Bitcoin: Untitled

△△

by G. R. Secco
ramiro@duck.com
ramirosecco.com

0. Abstract

Originalmente, este era un proyecto personal con el objetivo de entender en detalle el funcionamiento de Bitcoin, ese nuevo sistema destinado a revolucionar la industria digital. Grande fue mi sorpresa al percatarme que parecía haber ciertos aspectos cuyas respuestas eran incompletas, como mínimo. Mi primer instinto fue culpar a mi propia ignorancia. Paulatinamente, fui incorporando nuevos conceptos a mi caja de herramientas con el fin de interpretar mejor aquellas ideas que me eran esquivas. Estudié conferencias, paneles de expertos, y escuché a todos los gurús venerados por la industria. Sin embargo, sentía que cada vez entendía menos. Lo que más me desconcertaba acerca de Bitcoin era que parecía estar en permanente proceso de reparación.

Fue así como me fui adentrando en lo que parecía una novela de ficción. Una historia de traiciones y mentiras que oscurecía un mundo que se jactaba de ofrecer un nuevo paradigma en su manera de trabajar.

Finalmente, una nueva forma de entender Bitcoin se presentó ante mí y por fin todas las dudas fueron desapareciendo. En el camino, entendí que nada había sido un malentendido. Ni yo había interpretado mal, ni aquellas explicaciones originales eran simples errores. No podía ser casualidad que trece años después del lanzamiento de Bitcoin, su mismo código fuese literal y figurativamente manipulado para representar algo que ni había sido, ni era, ni iba a ser jamás.

La información aquí vertida, más que un trabajo académico, conforma un deber moral, y está dirigido a aquellas personas dispuestas a escuchar. Nunca fueron más ciertas las palabras de un viejo sabio: "*La ignorancia no es un derecho, sino un abuso*".

1. Introducción

En el año 2008, el entonces asesor financiero Bernie Madoff admitió a las autoridades llevar adelante la mayor estafa bursátil en la historia. Su estrategia era simple: pagar los dividendos pactados utilizando el dinero de nuevos inversores. A este sistema fraudulento se lo conoce como esquema de *Ponzi*. El arte de este fraude radica en encontrar el equilibrio entre nuevos inversores y dividendos pagados a los actuales.

En este caso, la verdad sólo salió a la luz cuando estalló la crisis financiera de 2008, y demasiados de sus inversores quisieron retirar su capital para enfrentar otras obligaciones. Sin crisis, es muy probable que el nombre de Madoff sería aún hoy sinónimo de honor y prestigio como lo era hasta entonces.

Lo cierto es que Madoff fue denunciado en múltiples ocasiones. Matemáticamente era imposible generar en los mercados bursátiles sus resultados. La evidencia era irrefutable. Es un caso especialmente interesante porque estafó a las personas más ricas del planeta. Había sobrado interés por descubrir un posible fraude.

En las estafas, el factor común es el abuso de la confianza depositada. Las grandes mentiras se construyen ladrillo a ladrillo y necesariamente cuentan con la complicidad involuntaria de los engañados. La clave en los esquemas de Ponzi se encuentra en el equilibrio. Encontrar el siguiente escalón de víctimas para propagar la mentira.

También es fundamental distribuir lo máximo posible los procesos internos. De esta manera, la información de la operación se diluye entre las partes. Cada cual piensa que la otra parte tiene la información que a ellos les falta. Es parte del manual de las sectas, donde su líder es la única persona con todos los fundamentos. De esta manera magnifican su aura omnisciente al mismo tiempo que socavan a sus seguidores.

La incapacidad para revelar un delito a este nivel sólo se puede explicar a partir de este tipo de distribuciones de poder e información. Las personas sentimos orgullo por nuestros logros y vergüenza por nuestras carencias. El mismo reflejo que evita que levantemos la mano en clase para admitir una duda, se hace presente de adultos en el cumplimiento de nuestras tareas. Aun cuando manejamos una posición que implica detectar e investigar, preferimos evitar cualquier escenario que pueda poner en evidencia nuestras carencias. Esto se hace aún más evidente cuando nos enfrentamos a una figura de autoridad, ya sea un gurú espiritual o el líder de una corporación. Incluso en muchos casos encontramos ambos roles en las mismas personas.

En el ecosistema de la tecnología e innovación, el universo de aquellos privilegiados que pueden dominar un área suele ser muy limitado. Requiere el dominio de ramas de la ciencia muy específicas dentro de las matemáticas, física y electrónica, por nombrar algunas. Sostener un fraude en el tiempo en estas áreas es prácticamente imposible. La mejor manera de hacerlo es dominando el discurso desde el comienzo, cuando el universo de potenciales victimarios es casi total. El caso de Bitcoin es único.

Es uno de los desarrollos tecnológicos más importantes desde la creación de Internet. Su inventor, la única persona con la capacidad real de entender sus mecanismos y las verdaderas posibilidades de esta herramienta, ha sido desterrado y vilipendiado por la industria.

Bitcoin ha sido tomado de rehén. El ecosistema de las criptomonedas es en igual parte cómplice y víctima. Como siempre, los principales perjudicados serán pequeños inversores atraídos por falsos profetas. Los verdaderos culpables seremos aquellos que abusamos de nuestra ignorancia.

2. El universo digital

El mundo se encuentra en un proceso de digitalización de las actividades humanas desde el nacimiento de las primeras computadoras. Esta forma de interactuar con nuestro ambiente y terceros fue posible gracias a un nuevo lenguaje habilitado tras la invención de los microprocesadores cincuenta años atrás.

2.1 1970: La transmisión de datos

Para entender Bitcoin, primero es necesario comprender cómo se transmite la información en las redes.

En todo sistema de comunicación electrónica, la información viaja a través de pulsos eléctricos de 0's y 1's. Una forma de código *Morse* llamado código binario. Para que esta comunicación sea posible, una serie de protocolos y reglas preparan el mensaje para su transmisión. Se le agregan encabezados y descripciones, siempre en código binario. De esta forma, los distintos actores del sistema pueden interpretar qué hacer con el mensaje en cada etapa del envío. Posteriormente, se descompone en pequeños paquetes que son enviados individualmente; y finalmente el mensaje se vuelve a unir una vez arribado a destino.

Un ejemplo de un sistema de comunicación que todos usamos es el correo electrónico. Su mecanismo es idéntico al del correo tradicional, pero en versión digital. Para enviar un paquete, escribimos ambas direcciones, y lo depositamos en una buzonera del correo. El destinatario se dirige a la oficina de correo y, mostrando sus credenciales, lo recibe. En vez de una oficina física, en el correo electrónico usamos una oficina virtual: los servidores de nuestro prestador de correo. Estos no son más que computadoras conectadas a Internet. Para acceder a nuestra cuenta de correo electrónico ingresamos dos claves, una pública y otra privada. Así accedemos a nuestra

buzonera individual alojada en estos servidores. La llave pública es tu nombredecorreo@mail.com, mientras que la privada, tu contraseña.

Tanto el sistema del correo tradicional como el electrónico, tienen sus propios protocolos para asegurar que los mensajes lleguen a destino. Mecanismos internos que garantizan el correcto envío y recepción de todos los paquetes. Estos pueden tomar la forma de códigos de barra, tickets, entre otros. Los usuarios desconocemos los específicos de dichos procesos. Sólo nos iinteresa que el mensaje llegue de manera rápida y segura.

2.2 1990: Internet y la revolución digital

En las primeras computadoras, la forma de compartir información entre ellas era mediante discos externos. Los más populares y prácticos eran aquellos cuya forma física dio lugar al ícono que universalmente sigue significando 'guardar'. También se podía conectar varias computadoras entre sí mediante cables, formando una 'red' cerrada. Internet es el sistema que permitió conectar computadoras mediante la línea telefónica que ya se encontraba instalada en todos los hogares y oficinas del mundo. Después de todo, no eran más que simples pulsos eléctricos ordenados viajando por cables.

En la década de 1990 nace la World Wide Web (más conocida por sus siglas "*www*" o simplemente Web), un protocolo de comunicación electrónica que simplificó de forma tal el uso de Internet que, al día de hoy, seguimos usando el mismo sistema. Los navegadores como Google Chrome o Mozilla Firefox nos permiten usan dicho protocolo Web de manera ordenada. Esta nueva forma de compartir información, sumado al lanzamiento de Windows 95 por parte de Microsoft, dio lugar a la primera gran revolución tecnológica. Significó un cambio fundamental en la forma de interactuar y compartir ideas. Fue un componente clave en la aceleración del proceso de globalización, derribando las fronteras físicas y fomentando una nueva forma de vincularnos.

El correo electrónico enseguida ganó terreno como alternativa al correo postal. Los buscadores sustituyeron al poco tiempo a las enciclopedias y páginas amarillas. Hasta entonces, las grandes compañías del mundo eran productoras de bienes o servicios físicos. Internet era un puente entre el mundo tangible y el digital. No había dudas de su potencial, pero restaba entender qué tipo de empresas iban a ser las que liderasen esta nueva revolución. Este escenario dio lugar a una burbuja especulativa en los mercados bursátiles vinculados a este tipo de empresas conocidas como Punto.com.

El problema alrededor de estas nuevas empresas tecnológicas era simple: la gran mayoría no generaba dinero. No vendían ni bienes ni servicios, sino que eran pura potencialidad. Eso no detuvo el flujo constante de dinero por parte de los inversores.

Este aumento en la demanda de acciones en tales compañías tenía el efecto automático de apreciar su valor. Las empresas multiplicaban su valor solamente en base al furor de estos inversionistas, quienes no querían perderse la oportunidad de tener una participación en las empresas del futuro. Estas variaciones generalizadas al alza de las acciones se traducían en ganancias para todos. Por supuesto, esto solo atraía más dinero y más inversionistas. Esto aumentaba aún más la cotización de dichas acciones, generando más ganancias y más inversiones. Este fenómeno, donde las acciones aumentan de valor por la simple confianza en que van a seguir creciendo, se conoce como burbuja especulativa. Esta dinámica duró lo que podía durar. Las cotizaciones bursátiles deben tener un sustento en el verdadero poder de una compañía de generar valor, siendo los ingresos el más simple indicador. En el año 2000, la realidad tocó la puerta y las acciones vivieron un desplome generalizado. Las burbujas pueden tardar meses o años en generarse, pero solo días en evaporarse. El mundo recordará – y olvidará- este episodio como la burbuja de las Punto.com.

Ese mismo año aparece Napster, un programa que permitía a los usuarios compartir archivos musicales entre sí de manera gratuita, ilimitada, y por supuesto ilegal. Nacía la piratería digital. El novedoso sistema utilizado para compartir archivos se conoce como "*Peer-To-Peer*" o "*P2P*". Este sistema establece una conexión directa entre las computadoras de dos completos desconocidos para compartir programas, documentos o música. En esa época, no existía forma legal de comprar una sola canción, se debían adquirir los discos completos. Al no existir un prestador de servicio que hiciera de intermediario, no había forma práctica de detener este flujo de archivos. Fue un escándalo. Revolucionó una industria donde hasta entonces la mayoría de las ganancias eran producidas por la venta de discos.

Mientras la industria musical invertía sus recursos y energías en declararle la guerra a la piratería, hubo quien tuvo una mirada diferente. Esta persona entendió que los usuarios no tienen interés en robar música. Por el contrario, prefieren pagar, pero solo por aquellas canciones que realmente les interesa; y hacerlo de forma práctica y segura. En el año 2001 Steve Jobs, fundador de Apple, presentó iTunes, la plataforma que permitía la descarga de música de manera legal y segura. Cambió la industria de la música para siempre. Las industrias se adaptan o desaparecen.

