Bitcoin, no Cripto

Un análisis comparativo de las

propiedades únicas e

irreplicables de Bitcoin

Vijay Selvam

10 de junio, 2021.

Traducido por Adam Dub. Corregido por Jacky Rivero.

Resumen

La industria cripto está compuesta por miles de criptomonedas que ofrecen diferentes versiones de descentralización basadas en cadenas de bloques (blockchain) —un concepto que fue descrito originalmente en el *libro blanco* de Bitcoin en 2008—. Bitcoin es un activo monetario que logra la inmutabilidad a través de la gobernanza descentralizada del protocolo. Tal inmutabilidad es, en teoría, la principal razón detrás de las cadenas de bloques abiertas. Además de Bitcoin, lo que vemos en la industria son *tokens* alojados en la blockchain que ofrecen una descentralización diluida o espuria, que contradice y frustra el propósito de inmutabilidad en su conjunto. Este artículo académico destaca estas 'falacias de la *blockchain* a través un análisis contra el logro único e irrepetible en materia de gobernanza descentralizada'.

Inimitable Inmutable

El Diccionario Oxford de Inglés define "inimitable" como "imposible de copiar". Mientas que "inmutable" es definido como "algo que no puede ser modificado". El verdadero logro de Bitcoin es la invención del primer y único activo digital al portador con *inimitabilidad inmutable*. Para entender en profundidad a Bitcoin es necesario apreciar estas dos propiedades específicas que lo definen.

El camino de la persona promedio en la industria cripto típicamente comienza con Bitcoin. Después de todo, ha sido la criptomoneda que lleva más tiempo entre nosotros, tiene la porción de mercado más grande de la industria, y es la que más atrae atención en los medios.

Brevemente, después del paso inicial, el individuo, sin variación alguna, escucha el irresistible canto de sirena de otras criptomonedas supuestamente más rápidas, más eficientes, más seguras, y más versátiles, promocionadas por influencers de redes sociales, personalidades del deporte y multimillonarios excéntricos. Han existido incontables *tokens* presentados como los "asesinos de Bitcoin" en la última década. ¿Cómo le va a la "vieja" tecnología de 2008 "compitiendo" con las últimas criptos de 2021? Este artículo académico es un intento de responder esta pregunta diferenciando "la señal del ruido" con respecto a la industria cripto y la tecnología *blockchain*.[1]

Desde su invención en 2008, la capitalización de mercado de bitcoin pasó de cero a más de

un billón de dólares. Se estima que más de 110 millones de personas en el mundo, y más de un 17% de los adultos en Estados Unidos, tienen algún tipo de exposición a Bitcoin. [2] Empresas que cotizan en la bolsa, empresas privadas, fondos de pensiones, aseguradoras, gestores de activos y algunos de los nombres más destacados en la industria de servicios financieros ahora reconocen a Bitcoin como una nueva clase de activo y están comprometiendo inmensas cantidades de su capital y recursos en él. Algunos de los inversores más reconocidos, incluidos Paul Tudor Jones, Stanley Druckenmiller, Alan Howard, Carl Icahn y Ray Dalio han hablado acerca de sus inversiones en Bitcoin. Y el Estado de El Salvador recientemente ha adoptado a Bitcoin como dinero de curso legal.

En paralelo, Bitcoin ha generado una "criptoindustria" con más de 10.000 criptomonedas. Lo que une a estas miles de criptomonedas con Bitcoin dentro de la misma industria es la afirmación de que todos usan alguna versión de la tecnología subyacente de Bitcoin, llamada tecnología *blockchain*. Es poco probable que el o los autores del libro blanco de Bitcoin, de 2008, alguna vez hayan vislumbrado la separación de la tecnología subyacente del propio Bitcoin. De hecho, palabras como "*blockchain*" o "criptomonedas" no aparecen en ningún lugar del texto original de dicho documento. Sin darle mucha importancia, la industria ahora sigue al espacio entero como si fuese uno solo, y publica métricas como la "Dominancia de Bitcoin" que compara la participación del mercado de Bitcoin en relación con el resto de las criptomonedas combinadas, infiriendo que están compitiendo unas y otras por un pedazo de la misma torta.

En este artículo académico primero analizaremos el logro único de Bitcoin, en conseguir la descentralización digital que respalda su inmutabilidad. Luego haremos un análisis

comparativo de Bitcoin con otras criptomonedas, para demostrar los aspectos tecnológicos e históricos únicos que hacen que tal descentralización no tenga precedentes, sea revolucionaria y, por sobre todas las cosas, sea imposible de replicar. Finalmente, evaluaremos si Bitcoin debería ser considerado una clase de activo separada del resto de la industria cripto, dado su rol diferenciado como reserva de valor y su política monetaria alternativa políticamente neutral. El potencial que Bitcoin tiene para la economía global, y la humanidad en general, lo convierte en una industria en sí misma, mucho más allá de la industria cripto.

El rol de la inmutabilidad

Una equivocación obstinada y popular en los medios masivos y el *establishment* económico y financiero es que Bitcoin representa una "tecnología de pagos" de uso cotidiano. El "lento" tiempo de liquidación de operaciones de 10 minutos es señalado frecuentemente como muy inferior a Visa, Mastercard y Venmon, que te permite completar una compra de café en tan solo segundos. Esto deriva en objeciones tales como que Bitcoin no tiene ningún caso de uso real en el frente transaccional. Dejando de lado que aquellos argumentos son invalidados con la existencia de tecnologías en capas superiores como la Red Lightning, que permite hacer pagos instantáneos en la red de Bitcoin, esta perspectiva está totalmente errada.

El objetivo de Bitcoin siempre ha sido funcionar como un activo descentralizado con una política monetaria fija, transparente e inmutable, con el potencial de emerger como alternativa a la política monetaria de los bancos centrales. Esta intención está clara a partir

de las declaraciones de su(s) creador(es) donde describen que el mundo necesita un activo que no requiera confiar en terceros (*trustless)*, inmune al envilecimiento a través de las políticas inflacionarias de los bancos centrales:

"La raíz del problema con las monedas convencionales que es que para todas es necesario que exista confianza para hacerlas funcionar. Se debe confiar en que los bancos centrales no degraden la moneda, pero la historia de las monedas fiat está plagada de violaciones a esa confianza."

