero, la oferta y la demanda son impredecibles con carácter general. Un estado puede "vincular" su emisión de billetes[2] a otro tipo de dinero, como el oro. Esta relación puede incluso mantenerse durante muchas décadas. En este caso, la razón de existencias-flujo indicaría incorrectamente una "dureza" comparable con la del oro.

Dado que la razón existencias-flujo del dinero es la tasa de inflación monetaria invertida, su relación con la inflación monetaria es tautológica. No tiene ninguna implicación sobre la inflación monetaria futura. Se puede utilizar para analizar relaciones históricas, y para calcular las existencias futuras sobre la base del flujo futuro *supuesto*, pero no se puede utilizar para *predecir* la inflación monetaria futura. Cualquier afirmación de que una especulación será más beneficiosa que otra sobre la base de las razones históricas de existencias-flujo constituye un error.

Reference

[1] https://mises.org/library/theory-money-and-credit/html/ppp/1234

[2] Capítulo: Principio de Reserva

ESCALABILIDAD

Falacia de la Auditabilidad

La solvencia de un custodio de Bitcoin no puede ser auditada. Un custodio es una persona con discreción tanto para librar un activo como para emitir títulos contra él. Si tanto la libranza del activo como la emisión de títulos contra él se controlan mediante reglas de consenso, entonces la relación no es realmente de custodia. Existe una distinción entre una reserva[1] y una capa. Una capa impone el cumplimiento mediante el protocolo (no supone custodia) y, por consiguiente, no tiene nada que auditarse.

Una auditoría de solvencia requiere una prueba simultánea (atómica) tanto del importe íntegro del activo mantenido por un custodio como de los títulos emitidos contra él. En el caso de una reserva nacional de Bitcoin, esto requeriría una prueba completa de todos los activos fiduciarios (por ejemplo, el título) emitidos contra la reserva, así como del Bitcoin mantenido en reserva. Incluso en el caso en el que el título se emita en una cadena pública diferente, no se satisface el requisito de atomicidad.

En algunos casos, podría considerarse suficiente rechazar el requisito de atomicidad, aceptando la falta de corrección bajo la suposición de que las desviaciones significativas terminarían por descubrirse. Sin embargo, en el caso de la banca estatal[2], detectar la desviación resulta insuficiente. Históricamente, no ha sido difícil detectar tales desviaciones. La dificultad se encuentra en detenerlas.

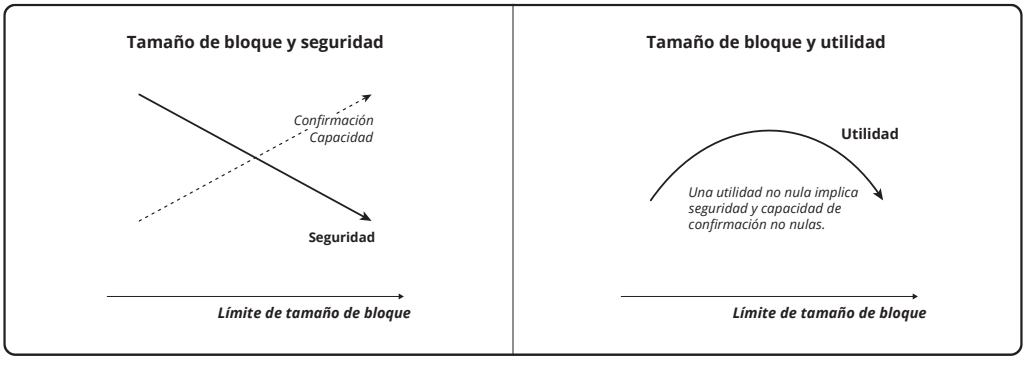
Reference

[1] Capítulo: Principio de Reserva

[2] Capítulo: Falacia de la Divisa de Reserva

Principio de Escalabilidad

Escalabilidad[1] es el aumento proporcional en algún aspecto del desempeño a medida que se emplea más equipos físicos (*hardware*). El volumen de transacciones de Bitcoin es perfectamente no escalable ya que ninguna cantidad de *hardware* lo aumenta.