2.3 2000: Web 2.0, La Internet Dinámica

El desarrollo del ecosistema internauta y las nuevas formas de interacción entre sus usuarios, dio lugar a lo que se conoce como Web 2.0. Es la red que conocemos hoy en día. Ya no se trata solo de acceso; ahora se puede crear, compartir e interactuar entre distintas plataformas. Los celulares inteligentes pusieron una computadora en la mano de cada persona.

Es la era de las aplicaciones. Nace Uber, la aplicación de transporte que permite conectar choferes y usuarios. Spotify, que toma la posta de Apple, y ofrece acceso

musical ilimitado por un precio fijo. Lo mismo había hecho Netflix unos años antes con su catálogo de series y películas. Esta forma de hacer dinero se la conoce como "*Software as a Service*", servicios 100% digitales. Usuario, contraseña, y tarjeta de crédito.

También es la era de las redes sociales que desplazan al correo electrónico como forma de interacción social digital. Explotan Facebook, Twitter e Instagram. YouTube termina con el monopolio de los canales de televisión en la creación de contenido.

Facebook, pionera en la expansión masiva del concepto de red social; y Google, el buscador por defecto de los últimos veinte años, solucionaron el problema de las Punto.com. Al igual que ellas, durante años perdieron dinero. Incluso, al no cobrar por su uso, prácticamente carecían de ingresos.

La solución que encontraron fue convertirse en empresas de publicidad. Al recolectar información sobre nuestros hábitos y preferencias, lograron ofrecer un servicio de publicidad en línea a un precio accesible. Lo que hasta entonces era un lujo reservado exclusivamente para las grandes empresas, ahora estaba al alcance de las Pymes del mundo. Así es que nace el concepto de "*Consumer as a Service*". Nada es gratis en la vida, e Internet no es la excepción. Si no estás pagando por el producto, tú eres el producto.

2.4 La Digitalización del Dinero

El dinero es información. Cada país transmite esta información en su moneda local. Cualquiera sea la moneda, existen dos métodos de almacenamiento: físico y digital. Ambos son intercambiables entre sí. Cuando retiramos dinero de un cajero automático, estamos convirtiendo dinero digital en dinero físico.

El dinero físico requiere una protección física, por eso se almacena en bóvedas o cajas de seguridad. En cambio, el registro del dinero digital se mantiene en computadoras. Su almacenamiento requiere una protección especial para cuidar la integridad de los registros. Se deben establecer permisos especiales para el acceso y modificación.

La digitalización del dinero trajo consigo la ventaja de dejar de depender de registros en papel para almacenar la información de los clientes. La masificación de Internet introdujo la posibilidad a los bancos de ofrecer accesos en línea. Esto supuso no sólo visualizar la disponibilidad de fondos, sino también realizar operaciones desde la comodidad de la casa. Como contracara, esta facilidad de acceso se traduce en un aumento en el riesgo. No es lo mismo proteger una computadora sin acceso a Internet que una abierta a interacciones con el mundo exterior. Cuantos más puntos de acceso, más vulnerabilidades tiene un sistema.

Otra dificultad que presenta el sistema de banca online es la de garantizar una correcta actualización en tiempo real de los movimientos. El riesgo más común para evitar es que un usuario intente hacer el mismo movimiento dos veces antes que el sistema reconozca el doble gasto. Para ello, se deben procesar los movimientos de forma cronológica. Si bien puede sonar algo simple, en la realidad informática esto supone un gran desafío.

Digamos que desde una misma cuenta se intenta hacer el mismo giro exactamente al mismo tiempo, pero desde dos computadoras ubicadas en lados opuestos del mundo. La información debe viajar por los cables del mundo hasta llegar a los servidores más cercanos del banco. Estos a su vez deben cotejar todas las transacciones recibidas entre sí, ordenarlas y ejecutarlas, todo al mismo tiempo. No es una tarea simple, menos considerando los millones de transacciones recibidas por segundo, y el siempre latente riesgo de accesos ilegítimos. Por estas razones utilizamos terceros agentes de confianza, como bancos o tarjetas de crédito, para cuidar nuestro dinero electrónico. Estos establecen controles automáticos para evitar este tipo de situaciones, pero deben estar permanentemente monitoreando el sistema. Dichos controles, basados en estrictos y robustos sistemas de seguridad informática, tampoco están libres de ser objeto de ataques cibernéticos.

La complejidad en la seguridad informática se ha convertido en una distracción importante y por tanto una desviación de recursos, comprometiendo la eficiencia de la labor principal del sistema bancario.

2.5 El sistema financiero

En el sistema bancario, usamos cuentas para llevar un balance del saldo del dinero que tiene disponible cada persona. Con cada transacción, el saldo aumenta o disminuye. En Bitcoin en cambio, cada moneda lleva un registro de posesión. Sería como si los bancos tuviesen un registro de cada billete, con su número de serie y la cadena de posesión desde que el billete entró al sistema.

También puede ser útil imaginar que cada bitcoin es un cheque por un valor de '1'. Para transferirlo, el último beneficiario debe firmar al dorso (endoso) e incluir la identidad del nuevo titular.

Debemos recordar que el sistema financiero actual debe:

a) Confirmar los fondos.
b) Confirmar la identidad.
c) Velar por la integridad del sistema.

Dada la complejidad, cada movimiento de dinero implica un mayor costo de mantenimiento. A mayor volumen de transacciones, más sensible es el sistema y más

seguro debe ser al mismo tiempo. También es importante recordar que el verdadero espíritu del negocio de los bancos es utilizar parte de los fondos depositados para dar préstamos -cobrando intereses con el otorgamiento de estos - y realizar inversiones con el dinero.

3. Bitcoin, el sustituto del efectivo

Bitcoin es un nuevo instrumento informático que permite la transmisión de valor en formato digital.

El documento original de Bitcoin o 'White Paper' se titula: *Bitcoin: A Peer-To-Peer Cash System [1]*. Es decir, un sistema de transferencia de *efectivo* entre pares.

Es un nuevo tipo de dinero. Un híbrido entre el dinero electrónico y el efectivo. Fue concebido para cumplir la función del dinero físico, pero en vez de utilizar billetes, se intercambian monedas virtuales. A estas monedas virtuales nos referiremos a partir de ahora como *bitcoins* en minúscula para diferenciar del sistema *Bitcoin,* en mayúscula.

El sistema basa su funcionamiento en un registro público donde se ingresan todos los movimientos de manera cronológica. El programa funciona bajo un nuevo sistema de almacenamiento y distribución de la información llamado *Blockchain* o cadena de bloques. Su mantenimiento es llevado a cabo por un grupo de personas a las que se conoce como *mineros*.

En capítulos posteriores explicaremos en detalle estos términos y su funcionamiento.

Para lograr entender qué es Bitcoin y cómo puede cambiar la interacción con el dinero es fundamental olvidar todo lo que creemos saber o entender respecto a este sistema. La mayoría de los conceptos y explicaciones presentadas en este documento contradicen la información disponible en prácticamente todos los sitios accesibles.

3.1 Bitcoin, el origen

El 31 de octubre de 2008 es publicado el White Paper original donde se describe el objetivo y la tecnología aplicada para conseguirlo. El documento lleva la firma de Satoshi Nakamoto, un pseudónimo elegido por su verdadero autor, quien prefirió permanecer en el anonimato.

El software de Bitcoin fue lanzado en enero de 2009. Satoshi se mantuvo como una figura activa. Interactuaba en línea con quienes mostraban interés en el sistema. Al principio, no distaba demasiado de cualquier proyecto escolar. Lo más probable era que fuera un experimento interesante, pero termine en un fracaso. Después de todo, estaba intentando solucionar un problema que los especialistas informáticos llevaban más de veinte años intentando resolver. Realizó ajustes y se corrigieron errores y debilidades menores identificadas en el software. En este proceso, Satoshi, siempre anónimo, fue sumando algunas de estas personas como colaboradores.

Inevitablemente, Bitcoin atrajo, al poco tiempo, usuarios que lo vieron como una oportunidad ideal para llevar a cabo actividades ilícitas. Esta no es una buena idea ya que, como veremos más adelante, todos los movimientos son permanentemente registrados en un registro público. Además, eventualmente es necesaria una identidad para convertir las monedas digitales a dólares. En 2011 nacía Silk Road [2-3], un mercado de drogas y demás productos ilegales, que utilizaba Bitcoin como moneda de pago entre los usuarios. Fue entonces que la moneda virtual empezó a ganar popularidad y su uso se extendió más allá del pequeño círculo de personas que conocía el sistema.

Con el número de usuarios activos intercambiando bitcoins en alza, también lo hizo su cotización. Esto fue recibido con alegría y entusiasmo por los usuarios pioneros que tenían monedas guardadas. Por su parte, Satoshi mostró reparos al respecto, notando que podía ser un riesgo atraer público indeseado y al mismo tiempo ganar mala prensa. Incluso en 2010, cuando desde el WikiLeaks de Julian Assange manifestaron que estaban considerando aceptar donaciones en la moneda virtual, Satoshi pidió públicamente que no lo hagan ya que podría destruir el sistema [4].

Tal era su preocupación, que en diciembre 2010 se retira de los foros de conversación y comienza a delegar el proyecto. En su último acto, otorga permisos sobre el software a Gavin Andresen, uno de los primeros colaboradores.

3.2 Bitcoin post-Satoshi

El objetivo era que Bitcoin cumpliese su cometido final de ser efectivo digital. Para ello, debía ser capaz de procesar cientos de miles de transacciones por minuto. La dificultad radicaba en que, a medida que aumentaba su uso, se acumulaban muchísimas transacciones juntas.

En esta instancia lo único que debemos entender sobre el funcionamiento de Bitcoin es que las transacciones se agrupan y registran en lo que llamamos '*bloques*'. Cada bloque no es más que una entrada en un libro donde se anotan todos los movimientos de bitcoins.

La simple intuición nos dice que, si los bloques son más grandes, se pueden ingresar más transacciones por bloque. El tamaño de dichos bloques había sido

momentáneamente limitado por Satoshi luego de ser advertido de posibles riesgos de ataques informáticos. Estos riesgos eran reales en los primeros años donde el sistema era sostenido por pocas personas. Satoshi no podía haberse imaginado que este iba a ser el centro de una de las disputas más grandes respecto a Bitcoin, la cual se encuentra en plena vigencia al día de hoy.

Andresen, ahora a cargo, tenía buenas intenciones, pero cometió el error de tomar Bitcoin como un proyecto colaborativo. Le entregó poder a más desarrolladores, e incluso estableció un sistema de votación para que los mineros aprueben cambios. Este fue su segundo error. Los mineros, como veremos más adelante, no toman decisiones, su trabajo es puramente técnico. Ellos no aprueban transacciones, solo disputan una competencia de manera honesta. El sistema está diseñado para que el protocolo sufra la menor cantidad de modificaciones posibles. Nunca podría funcionar un sistema de transmisión de dinero si las reglas del juego pueden ser cambiadas en cualquier momento.