– Satoshi Nakamoto, febrero 2009

El oro ha funcionado históricamente como este activo inmutable. Pero tiene desventajas significativas en la era digital dados los inconvenientes en torno a su portabilidad, almacenamiento, seguridad, divisibilidad y verificabilidad. El oro tampoco es difícil de confiscar por una autoridad con el poder y los medios para hacerlo. La intención de Satoshi era crear "oro digital" más que un mero sistema transaccional de pagos. Aquellos inclinados a las *trivias* notarán que Bitcoin hace referencia a la Orden Ejecutiva *6102* de fecha 3 de abril de 1933, en la cual Franklin D. Roosevelt prohíbe mantener la propiedad sobre monedas de oro, lingotes y certificados: (i) el seudónimo del autor del libro blanco de Bitcoin, Satoshi Nakamoto, declara su fecha de cumpleaños como 5 de abril, el mismo día que se firma la Orden Ejecutiva, y (ii) el "ajuste de dificultad" el protocolo Bitcoin se ajusta cada 2016 bloques (Orden 6102 al revés). El oro, o mejor dicho, oro digital, estaba definitivamente en la cabeza de Satoshi. Y más crucialmente, la intención de crear un activo que sea inmune al envilecimiento o corrupción por parte de un gobierno o cualquier otra

autoridad, y que no sufre de defectos del oro físico.

La característica más crítica para cualquier reserva de valor es su escasez. Este hecho está demostrado a lo largo de la historia humana por lo que las sociedades han decidido darle su valor como "moneda", ya sea sal, conchas marinas, ganado, marfil o metales preciosos. Cuanto más escaso el activo, y/o más trabajo es necesario para producirlo, más "duro" es el activo y, en consecuencia, mayor es su efectividad como reserva de valor. Mark Twain describe la relación entre escasez y valor cuando observó: "compre tierras, no están fabricando de esas".

En palabras del criptógrafo, jurista e informático Nick Szabo, una buena reserva de valor debe tener un "costo infalseable" o, en inglés, "*unforgeable costliness*".[4] Es incorrecto afirmar que el valor del oro deriva de su uso en la joyería o de las aplicaciones industriales –en realidad, su valor se deriva de su escasez y del consenso del mercado de su rol como reserva de valor.

El precio de un activo en el tiempo, y consecuentemente su efectividad como reserva de valor, es una función de la oferta y la demanda. Cuando la demanda sube y la oferta se mantiene constante, resulta en precios más altos. Los precios más altos incentivan un crecimiento en la oferta, que termina equilibrando el precio. El aumento en la oferta, simplemente podría ocurrir por una mayor inversión en la producción de ese activo. Por ejemplo, el caso de la minería de oro y la exploración dirigida por la demanda de oro. O por el emisor del activo, que simplemente abre el grifo a su voluntad, como es el caso de los gobiernos y bancos centrales cuando emiten más deuda y dinero fiat, dirigidos por

incentivos políticos y económicos. En general, hay varios grados de ambigüedad sobre el verdadero nivel de escasez de dichos activos.

Ahora consideremos a bitcoin, que es un activo que no está respaldado por ningún bien físico, acción, o bono, ni por ninguna garantía o seguro de algún organismo público o privado. A diferencia de las acciones y bonos, no hay flujo de fondos en el cual poder utilizar modelos financieros que podría permitir calcular el valor del flujo de fondos descontados. Similar al oro, lo que le da valor a bitcoin es el consenso entre los participantes del mercado acerca de su integridad y su capacidad para retener poder de compra en el tiempo. Lo que marca la integridad de bitcoin como reserva de valor es su escasez, es decir, el *límite duro de 21 millones de monedas* que es parte del protocolo de Bitcoin.

A diferencia del oro o cualquier otro *commodity,* no hay monto invertido que pueda incrementar la oferta de Bitcoin – es, entonces, la primera y única clase de activo cuya oferta no se ve afectada por la demanda–. Pero este límite de 21 millones no tiene ningún sentido si no es inmutable en el tiempo y en el espacio. ¿Cómo Bitcoin alcanza tal inmutabilidad incorruptible? Lo hace a través de la robustez de la gobernanza y el consenso descentralizado.

La inmutabilidad de Bitcoin

El Sistema monetario global tal como lo conocemos es producto de la evolución del dinero durante miles de años. Hoy, el sistema bancario del planeta está hecho a partir de las entradas en registros contables del dinero de la humanidad. Como resultado, la "riqueza" hoy se toma a partir de registros contables existentes en bases de datos electrónicas. Estas bases de datos electrónicas están alojadas en cada banco (a un nivel de subregistro) y en última instancia en el banco central relevante (por lo general, al nivel general del registro). Es decir que lo que damos por sentado como nuestra reserva de valor son, esencialmente, entradas digitales alojadas en un servidor o en la nube de una entidad centralizada en la que hay que confiar. El elemento clave aquí es la confianza. Si la confianza se fuera a evaporar por cualquiera que sea la razón, también lo harán los dígitos que representan la riqueza de cada quien.

Bitcoin es, originalmente, el producto de una iniciativa *cypherpunk* que pretende separar al dinero de los gobiernos, empresas y otras entidades centralizadas. En otras palabras, el objetivo era eliminar la intermediación de los bancos centrales y el sistema bancario del dinero mediante la creación de un sistema de registros de igual-a-igual *(peer-to-peer)*. En el sistema monetario existente, las entidades centralizadas en las que hay que confiar administran el registro principal y validan las transacciones para la inclusión en el mismo.

La solución de Bitcoin fue crear una red descentralizada donde todos los participantes alcanzaran un consenso sobre el estado de la "verdad" respecto del registro en cualquier

momento en el tiempo.

Cuando la gente piensa en Bitcoin como "dinero de internet" habitualmente imagina que el libro mayor de Bitcoin debe estar alojado en alguna nube o base de datos en algún servidor central. Sin embargo, no hay tal cosa como una fuente central de la verdad en la red de Bitcoin. No hay un registro centralizado donde son publicadas todas las transacciones. En cambio, el registro de transacciones está alojado en miles de discos de individuos repartidos por todo el mundo, conocidos como "nodos". Esto hace a Bitcoin un registro público y descentralizado. El logro tecnológico primario de Bitcoin fue la creación de una estructura de incentivos que asegure que todos los participantes de la red sean honestos, sin la necesidad de recurrir a una entidad centralizada para validar las transacciones. En otras palabras, un protocolo que opera sin requerir la confianza en terceros *(trustless)*.