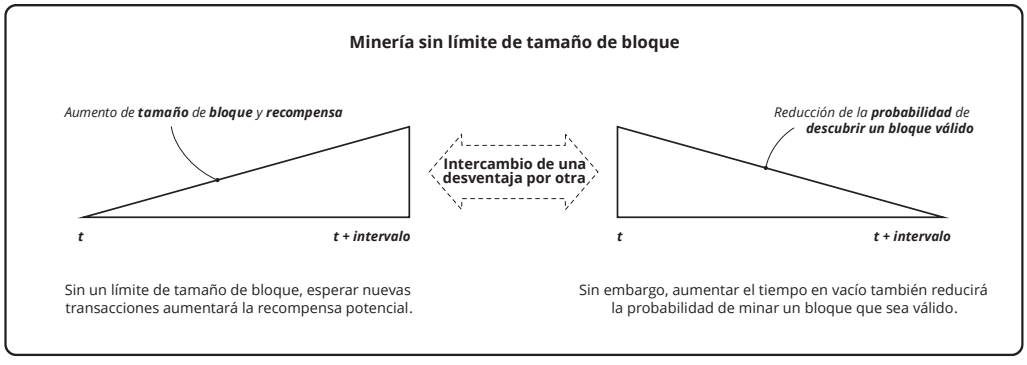


La regla de consenso sobre el límite del tamaño de bloque establece el compromiso arbitrario entre la utilidad y la seguridad del sistema. Un aumento del tamaño de bloque aumenta marginalmente el volumen de transacciones y, por consiguiente, el coste de recursos para la validación de transacciones (esto es, el procesamiento, el almacenamiento y el ancho de banda). A medida que aumenta el coste de la validación, la seguridad económica sufre un impacto adverso por el mayor riesgo de centralización[2]. Dado que el compromiso es arbitrario, no existe un tamaño ideal.

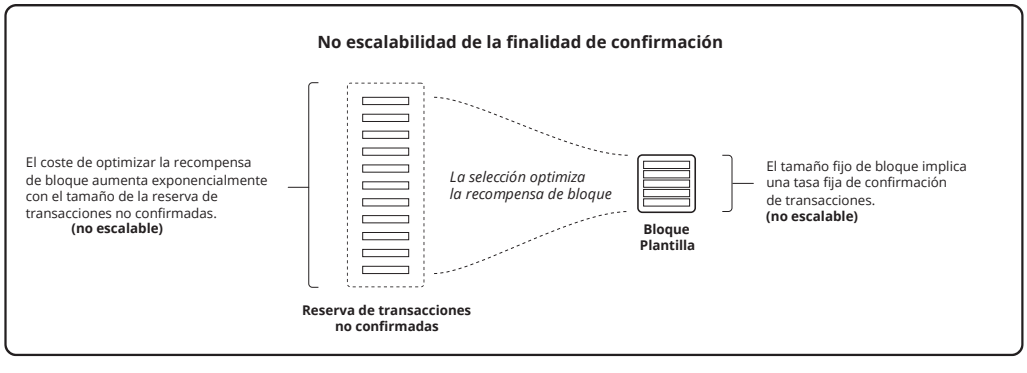
Reference

[1] https://es.wikipedia.org/wiki/Escalabilidad

[2] Capítulo: Riesgo de Centralización



Para cualquier tamaño de bloque, el sistema sigue siendo no escalable por la necesidad del carácter definitivo de las confirmaciones. Debe seleccionarse un conjunto finito de transacciones, lo cual implica que otras podrían ser excluidas. Esta exclusión está motivada financieramente por el coste de oportunidad[1] de no utilizar capital de minería desplegado, y es la manifestación de la no escalabilidad. Este límite inherente necesita un mercado competitivo para la confirmación, y lo financia en proporción a la demanda de dinero[2].