3.3 Bitcoin: Guerra Civil

En 2015, Andresen presentó un proyecto a la "comunidad" para aumentar el tamaño de los bloques de manera paulatina. Por razones que serán claras a continuación, no contaba con el apoyo de la mayoría de los desarrolladores que él mismo había introducido [5-8]. Lo que sostenían quienes se oponían era que un aumento en el tamaño de los bloques llevaría a que el sistema sólo pudiera ser sostenido por grandes grupos de capital; lo que en la práctica llevaría a un nuevo tipo de centralización de Bitcoin. Para este grupo, el tamaño debía mantenerse para que cualquier persona desde una computadora estándar pueda colaborar en el mantenimiento del sistema. La propuesta de Andresen fue descartada, y al día de hoy, el límite sigue en pie.

Lo que este mismo grupo omitía es que muchos de los integrantes se habían sumado a un proyecto privado llamado Blockstream.

Blockstream propone distintas opciones para solucionar las limitaciones de Bitcoin derivadas del límite en el tamaño de los bloques. Han creado abominaciones técnicas con nombres rimbombantes como "Lightening Network" o "Liquid". A grandes rasgos, su plan es crear una blockchain paralela que agrupa y concilia muchas transacciones, pero administrada y mantenida por Blockstream. Las comisiones entonces irían para esta empresa, en vez de pasar por los intermediarios "oficiales" que serían los mineros. En el punto 5. explicaremos en detalle el funcionamiento real de Bitcoin y esto será más claro.

Blockstream es uno de esos proyectos tecnológicos con misiones y objetivos ambiguos pero que básicamente se creó para ofrecer sistemas que faciliten y mejoren el funcionamiento de Bitcoin. El problema es que esa era precisamente la tarea que

debían estar llevando a cabo los desarrolladores de Bitcoin. Este punto es clave para entender lo que está pasando hoy en el ecosistema.

Los mismos individuos a cargo de implementar mejoras en el sistema, los mismos que habían decidido que Bitcoin era un proyecto 'comunitario', fundaron una empresa -con fines de lucro- con los mismos objetivos que ellos decían perseguir desinteresadamente. El mismo grupo que sigue intentando y fracasando siete años después. El mismo grupo que en 2016 realizó un cambio en las reglas originales que ellos mismos decían respetar [9]. Si lo que se quería evitar era una centralización del sistema, crear una corporación que hiciera de intermediaria en las transacciones suena, como mínimo, inconsistente.

Tengamos en cuenta que estas personas controlaban las propuestas que se iban a considerar, todos los aspectos de comunicación en Bitcoin, e incluso censuraban conversaciones en foros públicos como Reddit. También hay que considerar que entre sus inversores se encuentran el CEO de Twitter, Jack Dorsey y varias personalidades y grupos relacionados con el mundo financiero. Con esto no es mi intención señalar que se trata de una estrategia de los bancos o tarjetas de crédito por tomar o mantener el control del mundo de las finanzas. Parte de la estrategia que siguen los grandes fondos es invertir en empresas tecnológicas que puedan resultar beneficiosa. Blockstream es una de miles de empresas donde han invertido estos grupos.

La verdadera corrupción radica en los desarrolladores de Bitcoin (técnicamente ahora estamos hablando de una deformación de Bitcoin llamada *BTC*). Tanto aquellos que son parte de Blockstream como aquellos que no lo son y no denuncian esta realidad están defraudando al público. En ninguna otra organización sería permitido este flagrante conflicto de intereses. Si trabajan como desarrolladores de un servicio abierto y público, no pueden al mismo tiempo trabajar para una empresa cuya única razón de existir es su incapacidad para realizar sus funciones en el primer lugar. Esto, sin entrar en la discusión real de fondo respecto a quién los contrató y con qué autoridad. También es necesario señalar el engaño que suponen personalidades como Jack Dorsey, firme y vocal impulsor de BTC desde su posición de poder, aunque no tan vocal a la hora de expresar su posible conflicto de intereses.

Cabe aclarar que toda esta información es de público conocimiento hace años. Los detalles de las inversiones no siempre son muy transparentes, pero eso es algo normal cuando las empresas aún son privadas. Lo que sí es llamativo es la poca repercusión que tienen estos eventos. En gran medida se debe a la falta de comprensión respecto a todo el mundo de las criptomonedas. Parte del objetivo de este trabajo es presentar un panorama real de los distintos elementos que lo componen.

Por último, es fundamental resaltar que ninguna de estas personas inventó Bitcoin. Tampoco fueron fundamentales en su desarrollo. Todo el funcionamiento del sistema explicado en este documento se desprende del White Paper original escrito por Satoshi Nakamoto.

3.4 La Separación

Como explicaremos más adelante, un sistema de blockchain como Bitcoin se mantiene por mineros que llevan el registro de los bloques con las transacciones. Para ello, los mineros descargan un programa que conecta con dicho registro. Si un número suficiente de mineros mantiene el sistema estamos ante una cadena de blockchain operativa. En este documento nos hemos enfocado en la cadena original que es Bitcoin, pero pueden existir diversas cadenas, cada cual con sus reglas.

Existe además un fenómeno que se conoce como '*Fork'* o 'tenedor', donde una misma cadena se separa en dos. Sería como una bifurcación de caminos, donde un grupo empieza a seguir unas reglas y el otro, otras. Hasta ese momento, el pasado es exactamente el mismo; lo que cambia son las reglas a partir de ese momento. Un paralelismo hipotético sería imaginar que EE.UU. se divide en dos países y cada uno mantiene el dólar como su moneda, pero a partir de la fecha de división cada cual maneja su emisión y reservas bajo sus propias reglas. El resultado sería dos monedas que siguen funcionando, pero independientes entre sí, cada cual con su cotización.

Luego de un cambio importante en las reglas implementado en 2016 (conocido como '*SegWit'*, que en los hechos fue un tipo de '*Fork*'), un grupo en desacuerdo realizó una de estas bifurcaciones. Bitcoin así se dividía en dos: Bitcoin Core (BTC), y Bitcoin Cash (BCH).

Bitcoin Core, o BTC desde ahora, es el Bitcoin más conocido. Es aquel cuya cotización se repite en los medios; y es considerado por toda la comunidad como 'el' Bitcoin. Mal llamado el 'original', es el mismo que fue tomado de rehén por un grupo de desarrolladores. Bitcoin Cash, por su parte, se volvió a bifurcar, y uno de sus producidos es la cadena llamada Bitcoin Satoshi Vision. Esta última, apodada BSV, busca seguir el verdadero espíritu de Bitcoin como instrumento de intercambio barato y eficiente. Tiene otra particularidad que la hace una de las monedas menos conocidas y respetadas del ambiente: el hombre detrás de ella es el mismísimo Satoshi Nakamoto.

3.5 Satoshi Nakamoto

Cualquier persona con un mínimo conocimiento del mundo de las criptomonedas te dirá que su verdadera identidad es un misterio; nadie lo sabe y probablemente nadie lo sepa jamás. La misma respuesta obtendrías tras consultar cualquier medio especializado, formal o informal. Están equivocados. Su verdadero nombre es Craig S. Wright, un ciudadano australiano con una extensa trayectoria en las áreas de ciberseguridad, auditoría y finanzas. Su historial académico incluye al menos dos

doctorados y una veintena de títulos profesionales, además de decenas de certificados. Todos ellos pueden ser consultados en su página web [10].

Las revistas Wired y Gizmodo revelaron su identidad en el año 2015 [11-12] tras recibir información anónima. Wright admitió ser el cerebro detrás de Bitcoin, pero, al no conformar el ideal imaginario construido, la "comunidad" lo rechazó. Así es, la misma comunidad que modificó el protocolo original y que durante años fracasó en hacer de Bitcoin una herramienta práctica para el intercambio de valor, determinó que esta persona era un impostor. Inversores, medios formales e informales y "expertos" de todo el mundo coincidieron con ellos. Era el 2015 y el universo que comprendía los interesados era sensiblemente pequeño. Siete años después, tanto poderosos medios de comunicación como grandes fondos de inversión siguen negando su identidad.

Una de las razones esgrimidas para sostener que Craig Wright no es Satoshi es debido a que él se niega a utilizar la clave asociada a las cuentas de Satoshi para realizar una demostración pública. Por un lado, no es del todo cierto esto, ya que lo hizo en privado a personas como Gavin Andresen y al menos un periodista de la BBC. Pero lo más importante que Wright quiere demostrar es que la posesión de las llaves no se traduce necesariamente en titularidad. Del mismo modo que tener las llaves de una casa no lo convierten a uno automáticamente en su dueño. La prueba absoluta e irrefutable no puede descansar en el acceso. Bitcoin no garantiza la posesión ni sustituye las leyes reales creadas por las autoridades de cada país. Bitcoin representa un registro, nada más. Entiendo que esta puede tomarse como una postura conveniente para un hipotético impostor, pero basta con leer y escuchar lo suficiente a Craig Wright para llegar a la conclusión inequívoca de que él es el creador del sistema. Aún antes de revelarse su identidad Craig figura en conferencias mostrando un dominio tal del sistema que al día de hoy no puede ser equiparado.

También vale la pena destacar que Craig Wright no le debe una explicación a la comunidad, ni a nadie. Él no pidió ser reconocido como el creador de Bitcoin, sino que fue obligado a aceptarlo. Bitcoin es un sistema que debería funcionar independientemente de quién lo creó. Es una herramienta al mundo.

Por desgracia, los poderosos intereses existentes actualmente han forzado un circo mediático lleno de inconsistencias. No se trata sólo de malas intenciones, existe un aparato instalado de características mafiosas cometiendo delitos impunemente.

Para entender el rechazo que despierta Craig Wright en el mundo cripto, es importante entender la profundidad del falso relato que se ha fabricado en torno a Bitcoin, su historia, y su potencial.

4. Bitcoin, efectivo digital

El principal aporte práctico que ofrece Bitcoin es la posibilidad de realizar micropagos a través de Internet. Es algo que suena simple y de menor impacto, pero tiene la capacidad de revolucionar la forma en cómo interactuamos con el mundo digital.

Hoy la única forma de hacer pagos online es mediante transacciones bancarias o tarjetas de crédito. El promedio de comisiones pagadas por transacción a las tarjetas de crédito en 2021 en EE.UU. es del 2% [13-14]. Esta cifra puede representar el margen de ganancia de muchas empresas. A nivel económico, un ahorro en dichos costos tendría un efecto significativo en las pequeñas y medianas empresas, ayudando especialmente a dinamizar economías emergentes.

Tomemos por ejemplo un buscador como Google. Como ya explicamos, al ser gratuito, sus ingresos dependen de la publicidad y explotación de datos. Con Bitcoin, Google podría cobrar a los usuarios centavos de dólar por cada búsqueda. Hoy esto es inviable económicamente por los costos mínimos de transacción de cualquier tarjeta de crédito. Similar caso sería el de YouTube, que podría cobrar cifras minúsculas por cada reproducción.

Un sistema así puede significar también el fin del correo basura o spam. Al introducir una barrera económica al envío masivo de correos, ya no sería tan atractivo llenar casillas enteras con contenido basura.

El comercio tradicional también puede verse beneficiado con una herramienta segura y práctica de poder comprar y vender de manera más fluida y con menores costos asociados que hoy no agregan valor.

En la escala internacional, puede servir de impulso especialmente en la prestación de servicios al exterior, reduciendo considerablemente costos y fricciones que hoy limitan el desarrollo de muchas economías.

Para poder concebir estos casos y es buena idea entender de qué hablamos cuando hablamos de Bitcoin y la forma de operar sus monedas virtuales.