La verificación de las transacciones de la red son llevadas a cabo por miles de "mineros" alrededor del mundo, que verifican las transacciones anónimamente. Las transacciones de bitcoin son distribuidas en la red continuamente y recibidas por los mineros, que luego proceden a verificar las transacciones para asegurarse de que quien envía bitcoin tiene actualmente ese bitcoin, es decir, es el dueño legítimo, y no está incurriendo en un doble gasto de esos fondos. El minero entonces agrupa las transacciones verificadas en un "bloque". El bloque es luego sometido a un proceso de *hashing* criptográfico, y el primer minero en completar el proceso de *hashing* gana el derecho a agregar el bloque a la *blockchain*. Para incentivar la minería, ese minero recibe más bitcoin una vez que el bloque ha sido agregado a la cadena de bloques.

Un bloque verificado y con el *hash* encontrado es publicado a los miles de nodos de alrededor del mundo, validado por su software y luego registrado en sus libros mayores. El punto clave es que nadie confía en nadie – cada nodo valida por sí mismo cada transacción, desde la primera en 2009 hasta la última hoy–. Como resultado, si un nodo registra un bloque que no sigue las reglas de consenso, otros nodos lo rechazarán, es decir, que será inválido. Es a través de este proceso de verificación individual independiente y de "consenso distribuido", que la red de Bitcoin puede dispensar la necesidad de una entidad centralizada en la que se requiera confiar.

El software de Bitcoin operando en estos miles de registros estipula que solo se crearán 21 millones de monedas. ¿Qué podría ocurrir para cambiar este límite 21 millones, así destruyendo la santidad de la escasez de Bitcoin?

El único escenario en que el límite de bitcoin a emitir pueda ser alterado sería por un consenso entre los nodos, que estos actualicen su software para cambiar el límite. Aquí entra en juego la estructura de incentivos de Bitcoin. Si un nodo determinado decide cambiar el límite de emisión a, digamos, 100 millones de bitcoin, el nodo sería libre de hacerlo, pero el software de ese nodo no seguirá siendo compatible con las decenas de miles de nodos restantes. Por lo tanto, la moneda con un techo de 100 millones de unidades ya no sería "bitcoin". En una analogía con el ajedrez, cualquiera puede cambiar las reglas del ajedrez, pero nadie jugaría con la persona que quiera hacerlo. Además, al aumentar el límite de suministro, el nodo efectivamente estaría diluyendo el valor de sus propias monedas y, en consecuencia, no tiene un incentivo económico para hacer tal cosa.

Esta poderosa estructura de incentivos forman la base de la inmutabilidad incorruptible de Bitcoin.

La inimitabilidad de Bitcoin

¿Es posible mejorar el sistema de Bitcoin para lograr un consenso descentralizado? Expertos en el área, como el Dr. Adam Back, CEO de Blockstream, han señalado que no hay virtualmente espacio para mejoras en el diseño fundamental de Bitcoin. De acuerdo al Dr. Back, "por una curiosa casualidad, bitcoin existe dentro del estrecho óptimo, en medio de un semiespacio infinito para diseñar".[5] Sin embargo, cualquier tecnología de código abierto, incluso si es perfecta, puede ser copiada. Bitcoin necesitaría ser un evento que ocurre "una vez en la historia" para ser verdaderamente inevitable.

De acuerdo a Jack Dorsey, fundador y CEO de Twitter y Square (N. del T.: Dorsey abandonó su cargo como CEO de Twitter en diciembre de 2021), la replicación o reemplazo de Bitcoin es "extremadamente improbable, ya que la condiciones necesarias para crearlo y sostenerlo fueron muy especiales".[6]

Para entender el poder de la inimitabilidad de Bitcoin es necesario apreciar a Bitcoin como "una invención única, dependiente de un sendero". [7] Bitcoin es mucho más que el software de Bitcoin Core que corre el protocolo, que es muy fácil de copiar. Bitcoin es una red de más de 100.000 nodos, más de 1.000.000 de mineros, más de 100.000.000 de usuarios, y miles de millones de dólares en equipo de minería distribuidos en todo el

mundo, construido de forma orgánica durante más de 13 años, y ahora asegurando mil millones de dólares de riqueza.

Como destaca Robert Breedlove, fundador y CEO de Parallax Digital, la dependencia de un sendero quiere decir que la secuencia en la que acontecen los eventos importa tanto como los eventos mismos. Cualquier criptomoneda nueva tratando de competir con Bitcoin hoy tendría, en comparación, una seguridad muy débil, ya que su red de minería y poder de cómputo sería significativamente menor al de Bitcoin. Dado el interés de la industria por cómo funciona la tecnología *blockchain*, la nueva moneda sería atacada por los dominantes si alguna vez amenazara a Bitcoin. La dependencia de un sendero evita la disrupción de Bitcoin, dado que la serie de eventos que deben ocurrir de manera orgánica y que llevaron a su lanzamiento, y posterior asimilación en el mercado, no pueden ser replicados.

Además, los efectos de red y la Ley de Metcalfe hacen imposible que Bitcoin pueda ser destronado de su posición actual. Los inversores estarían incentivados a mantener el activo con la mayor liquidez, seguridad y efectos de red. Jeff Booth, autor del libro *El precio del mañana,* ha argumentado que para que una red existente sea amenazada, un nuevo competidor debe ser 10 veces mejor.[8] Dado que las redes existentes le dan al líder una sólida y gran ventaja, una nueva red no puede ser un poco mejor – tiene que ser un orden de magnitud mejor para que los usuarios sean alentados a hacer un cambio–. Cuando se trata de la función de reserva de valor sería virtualmente imposible mejorar la escasez, transportabilidad, verificabilidad, durabilidad, y divisibilidad de Bitcoin, al menos

de tal manera que brinde una propuesta 10 veces mejor que Bitcoin para poder destronar la red.

Un análisis comparativo

Analicemos dos características específicas de Bitcoin que contribuyen a su inmutabilidad e inimitabilidad y comparemos esos aspectos con otras criptomonedas, en particular, con la segunda más grande, Ethereum.