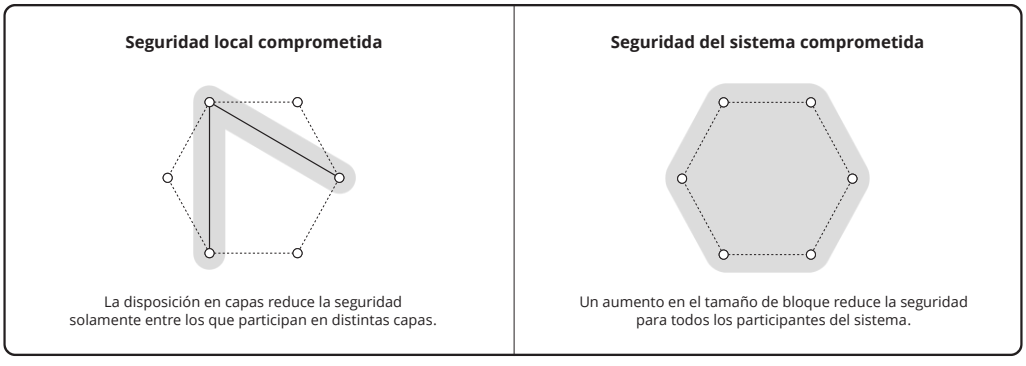
La capacidad de carga de transacciones efectiva, y por consiguiente la utilidad, se puede aumentar mediante la estratificación (disposición en capas). Esto representa una

Reference

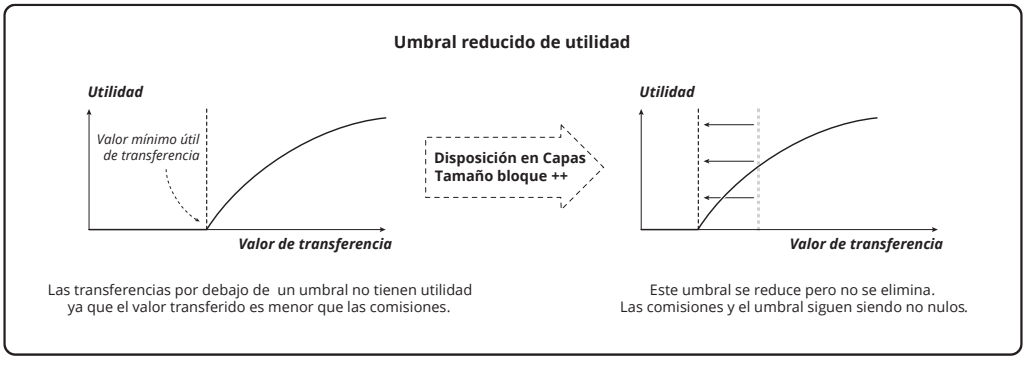
[1] https://es.wikipedia.org/wiki/Coste_de_oportunidad

[2] Capítulo: Taxonomía del dinero

renuncia de seguridad *local* y *limitada en el tiempo*, en oposición a la renuncia de seguridad *sistémica* y *persistente* de aumentar el tamaño de bloque.



Cualquiera de los compromisos reduce pero no elimina el umbral de utilidad[1], lo cual implica que se conserva la propiedad de estabilidad[2].



Por consiguiente, la estabilidad y la no escalabilidad existen para cualquier tamaño de bloque y cualquier nivel de disposición en capas.

Reference

[1] Capítulo: Propiedad del Umbral de Utilidad

[2] Capítulo: Propiedad de Estabilidad

Principio de Sustitución

Un bien sustitutivo[1] es un bien que puede ser utilizado en lugar de otro. A medida que aumenta el precio de un producto, en algún nivel las personas o bien se pasan a sustitutos o dejan totalmente de utilizarlo.

Si bien un sustituto sería menos deseable al mismo precio que el producto original, su menor precio compensa esta preferencia. De esta manera, la presencia de sustitutos reduce la demanda por el producto original. El sustituto compite con el original de la misma manera que lo hace una mayor oferta del original.