4.1 Conversión a dinero y cotización

Los bitcoins se almacenan en billeteras electrónicas. No es importante su funcionamiento, basta con imaginarlas como una aplicación de celular donde se lleva el registro de nuestras monedas virtuales. Como es un sistema abierto, cualquier desarrollador puede crear estas aplicaciones y los usuarios pueden elegir la que más les convenga.

Todos los bitcoins en circulación provienen de premios previamente obtenidos por los mineros que mantienen el sistema. Al principio, al no haber casi transacciones

ni competencia entre mineros, el minado se podía realizar con cualquier computadora. A medida que la moneda fue ganando tracción, se empezó a requerir una mayor inversión para realizar esta tarea, y por lo tanto los mineros necesitaron vender sus bitcoins para pagar cuentas y demás gastos asociados.

Así es cómo fueron surgiendo los primeros cambios o 'exchanges'. Al principio eran sitios informales donde no existía realmente una cotización. A medida que fue creciendo el mercado y desarrollando negocios a su alrededor, el sistema fue cobrando cierta formalidad. La realidad es que un cambio debería funcionar como cualquier otro. Son agentes fiduciarios que intermedian en un intercambio de valor. En un escenario debidamente regulado deberán registrar la identidad de los usuarios para determinadas operaciones y ejecutar transacciones de acuerdo con la ley que los regule.

En el corto plazo, Bitcoin es una herramienta ideal para hacer pagos pequeños. Los precios no se van a fijar en Bitcoin, sino en las monedas locales, y a partir de la cotización del momento se hará la conversión y pago mediante bitcoins. En el caso de Google, podría definir sus precios en dólares y cobrar su equivalente en bitcoins. De igual forma, un comerciante en cualquier parte del mundo puede vender sus productos en su moneda local y cobrar en la moneda virtual.

En general, los precios de los bienes son el resultado de una cadena de costos que se van agregando. Para medir y determinar dichos costos, la mejor medida que tenemos son las monedas de cada país.

No importa la cotización del bitcoin, importa que cumpla la función de transmisión de información.

No es sensato pensar que hoy alguien va a almacenar en su celular el equivalente al valor de una casa en bitcoins, por lo menos en el mediano plazo. Mucho menos intentar hacer una compra de esa naturaleza así. Hoy en día podemos tener acceso a nuestras cuentas bancarias desde cualquier computadora, pero solo para darle órdenes a la entidad que tiene nuestro dinero.

4.2 Riesgos

La seguridad de todo sistema depende del nivel de garantía que se requiera. Por lo tanto, si se trata de efectivo digital, la seguridad debería ser mayor o igual al efectivo tradicional.

Más adelante explicaremos el sistema que hace a Bitcoin extremadamente seguro a la hora de garantizar la fidelidad de la información desplegada.

Como ya dijimos, los bitcoins se almacenan en billeteras electrónicas. Estas no

son más que programas de computación que se integran al sistema de Bitcoin de manera fluida. Las mismas pueden ser privadas, pero eso no significa anónimas. Al igual que una cuenta de banco, se puede requerir identificación y registro. La diferencia es que se pueden establecer registros legales donde sólo mediante determinados permisos se pueda acceder a determinada información. Esto es posible hoy, pero la diferencia es la transparencia que ofrece el sistema de Bitcoin. Cada acceso permitido generaría un registro público, asegurando mayores garantías a las partes.

4.3 ¿Son reversibles las transacciones?

En un caso de estafa, un juez podría ordenar que una transacción sea devuelta. Las transacciones no pueden ser borradas ni manipuladas, pero sí pueden ser revertidas. Lo importante es que todo lo acontecido queda registrado. Para ejecutar la orden del juez se podrían usar determinados permisos especiales que servirían para ejecutar dichas órdenes. Claro está que esto no sería práctico para cualquier tipo de importe dada la complejidad que requeriría un proceso judicial de esta naturaleza y su posterior ejecución.

4.4 ¿Bitcoin va a substituir a los bancos?

No. Si bien es cierto que se podría utilizar como alternativa a algunos servicios bancarios, eso no es lo mismo que decir que pueden sustituir la función que realizan los bancos. No es razonable imaginar un mundo donde tengamos cientos de miles de dólares en una computadora en nuestra casa.

Además, esto supone no entender la dinámica de la economía y el rol del sistema financiero en la salud de esta. Que el sistema actual esté pervertido en muchas de sus funciones originales no significa que desmantelarlo sea prudente y muchos menos viable.

Los intermediarios financieros cumplen además un rol fundamental a la hora de evitar el lavado de activos. Para ello deben seguir las provisiones conocidas como *KYC (know your customer) y AML (anti-money laundering)*. Esto no puede automatizarse por completo, sino que se deben asignar responsables, existiendo de hecho regulación a nivel de cada país sobre determinados controles y procedimientos a seguir para ejecutar estos procesos.

Bitcoin es un refuerzo a todo el sistema. Los bancos pueden volver a ser bancos. Conocer a sus clientes. Captar los fondos de aquellos con capacidad de ahorro, y ofrecer préstamos e invertir en proyectos que creen valor.

4.5 ¿Se puede transmitir otro tipo de información?

Sí, Bitcoin es un programa de computadora. En su más mínimo nivel de complejidad mueve monedas digitales. Estas monedas digitales pueden representar otros activos u otras formas de información. También se pueden escribir programas enteros que utilicen el sistema de transferencia de información para cumplir sus funciones.

5. Blockchain: la tecnología

En la contabilidad, los movimientos se registran en lo que se conoce como Libros Contables. El principal es el Libro Diario. En él se registran los hechos económicos de forma cronológica. A diferencia de una simple caja registradora, donde se registran ingresos y egresos, los libros contables llevan un registro también de bienes, derechos, y obligaciones. Esta información correctamente ordenada y expuesta se usa por las empresas para medir su salud económica y su evolución en el tiempo.

Una particularidad del sistema contable es que no se pueden editar registros una vez ingresados. Si, por ejemplo, se registra una venta por error, corregirlo significa registrar el mismo movimiento, pero al inverso. A este movimiento se le conoce como ‘’extorno’. Las reglas contables, para asegurar que se cumpla con esta regla, mandan que en cada hoja se debe ingresar un valor proveniente de la hoja anterior. De esta forma, todas las hojas quedan concatenadas. Intentar cambiar un sólo número, obligaría a tener que modificar todas las hojas posteriores.

Bitcoin se inspira en el Libro Diario contable, e introduce un registro similar, pero en formato digital y público. A este sistema se le llama *Blockchain*. En vez de hojas, usamos bloques. El resto es el mismo principio. Los bloques se registran en fila, uno a continuación de otro, encadenados mediante un valor asociado al bloque anterior. Cualquier intento de manipulación, rompe automáticamente la unión de la cadena.

Para simplificar su comprensión, podemos imaginar que cada bloque es una nueva transacción, por lo que la blockchain es una cadena donde cada eslabón que se agrega corresponde un movimiento de monedas. En realidad, cada bloque puede contener cualquier número de transacciones juntas, siempre y cuando sean válidas.

5.1 Identidad y Llaves Públicas / Privadas

Una de las fortalezas del sistema es que todas las transacciones son públicas. Cualquiera puede ver los movimientos, no así la identidad de las personas. El Libro Diario, con todos los movimientos, está a disposición de cualquier interesado. Esto no sólo asegura transparencia, sino que también hace imposible cualquier tipo de intento de destrucción de este.

En el sistema bancario tradicional se usan cuentas y la información se transfiere encriptada, de modo tal que sólo aquellos con acceso puedan descifrar su contenido. En Bitcoin, las transacciones son públicas y la información no viaja encriptada. Por esta razón, se debe usar un sistema alternativo para validar la identidad de las partes, proteger su privacidad y al mismo tiempo ofrecer garantías de seguridad.

Así es como entra en juego la famosa criptografía. En vez de un número de cuenta, se utiliza un código denominado *llave pública*. Para recibir bitcoins, basta compartir la llave pública. Una buena forma de imaginar este sistema es pensar en estas llaves como ranuras donde depositar sobres con valores. Un aspecto esencial de este sistema es que se puede disponer de una infinidad de estas ranuras o llaves públicas con una particularidad: todas se abren con una misma clave, la *llave privada*. Podemos imaginar esta como una llave maestra física que permite abrir cada una de nuestras cajas de seguridad. Por esta razón es que decimos que las llaves públicas se derivan de la llave privada.

En el punto 2.5 dijimos que la forma de compartir bitcoins podía ser comparada al sistema de endoso de cheques. Esto es así porque eso es lo que efectivamente hace la llave privada. En los hechos funciona como una firma digital. La famosa criptografía lo único que hace es confirmar que la 'firma' sea la correcta. Es decir, verifica que la llave privada sea la asociada a la llave pública que se usó para depositar los fondos. Cuando hacemos uso de nuestras monedas virtuales en realidad estamos reenviando los valores hacia otras cajas de seguridad.

Este complejo mecanismo de llaves no debería ser entendido por ningún usuario. La idea real no es que sepamos nuestras llaves ni corramos el riesgo de ingresar un dígito mal y perder nuestro dinero. Está diseñado para funcionar automáticamente con billeteras electrónicas producidas por desarrolladores privados. En ellas se crea un nombre clave, como puede ser @Craig_22, y nuestra firma es una contraseña. A nosotros como usuarios sólo nos debería importar que las transacciones se hagan.

Es importante señalar en esta instancia que el uso de llaves públicas no significa la imposibilidad de establecer registros de identidad. Precisamente, las billeteras electrónicas pueden crearse para establecer controles de identidad, independientemente de las llaves utilizadas. Lo que Bitcoin permite es que la cuenta @Craig_22 esté asociada a un individuo registrado y pueda traspasar fondos a la cuenta de @Amazon, también debidamente registrada. Todo esto sin que Amazon tenga que saber el sexo, edad, estado civil ni ninguna otra información de carácter personal del usuario. Tampoco tendría que reportar operaciones superiores a determinados montos, ya que esa información se podría compartir automáticamente con las

autoridades. Se puede cumplir con todos los requisitos legales y al mismo tiempo contar con un merecido nivel de privacidad.

Resta explicar aún cómo resolver el orden cronológico de las transacciones. Para ello, se implementa un "juego" en el que se compite por un premio. A esta competencia se le llama '*Proof of Work*' o '*Prueba de Trabajo*', y a quienes participan de ella se les conoce como '*mineros*' o '*nodos*'.

5.2 Proof of Work, el soporte

Bitcoin es, al fin y al cabo, un programa informático. Como todo programa, tiene un conjunto de reglas o protocolos. Al no existir una organización formal detrás, el protocolo incluye un sistema de incentivos establecidos como forma de 'premio' a quienes lo mantienen funcionando. Para ganar un premio todo lo que hay que hacer es agregar un bloque al sistema. La trampa es que sólo puede haber un ganador por bloque. Esto es porque, como dijimos antes, los bloques tienen que ser agregados uno detrás del otro para asegurar un orden en las transacciones y evitar fraudes.

Quienes participan agregando bloques y recolectando recompensas se los conoce como *mineros*. Cualquier individuo o grupo de personas puede ser un minero. Para ello deben descargar un programa informático que propone una competencia entre ellos. Esta competencia o juego es la que permite el mantenimiento del sistema.

5.3 El Juego

Los mineros son quienes mantienen el sistema funcionando. Para hacerlo necesitan computadoras y conexión a Internet. Su tarea es competir en un juego que consiste en resolver unos puzzles para así ganar bitcoins como recompensa.

