Bitcoin: mapa de una arquitectura tecno-financiera

Pablo Delgado
pablo_cspolitica_15@hotmail.com
Universidad Nacional de Villa María

SOCIALES INVESTIGA. Escritos Académicos, de Extensión y Docencia
Nº13, Enero-Junio de 2022 (pp. 71-84)
e-ISSN 2525-1171
Villa María: IAPCS, UNVM
http://socialesinvestiga.unvm.edu.ar

Bitcoin: mapa de una arquitectura tecno-financiera

Resumen

El presente escrito confecciona un mapa con las ideas y conceptos fundamentales del funcionamiento de Bitcoin (BTC), la criptomoneda de mayor capitalización de mercado, como también algunas características de la Red Ethereum y de distintos casos de criptomonedas estables o "Stablecoins", ambas innovaciones claves para el crecimiento y expansión tanto de la novedosa arquitectura financiera que suponen estos ejemplos como para el apuntalamiento de la adopción masiva tales herramientas. Así, se toma a BTC como referencia en tanto es el lugar desde el cual comenzar a comprender todas las variantes de las finanzas descentralizadas (DeFi). Ya sea por continuidades y rupturas, como también por constituir un complejo de relaciones, ideas y tecnologías desde el cual interrogar la subjetivación contemporánea en línea con los objetivos de los núcleos de investigación en el que se enmarca el trabajo. En consecuencia, se intentará aportar claridad al fenómeno de referencia y lo plasmado aquí será la base conceptual para próximos escritos en los cuales se abrirá al escrutinio dicho objeto de estudio.

Palabras clave: bitcoin; blockchain; criptomonedas; minería; nodos

Introducción

Las criptomonedas son instrumentos financieros digitales que funcionan sobre una red llamada "Blockchain" y que, a diferencia del dinero tradicional, no se basan en el respaldo de un Estado-Nación o Banco Central. Es decir, no hay una institución pública detrás. Se trata de una determinada forma de dinero digital privado, paraestatal o "descentralizado" y basado en criptografía que se sostiene y se audita por sus usuarixs, cuya base de funcionamiento, la tecnología Blockchain, es de software libre, por lo que sus usos se pueden replicar y variar. La primera criptomoneda y la de mayor capitalización es Bitcoin (BTC), que en su último ciclo alcista rozó los 70.000 usd de valor por unidad y en lo que va del actual ciclo bajista por el momento tuvo su caída máxima hasta por debajo de los 16.000 usd, una cifra que probablemente no sea el piso definitivo. En ese contexto, el mercado de las criptomonedas ha experimentado un crecimiento exponencial y la adopción de estas tecnologías ya no es un experimento de unxs pocxs. Sobre tales instrumentos se han construido comunidades enteras de operación, discusión y desarrollo que navegan entre el mundo off-line y el on-line, incluyendo diversas empresas de servicios financieros como las exchanges[1], múltiples billeteras electrónicas para su almacenamiento, eventos de todo tipo y cursos, organizaciones propias e iniciativas de activismo social, portales de noticias dedicados al cripto-market y contenidos web en diversos formatos hasta academias de trading[2], un universo en el que tampoco faltan los "esquemas Ponzi" (estafas piramidales). En otras palabras, un completo ecosistema o "mundo cripto" compuesto de miles[3] de criptodivisas.

En el marco del equipo de investigación: *Actores sociopolíticos de Córdoba (2003-2019): transformaciones y continuidades ideológicas bajo el signo neoliberal* enmarcado en el programa de estudios "Subjetividades Políticas en la Época del Discurso Capitalista" (SPEDC) de la Universidad Nacional de Villa María, hemos abierto un espacio de indagación en torno al fenómeno de referencia, por lo cual aquí presentaré un mapa exploratorio de las ideas y conceptos principales de Bitcoin, el referente empírico sobre el cual versa la indagación, y me referiré de manera introductoria al ecosistema de Ethereum y a las denominadas Stablecoins o criptomonedas estables. Este escrito intentará ser el comienzo de una serie de intervenciones que, atendiendo a los objetivos generales del programa y los específicos del espacio de investigación en particular, intentaran -parafraseando a Arjun Appadurai (2017)- abrir al escrutinio el *habitus* del pensamiento cripto-económico y exponer, en caso de hallazgo, la *doxa* en su estructuralidad. Para ello, la pregunta por las implicancias de este complejo de relaciones, ideas y tecnologías en la subjetivación contemporánea será la clave de lectura de las futuras intervenciones.

[1] Empresas de compra, venta y operación financiera de criptomonedas.

[2] El trading en mercados de valores puede definirse como la especulación sobre ciertos instrumentos financieros e indicadores en busca de un beneficio o rendimiento a través de los denominados "análisis técnico" y "análisis fundamental", que juntos trazan las estrategias de "tradeo" para operar sobre diferentes activos por parte de los distintos operadores e inversores.