A. Toma de decisiones descentralizadas

La existencia de un fundador y de un equipo de líderes es antitético a la gobernanza descentralizada. A la luz de este hecho, las circunstancias bajo las que Bitcoin fue concebido son destacables. "Satoshi Nakamoto" es un perfil ficticio de un hombre japonés, nacido el 15 de abril de 1975, que afirmaba vivir en Japón al momento en el que el libro blanco fue publicado en un foro en internet. El 23 de abril de 2011, el operador de la cuenta seudónima afirmó que decidió "dedicarse a otras cosas", y poco tiempo después desaparecería. Desde entonces, nunca ha habido información confiable sobre su/sus ubicación. Aunque esta historia parezca sospechosa y dudosa, el resultado final es lo que importa: Bitcoin no tiene fundador ni líder. Nunca lo tuvo, nunca lo tendrá.

Comparemos esto con otras criptomonedas incluyendo Ethereum, que tiene a Vitalik Buterin, quien tiene un estatus de casi dios dentro de la Fundación Ethereum –ni mencionar la contradicción en términos de una "fundación" administrando una red supuestamente descentralizada–.

Virtualmente, todas las demás criptomonedas tienen fundadores, un equipo de liderazgo, patrocinadores, inversores de capital semilla y otras partes interesadas claves. La ausencia de liderazgo es relevante en términos de descentralización porque con el liderazgo viene la influencia. Vitalik Buterin mantiene una enorme influencia sobre el futuro de Ethereum, lo que desvirtúa la inmutabilidad del protocolo. Él ha modificado la política monetaria de Ethereum varias veces durante su corta existencia. Por el otro lado, no hay ningún individuo o individuos específicos que puedan influenciar fuertemente la política monetaria de Bitcoin, y en 13 años de historia, no se ha modificado.

Los únicos que pueden tomar decisiones en Bitcoin son los usuarios económicos de la red que mantienen y validan copias completas de la cadena de bloques de Bitcoin, en otras palabras: los nodos. Se estima que hay más de 100.000 nodos en todo el mundo. La mayor parte de estos nodos están en Estados Unidos (un 19%), seguidos por Alemania (18% aproximadamente); China mantiene un poco menos del 2% de los nodos.[9] El número de nodos a la vista es aproximadamente de 10.000 mientras que el total de los nodos a nivel global es superior a los 100.000.[10] Una característica que ha permitido tan amplia distribución de nodos como validadores completos es el pequeño tamaño de los bloques de Bitcoin. Cuando un individuo instala un nodo en su casa deberá descargar toda la *blockchain*, que en la actualidad son unos 700.000 bloques. Cada bloque pesa individualmente menos de 1,5 megabytes de tamaño. Como resultado, la cadena de bloques entera pesa unos 350 gigabytes. Este es un tamaño que puede ser alojado en una casa con un costo relativamente bajo. Cualquier individuo con una conexión básica a internet y una computadora portátil, en cualquier lugar del mundo, puede descargar la cadena de bloques completa de Bitcoin, validar bloques, y participar en el consenso

descentralizado del protocolo.

Tener un tamaño de bloques pequeños implica un sacrificio, ya que hay un límite a las transacciones que puedan ser procesadas.
Los nodos de Bitcoin han hecho una decisión consciente de preferir descentralización por sobre volumen de transacciones o velocidad.[11]

En contraste, en el caso de Ethereum, un individuo consciente de los costos no podría formar parte del proceso de consenso. Con Ethereum 2.0, solamente "nodos supercompletos" tendrán la historia entera de transacción. Un nodo supercompleto necesitará una gran cantidad de inversión en infraestructura de red y computacional, que va más allá de los medios de la gran mayoría de usuarios. Las entidades más pequeñas deberán confiar en que estos nodos supercompletos estén actuando de forma honesta. Ethereum también depende en gran medida de operadores de nodos de gran escala como Infura. Infura usa Amazon Web Services, lo cual multiplica el nivel de centralización. Esto crea puntos singulares de falla. En noviembre de 2020, el riesgo finalmente ocurrió cuando Infura afrontó un apagón masivo. La caída causó una demora en los *feeds* del precio de tokens de Ethereum. Este tipo de centralización también crea vulnerabilidades donde una entidad poderosa podría atacar, coartar o influenciar a la red.

En un intento de imitar el límite máximo de 21 millones de Bitcoin y su tesis de escasez, se espera que Ethereum 2.0 tenga una política monetaria deflacionaria en la cual las monedas son sacadas de circulación con el tiempo, aumentando su escasez. El liderazgo de Ethereum, sin embargo, podría estar ignorando el asunto central: la "solidez" de un activo deriva de su inmutabilidad.

El hecho de que Ethereum modifique su protocolo a un sistema deflacionario no ayuda a su causa por la inmutabilidad, sino al contrario, la daña. La historia de Ethereum muestra en distintas instancias en las que el protocolo fue modificado o influenciado, incluyendo en 2016, cuando un gran número de monedas fueron invalidadas como resultado de un hack, que terminó con una bifurcación de la red llamada Ethereum Classic. Por definición, si se cambia apenas una vez el protocolo, pierdes el privilegio de hacerte llamar inmutable. No hay segundas oportunidades. En el caso de Ethereum, ha cambiado su política monetaria más de una docena de veces. Su caso por la inmutabilidad está, en consecuencia, más allá de cualquier redención.

B. Prueba de Trabajo vs. Prueba de Participación

Como lo hemos comentado, los mineros compiten para verificar transacciones que serán incluidas en *blockchain*. La estructura de incentivos que gobierna a los mineros de Bitcoin se la conoce como *Proof of Work*(Prueba de Trabajo, PoW por sus siglas en inglés). Para que el sistema funcione sin la necesidad de confiar en un tercero, esta estructura de incentivos debe desalentar conductas deshonestas. ¿Cómo logra PoW esto?

En primer lugar, los mineros deben adelantar costos significativos para asegurar la red y solo reciben el pago si los bloques que minan cumplen con las reglas de consensos del software en los nodos. Esto incentiva a los mineros a minar exclusivamente bloques válidos.

Segundo, los nodos también validan cada bloque de manera independiente, y tienen la capacidad de invalidar bloques en el teórico evento de un ataque coordinado por mineros (conocido como un "ataque del 51%"). De esta manera es que los mineros no

controlan Bitcoin, más bien son sirvientes pagos de los nodos.