Para entender la competencia es más fácil imaginarnos un proceso manual donde solo contamos con un teléfono, lápiz y papel.

En este hipotético caso, trabajamos para la oficina encargada de registrar transacciones. Nuestra tarea consiste en estar alerta al teléfono donde se reciben transacciones. Cuando recibimos una, la anotamos en un pedazo de papel.

En primer lugar, debe cumplir dos requisitos formales:

1- Contiene el valor del bloque anterior. ✓

2- La transacción fue correctamente validada por la llave privada correcta. ✓

Cumplidos dichos requisitos, llevamos el papel al Registro para su ingreso. El funcionario a cargo procede entonces a romper el papel en mil pedazos. El juego consiste en volver a armar el picadillo de papelitos. El desafío se hace particularmente difícil por el hecho de que debemos hacerlo en la oscuridad absoluta. La única forma de ganar es probar combinaciones y presentarlas al Registro hasta dar con la correcta. Pero el desafío es aún mayor si consideramos que cualquiera puede llevar su hoja de papel y jugar al mismo tiempo.

Cabe señalar, que cada minero puede estar intentando procesar distintas transacciones, por lo que los puzzles pueden ser distintos entre sí.

El primero en resolver su puzzle, recibe la confirmación por parte del funcionario, y gana el premio. Los otros jugadores deben correr a buscar un nuevo papel que contenga el nuevo valor del ahora último bloque, y empezar de nuevo.

Al juego se lo conoce como *prueba de trabajo*. El objetivo del mismo es confirmar, como lo dice el nombre, que el minero ha invertido tiempo y recursos en resolver el puzzle. El proceso real es similar, pero utilizando computadoras en vez de papeles físicos. Estas no resuelven ecuaciones ni problemas matemáticos complejos. Simplemente juegan a adivinar un número. Esta arbitrariedad es la que imposibilita que un minero pueda hacer trampa. Para aumentar las chances de ganar se necesitan más computadoras para probar más números. No existe árbitro ni juez más que las propias reglas, que obligan a los jugadores a un juego limpio.

5.4 Las Reglas

Cada minero lleva su propia copia del Libro Diario (en adelante, lo llamaremos el "Libro").

Para ser un minero oficial, y por lo tanto ganar el derecho a escribir bloques en el Libro, debemos en primer lugar aceptar recibir y transmitir transacciones entre todos. Es decir, los mineros deben estar en constante comunicación entre ellos y con el resto del mundo. Es de su interés hacerlo de todas formas, porque sino no tienen forma de estar actualizados respecto al último bloque ni las próximas transacciones entrantes. Además, cada minero quiere publicar antes que el resto sus puzzles resueltos, por lo que es su interés maximizar la comunicación entre sí. En el ejemplo anterior, tendríamos que estar todo el tiempo llamando por teléfono a los demás mineros compartiendo tanto las transacciones recibidas como los puzzles resueltos. Esto requiere una gran conexión a Internet que permita maximizar la eficiencia de esta tarea. Esta es otra fortaleza implícita dentro del sistema. Un minero no puede estar escondido en medio de una selva tropical para cumplir su tarea.

La siguiente obligación es aceptar y agregar a su copia del Libro bloques correctos. No vale rechazar puzzles que cumplan los requisitos.

La última regla es que se toma como válido el Libro que tenga más bloques. Si un minero quiere hacer trampa e ignorar las transacciones de sus colegas, a nadie le importa, porque su Libro deja de ser de referencia para los demás. Puede pasar sí que dos mineros reciban dos bloques diferentes e ingresen de buena fe en sus registros el que ellos consideran correcto. Las reglas establecen entonces que se sigue jugando, cada cual con su Libro. Dijimos que la regla establece como válido el Libro que tenga más bloques. De esta forma, al poco tiempo de seguir jugando, el propio sistema se termina decantando por el Libro que fue continuado por más mineros.

En la génesis de Bitcoin, se crearon 21 millones de bitcoins para ser distribuidos a los mineros. Todos los bitcoins que existen hoy en circulación son el fruto de premios recibidos por los mineros. Ser minero implica aceptar las reglas del juego, por lo que legalmente se puede considerar como un contrato unilateral. Un buen ejemplo para entender este tipo de contrato es el de un aviso en un periódico ofreciendo una recompensa a cambio de encontrar una mascota perdida. Cualquiera puede aceptar el contrato y, en caso de encontrar al animal, tienen derecho a cobrar la recompensa ofrecida.

5.5 Trampas

Como ya explicamos, los mineros se valen de computadoras para los puzzles. Las computadoras no tienen forma de resolver de manera lógica o inteligente el problema. La única forma de maximizar las chances de ganar es usando más computadoras que lo único que hacen es probar más respuestas.

Es importante destacar que se usan más computadoras, y no mejores. Por esto, hoy en día los mineros forman lo que se llaman *granjas*. Estas granjas no son más que galpones repletos de computadoras todo el día probando soluciones. Esto se traduce en cientos de miles de dólares en equipamiento, energía eléctrica y personal.

Intentar forzar transacciones falsas es imposible por dos razones. En primer lugar, deben contar con la firma digital que hace la validación criptográfica. En segundo término, tenemos que pensar en la economía implícita del sistema. Un minero malicioso, que ingrese un bloque inapropiado, debería ganar en absolutamente todos los puzzles presentados consecuentemente para seguir teniendo la mayor cantidad de bloques. Esto no sólo es imposible estadísticamente, sino que además significaría violar las reglas del juego. Esto significa romper un contrato, y hacerlo a la vista de todo el mundo. Recordemos que para mantener un Libro se deben transmitir constantemente sus resultados. Imaginemos un galpón gigante lleno de computadoras transmitiendo datos a todo el universo. Sería muy fácil de identificar, excluir y posteriormente iniciar acciones legales contra sus dueños. No parece una buena estrategia considerando la cantidad de dinero invertido en dichas instalaciones.

En resumen, el sistema favorece jugar bajo las reglas y desincentiva el engaño. La especialización de los mineros refuerza la seguridad, obligándolos a invertir recursos para poder jugar. Que los recursos no sean más que computadoras inútiles sirve de mecanismo para reforzar la seguridad, ya que dejar de ser parte del juego significaría tirar a la basura todo el dinero invertido. Así, los mineros están económicamente incentivados a cumplir las reglas.

5.6 Mineros = Nodos

Un término que merece la pena explicar es el de *nodo*. Es un concepto repetido y manipulado en el mundo cripto y se presta a confusiones.

En computación, un nodo (nudo en español) es un punto de comunicación en una red. Para ser un nodo se debe por lo tanto recibir y enviar información. Es decir, sirve de conector entre puntos, por esto el término nudo.

Esta definición ha hecho que se considere a cualquier computadora que esté conectada a la red de Bitcoin como un nodo. Incluso, desde BTC se incentiva a todos los usuarios a hacerlo, descargando y manteniendo toda la Blockchain, aludiendo que cumplen una función importante en el mantenimiento de la red.

Bitcoin no funciona así. Si bien una persona puede descargar el programa y mantener un canal de comunicación, quienes mantienen el sistema son los mineros. Como explicamos anteriormente, ser minero implica obligatoriamente estar 'escuchando' y transmitiendo nuevas transacciones. Están incentivados económicamente a hacerlo. Eso quiere decir que invierten miles de dólares en los mejores equipos del mundo para recibir y enviar información. Ellos son los verdaderos nodos del sistema. Es inviable que una persona con una computadora establezca una mejor comunicación entre usuarios que un minero. Sería como intentar sostener la conexión eléctrica de una ciudad usando un alargue. Incluso, si tuviesen los mejores aparatos, lo único que harían sería repetir lo que reciben de los mineros, así que no agregarían ningún valor.

En definitiva, los verdaderos nodos del sistema son los mineros. Desde BTC se intenta mantener este mito para que las autoridades crean que el sistema no puede ser detenido.

5.7 Otras criptomonedas

Como Bitcoin es un programa, puede ser imitado. Eso llevó al nacimiento de otras monedas digitales con sus respectivas blockchains. A grandes rasgos, son variantes de

Bitcoin, pero con distintas reglas. Algunas buscan que la información sea más anónima. Otras buscan poder compartir información más rápido. Muchas de ellas se usan para representar titularidad o poderes dentro de nuevos proyectos.

La mayoría de estas monedas alternativas alegan resolver las limitaciones de Bitcoin. Sin embargo, en todos los casos incluyen una discrecionalidad de parte de sus propulsores a la hora de hacer modificaciones a los protocolos internos. Tampoco son transparentes respecto a quiénes son las personas que están efectivamente a cargo esos proyectos.

Debemos aclarar que Bitcoin no es técnicamente una criptomoneda. Utiliza criptografía al igual que muchos sistemas de seguridad. Pero la información viaja y se presenta de forma transparente y legible.

La segunda blockchain más popular después de Bitcoin es Ethereum. Originalmente se creó con la novedad de poder ejecutar programas informáticos, algo que se creía Bitcoin no podía hacer. Esto mismo había sido desmentido por un entonces ignoto Craig Wright en 2015, lo cual fue confirmado posteriormente como cierto por toda la industria.

Una de sus particularidades de Ethereum es que admite la creación y distribución de otras monedas por parte de desarrolladores informáticos. Muchas de estas monedas son lanzadas como forma de financiar proyectos. En la mayoría de los casos, su valor suele sostenerse en base a la especulación más que a sus aportes económicos reales.

Ethereum en sus primeros años usó también *Proof of Work* para mantener su Blockchain funcionando. Se encuentra ahora haciendo la transición a lo que se conoce como '*Proof of Stake'*. Esto significa que, en vez de poder computacional, los mineros deben dejar fondos en la moneda digital en una suerte de depósito de garantía. El sistema entonces confía en aquellos mineros con mayores depósitos. De esta forma, aquellos con más recursos son quienes más bloques aportan a la cadena y, por lo tanto, más comisiones generan. Este sistema es considerado más amigable con el medio ambiente ya que suprime la necesidad de invertir en poder computacional y energía. Solo requiere fondos. Lo que este sistema alternativo promueve en realidad es una oportunidad para los mineros de ser anónimos. Esto se puede lograr distribuyendo grandes cantidades de capital en pequeños usuarios anónimos. Además, este tipo de sistema no busca la eficiencia. Los mineros en Bitcoin invierten dinero, pero, por el carácter competitivo del juego, también deben asegurarse de ser mejores que los otros. Ellos prestan un servicio que sirve de mecanismo de seguridad indirecto. Con el sistema de '*Proof of Stake*', el dinero produce dinero por el sólo hecho de estar depositado. Así no es cómo funciona la economía y sólo produce una mayor concentración de la riqueza.

Otro tipo de monedas que han surgido son las denominadas '*stablecoins*' o monedas estables. El espíritu de dichas monedas es ofrecer una moneda virtual donde cada unidad corresponda a una unidad real de dinero que se encuentra depositada en

un banco. Es decir, por cada dólar virtual, existe un dólar efectivamente respaldando dicho valor. El problema que ha ocurrido con algunas de estas reconocidas monedas es que en los hechos no existe respaldo. Quienes las operan no rinden cuentas respecto a los depósitos reales, convirtiéndose en los hechos en emisores de dinero sin ningún respaldo. Lo que es más grave aún, utilizan estas monedas virtuales sin respaldo, pero que en teoría sí lo son, para manipular los mercados de otras monedas, generando la falsa ilusión de liquidez.