[3] Véase: https://coinmarketcap.com/all/views/all/

La red Bitcoin. Algunas definiciones

Ya no es ninguna novedad el desacople total del dinero con respecto al célebre circuito descripto por Marx en *El Capital* (D–M–D') en el que la mediación con una mercancía "X" era necesaria para la reproducción y el crecimiento monetario. Tampoco lo es el agotamiento de la relación entre dinero y referente material[4], en dirección hacia su desmaterialización en un contexto de generalización de billeteras y bancos virtuales[5]. Lo que si constituye una novedad es la posibilidad técnica que otorgan las criptomonedas de imprimir dinero por fuera del monopolio estatal y de crear instrumentos financieros al margen de los mercados tradicionales. De ellas existen miles, pero solo una (todavía) mueve el amperímetro del mercado de tal forma que afecta a todas las demás: Bitcoin. ¿Qué es y cómo funciona? En los siguientes párrafos haremos especial referencia al libro Mastering Bitcoin de Andreas Antonopoulos, uno de los textos más importantes para introducirse en la temática.

Las criptomonedas cobraron vida a partir del nacimiento de Bitcoin en 2009 de la mano del todavía anónimo Satoshi Nakamoto, quien plasmó las ideas principales de esta tecnología en un escrito de corte, en apariencia, meramente técnico titulado "Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer"[6]. Entre sus defensores más acérrimos, existen quienes no dudan en referirse a este fenómeno como una "revolución tecnológica", como el "nuevo oro digital" y otrxs como la herramienta de todas las libertades; en sus detractores o en quienes despliegan un manto de sospecha, la idea de que es una burbuja financiera está bastante extendida, y dada su gran volatibilidad, ponen en duda sus usos más allá de la mera especulación. Lo cierto es que, si bien cada criptomoneda tiene sus particularidades, diversas aplicaciones y "narrativas", Bitcoin es una red que está "resguardando valor" por cientos de miles de millones de dólares, incluso en el tope de su último "Bull Run"[7] del 2021, la capitalización de mercado llegó a equivaler a más de un billón de USD.

Ahora bien, ¿Qué es lo que posibilita la existencia de una criptomoneda? Muchxs bitcoiners afirman que el acierto de Nakamoto con Bitcoin es haber logrado combinar y sintetizar en ese solo producto distintas tecnologías que ya existían y con ello resolver problemas tales como el de los Generales Bizantinos, aquella "circunstancia donde los actores deben acordar una estrategia o consenso para evitar el fracaso catastrófico del sistema"[8], y el de cómo imprimir dinero sin respaldo estatal. Entre aquellas tecnologías están la Criptografía Asimétrica, Arboles de Merkle, BitTorrent, Proof of Work, B-money, Hash Cash y la Blockchain o "cadena de bloques". Pero de todos estos términos, el de mayor relevancia para nuestra intervención es "Blockchain". Como sostienen lxs autores Alberto Carmona et al. "... Bitcoin es el primer caso de aplicación de la tecnología blockchain de forma exitosa" (2019:11) pero las cadenas de bloques tienen existencia más allá de la creación de *cryptocurrencies*; son ante todo un software de código abierto, por

[4] Recuperado de: https://comunitat.canodrom.barcelona/assemblies/ElVector/f/1877/meetings/2293?fbclid=IwAR3KigDMXqJ3sB5snXPv2pIoJI9M991vW2F0rMBumiahTzeNICPn64ckUWo

[5] Ruiz, B. Suarez, J. (2021). *El fetichismo de la inclusión financiera*. Recuperado de: https://revistacrisis.com.ar/notas/el-fetichismo-de-la-inclusion-financiera

[6] Puede consultar el documento en la página https://bitcoin.org/es/

[7] Término en ingles que significa "carrera de toros" y que alude al ciclo alcista de un activo financiero en un mercado de valores determinado.

[8] Para profundizar al respecto, véase: https://academy.bit2me.com/que-es-falla-bizantina/

lo que sus funciones varían y se pueden adaptar de distintas formas según lo requieran empresas, gobiernos o personas.

Para lxs autores Álex Preukschat e Íñigo Molero Manglano se trata de "una herramienta nueva que sirve para compartir y gestionar el valor de activos o bienes digitales sin la necesidad de depender de una entidad central de confianza que centralice el proceso." (2017:8). En este sentido, las blockchains se definen como "… una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente." (2017:14). Por su parte, en el sitio Blockchain Federal Argentina proponen la siguiente definición:

> A grandes rasgos, Blockchain se puede pensar como un libro contable, una bitácora o una base de datos donde solo se puede ingresar entradas nuevas y donde todas las existentes no se pueden modificar ni eliminar. Esas entradas, llamadas transacciones, se agrupan en bloques que se van agregando, sucesivamente, al registro en forma de cadena secuencial, cada uno de ellos relacionado necesariamente con el anterior.
> En ese esquema, si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento[9].

Pero ¿Qué es un "bloque"? Andreas Antonopoulos lo define como una estructura de datos contenedor que agrupa las transacciones para su inclusión en la cadena, compuesto de una cabecera y de una larga lista de operaciones que ocupan la mayor parte de su tamaño. Ergo, la cadena se va incrementando a medida que se produzcan nuevas transacciones, y cada una de ellas es un movimiento de un determinado token[10] en la red, en nuestro caso BTC, de manera tal que la salida de una transacción es la entrada de un siguiente movimiento (Antonopoulos, A. 2016). En efecto, esta base de datos lleva en su registro cuantos bitcoins se hallan en cada dirección y sus movimientos. Asimismo, toda transferencia se realiza de manera encriptada mediante la creación de dos tipos de claves: las públicas y las privadas. La primera hace las veces de dirección de correo a la que cualquiera puede mandar fondos; la segunda sólo es conocida por lx propietarix de ese buzón y, por lo tanto, esa persona es la única que puede enviar criptomonedas desde allí, o sea, gastar bitcoins y firmar las transacciones. En rigor, "gastar bitcoins" es básicamente "firmar una transacción que transfiera valor desde una transacción previa hacia un nuevo propietario identificado por una dirección bitcoin" (Antonopoulos, A. 2016:25) porque al fin y al cabo lo que se transfiere es propiedad de dirección en dirección (2016:57). En este marco, cada uno de estos envíos lleva una marca de tiempo (timestamp) que permite saber cuándo sucedió este evento.