Dado que una moneda tiene una oferta fija, habitualmente se supone que ningún aumento por el lado de la oferta puede reducir la presión alcista sobre el precio. Según se muestra en Propiedad de Estabilidad[2], Bitcoin integra comisiones de transferencia que necesariamente suben con el uso. Esta característica exclusiva crea una presión bajista sobre el precio al reducir la demanda. **Pero este coste ascendente también hace viables los sustitutos, creando una presión bajista sobre el precio al aumentar efectivamente la oferta.**

No hay nada que evite la evolución de múltiples monedas parecidas. Es posible que estas exhiban propiedades monetarias casi indistinguibles, lo que minimiza las renuncias asociadas a la sustitución. Según se muestra en Principio de Consolidación[3], siempre existe presión hacia un único dinero, ya que esto elimina el coste de cambio. Sin embargo, esta presión está reñida con el aumento de los costes y, en algún nivel de uso, debe dar paso a la sustitución (o al desuso).

Reference

[1] https://es.wikipedia.org/wiki/Bien_sustitutivo

[2] Capítulo: Propiedad de Estabilidad

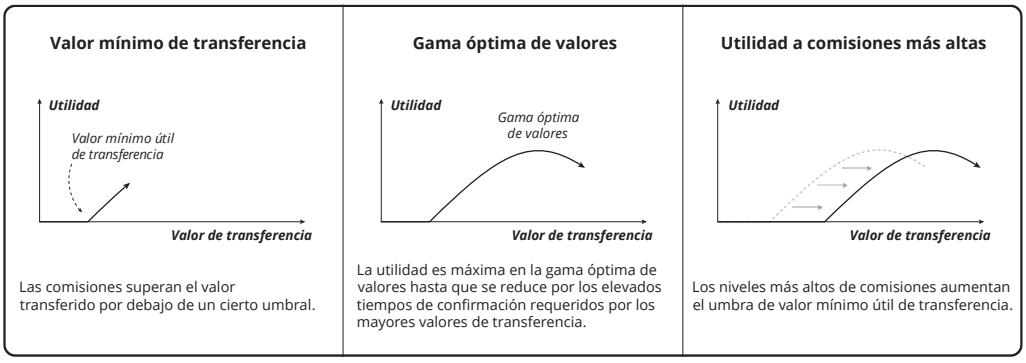
[3] Capítulo: Principio de Consolidación

Existe una teoría que dice que, puesto que la creación de nuevas monedas no cuesta nada, el principio de sustitución implica que Bitcoin tiene que dejar de tener valor a causa de la oferta gratuita ilimitada. Esto soslaya el hecho de que Bitcoin exige que las personas paguen por utilizarlo. Esto es tan cierto para una segunda moneda como lo es para la primera.

Y aumentar la oferta alivia la demanda. En algún punto, la demanda no es suficiente para producir/asegurar más oferta, y, por tanto, la teoría es inválida. Esta es la misma relación que existe con los dineros mercancía y, de hecho, con todos los productos.

Propiedad del Umbral de Utilidad

La utilidad se expresa como preferencia por la moneda antes que sus sustitutos, para transferencias de un valor comparable. Una utilidad creciente implica un nivel creciente de comisiones, dada la presuposición de un volumen creciente de transacciones. La competencia por la confirmación hace que se ofrezcan mayores importes de comisiones. Dadas las diferencias en el precio de mercado de las comisiones a lo largo del tiempo, uno podría ofrecer una comisión no competitiva esperando un plazo de confirmación más largo. Otros no realizarán transacciones en la cadena; en vez de esto, utilizarán sustitutos.



Por consiguiente, aumentar la utilidad implica aumentar el valor promedio de transferencia, ya que, de lo contrario, las comisiones crecientes harán que el coste de la transferencia supere el valor transferido. Una mayor profundidad implica una mayor seguridad de confirmación. Por consiguiente, se puede intercambiar tiempo por una *mayor* seguridad contra los gastos por duplicado. Sin embargo, el tiempo no se puede reducir por debajo de un periodo de bloque para lograr una *menor* seguridad. Los niveles mínimos de seguridad son ninguno (no confirmado) y mínimo (una confirmación). No existe ningún intercambio a realizar entre estos niveles.