6. Derribando mitos y mentiras

Satoshi Nakamoto es un mito popular. Es una leyenda cuyas proezas se transfieren en el criptouniverso de generación en generación. Todos los relatos y visiones de absolutamente todos los proyectos se sostienen en la visión de este ser tan sabio que eligió retirarse y dejar su creación en manos de la comunidad.

Se considera a Satoshi como parte de un movimiento 'anarcocibernético'. Representa el rechazo de las clases sociales medias y bajas al sistema financiero y su cercanía con los gobiernos de turno. Rechazo especialmente fortalecido en EE.UU. tras la crisis financiera de 2008.

Bitcoin es para muchos una religión, y Satoshi, su mesías. Es presentado como la respuesta a los males del mundo moderno y el capitalismo desenfrenado. El relato es tan poderoso que ha conquistado a millones de personas con la esperanza de ser parte de una revolución financiera. Para estas personas, Bitcoin supone retomar el control sobre las finanzas personales. 'Tu dinero, tus llaves' dice el lema cripto. Bajo esta óptica, los bancos son agentes innecesarios. Parásitos que buscan perpetuar su condición de intermediarios.

Además del romanticismo revolucionario que despiertan, basan su relato en mentiras técnicas respecto al funcionamiento del sistema. La principal es respecto a su condición de sistema descentralizado que, dicen, lo hace imposible de detener. También se lo quiere considerar como un sustituto al oro por existir un número limitado de bitcoins. A su vez, se inventó y solidificó el concepto de Finanzas Descentralizadas, o *DeFi*, como contrapunto al sistema financiero tradicionalmente identificado con Wall Street.

A continuación, detallaremos algunos de estos conceptos e ideas. Las mejores mentiras siempre son aquellas que tienen un componente de verdad y este caso no es la excepción. Lo que resulta increíble es que hayan logrado salirse con la suya por tantos años.

6.1 Descentralización

Descentralización es una de las palabras más repetidas en el mundo cripto. Este concepto, en sí mismo, se puede interpretar de diversas formas. La comunidad lo usa en el sentido de que el sistema funciona en miles de computadoras al mismo tiempo. Así, el programa no es mantenido en un servidor centralizado ni por un solo responsable, por lo que hablamos de un sistema descentralizado.

Como ya hemos explicado, se ha tergiversado la tecnología detrás de Bitcoin. Se quiere imponer la idea de que cualquier computadora corriendo el software está ayudando a sostener el sistema. Esto es mentira. Solo los mineros participan del mismo. Ellos están distribuidos, pero es una ilusión pensar que el sistema es completamente descentralizado. En la práctica, los mineros juntan su poder computacional en lo que se conoce como 'piscinas' o 'pools'. Esto ya había sido predicho por Satoshi en uno de sus primeros posteos en 2009, afirmando que a medida que el sistema crezca el mantenimiento sería llevado a cabo por "granjas con servidores especializados" *[15]*.

Hoy BTC, el Bitcoin famoso, cuenta con menos de treinta de estos 'pools'. Como dijimos anteriormente, necesitan una infraestructura enorme: contratos con compañías eléctricas, permisos municipales, conexión a Internet, etc. Como toda organización, están sometidos a las leyes de cada país. Si se quisiera detener BTC, BSV, Ethereum, o cualquier criptomoneda realmente, bastaría con detener las operaciones de esos mineros y el sistema colapsaría inmediatamente.

También podemos visualizar la centralización como los cuellos de botella de un sector. En el caso de Bitcoin, además de todos los factores necesarios para su funcionamiento, tenemos dos agentes intermediarios más: los cambios y las billeteras electrónicas. Quienes a su vez dependen del también regulado sistema bancario. Esto permite ver claramente cómo podría crearse un sistema debidamente regulado.

Existe sí una descentralización real en el sentido que no existe una entidad financiera que controle fondos ni emisión.

6.2 Regulación

Bitcoin es y será regulado. Esto no tiene ningún tipo de misterio. En realidad, lo que debe hacerse es considerar Bitcoin como un activo que al mismo tiempo puede usarse como moneda de cambio. Si lo pensamos bien, todo lo que hoy se puede pagar con efectivo tiene un nivel de trazabilidad menor que Bitcoin.

Basta entender que, para adquirir bitcoins, como cualquier moneda extranjera, hay que recurrir a cambios. Estos cambios, se regirán por las leyes de cada país. No hay más discusión. Aquellos cambios con oficinas físicas operarán como lo hace cualquier cambio. Por su parte, los cambios digitales que puedan existir deberán estar debidamente registrados para poder recibir transacciones ya sea por vía de giros bancarios o tarjetas de crédito.

Lo mismo puede ser dicho de las billeteras electrónicas. Como cualquier programa informático, está sometido a la reglamentación de cada país.

¿Qué pasa si alguien consigue burlar estos requisitos y comprar clandestinamente bitcoins utilizando además una billetera no registrada? Esa persona seguramente tenga serios inconvenientes a la hora de ir a cualquier tienda real a pagar por sus bienes. Sus planes serían todavía más absurdos si se tratase de cifras significativas. Sería sensiblemente más sensato mantener dichos valores en efectivo y evitarse dolores de cabeza.

Por supuesto que sería ridículo no aprovechar la tecnología que presenta Bitcoin para establecer registros personales donde la privacidad de las personas sea mantenida y al mismo tiempo se asegure que todas las partes cumplan con todas las obligaciones. Lo más razonable sería empezar a legislar lentamente a partir de montos reducidos donde todas las partes puedan familiarizarse con su uso de forma segura. El ecosistema de desarrolladores también necesita tiempo y espacio para poder ofrecer soluciones que sean escalables y seguras. Lo mismo puede ser dicho de los reguladores.

Paulatinamente se puede incrementar el valor máximo de los pagos que se puedan hacer integrados a los sistemas impositivos y reglamentarios de cada país. El rol de los gobiernos es crear registros o herramientas para facilitar el cumplimiento de todas las obligaciones de manera simple y práctica.

Del otro lado, la mayoría de los grupos de interés dentro de BTC promueven la no regulación sosteniendo la mentira de que es imposible regular y existe más allá del control de ninguna autoridad o poder.

Los mineros sólo corren un programa. No votan ni toman decisiones. La integridad del sistema depende de que sigan las reglas del juego. Es importante que sean identificables para sancionar a aquellos que intenten romper las reglas. No es razonable pensar que un minero se atrevería a desautorizar una orden judicial en ningún país serio. Tampoco lo sería que un minero decida invertir el dinero necesario para montar sus operaciones en un país sin un marco legal confiable.

Mineros, cambios y billeteras son empresas, y como tales tienen que respetar las leyes y regulaciones de cada país. Muchos de estos jugadores hacen todo lo posible por mantener los mitos en la comunidad. No tienen interés en enfrentar regulaciones ya que eso implicaría asumir responsabilidades. Lo cierto es que la responsabilidad es parte del contrato social cuando alguien presta un bien o servicio.

Hoy en día, la mayoría de los cambios legales y sistemas que directa o indirectamente permitan tener criptomonedas, exigen enviar documentación formal sobre la identidad personal de acuerdo al volumen que se maneje. Esto lo hacen para cumplir las reglamentaciones internacionales.

6.3 Finanzas Descentralizadas

El concepto de Finanzas Descentralizadas o *DeFi* refiere a un sistema financiero sin intermediarios. La lógica es que los bancos y el sistema financiero en general se han convertido en agentes cuya intermediación se traduce en un abuso sobre el control de nuestros recursos. Es un sistema financiero sin autoridades, en el que las personas pueden tanto conseguir financiamiento para sus proyectos como hacer de inversionistas. Si bien suena romántico, y tiene un gran componente de crítica válido al sistema actual, se simplifican ambos sistemas.

Por un lado, las empresas que cotizan en bolsa deben presentar y publicar sus estados contables auditados. Es cierto que una gran cantidad de inversores no hacen los análisis correspondientes, pero la solución tampoco parece ser eliminar cualquier tipo de requisitos. Se supone que cumplen una función de protección hacia las partes interesadas.

Además, se omite que ya existen otros espacios donde se pueden presentar proyectos para recibir financiación. Es cierto que muchas veces estos espacios obligan a resignar porcentajes por un servicio que parece no agregar demasiado valor. Un sistema financiero eficiente debería interceder entre las partes para ofrecer reglas claras y evitar fraudes y actividades ilegales. Un sistema que se diga 100% descentralizado no es más que una plataforma para girar dinero y recibir un vale o acción sin mayores garantías.

Esto no significa que el sistema financiero no necesite reformas. Las reglas no son siempre claras y demasiados intermediarios que no agregan valor alguno lucran exclusivamente con el capital y riesgo ajeno. Bitcoin es una herramienta que fomenta la transparencia y por lo tanto la honestidad de los sistemas. Es ilógico demonizar a los bancos y al mismo tiempo vender la ilusión de que un sistema sin controles va a ser más justo y noble. Los bancos están conformados por personas, no son entes independientes que aparecieron en la Tierra.

6.4 El dinero como ilusión

El movimiento cripto quiere convencer a inversores, economistas, políticos y usuarios

de que el dinero es una ilusión. El sustento es que, a diferencia de épocas pasadas, el dólar americano no está respaldado por oro.

Si bien eso es cierto, el dólar sí tiene el respaldo de la Reserva Federal. En cualquier parte de ese país y casi en cualquier parte del mundo, el dólar es aceptado como una moneda con valor. Además, el resto de las monedas del mundo tampoco tienen el respaldo del oro ni ningún otro commodity. Sin embargo, eso no significa que no tengan valor ni que sea una simple convención social. Las personas en todo el mundo aceptamos dinero a cambio de nuestras horas de trabajo. La sumatoria de ese dinero pagado por tales horas son las que terminan definiendo el precio final de los bienes y servicios producidos. El dinero es por lo tanto una fuente de información. Ayuda a traducir trabajo y bienes para poder intercambiarlos de manera efectiva.

El Bitcoin, en cambio, no es aceptado en casi ningún comercio del mundo. No podemos pagar sueldos, ni bienes, ni servicios. La única ilusión es creer que mágicamente vamos a generar riqueza inventando nuevas formas de medir el dinero.

Se puede y debe mejorar el sistema financiero. El manejo de las finanzas públicas e inflación son problemas que competen a muchos países y deben ser monitoreados con mucha más atención. La solución a la falta de control no puede ser menos control. El déficit de tantas economías y sus manejos irresponsables de la consiguiente deuda generada son un simple reflejo de la hipocresía y dualidad de criterio imperante en el universo político. En ningún ámbito empresarial o personal se permitirían tales niveles de negligencia financiera.

Es necesario entender que el movimiento cripto no se trata de locos ni estúpidos. Tiene que ver con gente que se siente permanentemente engañada y ven sus magros ahorros reducidos año a año a causa de la inflación. Al mismo tiempo que los países se embarcan en inversiones que no pueden afrontar utilizando eufemismos como *fideicomiso* o *fondos*, para no utilizar la siempre temida *deuda*. Al mismo tiempo que los intelectualmente debilitados medios de comunicación aceptan ser parte de este circo mientras la gente acepta con resignación.

Se necesita mejor control y mayor responsabilidad. Eso no se consigue mágicamente con solo desearlo.

6.5 Oro Digital

Esta es una de las piezas fundamentales del esquema piramidal funcionando particularmente al servicio de BTC.

Por protocolo, sólo pueden existir 21 millones de bitcoins. Esta cota hace de Bitcoin un bien finito, al igual que el oro. Además, ambos cumplen la función de preservar valor en el tiempo y ser fácilmente intercambiables. Se completa el

razonamiento explicando que, al saberse la oferta real y, dada la imposibilidad de generar más monedas, su precio va a reflejar de forma fidedigna su valor.