Previamente a la inscripción en la cadena, aparece un actor fundamental para el sostenimiento y la seguridad de la red: los llamados *Nodos,* es decir*,* aquellos ordenadores que ejecutan el software de Bitcoin y están conectados a dicha red. Su función principal es la de validar las transacciones, propagarlas hasta alcanzar a (casi) todos los demás nodos y posteriormente validar también los bloques creados. Lo que quiere decir que, entre una validación y la otra, cada nodo recibe transacciones para verificar que cumplan con las

[9] Recuperado de: https://bfa.ar/blockchain/blockchain

[10] Los tokens son un "objeto físico o digital que tiene valor en cierto contexto o para determinada comunidad, aunque su propia materialidad no contenga ese valor en sí". Recuperado de: https://launchpad.ripio.com/blog/que-es-un-token-y-como-funciona

reglas del consenso BTC[11] y luego retrasmitirlas. Por ello es de especial importancia este fragmento de Antonopoulos:

> La red bitcoin es una red entre pares (peer-to-peer), lo cual significa que cada nodo bitcoin se encuentra conectado a unos pocos otros nodos bitcoin que descubre durante su inicialización a través del protocolo entre pares. La totalidad de la red forma una malla parcialmente conectada sin una topología rígida ni estructura, haciendo de cada nodo un par equitativo. Los mensajes, incluyendo transacciones y bloques, son propagados de cada nodo a todos los pares a los que se encuentra conectado, un proceso conocido como "inundación" (flooding). Una nueva transacción validada inyectada en cualquier nodo de la red será enviada a todos sus nodos conectados a él (vecinos), cada uno de los cuales enviará la transacción a todos sus vecinos, y así sucesivamente. De esta forma, en apenas unos pocos segundos una transacción válida se propagará en una onda en expansión exponencial a través de la red hasta que todos los nodos de la red la hayan recibido... Para prevenir el spamming, ataques por denegación de servicio u otros ataques molestos al sistema bitcoin, cada nodo valida cada transacción independientemente antes de continuar con su propagación. Una transacción malformada no se propagará más allá de un nodo. (2016:119).

A la vez, es clave diferenciar entre aquellos que verifican completamente las reglas de esta red, denominados "Full Nodes" (que mayoritariamente implementan las reglas escritas para BTC mediante el software Bitcoin Core), y los "Light Nodes" o nodos ligeros, aquellos que "normalmente solo descargan la cantidad suficiente de datos de blockchain para procesar y verificar nuevas transacciones, por lo que su carga de trabajo computacional es mínima"[12]. Así, un nodo completo es de vital importancia porque:

> … hace todo lo que hace un nodo normal, pero también contiene una copia completa del libro mayor de la cadena de bloques, es decir, todas las transacciones de esa cadena de bloques, en tiempo real... Teóricamente, siempre que una sola computadora conserve una copia completa del libro mayor, una red de cadena de bloques podría restaurarse por completo en el improbable caso de una falla catastrófica en la red de nodos. Con muchas computadoras y servidores descentralizados en todo el mundo que mantienen una copia actualizada del libro mayor de blockchain, los nodos completos brindan una mayor seguridad a la red, ya que todos los nodos completos deberían destruirse para que la red cese[13].

Luego de esta dinámica, hace su aparición un segundo actor fundante de este sistema, lxs *Minerxs*. Su tarea consiste en "recoger" desde la mempool[14] las transacciones y verificarlas para incluirlas en un bloque con otros movimientos (Antonopoulos, A. 2016:12) ejecutando un proceso informático llamado "minería" (actualmente realizado en BTC con máquinas ASIC[15]) el cual a la vez crea la oferta monetaria de bitcoins. El producto que se obtiene es una concatenación de bloques en el que cada uno de ellos se identifica con una cifra alfanumérica exclusiva, una especie de "huella digital" que se genera por un determinado algoritmo criptográfico de "sentido único" denominado *función Hash*. Son varios los tipos de algoritmos hash y en el caso de Bitcoin se utilizan dos de ellos: el Secure Hash Algorithm (SHA) y el RACE Integrity Primitives Evaluation Message

[11] Para una lista de estas reglas o criterios, véase: Antonopoulos, A. 2016:197

[12] Recuperado de: https://www.gemini.com/cryptopedia/masternode-dash-bitcoin-node

[13] Véase: https://www.gemini.com/cryptopedia/masternode-dash-bitcoin-node

[14] Memoria temporal de entreacto que almacena provisoriamente los movimientos de los tokens en circulación.

[15] Véase: https://academy.bit2me.com/que-son-mineros-asic/#:~:text=Los%20mineros%20ASIC%20son,ser%20minado%20de%20otro%20modo.