En tercer lugar, el mecanismo PoW permite varias capas de descentralización incluyendo el frente geográfico y el frente temporal.[12]

(i) Ya que los mineros siempre están buscando las fuentes de energía más barata, y la mejor tecnología, hay una invariable dispersión de los mineros alrededor del mundo, en otras palabras: descentralización geográfica. Así, incluso si los mineros fueran atacados en una jurisdicción, los mineros en otras partes del mundo se asegurarían que la red continúe sin ser afectada. Este escenario es lo que está ocurriendo ahora en la inédita prohibición y ofensiva del gobierno chino contra operaciones mineras ubicadas en el país —que en un momento representó aproximadamente el 75% del poder global de hash, pero ahora ha caído a un 46% (N. del T.: al momento de la traducción, el poder de hash ubicado en China es insignificante)—. [13] Incluso con semejante proporción de los mineros sufriendo el apagón abrupto y obligados a reubicarse, la red no experimentó tiempo de caída, y solo sufrió una leve demora en los tiempos de producción de bloque por un período breve de tiempo hasta el siguiente "ajuste de dificultad" en la red.

(ii) Los chips ASIC utilizados en la minería de Bitcoin son un hardware especializado que es costoso y limitado en su disponibilidad –lleva unos 2 o 3 años montar una operación de minería significativa en cualquier lugar del mundo, e incluiría comprar equipos mineros ya existentes debido a que la oferta es limitada–. Esto permite descentralización en el frente temporal dado de que en el caso de que un potencial atacante comience a acumular equipos durante un largo período de tiempo, los participantes de la red indefectiblemente se enterarían y diseñarían un plan de defensa.

PoW introduce un elemento físico y mecánico en el activo digital. La minería es entonces la conexión de Bitcoin entre el dominio digital y el mundo real.

Ahora miremos otras criptomonedas. Primero, mientras que la Prueba de Trabajo de Bitcoin precisa de chips ASIC, que son costosos y hay limitaciones físicas sobre su oferta, la mayoría de las otras criptomonedas, incluyendo Ethereum, precisan de tarjetas GPU, que son baratas, para propósitos generales, y con alta disponibilidad. Sería ampliamente más sencillo para un atacante comprar una cantidad inmensa de poder de GPU en la nube por un período de tiempo breve, y llevar a cabo un ataque del 51% en Ethereum 1.0. Reconociendo estas limitaciones, se espera que Ethereum 2.0 utilice un modelo de Proof of Stake –Prueba de participación, PoS por sus siglas en inglés– en algún momento cercano, aunque la fecha aún no está confirmada.

¿Cómo funciona la Prueba de Participación? Mientras que la Prueba de Trabajo recompensa a los mineros por resolver un problema matemático de *hash*, en la Prueba de Participación la entidad que más "participa" con más tokens de Ethereum es el que valida las transacciones. Los participantes que quieren hacer *staking* con sus monedas y validar transacciones obtienen una comisión en la misma moneda. La PoS elige aleatoriamente un ganador con base en el monto monetario que han comprometido en el proceso. El punto importante acá es que las probabilidades de obtener las comisiones de la transacción está directamente vinculado al porcentaje de monedas que se ponen en *staking*: es decir, tu riqueza. Entonces en otras palabras, los "ricos se convierten en más ricos", y con el tiempo, el sistema inevitablemente tiende hacia la centralización.

Los defensores de la Prueba de Participación dirán que la Prueba de Trabajo de Bitcoin

sufre de falencias similares, ya que la minería requiere gastar en equipos de alto valor e incurrir en costos que están concentrados entre un puñado de *pools* de minería. Sin embargo, este argumento deja de lado un aspecto crítico. Para que el sistema de incentivos funciones adecuadamente es necesario desalentar las conductas deshonestas. Como hemos visto con la Prueba de Trabajo, si hay una disputa sobre cuál es el último bloque, un minero solo puede trabajar con uno de los dos bloques, y la cadena de bloques más larga (N. de T.: con mayor trabajo acumulado) termina siendo aceptada por una mayoría. Cuando se desarrollan dos cadenas que compiten entre sí, los mineros deben elegir qué cadena seguir cuando realizan el gasto de poder de cómputo para minar nuevos bloques y agregarlos y, en última instancia, la cadena a la que la mayoría de los mineros agregue nuevos bloques será la que prevalezca. La cadena más corta será descartada y los mineros que contribuyeron su poder de cómputo a ella habrán malgastado su dinero. Así, con la Prueba de Trabajo, hay que asumir un costo por estar equivocado o ser deshonesto. El problema con la Prueba de Participación es que no hay costo alguno para verificar de manera simultánea transacciones de múltiples cadenas. En vez de contribuir a una sola cadena, alguien con *stake* puede verificar todas las divisiones de la cadena al mismo tiempo, ya que no hay costo asociado a estar equivocado.

Para castigar la conducta deshonesta, se espera que Ethereum 2.0 tenga un mecanismo en el cual los tokens de Ethereum son removidos de los validadores que actúan de manera deshonesta. Sin embargo, como ha observado Andrew Poelstra, director de Investigaciones de Blockstream, el problema inherente en este sistema es que el sistema de penalidades depende de los *recursos dentro del sistema.*[14]

A diferencia de la minería de PoW, donde un minero incurre en costos externos en la forma de equipos de minería y gasto energético, PoS depende de su propia historia, una que está intentando formar para prevenir la pérdida de valor. Incluso si los validadores hacen *staking* con monedas de gran valor de mercado, de manera tal que las perderán si se comportan de modo deshonesto, este es el único efecto disuasorio a tal conducta hasta que mueven los fondos. Y una vez que lo hagan, ya no ponen nada en juego al garantizar la verdad de las transacciones históricas. Ni bien las monedas en *staking* son desvinculadas de las claves privadas relacionadas, sería teóricamente sencillo bifurcar la red y crear una nueva historia.

Los defensores del PoS argumentan que tal revisión deshonesta de la historia *post facto* será contradictoria de la historia como la recuerdan los participantes del sistema, y así, un ataque como este sería detectado, y la nueva historia rechazada. El problema aquí, sin embargo, es que los nuevos usuarios que encuentran múltiples historias ya no pueden distinguirlas por su cuenta, requieren preguntarle a los participantes existentes de la red que historia saben que es la verdadera. De esta manera ya no es un sistema que no requiere confianza en terceros como lo es Bitcoin. Nuevos usuarios y usuarios que estuvieron temporalmente desconectados tendrán siempre que confiar en otros para obtener el último registro de la historia de transacciones. Y dado que PoS por su naturaleza permite múltiples "historias baratas", esto genera vulnerabilidades significativas.