Un bien finito puede no tener valor en sí mismo, como el caso de una pintura, y aun así ser socialmente aceptado que es valioso. Eso no es lo mismo que decir que todo bien finito vaya a ser valioso sólo porque en un momento del tiempo mucha gente lo considere valioso.

Además, esta idea va en completo enfrentamiento con el concepto de Bitcoin como efectivo digital. Si bien el dinero cumple una función de preservar valor, asimilarlo a un commodity como el oro no hace más que convertirlo en un activo especulativo. Con esta visión, la demanda sólo existe porque su precio aumenta. Es decir, la demanda se convierte en un fin en sí misma.

Bitcoin como oro digital es nada más que otro intento más de aumentar su valor y al mismo tiempo generar reticencia en los inversores a la hora de desprenderse de los mismos. El mercado real de BTC y las criptomonedas es mucho menos líquido que otros mercados, y de esta forma se quiere esconder esta realidad.

6.6 Gobernanza

Bitcoin fue diseñado lo más simple posible para evitar su manipulación. El espíritu es que no tenga agente controlador, sino que los controles legales y su reglamentación se lleven a cabo mediante empresas y agentes diseñados apoyados sobre esta tecnología. Qué se hace y qué normas dominan el espacio es potestad de cada autoridad determinar.

La mayoría de las criptomonedas y blockchains suelen hacer referencia al control del individuo sobre su dinero y la libertad que esto representa. Casualmente suele existir muy poca información respecto a quiénes efectivamente toman las decisiones en ellas. Se quiere hacer creer que se usa el consenso de la 'comunidad' para proponer y ejecutar planes de acción. Lo cierto es que en su gran mayoría son proyectos que, independientemente de sus fines, terminan proporcionando un enorme lucro a sus impulsores. En el camino, la tan añorada transparencia brilla por su ausencia.

7. El verdadero potencial

Bitcoin, como se lo concibió, es una herramienta única y va a cambiar la forma en la

que interactuamos con el mundo digital. El intercambio de efectivo de manera electrónica es el primer y más básico uso. Su futuro dependerá de nuestra capacidad para innovar y ejecutar nuevas ideas.

A modo de ejemplo, estas son algunas posibilidades para realizar en dicho sistema.

7.1 Administración automatizada

Bitcoin es un libro contable. Con una correcta programación, muchos de los procesos vinculados a los registros contables pueden ser automatizados.

El sistema contable actual es complejo e ineficiente. Eso ha llevado a que se confunda la contabilidad con un sistema de liquidación de impuestos. Para la gran mayoría de empresas unipersonales y Pymes, los gastos en asesores contables son iguales o superiores a los vertidos por concepto de impuestos.

Bitcoin representa la primera alternativa real a un sistema automatizado de administración y pagos. Con un sistema automatizado, los impuestos se pueden liquidar y actualizar automáticamente. Tengamos en cuenta que toda actividad comercial que no genera valor agregado significa un desperdicio de recursos.

Los contadores pueden volver a ser contadores. Estudiar los flujos y ratios y asesorar a sus clientes a partir de métricas reales. Los Estados también pueden dejar de destinar recursos en procesar grandes caudales de información ultraprocesada. Con Bitcoin como sistema, se puede empezar a comprender y estudiar mejor las distintas dinámicas económicas que hacen a cada sector, y su interacción entre sí. Esto significa mejores herramientas para todos los actores para poder tomar mejores decisiones.

7.2 Impuestos automáticos

Como corolario del punto anterior, se desprende la posibilidad de un sistema de liquidación y pago automático de impuestos. Las Administraciones Centrales de los distintos países pueden generar instrumentos donde los impuestos puedan ser directamente retenidos por el sistema y derivados a las arcas del Estado.

El Impuesto al Valor Agregado (IVA) es el ejemplo más sencillo de imaginar. Cada vez que se haga una transacción de un bien gravado, el sistema puede directamente enviar al comercio su parte y el importe correspondiente al IVA puede ir directamente a una cuenta relacionada a la dirección impositiva.

En la práctica, es el fin de los agentes de retención, que hoy no agregan valor al proceso.

7.3 Celebrar contratos

Los contratos son acuerdos entre las partes. En los acuerdos formales se suele requerir el cumplimiento de ciertas pautas que son verificadas por notarios. Muchos de estos aspectos formales pueden reducirse considerablemente con información almacenada en una blockchain.

Hoy la digitalización ha llevado a trasladar muchos de los requisitos formales a computadoras. Esto ha llevado a una redundancia en los procesos. Además, esta información suele ser poco accesible y por lo tanto termina simplemente perdida entre millones de archivos pobremente catalogados. Esto es ineficiente porque no mejora procesos, sino que, por el contrario, aumentan su complejidad a cambio de ofrecer apenas mayores garantías.

Si bien en muchos países existe el concepto de firma digital para firmar contratos, Bitcoin permitiría hacerlo de forma más rápida y práctica. Desde alquilar automóviles a contratos más complejos donde aún deban participar terceros. En esos casos, por ejemplo, una escribana registrada podría utilizar sus llaves particulares para manifestar que un proceso ha cumplido todas las formalidades.

7.4 Propiedad intelectual digital

Uno de los conceptos más interesantes desarrollados en los últimos años es el de propiedad digital, conocido popularmente en la comunidad como *NFT*'s. Su nombre significaría algo así como Fichas No Fungibles.

Se trata de transacciones en las que, en vez de intercambiar monedas, se intercambia la posesión de un archivo digital, como puede ser una imagen. Estas imágenes deben ser únicas, y por lo tanto ser sujetas a derecho por parte de autor. Al igual que una obra de arte, pueden ser vendidas o solo compartidas. La misma blockchain guarda todo el historial de movimientos y transacciones.

En principio, puede sonar como un recurso sin aplicaciones en el mundo real más allá de comercializar bienes incorpóreos. Lo cierto es que este tipo de contratos virtuales pueden abrir un abanico de opciones monetizables muy importante.

Hoy en día, cada vez que un medio quiere usar una imagen de archivo para una noticia, puede acudir a un banco de imágenes y pagar por el uso de una foto. Con esta

tecnología, se pueden generar espacios donde los fotógrafos puedan directamente subir sus imágenes e imponer sus condiciones para la utilización de estas por terceros. Los dueños también podrían configurar la opción de cobrar por cada vez que se use la fotografía o imagen. Pero también, sería posible establecer una tarifa variable en virtud de la cantidad de veces que sea mostrada la noticia. Hay un sinfín de opciones, y no sólo abarca la fotografía. Memes y stickers también podrían comercializarse por centésimos, permitiendo a artistas y creativos generar valor de forma honesta y justa.

8. Bitcoin y el medioambiente

Una de las preocupaciones más comunes respecto a Bitcoin y otras criptomonedas, refiere al impacto que tiene el minado en el medioambiente.

Recordemos que las granjas de mineros son computadoras permanentemente conectadas a redes eléctricas. El daño entonces depende, en primer lugar, del tipo de generación eléctrica usado en cada caso individual. No es válido sumar el consumo total de todos los mineros y asumir un impacto ambiental en base a ello. Muchos mineros originalmente se vieron seducidos por países o regiones donde la energía es barata, lo cual suele asociarse con fuentes no renovables como el carbón. Esto es un problema, por supuesto, pero propio de todas las industrias del planeta.

La cantidad de mineros va a aumentar con el uso y adopción de la tecnología. Eso va a derivar indudablemente en un aumento en el valor absoluto de Kilowatts consumidos. Analizar simplemente este número es un sinsentido, ya que no tiene en cuenta los Kilowatts ahorrados en ineficiencias actuales en distintos sectores que Bitcoin soluciona.

Un caso análogo, pero del que poco se habla, es el de las famosas "*nubes*", servidores especialmente diseñados para garantizar acceso de manera remota. No existe empresa en el mundo que no utilice estos sistemas para en sus actividades. También las personas las usamos directa o indirectamente todos los días. Estas nubes son computadoras permanentemente conectadas enviando y recibiendo datos. Su consumo total eléctrico es enorme. A la hora de analizar su verdadera huella ambiental habría que, en primer lugar, estudiar el ahorro en discos duros, unidades de almacenamiento y servidores centralizados. Posteriormente, deberíamos hacer un análisis completo de todos los componentes detrás de la producción, distribución y venta de cada uno. Luego, estudiar el consumo actual de dichas nubes, aplicando correcciones a favor y en contra en virtud de eficiencias e ineficiencias propias de la centralización, creación de nuevas aplicaciones y ampliación de mercados preexistentes, entre otros. Entonces tal vez tengamos una idea simplificada de un posible impacto, lo cual en la práctica se traducirá en más y mejores medidas para su mitigación, cosa que, en teoría, ya estábamos haciendo de todas formas. Cualquiera

sea el resultado de dicho estudio, la conclusión nunca será desarticular la infraestructura instalada y volver al pasado.

Lo cierto es que es muy difícil, sino imposible, calcular el impacto real de cada industria sobre el medioambiente. Más allá de que las generalizaciones son útiles pues sirven de promedio, la trazabilidad real supone un rompecabezas mucho más complejo de lo que queremos admitir. La mayoría de los estudios e informes ambientales suelen tener enormes diferencias entre sí. Esto se debe a que los parámetros para la evaluación de dichos impactos suelen diferir tanto en el rigor técnico aplicado como en la verdadera comprensión de los distintos actores que intervienen en la cadena de un producto. Además, se suele dejar de lado la falta de alternativas aplicables y escalables para sustituir dichos mecanismos. No es mi intención profundizar demasiado en estos aspectos. Un verdadero análisis honesto comienza por los verdaderos costos de generación, conservación y distribución de la energía en todas sus opciones, y nunca puede resumirse a unas simples líneas.

Habiendo dicho esto, BSV es infinitamente más amigable con el medioambiente que BTC. Recordemos que esta última tiene un límite en el tamaño de sus bloques. Esto se traduce en un número reducido de transacciones por cada bloque minado, contribuyendo enormemente a la ineficiencia del sistema. Bitcoin es eficiente, no así el Bitcoin que todos conocemos, BTC. Por eso es tan importante entender lo que está pasando en este sector.

9. El futuro de Bitcoin

Es común catalogar a nuevas tecnologías con la capacidad de hacer cambios significativos de “disruptivas”. Lo cierto es que la gran mayoría suelen defraudar a la hora de cumplir dichas promesas. Siempre es un riesgo aventurarse a hacer conjeturas respecto al futuro, especialmente cuando de tecnologías se trata. Las expectativas no suelen cumplirse debido a limitantes no previstas y, al mismo tiempo, implementaciones imprevistas suelen colarse en el mundo real.

Una de las principales limitantes usualmente ignoradas a la hora de analizar dichas tecnologías suele ser la capacidad de escalar la producción de las herramientas necesarias para su pleno desarrollo. Todos los años vemos presentaciones increíbles de robots humanoides haciendo todo tipo de trucos y tretas, pero en la vida real lo más parecido a una implementación real que tenemos es una aspiradora automática con ruedas, pero sin ojos ni cerebro.

Bitcoin es un sistema de información. La infraestructura esencial que necesita para operar ya está en implementación hace años y es Internet.