Digest (RIPEMD), específicamente el SHA-256 para la prueba de trabajo e identificación de la cabecera del bloque y el RIPEMD-160 para la dirección de Bitcoin (Antonopoulos, A. 2016:76).

En este contexto, cada bloque de la cadena tiene el Hash del bloque anterior, que también es producto de otro bloque anterior y así hasta estructurar una cadena enlazada "hacia atrás en el tiempo" que nos lleva hasta el primer bloque o "bloque génesis", el único que no tiene hash de piezas anteriores. Luego, el hash se combina con un *Nonce* (un valor aleatorio de 32 bits), constituyendo una medida de seguridad para impedir que se altere la información contenida en el bloque (Carmona, A. *Et al*. 2019:59). La minería, entonces, es aquel procesamiento en el que para agregar nuevos datos a un bloque se debe resolver un desafío criptográfico llamado proof-of-work (PoW) o prueba de trabajo, que consiste en descubrir mediante todas las combinaciones posibles ese valor aleatorio llamado Nonce. Como define Antonopoulos:

> En los términos más simples, la minería es el proceso de hacer hash de la cabecera del bloque de manera repetitiva, cambiando un parámetro, hasta que el hash resultante coincida con un objetivo específico. El resultado de la función hash no puede determinarse de antemano, ni se puede crear un patrón que vaya a producir un valor hash específico. Esta característica de las funciones de hash significa que la única manera de producir un hash resultante que coincida con un objetivo específico es intentarlo una y otra vez, modificando aleatoriamente la entrada hasta que el hash resultante que se desea aparezca por casualidad (2016:210).

Seguidamente, el primer minerx en lograr descifrar tal prueba y ganar esa "carrera" es quien obtiene el derecho de registrar las transacciones en la cadena. Para ello transmite la solución al resto de la red para ser aceptada y así quedar distribuida. En otras palabras, allí se comprueba si la solución propuesta es correcta. Antonopoulos utiliza la siguiente metáfora para dar cuenta de esta última dinámica:

> La competencia entre los mineros termina efectivamente con la propagación de un nuevo bloque que actúa como un anuncio del ganador. Para los mineros, recibir un nuevo bloque significa que otra persona ganó la competición y que ellos perdieron. Sin embargo, el final de una ronda de la competición marca también el comienzo de la siguiente ronda. El nuevo bloque no es sólo una bandera a cuadros, que marca el final de la carrera; también es el pistoletazo de salida en la carrera por el siguiente bloque (2016:199).

Una vez que las transacciones forman parte del bloque y se agregan a la cadena, se las consideran "confirmadas". En consecuencia, lo que se busca todo el tiempo es obtener un consenso compartido por toda la red, o la mayoría, para que el nuevo bloque se agregue a la copia de la cadena en cada nodo. Finalmente, ese bloque recién resuelto, mientras se propaga a lo largo de la red, es sometido a una serie de pruebas de validación por cada nodo antes de propagarlo a sus compañeros, de tal manera de asegurar que sólo se distribuyan bloques válidos. Este proceso de validación es la única forma de crear nuevos tokens en la mayoría de las redes, por lo tanto, lxs minerxs compiten entre sí y reciben como compensación por su trabajo cierto valor en la criptomoneda de la red que están minando, más las tarifas de las transacciones. En el caso del algoritmo de Bitcoin, una de sus características principales es el establecimiento de que su política de emisión monetaria coincida con la recompensa de lxs minerxs, es decir, se crea una determinada cantidad de nuevos bitcoins únicamente como pago al minerx que extrajo o resolvió el bloque, a su vez, tal recompensa se reduce a la mitad cada 210.000 bloques (aproximadamente cada cuatro años) en un proceso conocido como *Halving* (que pasó de otorgar 50 BTC en 2009 a la actual cifra es de 6,25 BTC). Además, el código BTC gobierna

tanto la emisión de bitcoins (serán 21 millones) como la periodicidad de la extracción (se mina un bloque cada 10 minutos, en promedio). Por último, el código estipula que las combinaciones numéricas aleatorias que se prueban en el minado deben devolver un resultado menor al marcado por la llamada "dificultad", la cual: "… es un parámetro variable en función de la cantidad de capacidad computacional que hay en la red. Aumenta o disminuye para que el tiempo promedio en resolver un bloque sea de 10 minutos." (Carmona, A. Et al. 2019:59).

Amén de ello, es posible interrogarse lo siguiente: si hubiera un minero que concentre el suficiente poder computacional para generar y conservar la mayoría de los bitcoins ¿Qué es lo que le impide hacerlo?, ¿no cabría esperar que ese minero significativamente más poderoso genere la gran mayoría tokens y excluya a los más pequeños? Por otro lado ¿qué pasaría si los mineros deciden rechazar bloques correctamente minados? En la compilación de textos de Satoshi Nakamoto hecha por Phil Champagne se explica que:

> El sistema de pago de Bitcoin mantendrá su valor sólo cuando funcione correctamente. Si los mineros rechazaran todos los bloques, excepto los propios, no se alcanzaría un consenso, el valor del sistema en general se destruiría y, ninguno de los mineros se beneficiaría. En tal caso, cualquier cantidad de bitcoins que los mineros posean perdería su valor. Por lo tanto, todos los mineros se benefician si todos respetan el protocolo Bitcoin establecido en el software compartido de Bitcoin. (2014:26).