Otra desventaja del PoS que destaca Poelstra es que le provee a los participantes el incentivo y la capacidad de elegir las transacciones que validan o torcer la historia de

transacciones para que el participante tenga una recompensa mayor. Esto, una vez más, causa una centralización del sistema. Un participante deshonesto podría sesgar la selección del validador de bloques futuros o peor, censurar transacciones que de otra manera hubiese aumentado los participantes del sistema.

Para ilustrar las fallas inherentes al sistema PoS, un simple experimento de pensamiento ayuda. Imagina que estás creando una criptomoneda. El desafío principal estará en la distribución de esa moneda tanto como sea posible, de una manera justa. Si utilizas un sistema PoS, entonces tendrías que hacer un "pre-minado" para emitir *tokens* a un selecto grupo de poseedores iniciales –que invariablemente serán los fundadores de la moneda–, y que luego propagarán la red al hacer *staking* con estas monedas. Esto es obviamente un sistema manifiestamente injusto dada la asignación inicial de las monedas con criterio nepotista. En el caso de que la moneda gane adopción en el mercado y haya compradores secundarios a precios más altos, estos poseedores iniciales de las monedas subsecuentemente tendrán una gran ganancia al vender estas monedas por efectivo. Más allá de la injusticia inherente, también hay que considerar temas legales dado que las similitudes con oferta ilegal de valores es inevitable. En cambio, en el caso del sistema PoW de Bitcoin, cada moneda que ha sido creada, fue emitida a cambio de un gasto de energía en el proceso de minería.

Finalmente, también debería notarse que PoS es aún un experimento. Como con cualquier modelo de seguridad nuevo, lleva años probar ser resistente a un ataque. Es más, cuanto más compleja la estructura, más potenciales sorpresas hay. Es de esta manera virtualmente imposible argumentar que PoS es de alguna manera superior al sistema PoW

de Bitcoin, probado en batalla, y que ha demostrado ser increíblemente robusto en un período de 13 años –lo cual son eones en el mundo tecnológico–.

Falacias de la *blockchain*

Está teniendo lugar un tremendo progreso tecnológico alrededor nuestro y cambiando el mundo tal como lo conocemos. Sin embargo, cuando esta innovación está teniendo paraje en las supuestamente descentralizadas cadenas de bloques al lanzar tokens de utilidad con supuesto valor monetario, es necesario detenerse y contestar dos preguntas: (a) ¿necesita el proyecto realmente ser un token monetario descentralizado?, y (b) asumiendo que lo necesita, ¿es dicha *blockchain* realmente descentralizada?

Consideremos la primera pregunta. Sabemos que la descentralización es crítica a la propuesta de valor de Bitcoin como activo monetario imposible de inflar su oferta. De acuerdo con Lewis Parker de Unchained Capital, lo único que cualquier cadena de bloques puede ofrecer a cambio de seguridad es un activo monetario nativo en la red.[15]

Cuando el sistema depende de derechos exigibles por fuera de la red, en el mundo físico, la *blockchain* realmente no ayuda. Es por eso que una cadena de bloques descentralizada es solo útil en aplicaciones monetarias o como una reserva de valor inmutable, mientras que una cadena de bloques no logra nada salvo asegurar su propia inmutabilidad.

Vemos las aplicaciones de la *blockchain* en la industria de los videojuegos con la creación

de objetos virtuales o "*skins*", por ejemplo, o en el mundo del arte con los tokens no fungibles (NFT) y, con más importancia, en el floreciente campo de las finanzas descentralizadas ("DeFi"), intentando replicar el sistema financiero en un protocolo "descentralizado". Dichas *blockchain* supuestamente proveen de resistencia a la censura y la capacidad de teóricamente tener que evitar regulaciones KYC (siglas en inglés para Know Your Customer, Conozca a Su Cliente) que exigen casas de cambio reguladas y centralizadas. ¿Justifican estos casos de resistencia a la censura y eludir el KYC la existencia de una industria de más de mil millones de dólares? Quizás si o quizás no. Pero el aspecto frecuentemente pasado por alto es que, debido a la pseudo-descentralización, estos supuestos beneficios no son más que un espejismo. Como hemos discutido anteriormente, al estar construido principalmente sobre Ethereum, están sujetos a varios puntos centrales de falla y vulnerables a ataques de las autoridades en búsqueda de censurar o aplicar regulaciones KYC.

Es importante reconocer que la descentralización normalmente acarrea un costo. Uno de los secretos mejores guardados en la industria cripto es que almacenar algún tipo de información en la cadena de bloques es típicamente mucho más ineficiente que desplegarlo en una base de datos centralizada. Una cadena de bloques generalmente hace el servicio más caro –el costo del gas de ETH es notablemente exorbitante–, más lento y con una peor interfaz de usuario cuando se lo compara con lo que es posible con un sistema centralizado. Es más caro ejecutar un proyecto en Ethereum que en, por ejemplo, Amazon Web Services. Los participantes del mercado y usuarios están recién empezando a comprender esta realidad. Por ejemplo, el protocolo centralizado Binance Smart Chain, superó recientemente el volumen de transacciones diarias de Ethereum y

la cantidad de monederos únicos activos, como consecuencia del aumento en los costos de transacción de Ethereum a comienzos de 2021. Además, como con cualquier token de utilidad, dado que los costos de cambiar son bajos, siempre hay un riesgo de disrupción. En otras palabras, los usuarios de Tether están moviéndose en masa hacia Tron desde Ethereum, por razones de costos. Muchos de estos tokens de utilidad son análogos a fichas de casino: las necesitas para jugar en la ruleta cuando estás en el casino, pero no te las llevarías a tu casa y almacenarías tu riqueza en ellas. Lo que muchos proyectos cripto están intentando hacer es similar al casino afirmando que sus fichas de $10 de la mesa de ruleta son activos monetarios escasos.

¿Por qué estos proyectos continúan utilizando tokens basados en *blockchain* a pesar de las conclusiones de las secciones anteriores? Hay dos motivos:

1. Beneficiarse gratuitamente de la acción del precio de Bitcoin

La primera razón es esencialmente aprovecharse del éxito de Bitcoin como una reserva de valor escasa. Al ser asociado con Bitcoin y pretender ser parte de la misma "industria cripto", otras criptomonedas son arrastradas por el motor que es la acción del precio de Bitcoin.