Unas comisiones mayores implican un mayor coste en tasa de hash, lo que mitiga la necesidad de aumentar la profundidad de confirmación para transferencias de mayor valor. **Pero dado que no hay ninguna manera de reducir la seguridad para**

transferencias de menor valor, el valor mínimo útil de transferencia aumenta con la utilidad. No dar soporte a transferencias en una cierta gama de valores implica que los sustitutos son más baratos en esa gama. Esto implica la posibilidad de que coexistan dineros para dar servicio a distintas gamas de valores. Sin embargo, todos los Bitcoins[1] presentan inherentemente esta propiedad.

Las diferencias de reglas en términos de tamaño o periodo de bloque no modifican esta relación. El efecto de estas variaciones de la moneda es estrictamente proporcional. Incluso los bloques de tamaño ilimitado tienen que producir niveles de comisión que excluyan por precio las transferencias de poco valor.

Reference

[1] Capítulo: Etiquetas indicativas de Bitcoin

APÉNDICE

Glosario

Activación

Empezar a Hacer valer una nueva Regla.

Ajuste

Un cambio en la Dificultad.

Agregación

La tendencia hacia una participación reducida en la Minería o la Validación. Implica *Pooling* (compartición de recursos) o Centralización.

Anuncio

La primera Comunicación de un Bloque a otra Persona.

Potencia de Hash Aparente

Una fracción de Bloques en un Segmento de Cadena. Las estimaciones públicas de la Potencia de Hash de las Mineras se basan en esto.

Ataque

Utilización de la Potencia de Hash para permitir el Doble Gasto.

Bitcoin

El conjunto de principios que protegen una Moneda respecto del Estado. Los términos y principios están definidos por Satoshi en “Bitcoin: A Peer-to-Peer Electronic Cash System” ("Bitcoin: Un sistema de efectivo electrónico entre iguales").

Bloque

Un conjunto Válido de Operaciones con Sello y Prueba.

Reserva de Bloques

El conjunto de Bloques Débiles. Reserva Huérfana es una denominación poco apropiada también utilizada.

Pedir Prestado

Intercambiar tiempo por Unidades de propiedad que presentan una mayor Utilidad para el Prestador.

Rama

Una secuencia Válida de Bloques.

Candidato

Un Bloque potencial con Prueba no determinada.

Límite Superior

El límite de la Oferta a lo largo de todo el tiempo.

Capitalización

El producto de Precio y Oferta.

Censura

Confirmación subjetiva.

Centralización

La tendencia hacia pocos Comerciantes. Los Comerciantes controlan directamente la Validación. También puede referirse al *Pooling* (compartición de recursos).

Cadena

La Rama con la mayor Prueba acumulada.

Demandante

Una Persona que reclama una propiedad bajo el control de un Custodio. También: titular, accionista, prestador, o depositario.

Cliente-Servidor

Un Protocolo asimétrico.

Coacción

Empleo de actos de agresión para forzar la Activación.

Moneda

Un Consenso en relación con un medio mutuamente aceptable para el Comercio. El BTC es una Moneda.

Coinbase

Una Transacción que Transfiere una Recompensa.

Comunicación

Transmisión de datos entre Máquinas.

Confirmación

Inclusión de una Transacción dentro de un Bloque.

Consenso

Un acuerdo entre Personas. También, el conjunto de personas que participan en un acuerdo.

Reglas de Consenso

El conjunto de restricciones que define a una Moneda.

Contrato

Un Script que expresa las condiciones de Transferencia. Public Key Script es un anacronismo para decir esto.

Cooptación

Empleo de actos de agresión para controlar la Potencia de Hash.

Correlación

La capacidad de Contaminar mediante un análisis estadístico de la Cadena.

Custodio

Una Persona que controla la propiedad de otro por acuerdo.

Descentralización

La tendencia que se opone a la Centralización.

Desacoplar

Una Mina que comparte Recompensas con otra para reducir la Varianza.

Delegación

La tendencia a tener pocos Propietarios. Los propietarios controlan directamente el Gasto.

Negación de Servicio

Mediante Comunicación para explotar deficiencias del Protocolo o de la Implementación que degradan el rendimiento. DoS (del inglés *Denial of Service*) es un acrónimo de esto.

Profundidad

Uno más la cantidad de Bloques después de una Confirmación.

Desarrollador

Una Persona que crea una Implementación.