Por su parte, en la dinámica de validación Antonopoulos sostiene:

> La validación independiente también asegura que los mineros que actúan con honestidad consigan que sus bloques sean incorporados a la cadena de bloques, lo que les hace ganar la recompensa. Aquellos mineros que actúen deshonestamente verán que sus bloques son rechazados y no solo pierden la recompensa, sino que también pierden el esfuerzo realizado para encontrar una solución de prueba de trabajo, incurriendo así en el coste de la electricidad sin compensación. (2016:222).

Aquí es importante destacar que cualquier cambio que se haga en un bloque anterior provoca un efecto de cascada en todos los demás, tal es así que quien quiera modificar alguno de los bloques preexistentes se encuentra obligado a "minar" toda la cadena de nuevo, lo cual implica una cantidad enorme de recursos. Ergo, mientras más extensa es la cadena, más difícil es de cambiar o reescribir, mientras más nodos se le conectan y más usuarixs existan, también la seguridad y la estabilidad crecen[16]. Nakamoto sintetizaba en su artículo fundacional que: "El sistema es seguro mientras los nodos honestos controlen colectivamente más potencia CPU[17] que cualquier grupo cooperante de nodos atacantes." (2008:1). Esto bajo ningún aspecto quiere decir que el sistema esté exento de ataques informáticos[18], pero sí que dado su carácter distribuido sus niveles de resiliencia son muy altos porque no hay un único punto de ataque al cual dirigirse concretamente. Tampoco hay que descartar la posibilidad de tendencias monopolizadoras;

[16] A pesar de ello, es necesario destacar que: "Hasta ahora Bitcoin nunca ha sufrido este tipo de ataques, pero otras cadenas con menos hashrate sí. El hashrate recordemos que es la capacidad computacional total de la red, y si es suficientemente baja, podríamos contratar la potencia necesaria en servidores para realizar un ataque satisfactorio" (Carmona, A. Et al. 2019:66).

[17] Se recuerda que el minado con CPU en BTC ha sido reemplazado por los mineros ASICs.

[18] Por ejemplo, se conoce entre usuarixs el llamado "el ataque del 51%" a la posibilidad latente de que alguien llegue a controlar el 51% de la red y así obtener el poder para reescribir los bloques subsiguientes a su antojo. Sin embargo, en teoría el costo de hacerlo es tan elevado que desincentiva tal estrategia y constituye una barrera para criptoataques de esta envergadura.

por ejemplo, en la actualidad existen pools de minería[19] que concentran grandes cuotas de poder computacional mientras que el hardware necesario para minar se especializa y encarece cada vez más. Además, el equipamiento que utilizan lxs minerxs consume grandes cantidades de energía[20], haciendo que su huella ecológica sea uno de los aspectos más criticados de las criptomonedas.

En general para sus usuarixs, tales efectos son el costo a pagar por la idea estandarte de Bitcoin: la descentralización, la cual se encuentra ligada directamente a su esquema de seguridad. En primer lugar, porque no hay un único núcleo que maneje toda la información "on-chain" (en la cadena de bloques) dado que cada nodo de la red tiene una copia de la cadena y ésta se actualiza de forma automática. En segundo lugar, la única información relevante para la red son las direcciones y los montos (términos de un acuerdo) de las operaciones, por lo que los datos privados de sus usuarixs permanecen ocultos. Pero fundamentalmente la seguridad en Bitcoin se resume en su sistema de minería, de tal forma que Antonopoulos expresa que "La recompensa de las monedas recién acuñadas y las comisiones de transacción es un plan de incentivos que alinea las acciones de los mineros con la seguridad de la red, mientras al mismo tiempo aplica la oferta monetaria" (2016:193). Esto indica que la minería es más que un mecanismo de oferta monetaria, es a la vez un "mecanismo de consenso descentralizado en toda la red, en el que se basa la seguridad de bitcoin". Sin embargo, si no se cuenta con los Nodos, el modelo de seguridad Bitcoin está incompleto.

Sobre lo dicho, ¿quiénes toman las decisiones en Bitcoin? En general existen dos posibilidades para cualquier criptomoneda: sea por mecanismos de gobierno "on chain", en la cual la tenencia de cierto token le otorga a les usuarixs la potestad de tomar decisiones sobre el futuro de la cadena. La segunda vía es la "off chain" o fuera de la blockchain y aquí el poder de decisión sobre los cambios en la tecnología es de quienes llevan adelante el proyecto, como puede ser el grupo de desarrolladores del código fuente. Y esta segunda opción es el caso de Bitcoin. Aun así, ambos modelos de gestión comparten la necesidad de priorizar el consenso como uno de los criterios principales, dado que una arbitraria decisión puede provocar la fuga de usuarixs de la cadena o la depreciación del criptoactivo. Todo lo cual quiere decir que si hay consenso hay cooperación de los nodos, para validar y seguir la cadena más larga y segura.