Las manías especulativas a lo largo de toda la industria están virtualmente correlacionadas en un 100% con los ciclos alcistas y bajistas de Bitcoin. Esto es exacerbado por varios grandes inversores y gestores de fondos que tienen

"asignaciones cripto" a través de las cuales adquieren otras criptomonedas como una forma equivocada de diversificarse de su principal objetivo de inversión, que es Bitcoin. Hay entonces un alto incentivo para los proyectos cripto de sumarse al tren de la descentralización y "vestir a la mona de seda" disfrazando las tokens de su proyecto centralizado como un activo escaso y descentralizado. Esta estrategia ha sido estupendamente rentable para los fundadores y promotores de estos tokens. La consecuencia desafortunada de esto es que la reputación de Bitcoin se ve manchada por estafas y engaños que a lo largo y ancho de la industria.

Tomemos Dogecoin, una criptomoneda cuyo creador la configuró en algunas horas como una broma y tiempo después abandonó el proyecto por completo, como ejemplo. La moneda, a pesar de todo, tiene una capitalización de mercado superior a los $50.000 millones. Es muy fácil para alguien ajeno mirar a la industria cripto como un todo, y pintar a Bitcoin con la misma brocha que Dogecoin, es decir como una broma y una burbuja. Como comentó Alyse Kileen, "si otras criptomonedas tienen éxito, será *por Bitcoin;* y si Bitcoin tiene éxito, será a *pesar* de todas las demás criptomonedas turbando el agua". [16]

2. Regulación de Valores

La segunda razón es que muchos de estos tokens apuntan a evitar registrarse como oferta pública de valores intentando caminar en una borrosa línea que presenta el token como supuestamente descentralizado. La profesora de leyes, Angela Walch, se refiere a esto como el "Velo de la Descentralización" bajo el cual muchos promotores de tokens creen

que se le garantiza una exención en cuanto a las regulaciones sobre títulos valores.[17] La realidad es que la mayoría de las criptomonedas, más allá de Bitcoin, tiene un riesgo de mediano a alto de ser sujeto de una investigación por parte de reguladores financieros, bajo la figura de oferta pública ilegal de valores.

Esta determinación en Estados Unidos está basada en el "Test Howey" –en el caso de la Comisión de Bolsa y Valores (SEC) contra W.J. Howey Co.–, la Corte Suprema de Estados Unidos sostuvo que cuando "hay un contrato, transacción o esquema en el cual la persona invierte su dinero en un emprendimiento común y su expectativa es obtener ganancias únicamente a partir de los esfuerzos del promotor, patrocinador u otro tercero" se trata de un título valor. Con respecto a la mayoría de las criptomonedas excepto Bitcoin, siempre hay un tono gris en torno a preguntas como la existencia de una "inversión" en una "empresa común" con una expectativa de obtener ganancias de los esfuerzos de "promotores, patrocinadores u otros terceros". Ethereum fue "absuelto" en este frente durante un discurso de William Hinman, director de la División de Finanzas Corporativas de la SEC, aunque fue de manera no oficial, lo cual varios comentaristas lo describieron como el "Enigma Hinman". [18]

Hinman sugirió que Ethereum fue inicialmente ofrecido como un valor, pero subsecuentemente cesó de serlo. Este análisis ha sido objeto de críticas por su ambigüedad. Sin embargo, otros tokens no se beneficiarían de tal grado de blandura y siempre está el riesgo de una recaracterización *post facto*. Varios promotores de criptomonedas han sido procesados y esto probablemente continuará. El caso de más alto

perfil de estos procesos es el de Ripple Labs, que involucra su token XRP.

La señal y el ruido

¿Cuál es el valor de un activo monetario inimitablemente, inmutable y con escasez absoluta? Aquí algo de material para pensar:

El 8 de noviembre de 2016, el gobierno de India anunció que los billetes indios de determinadas denominaciones ya no serían válidos. No solo estos billetes de ciertas denominaciones perdieron todo su valor, sino que se criminalizó el acto de poseerlos. Los poseedores debían cambiar sus billetes anulados por unos nuevos dentro de un tiempo determinado. En efecto, la "promesa de pago al portador" del Banco Central indio en esos billetes específicos fue invalidada y anulada unilateralmente. El mérito y demérito de este paso que tomó el gobierno indio con el objetivo de combatir el dinero negro, van más allá del enfoque de este artículo académico. Pero este incidente es un duro recordatorio de la capacidad, no únicamente del gobierno democráticamente elegido en la India, si no de cualquier gobierno o banco central, de invalidar por medio de un discurso televisado, el activo en el que podrías tener guardado los ahorros de tu vida.

En Estados Unidos, desde 2008, la Reserva Federal ha impreso aproximadamente el 70% de los dólares que han existido.[19] En otras palabras, cada dólar estadounidense que tenemos ha sido diluido a aproximadamente un 30% de su valor inicial, en términos

absolutos, durante los últimos 13 años. Los debates sobre el verdadero impacto del aumento de la oferta monetaria (M2) y los desacuerdos entre defensores de la Escuela Austríaca de Economía y la Teoría Monetaria Moderna también están fuera del alcance de este artículo.

Pero esto es una descripción objetiva de cómo opera el banco central de Estados Unidos: un grupo de siete individuos, designados como gobernadores de la Reserva Federal, se reúnen en privado y toman decisiones unilaterales sobre diluir, de manera significativa, el activo que actualmente sirve como moneda de reserva mundial.