Dificultad

El nivel de Prueba exigido para la Validez.

Distorsión

Acto de agresión contra el Mercado que sesga el coste de Minar.

Doble Gasto

La Aprobación del mismo Contrato de Salida por parte de Gastos diferentes.

Polvo

Un número insuficiente de Unidades para Transferir a través de una Salida. Las Reglas de Consenso de BTC prohíben transferir menos de una unidad.

Poder Económico

Una fracción de toda la propiedad ofrecida a Cambio.

Economía

El conjunto de todos los Comerciantes.

Aprobación

Un Script que satisface un Contrato. Script de Firma es un anacronismo para referirse a esto.

Imposición del Cumplimiento

La acción de descartar datos Inválidos.

Cambio

El Intercambio de Unidades por otras propiedades.

Comisión

Una Transferencia implícita a una Minera.

Bifurcación (*fork*)

Una divergencia en las Reglas de Consenso.

Génesis

El primer Bloque de todas las Ramas de una Moneda.

Equipo de Machacado (*grind*)

Una Herramienta que realiza conversiones de Hash.

Machacadora (*grinder*)

Una Persona que opera un Equipo de Machacado (*grind*).

Reducción a la Mitad (*halving*)

Una reducción de la tasa de Subvención (a la mitad).

Bifurcación dura (*hard fork*)

Una Bifurcación que implica una División (*split*). Expansión del conjunto de Bloques potencialmente Válidos.

Hash

Una computación elemental para Probar la Validez del Candidato.

Potencia de Hash

Una fracción de la Tasa de Hash de todas las Minas.

Tasa de Hash

La tasa de conversiones Hash.

Altura

La cantidad de Bloques precedentes en una Rama.

Atesorar

Poseer para usar en el futuro.

Honesto

Una Minera que se basa en los Bloques de los demás.

Identidad

La vía para asociar a una Persona una Comunicación.

Implementación

Un conjunto específico de Herramientas.

Inflación

El aumento de la Oferta como resultado de la Subvención. Una inflación monetaria, que no debe confundirse con la Inflación de Precios.

Entrada

Un Punto de Salida y una Aprobación.

Interés

La velocidad de aumento de la Utilidad procedente del Préstamo.

Latencia

El retardo inherente a la Comunicación.

Disposición en Capas

Intercambio que utiliza una secuencia de Transacciones No Confirmadas que puede ser Cerrada por cualquiera de las partes.

Prestar

Intercambiar tiempo sin Unidades por propiedades de mayor Utilidad. Invertir es otra denominación para lo mismo.

Tiempo de Bloqueo

Una expresión de la Validez de Transacción más temprana.

Pérdidas

Cuando la Inversión no logra el tipo de Interés del Mercado.

Máquina

Un seguidor de instrucciones.

Potencia de Hash Mayoritaria

Un subconjunto de las Mineras con una Potencia de Hash suficiente para ejecutar un Ataque sostenido. 51% es una aproximación habitual de potencia suficiente.

Mercado

El Comercio de cierta propiedad.

Madurez

La Profundidad a la que una Salida de Coinbase pasa a ser Transferible.

Tiempo Medio Transcurrido

Un promedio de los Sellos de Tiempo de Bloques precedentes.

Comerciante

Una Persona que acepta Unidades durante el Comercio. Usuario es otra denominación habitual para ello.

Mina

Una Herramienta que realiza el Trabajo.

Minera

Una Persona que opera una Mina.

Nodo

Una Herramienta que realiza la Validación.

Operación

Una declaración elemental de intenciones.

Optimización

Un cambio de Herramienta que reduce el coste de Minar.

Organización

Un Anuncio que añade un Bloque a la Cadena.

Salida

Una Transferencia explícita y un Contrato.

Propietario

Una Persona que controla ciertas Unidades. Titular es otra denominación habitual para ello.

Partición

La incapacidad de Comunicarse de ciertos Nodos.

Particionamiento

La tendencia hacia Particiones persistentes.

Entre pares (*Peer-to-Peer*)

Un Protocolo simétrico.

Periodo

El tiempo medio entre Organizaciones.