Un software, una construcción social

Bitcoin antes que nada ha sido definido desde su manifiesto fundacional como un sistema electrónico de pagos directos, y quizás esta haya sido la idea original de sus creadores, pero actualmente ese no es su uso principal. Como sostienen lxs autores David Arroyo Guardeño et al, constituye "mucho más que un mecanismo de intercambio de valor financiero, ya que genera todo un ecosistema de actividad económica que se conoce bajo el nombre de criptoeconomía." (2019:45). En concatenación, también existe una "comunidad" detrás de la criptodivisa, marcada tanto por discusiones, definiciones abiertas como por acordes básicos comunes, una heterogeneidad de debates que forman parte de

[19] Véase: https://www.blockchain.com/es/pools

[20] En: https://digiconomist.net/bitcoin-energy-consumption se puede consultar un índice de consumo de energía de Bitcoin, cuya "huella total anualizada" es de aproximadamente 77,78 TWh (Teravatio-hora). En 2017 el mismo índice daba por resultado la estimación de 9,58 TWh. Según este sitio, actualmente el consumo de energía en BTC es comparable al de Chile y la huella de carbono a los niveles de Nueva Zelanda.

un ensamblaje discursivo (Laclau, E. Mouffe, C. 1987) cuyo consenso se estructura como oposición a las "injerencias centralizadoras o de control en cualquier ámbito social" e inscripto "en una ideología *cypherpunk*, donde los elementos libertarianos o anarcocapitalistas son los destacables" (Correa Lucero, H. 2019:209). En otras palabras, si la Red Bitcoin y las demás criptomonedas fueron diagramadas para operar más allá de la regulación estatal, el "ascenso hacia la independencia de los intercambios une en éxtasis a los cyberpunks y a los ultraliberales." (Sadin, É. 2020:199).

Expuesto lo anterior, se identifican los siguientes planos básicos y generales constitutivos del sistema BTC:

- Es un protocolo contable y de comunicación no centralizado que construye una cadena de bloques a modo de "un libro públicamente disponible y que contiene los registros contables de todas las transacciones realizadas en el sistema Bitcoin, al que constantemente se le añaden nuevas páginas" (Champagne, P. 2014:21).
- Es una red informática distribuida de nodos y minerxs que hacen las operaciones (verificación y validación) de la hoja de cálculo con un esquema criptográfico de protección de la información de las transacciones. Aquí los bloques de información se van encadenando y ello va actualizando el "libro contable".
- Posee una unidad de cuenta (o token) que es única: la criptomoneda bitcoin, es decir, una divisa enteramente digital para realizar transferencias de valor. La misma se puede convertir fuera de la red en dinero de curso legal. Esos bitcoins se envían desde y hacia direcciones de bitcoin, que son esencialmente números aleatorios sin información que los identifique (Champagne, P. 2014:111).
- Por último, es una comunidad de consenso, desarrollo y discusión cuyo modelo es impulsado por sus usuarixs. La idea es que elles encuentren como más racional y provechoso seguir las reglas del modelo.

Sin embargo, Bitcoin no tuvo una historia lineal y ello incluye varias problemáticas, como el robo de miles de criptomonedas y hackeos a Exchanges, las complicaciones propias de los ciclos bajistas de su precio, problemas técnicos y legales en las plataformas, debates por las actualizaciones del código y las diferentes divisiones de la cadena ("forks") producidos, hasta su utilización para operar en sitios de la llamada *Deep Web.*

Variantes de Bitcoin, llegada de Ethereum y las Stablecoins

La multiplicación de criptomonedas no se debe solamente a que sus códigos sean de acceso abierto ni simplemente a las oportunidades de crear servicios financieros alternativos que abre el ecosistema como tal. Lejos de la hipótesis neoliberal de una ontología de los mercados espontáneos, los denominados hard forks o bifurcaciones en una blockchain son contundentes episodios donde afloran las tensiones políticas que hasta el momento mantenían cierta convivencia hacia el interior de determinado proyecto cripto-monetario. En el caso de BTC con el correr del tiempo se desprendieron los proyectos de Bitcoin Cash (BCH), Bitcoin Gold (BTG), Bitcoin Diamond (BTD), Bitcoin Satoshi Vision (BST), Bitcoin Private (BTP) y un largo etcétera. En el sitio de Coin Market Cap se pueden encontrar alrededor de cien (100) criptomonedas o tokens con la palabra "Bitcoin". Y es que:

> "A diferencia de un soft fork, en un hard fork se produce un cambio en el código de una criptomoneda que hace incompatible la nueva versión con las versiones anteriores.

> Este proceso que provoca lo que denominamos 'bifurcación de la red'; hay que elegir entre usar la nueva versión del software o la anterior"[21].

No obstante, el ecosistema se compone también de los proyectos surgidos sobre la innovación de Bitcoin, pero con una blockchain diferente desde cero. El caso por excelencia lo constituye Ethereum (ETH), la red y la criptomoneda de mayor importancia luego de BTC, tanto en su precio por unidad monetaria, su capitalización de mercado, como por sus características distintivas. Surgida a mediados de 2015, entre sus adjetivos podemos destacar que:

- Es, ante todo, una plataforma digital basada en tecnología blockchain para ejecutar aplicaciones descentralizadas (Dapps) frente a la falta de flexibilidad del protocolo de Bitcoin[22], es decir, su poca capacidad para generar nuevos servicios más allá de la transferencia de valor.
- Para ello, su blockchain tiene la capacidad de crear Smart Contracts (SC) y nuevos tokens. Por un lado, un Smart Contract es un programa informático que ejecuta determinadas acciones preestablecidas en su código que han sido revisadas y aceptadas por las distintas partes que han "firmado" dicho contrato. Luego, aquellas condiciones programadas presentan una respuesta acorde a sus cláusulas de forma autónoma[23]. Por otro lado, esta red cuenta con los ERC (*Ethereum Request for Comments*), una serie de documentos técnicos que perfilan estándares para programar en Ethereum y permiten establecer convenciones que faciliten la interacción de aplicaciones y contratos[24]. Entre ellos está el estándar ERC-20 que provee de un formato para crear nuevos tokens sobre una base compartida, los llamados Tokens ERC-20, básicamente un SC para generar interoperabilidad y compatibilidad de tokens y funciones.
- Cuenta con una moneda denominada Ether, se puede utilizar como método de pago y no depende de ningún Estado o banco central. Si bien la emisión anual se limita a 18 millones de Ethers, la emisión total no tiene restricciones, es infinita. Sin embargo, se ha introducido en los últimos tiempos la denominada "quema de ethers" en el pago de las tarifas, es decir, la eliminación definitiva de unidades de esta criptomoneda para reducir la oferta de ETH en circulación y así lograr el efecto deflacionario que ocurre con BTC. Además, sus bloques se generan cada 15 segundos.
- Actualmente Ethereum se actualizó a su versión 2.0 y ha reemplazado la minería de Proof of Work por el protocolo Proof of Stake (PoS), en el que para ser un validador ya no es necesario tener un equipo especializado con poder de cómputo para solucionar un enigma criptográfico sino "solamente" una determinada cantidad del token en cuestión como colateral, en este caso 32 Ethers.
- Al igual que Bitcoin, su gobernanza es off-chain, esto es, sin mecanismos fijos de deliberación programados dentro de la cadena de bloques e implicando que los actores que dan vida a la red deban discutir entre la escena off-line y la on-line de nuestras sociedades. Pero a diferencia del primero, ETH cuenta con un referente visible en tanto líder del proyecto, Vitalik Buterin, y ello supone toda una discusión

[21] Recuperado de: https://academy.bit2me.com/que-es-hard-fork/

[22] Recuperado de: https://academy.binance.com/es/articles/an-introduction-to-erc-20-tokens

[23] Recuperado de: https://academy.bit2me.com/que-es-ethereum-eth-criptomoneda/

[24] Recuperado de: https://academy.binance.com/es/articles/an-introduction-to-erc-20-tokens

en términos de seguridad nada menor como así también una distinción esencial con respecto a BTC y el anonimato de Nakamoto.

Un último punto necesario por el cual pasar son las Stablecoins (criptomonedas estables), aquellas que anclan su precio a un activo manteniendo una relación de paridad. Las hay centralizadas o descentralizadas y con una gama de grises entre esos dos polos, pero fundamentalmente existen tres tipologías o esquemas: las de respaldo no-crypto, ya sean las basadas en algún dinero "tradicional" como el dólar (de relación 1 a 1) mediante reservas en esa misma moneda como forma de garantía (por ejemplo USDT, USDC Y BUSD) o las ancladas a un metal precioso (tal es el caso de PAX Gold con la onza de oro); luego están las que fijan su valor y/o respaldo sobre una o varias criptomonedas, por lo que sus tokens se colateralizan teniendo en cuenta la volatilidad del criptoactivo elegido (como el caso de DAI); por último se encuentran las stablecoins algorítmicas, las cuales controlan su suministro mediante algoritmos y contratos inteligentes que, o bien reducen el suministro del token si el precio cae por debajo de la moneda tradicional que emula, o emiten nuevos tokens para reducir el valor de la "stable" en caso de que su precio supere el de la moneda en cuestión[25]. No obstante, este último esquema se encuentra frente a profundos problemas y un futuro incierto: en mayo del 2022 entró en crisis el ecosistema de la fundación Terra porque su cripto estable y algorítmica llamada UST perdió la paridad con el dólar en el marco de una corrida cambiaria sobre el token Luna, otro activo de Terra que respaldaba (junto a una reserva de bitcoins) a este "dólar cripto". Tanto Luna como el UST perdieron totalmente su valor hasta quedar en cero en el lapso de unos días, lo que rápidamente extendió una crisis de confianza al mercado cripto en general.

Para finalizar, y debido a los límites de extensión, existe una variedad de temas de la economía de las criptomonedas que no es posible abordar por el momento, pero si es factible nombrar una grilla de temáticas a modo de que lxs lectorxs tengan una especie de "índice" para profundizar más allá del presente escrito. Algunos temas son: variedades de blockchains (públicas, privadas e híbridas) y posibilidades de construcción de nuevas funcionalidades sobre las mismas, problemas de escalabilidad y ejemplos de cadenas como Algorand, Binance Smart Chain o Solana; Exchanges centralizados (Binance, Kraken) vs descentralizados (Uniswap, MDEX); tipos de oráculos para blockchains; diferentes formatos de minería; protocolos DeFi (finanzas descentralizadas) como Aave y diversos estándares de tokens como las distintas tipologías del ERC; economía de Tokens No Fungibles (NFTs) y de juegos Play-to-Earn; las características de otras criptomonedas (Altcoins) y sus correspondientes "narrativas"; nociones de criptografía aplicadas a estos temas, etc.