La inmutabilidad inimitable de Bitcoin es un instrumento de libertad que ofrece una ruta de escape o "protección" frente a acciones de gobiernos y bancos centrales. El punto aquí es que la inmutabilidad solo se logra alcanzar con el ingrediente mágico de una verdadera descentralización sin compromisos. Si tienes que depender de fundadores, fundaciones, bases de datos centralizadas, o los actuales *stakeholders* ricos que pueden viciar el sistema a su favor, entonces la magia se pierde. Cualquier cosa sin una descentralización sin compromiso es una *blockchain* falaz dado que el resultado es un proyecto que no es inmutable, es más lento, más caro y menos eficiente que un competidor centralizado. Por ejemplo, un proyecto que puede ser conducido desde una compañía, con un equipo de administración formal, consejo de directores, accionistas y bases de datos centralizadas. Como señala Nick Szabo, "si vas a invertir en algo centralizado, deberías invertir en un sistema financiero con cientos de años de historia institucional detrás [es decir, mercados de acciones y bonos], no en sistemas centralizados pretendiendo ser descentralizados, o

con nociones de gobernanza del nivel de la novela *William Golding, El Señor de las Moscas*".[20]

Si aceptamos la inimitabilidad de la descentralización de Bitcoin, entonces tendría sentido construir la "economía digital" sobre Bitcoin, en vez de hacerlo en los miles de tokens que se disfrazan de activos monetarios. Estamos viendo pasos agigantados en este frente, con el desarrollo de las "capas superiores" de Bitcoin. Por ejemplo, RSK y Stacks son protocolos construidos sobre Bitcoin que pueden incorporar Finanzas Descentralizadas (DeFi) a la red de Bitcoin, utilizando Bitcoin como la capa de liquidación. En noviembre de 2021, Bitcoin adoptó una experimentación sustancial conocida como Taproot, que incrementará de manera significativa la maleabilidad y programabilidad del protocolo, desbloqueando el potencial para contratos inteligentes más complejos y menos costosos.

Así, Bitcoin será capaz de ofrecer muchas de las funcionalidades y programabilidad de Ethereum, por ejemplo. La diferencia principal será que la primera será construida sobre las bases sólidas de la inmutabilidad descentralizada, mientras que la segunda será construida, en gran medida, sobre las arenas de la falacia de la descentralización.

La inmutabilidad de Bitcoin a través de la descentralización inimitable es una herramienta democrática que le saca el poder a cualquier autoridad central y los dispersa a través de miles de nodos y mineros distribuidos en todo el mundo, unidos por una estructura de incentivos única diseñada para preservar la seguridad y escasez del activo. Esta invención única, dependiente de una secuencia que modifica paradigmas, es más profunda y de mayor alcance que el resto de la "industria cripto" combinada. Sería un error confundirlas.

“Y el fin de todas nuestras búsquedas

será llegar adonde comenzamos

Y conocer el lugar por primera vez”

-T.S. Eliot

Al comienzo de este artículo académico discutimos la perspectiva de un individuo sumándose a la industria cripto por primera vez, empezando con Bitcoin, y luego distrayéndose con otras criptomonedas en el camino. Si esa persona continuara su camino, desarrollando una curiosidad honesta en cada etapa, eventualmente cerrarán el círculo para llegar al mismo lugar en el que comenzaron: Bitcoin.

Referencias

1. Las referencias a "cadena de bloques" o blockchain en este artículo académico solo se refieren a cadenas de bloques públicas utilizando tecnologías distribuidas, y no cadenas de bloques privadas que no son relevantes en este tema.
2. Crypto.com, Measuring Global Crypto Users – A Study to Measure Market Size Using On-Chain Metrics, February 2021.
3. Saifedean Ammous, The Bitcoin Standard, John Wiley & Sons Inc., 2018.
4. Nick Szabo, Shelling Out: The Origins of Money, Nakamoto Institute, 2002. https://nakamotoinstitute.org/shelling-out/
5. Adam Back, Twitter. https://twitter.com/adam3us/status/1396200110351163395
6. Jack Dorsey, Twitter. https://twitter.com/jack/status/1393336348216631300
7. Robert Breedlove, An Open Letter to Ray Dalio re: Bitcoin, 2019. https://breedlove22.medium.com/an-open-letter-to-ray-dalio-re-bitcoin-4b07c52a1a98
8. Jeff Booth, The Price of Tomorrow: Why Deflation is the Key to an Abundant Future, Stanley Press, 2020.
9. Bitnodes https://bitnodes.io/
10. Nodes.com, 100.000 nodos de bitcoin https://nodes.com/news/bitcoin-nodes-total-100000-and-potential-vulnerabilities

11. Jonathan Bier, The Blocksize War: The battle over who controls Bitcoin's protocol rules, March 2021.
12. Michael Saylor, CEO of MicroStrategy ha descrito siete capas de seguridad que existen en los sistemas PoW. https://twitter.com/michael_saylor/status/1392904263123283975?lang=en
13. Mining map https://cbeci.org/mining_map
14. Andrew Poelstra, On Stake and Consensus, Nakamoto Institute, 2015 https://nakamotoinstitute.org/static/docs/on-stake-and-consensus.pdf
15. Parker Lewis, Bitcoin, Not Blockchain, Unchained Capital, 2019. https://unchained- capital.com/blog/bitcoin-not-blockchain/
16. Alyse Killeen, Bitcoin Conference 2021, Miami.
17. Angela Walch, Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems, 2019, Chapter in Crypto Assets: Legal and Monetary Perspectives (Chris Brummer, ed), Oxford University Press, 2019.
18. Johnny Jaswal, Ethereum 2.0 – Ether's journey from a security to a security, 2021. https://coingeek.com/ethereum-2-0-ethers-journey-from-a-security-to-a-security /
19. Federal Reserve Economic Data https://fred.stlouisfed.org/series/M2#
20. Nick Szabo, Twitter https://twitter.com/nickszabo4/status/1365852687875461122?lang=en
21. Satoshi Nakamoto, A Peer-to-Peer Electronic Cash System, 2008.

22. Lyn Alden, An Economic Analysis of Ethereum, Lyn Alden Investment Strategy
https://www.lynalden.com/ethereum-analysis/

23. Vijay Boyapati, The Bullish Case for Bitcoin, 2018.
https://vijayboyapati.medium.com/the- bullish-case-for-bitcoin-6ecc8bdecc1

24. Gary Gensler, Blockchain and Money, MIT Course Number 15.S12, 2018.

25. Casey, Crane, Gensler, Johnson, and Narula, 21st Geneva Report on the World Economy – The Impact of Blockchain Technology on finance: Catalyst for Change, 2018

26. James Park, When Are Token Securities? Some Questions from the Perplexed, Harvard Law School Forum on Corporate Governance, 2018.

27. Saifedean Ammous, The Bitcoin Standard, John Wiley & Sons Inc., 2018.

28. Nik Bhatia, Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies, 2020.

29. Jeff Booth, The Price of Tomorrow: Why Deflation is Key to an Abundant Future, Stanley Press, 2020.

30. James Davidson and Lord William Rees-Mogg, The Sovereign Individual, Touchstone, 1997.