Persona

Un decisor.

Punto

Una referencia a una Salida o Entrada.

Político

Relativo a las acciones de los Estados.

***Pooling* (compartición de recursos)**

La tendencia a tener pocas Mineras, incluida la consolidación mediante Repetidores.

Poder

El nivel relativo de control de una Persona sobre la Cadena o la Moneda.

Salida anterior

La Salida a la que se refiere una Entrada.

Precio

Un tipo de Cambio promediado o instantáneo.

Inflación de Precio

El aumento del Precio a lo largo del tiempo.

Beneficios

Una rentabilidad de la Inversión por encima del tipo de Interés del Mercado.

Prueba

Evidencia Válida.

Prueba de Memoria

Prueba probabilística de una cantidad de memoria de computación utilizable (PoM, del inglés *Proof-of-Memory*).

Prueba de Participación

Prueba criptográfica de una cantidad de Propiedad (PoS, del inglés *Proof-of-Stake*).

Prueba de Trabajo

Prueba probabilística de una cantidad realizada de Trabajo realizada (PoW, del inglés *Proof-of-Work*).

Protocolo

Un conjunto de convenciones para la Comunicación.

Repetidor

Una Herramienta que difunde nuevos Bloques.

Operario de Repetidor

Una Persona que opera un Repetidor .

Reorganización

Un Anuncio que promueve una Rama Débil en la Cadena. Reorg es una abreviatura para esto.

Recompensa

La suma del Subsidio y las Comisiones para un Bloque.

Regla

Un subconjunto de Reglas de Consenso.

Script

Un conjunto de Operaciones que autoriza la Transferencia.

Segmento

Un subconjunto contiguo de una Rama.

Egoísta

Una Minera que no está siendo Honesta.

Cierre

Confirmación de Transacciones En Capas.

Señal

Una indicación de una Minera por medio de datos de Bloque con la intención de Hacer valer una nueva Regla.

Bifurcación blanda (*soft fork*)

Una Bifurcación que implica una División (*split*) salvo que una Potencia de Hash Mayoritaria Imponga el Cumplimiento. Contracción del conjunto de Bloques potencialmente Válidos.

Especular

Poseer con la expectativa de un aumento de Precio. También Tomar Prestado con la expectativa de una disminución del precio.

Gasto

La publicación inicial de una Transacción.

División (*split*)

Una bifurcación de la Moneda.

Parada

Que no aumente la Altura con el tiempo.

Estado

Un conjunto de Personas que emplea actos de agresión en lugar de Intercambios. Típicamente opera con impunidad dentro de límites geográficos.

Fuerte

Una Rama con más Prueba acumulada que otra.

Subsidio

La emisión de nuevas Unidades para una Minera.

Oferta

El conjunto de todas las Unidades emitidas.

Contaminación

Determinación de los Propietarios.

Marca Temporal

Una declaración de la fecha y hora en que se produjo el Bloque.

Herramienta

Un conjunto de instrucciones para Máquinas.

Intercambios

Un canje voluntario de propiedades entre dos Personas.

Transacción

Un registro Válido de la Transferencia.

Reserva de Transacciones

El conjunto de Transacciones No Confirmadas. Reserva de Memoria es una denominación poco apropiada también utilizada.

Transferencia

El cambio de control sobre ciertas Unidades.

No Confirmada

Una Transacción que no existe en un Bloque de la Cadena.

Unidad

Una cantidad Transferible mínima de propiedad representada por una Moneda. El satoshi es la unidad de Bitcoin.

Utilidad

La utilidad que cierta propiedad tiene para una Persona.

Validación

El proceso de determinar la Validez.

Validez

Conformidad con las Reglas de Consenso.

Valor

La preferencia que tiene una Persona por cierta propiedad más que por otra.

Varianza

La frecuencia cambiante con que se logra una Recompensa.

Variación

Diferencias en el coste de los recursos de la Minería.

Volatilidad

Desviación del Precio a lo largo del tiempo.

Monedero

Una Herramienta que crea Transacciones.