Tiene la fortaleza de ser infinitamente escalable. Esto se debe a la permeabilidad a la hora ser parte del minado y por consiguiente colaborar con el mantenimiento del sistema. A medida que aumente su uso, más atractivo será para nuevos mineros sumarse al mercado. Además, siempre tenemos que recordar que ellos compiten entre sí, por lo que la eficiencia es intrínseca al sistema.

Lo más probable es que Bitcoin, o BSV, eventualmente se superponga a esta nube de desinformación y empiece a ser usado en el corto plazo para realizar pagos minúsculos. Por ejemplo, los diarios y portales podrán a cobrar centavos de dólar por leer una noticia puntual, algo que se podrá hacer con sólo apretar un botón. Es muy probable también que creadores de contenido, como YouTubers, empezarán a aceptar propinas en dicha moneda. Solemos cometer el error de pensar en ellos como jóvenes ricos y la realidad de la mayoría de ellos dista mucho de esto. Hoy, para hacerles llegar una recompensa por algo que hoy hacen gratis, debemos asociarnos a un sitio, ingresar nuestros datos, la tarjeta de crédito y, en la mayoría de los casos, comprometernos a un pago mensual. Con Bitcoin, sencillamente podemos enviarle tres dólares al responsable de un video de YouTube como hoy le podemos dejar un billete en la gorra al músico que practica su arte en las calles. Esto no es quitarles mercado a las tarjetas de crédito, sino abrir un mercado que antes no existía. Los principales beneficiados serán aquellos en otras partes del mundo a los que 3 dólares les pueden cambiar la vida.

Ante la duda, siempre es recomendable estudiar las implementaciones técnicas en la industria pornográfica, pionera en todas las innovaciones tecnológicas: VHS, Webcams, Pay-Per-View, Live streaming, por nombrar algunas. Como les ocurre actualmente también a los negocios legales de cannabis, siempre han tenido dificultades a la hora de cobrar y hacer pagos formales, por lo que este tipo de herramientas no tardaran en funcionar de forma regulada y segura.

Se cometerán errores en el camino. Siempre existirán agentes maliciosos dispuestos ejecutar fraudes y engaños. Por ello, es natural que al comienzo sus usos sean para cantidades no significativas. Esto también quita presión a los gobiernos a tener que desarrollar sistemas de monitoreo robustos y funcionales. Sería un desperdicio de tiempo y recursos intentar generar mecanismos para el control de unos pocos dólares. Es con el desarrollo de tecnología, conocimiento, y su materialización en la vida real, que podremos avanzar en los distintos usos de Bitcoin como complemento al efectivo.

Asimismo, ya se están desarrollando cientos de programas y aplicaciones, desde videojuegos a bases de datos, que usaremos en un futuro sin siquiera ser conscientes de que funcionan usando la blockchain de Bitcoin como parte de su estructura.

En este contexto, lo más probable es que en el futuro utilicemos una sola moneda virtual, Bitcoin; y una zona sola blockchain para la programación de otras aplicaciones, también la de Bitcoin. Esto no es por necesidad, sino practicidad. Utilizar diversas blockchains implicaría tener que desarrollar soportes extras para interactuar

entre sí. Eso no supondría más que un desperdicio de recursos. Por esa misma razón la mayoría de las computadoras utilizan Windows, Linux o Mac. No sería viable que cada programa con el que interactuamos en nuestras computadoras debiera ser desarrollado para soportar veinte sistemas distintos. Tampoco lo sería intentar crear parches para adaptar los mismos. Claro que es posible, pero no tendría sentido. Un protocolo estándar que funciona y es escalable sí tiene sentido.

10. Conclusión

A la fecha de realización de este trabajo, la cotización de BTC rondaba los setenta mil dólares cada moneda, mientras que BSV no alcanzaba los doscientos dólares. La diferencia sustancial entre ambos es que el último funciona y el primero, no. No debe haber existido otro momento en la historia donde la desinformación haya sido tan poderosa a la hora de manipular los precios. Lo cierto es que su cotización es irrelevante y muestra la falta de comprensión sobre la herramienta que es en verdad Bitcoin. Su aplicación en el mundo real es lo que debería importar acerca de cualquier tecnología. Los ciudadanos seremos sus usuarios finales. Personas comunes y corrientes. No los inversores ni especuladores financieros. Como tales, no podemos permitir que un conjunto de iluminados, bajo un paraguas mediático, usen y abusen de su posición para crear un mercado ficticio y al mismo tiempo aumentar su poder a base de dólares mal habidos.

El Dr. Craig Wright es Satoshi Nakamoto y ninguna persona seria que diga haber estudiado Bitcoin y escuchado sus palabras puede negarlo. Su nombre ha sido cruelmente enchastrado, y con él su integridad, y la de su familia. Una persona cuyo único crimen fue brindar una herramienta para mejorar el mundo. Él no necesita de este documento para defender su obra, ni su legado. Somos nosotros, los individuos, quienes sí tenemos la obligación moral de alzar la voz ante la injusticia. En asumir nuestro rol de testigos frente a lo que está pasando y denunciar a los verdaderos culpables. De otra forma, ninguna tecnología rescatará nuestra sociedad de nosotros mismos. Es hora de dejar de delegar las responsabilidades morales en terceros y hacer lo correcto simplemente porque es lo correcto.

Toda verdad atraviesa tres fases.
Primero, es ridiculizada.
Segundo, se le opone violentamente.
Tercero, es aceptada como evidente.

Arthur Schopenhauer

Notas finales del autor

Este trabajo fue realizado en carácter personal con la motivación de brindar claridad a un tema verdaderamente complejo por la multiplicidad de disciplinas que abarca. Mi formación profesional es en Ciencias Económicas y Contabilidad y mis ingresos provienen de mi actividad privada como fundador y director de Tajes 5, empresa que no está bajo ningún concepto relacionada al mundo tecnológico o financiero. A la fecha original de publicación, 22 de noviembre de 2021, no tengo valores en Bitcoin en ninguna de sus variantes. Tampoco tengo intereses creados en ninguna empresa u organización del ambiente, ni vínculo con personas que puedan tenerlo.

Siempre es buena idea ir a las fuentes. Además de leer el White Paper original, recomiendo escuchar a Craig Wright directamente en la siguiente entrevista. Como él mismo aclara, tiene Asperger, síndrome dentro del espectro autista. Esto le presenta dificultades a la hora de interactuar con las personas.

1) Bitcoin's Most Hated Man - Craig Wright, Por Patrick Bet-David, Valuetainment, YouTube, https://www.youtube.com/watch?v=0JvDauIX5lg, 16 de julio de 2020.

Para entender mejor el funcionamiento de Bitcoin de forma gráfica:

2) But how does bitcoin actually work?, Por 3Blue1Brown, YouTube, https://www.youtube.com/watch?v=bBC-nXj3Ng4, 07 de julio de 2017.

Para interiorizarse respecto a la cronología de los hechos desde el lanzamiento de Bitcoin recomiendo:

3a) The Most Elusive Identity On The Internet - Pt. 1 (Ft. Nexpo), Por Barely Sociable, YouTube, https://www.youtube.com/watch?v=_Kav2K1DVWo, 18 de enero de 2020.

3b) The Most Elusive Identity On The Internet - Pt. 2, Por Barely Sociable, YouTube, https://www.youtube.com/watch?v=fMWnaR5uJxQ, 07 de febrero de 2020.

3c) Bitcoin - Unmasking Satoshi Nakamoto, Por Barely Sociable, YouTube, https://www.youtube.com/watch?v=XfcvX0P1b5g, 11 de mayo de 2020.

4) Why I Believe Craig Wright is Satoshi, Por Kevin Healy, YouTube, https://www.youtube.com/watch?v=3MJSEGnpgB8, 29 de abril de 2021.

Para profundizar en todos los conceptos y aspectos técnicos detrás de Bitcoin, el siguiente canal contiene 70 horas de entrevistas a Craig Wright por parte de Ryan X. Charles. En ellas, repasan línea por línea el papel original de Bitcoin, así como todos los sucesos que llevaron al estado de situación actual del sector. Sin lugar a duda no existe mejor material que este para comprender todo lo relacionado a Bitcoin, y su historia.

5) Theory of Bitcoin - Dr. Craig S. Wright & Ryan X. Charles, YouTube, https://www.youtube.com/c/TheoryofBitcoin/videos, 22 de junio de 2020.

Para comprender un poco más respecto al funcionamiento de las redes, recomiendo:

6) Curso de Redes desde 0, por NASeros, YouTube, https://www.youtube.com/playlist?list=PLSvxAUzJ-XSfY0KpwV8SHBlyLVcrZkENc, 18 de julio de 2021.

Invito a los interesados a seguir sus propias investigaciones y sacar sus propias conclusiones. Internet puede ser una maravillosa fuente de información, pero requiere de muchísima flexibilidad mental a la hora de procesar y separar entre hechos, especulación y mentiras. Esto es especialmente cierto en industrias que mueven tanta cantidad de dinero bajo el escudo del altruismo.

Referencias

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, https://craigwright.net/bitcoin-white-paper.pdf, 31 de octubre de 2008.

[2] Bitcoin: $1bn seized from Silk Road account by US government, BBC.com, https://www.bbc.com/news/technology-54833130, 05 de noviembre de 2020.

[3] Hace 10 años nació Silk Road, primer mercado de la dark web que aceptó bitcoin, Por Luis Esparragoza, CriptoNoticias, https://www.criptonoticias.com/comunidad/10-anos-nacio-silk-road-primer-mercado-darkweb-acepto-bitcoin/, 27 de enero de 2021

[4] Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/posts/bitcointalk/523/, 05 de diciembre de 2010.

[5] Inside the Fight Over Bitcoin's Future, Por Maria Bustillos, The New Yorker, https://www.newyorker.com/business/currency/inside-the-fight-over-bitcoins-future, 25 de agosto de 2015.

[6] Bitcoin's forked: chief scientist launches alternative proposal for the currency, Por Alex Hern, The Guardian, https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist, 17 de agosto de 2015.

[7] Scaling Bitcoin: The Great Block Size Debate, Por Brian Armstrong, The Coinbase blog, https://blog.coinbase.com/scaling-bitcoin-the-great-block-size-debate-d2cba9021db0, 03 de enero de 2016.

[8] Bitcoin swings as civil war looms, Por Leo Kelion, BBC.com, https://www.bbc.com/news/technology-40654194, 20 de julio de 2017.

[9] Bitcoin's SegWit and Lightning: Need of the hour or not needed at all?, Por Biraajmaan Tamuly, AMBCrypto, https://eng.ambcrypto.com/segwit-and-lightning-need-of-the-hour-or-not-needed-at-all/, 15 de diciembre de 2019.

[10] Dr. Criag S Wright, https://craigwright.net/about/#biography.

[11] Is Bitcoin's Creator this Unknown Australian Genius? Probably Not (Updated), Wired, https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/, 8 de diciembre de 2015.

[12] This Australian Says He and His Dead Friend Invented Bitcoin, Por Sam Biddle y Andy Cush, Gizmodo, https://gizmodo.com/this-australian-says-he-and-his-dead-friend-invented-bi-1746958692, 8 de diciembre de 2015.

[13] Credit Card Processing Fees and Costs, Por Joe Resendiz, Value Penguin, https://www.valuepenguin.com/what-credit-card-processing-fees-costs, 9 de septiembre de 2021.

[14] Average Credit Card Processing Fees and Costs in 2021, Por Lyle Daly, the ascent, 13 de abril de 2021.

[15] Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/emails/cryptography/2/, 03 de noviembre de 2011.