Algunas notas para concluir

A partir de lo expuesto, podemos ensayar algunas ideas en relación a los debates sobre la subjetivación contemporánea y, dentro de estos, la respectiva orientación teórica-política-metodológica que identifica a nuestro programa de estudios, aquí resumida como *las izquierdas lacanianas*. El programa SPEDC parte de una distinción conceptual fundante: la diferencia radical entre el Sujeto del inconsciente (para Lacan el sujeto dividido, en falta, como efecto –no pasivo- de una cadena significante), y la subjetividad, producto de diversos dispositivos de poder (Alemán, J. 2016). Así, la subversión del sujeto cartesiano producida en la enseñanza lacaniana puede leerse bajo dos lemas suyos: por un lado, que

[25] Recuperado de: https://academy.binance.com/es/articles/what-are-stablecoins

"el significante representa un sujeto para otro significante." (Lacan, J. 2010:164), por otro, que "pienso donde no soy, luego soy donde no pienso" (Lacan, J. 2009:484). En consecuencia, tal sujeto habita en el encadenamiento recíproco de las dimensiones de lo Simbólico, lo Imaginario y lo Real en el lenguaje, anudamiento que Lacan graficará con el llamado nudo Borromeo[26].

Este rodeo nos permite tres planos de discusión. A saber: con el despliegue tecno-financiero que hemos descrito, encontramos una novedosa vía de capilarización acelerada de las finanzas, lo que sin dudas ha ayudado a corroer aún más las fronteras entre aquellas (el sistema bancario, la bolsa de valores, los mercados financieros, etc.) y la ciudadanía en general. En esta suerte de desterritorialización y reterritorialización de flujos monetarios y bursátiles es posible arriesgar 1) como correlato la idea de una profunda afectación de dicha categoría de sujeto y del lazo social con resultados todavía inciertos pero cercanos, si no hacemos nada, a un puro automatismo circular bajo la ley del valor o, en palabras de Jorge Alemán, intentando eliminar la propia constitución simbólica del sujeto (2016:22), fin último de la razón neoliberal; 2) que un ecosistema con tales características (propias de la creciente ontología de las "no-cosas") puede ser pensado como una economía política de signos, al decir de Baudrillard (1986), dada la carga significante que es posible rastrear en su campo de discursividad constitutivo, el cual acolchona a todos estos "cripto-instrumentos" en su prestación social; y 3) que su modelo de subjetivación no se ajusta del todo a la del *empresario de si* foucaultiano (generalmente consideradx arquetipo de la gubernamentalidad neoliberal) porque, al relanzar la abstracción social del capital, con dicha economía se abren puertas a otras prácticas de subjetivación: quizá no se trate solamente de la desvinculación como forma de ser de la que habló Badiou, ni simplemente del privatismo cívico habermasiano, tentativamente quizá sea algo como una "identificación rizomática" lo que se esté poniendo en juego, pero siempre en carácter de mixtura.

[26] Lacan, Seminario 19. "...o peor". 2012. Paidós.

Bibliografía

Alemán, J. (2016). *Horizontes neoliberales de la subjetividad*. Grama ediciones.

Antonopoulos, A. (2016). *Mastering Bitcoin. Programming the open Blockchain*. O' Reilly Media. Traducción al español.

Appadurai, A. (2017). *Hacer negocios con palabras. El fracaso del lenguaje como clave para entender el capitalismo financiero*. Siglo XXI editores.

Arroyo Guardeño, D. Díaz Vico, J. y Hernández Encinas, L. (2019). *¿Qué sabemos de blockchain?* Editorial Catarata y el Consejo Superior de Investigaciones Científicas de España (CSIC).

Baudrillard, J. (1979). *Critica a la economía política del Signo*. Siglo XXI editores.

Carmona, A. Orellana, D. y Pulido, S. (2019). *Trading, blockchain y criptoeconomía. La punta del iceberg*. Uno editorial.

Champagne, P. (2014). El Libro de Satoshi. *Libro Blockchain*. Recuperado de: http://www.libroblockchain.com/satoshi/

Correa Lucero, H. (2019). Tecnología, sociedad e internet: hacia una comprensión crítica de la tecnología, las tecnologías digitales y su cambio. Un estudio de las tensiones en torno a la mercantilización en Internet. (Tesis de posgrado). Bernal, Argentina: Universidad Nacional de Quilmes. Disponible en RIDAA-UNQ Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes: http://ridaa.unq.edu.ar/handle/20.500.11807/1042

Lacan, J. (2009). *Escritos 1*. Siglo XXI editores.

Lacan, J. (2010). *El Seminario 11. Los Cuatro Conceptos Fundamentales del Psicoanálisis*. Paidós.

Lacan, J. (2012). *El Seminario 19. ...o peor.* Paidós.

Laclau, E. y Mouffe, C. (1987). *Hegemonía y estrategia socialista. Hacia una radicalización de la democracia.* Siglo XXI.

Nakamoto, S. (2009). Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. Recuperado de: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Preukschat, Á. y Molero Manglano, I. (2017). Introducción ¡Bienvenido a la generación blockchain! En: Á. Preukschat, I. Molero Manglano, C. Kuchkovsky Jiménez, G. Gómez Lardies y D. Díez García, (coord.), *Blockchain: la revolución industrial de internet*. Recuperado de: https://libroblockchain.com

Sadin, E. (2020). *La inteligencia artificial o el desafío del siglo. Anatomía de un antihumanismo radical*. Caja Negra.