Débil

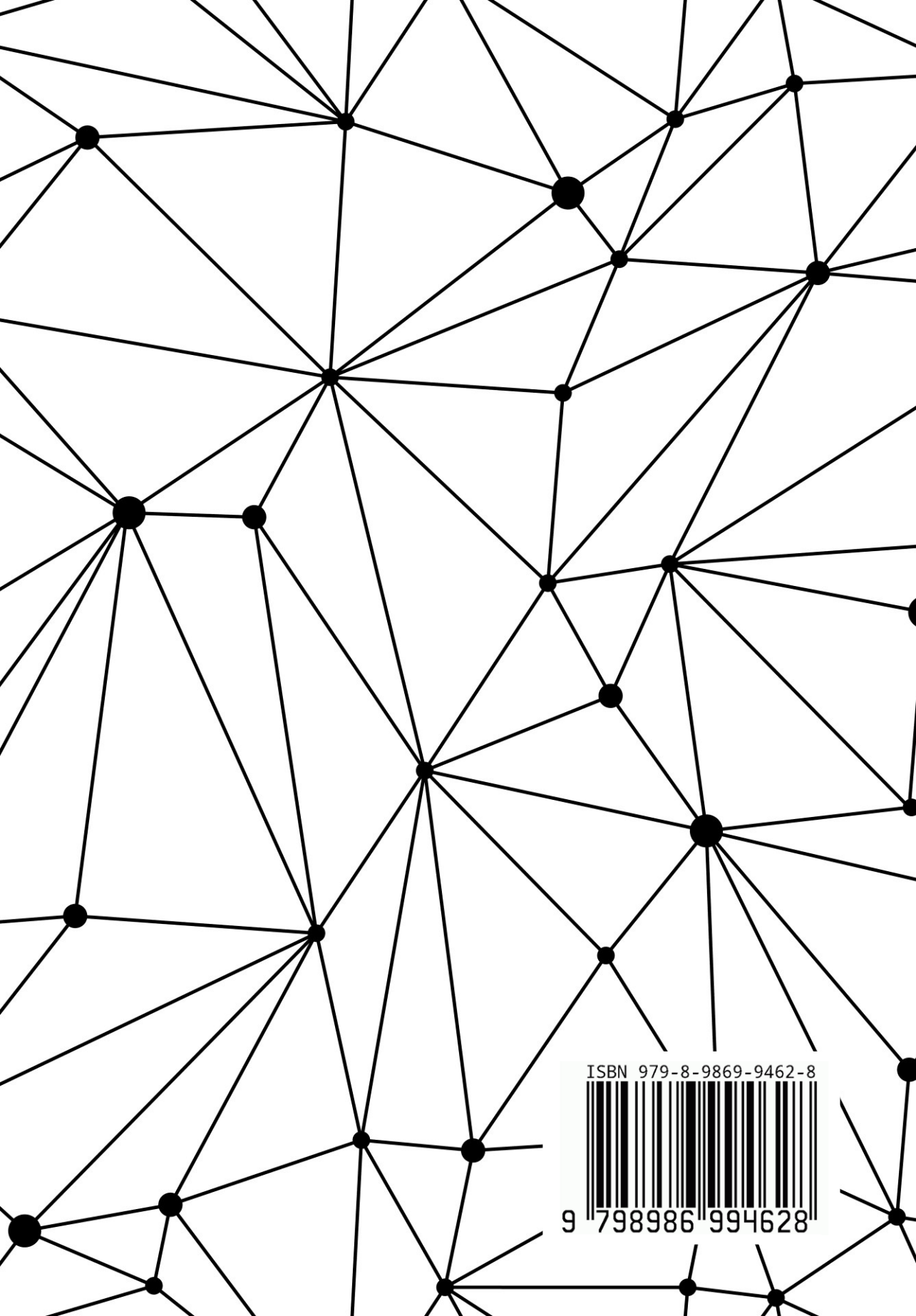
Una Rama con menos Prueba acumulada que otra. Huérfana es una denominación poco apropiada también utilizada.

Retención

El retraso intencionado de un Anuncio.

Trabajo

El proceso de producir Bloques.


ISBN 979-8-9869-9462-8