Unidad 1: Bitcoin y Ethereum

2.1.1 Bitcoin

Bitcoin es un fenómeno social basado en el potente sistema tecnológico de transacciones que se viene desarrollando y, como medio de intercambio, no parece tener rivales en este momento. Es, actualmente, la moneda virtual convertible más grande por capitalización bursátil, cerca de US$ 72 mil millones de dólares en agosto de 2017. Fue creado en 2008 por Satoshi Nakamoto, con la idea de que "Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas, lo que permite que dos partes interesadas transmitan directamente entre sí sin la necesidad de un tercero de confianza" (https://goo.gl/6sSczk).

Carranza Torres caracteriza *bitcoin* de la siguiente manera:

- Es parcialmente anónimo, las personas participantes del sistema pueden ser identificadas por una clave pública.
- Se basa en criptografía y firmas digitales únicas.
- Se ejecuta en una red descentralizada de computadoras y "mineros" que operan con software de código abierto y "trabajan" para validar y registrar las transacciones en un libro mayor público permanente distribuido que puede ser visto por cualquiera en la red.
- Registra las transacciones en un libro de contabilidad público de transacciones validadas.
- Permite la transferencia de propiedad sin la necesidad de un intermediario central de confianza. (https://goo.gl/jimcnL)

Existe un misterio alrededor del fenómeno que conocemos como criptomonedas respecto de quién es su creador. Como dijimos, se sabe que se llama Satoshi Nakamoto, una especie de John Galt[1] japonés, pero no se sabe si efectivamente existe o ha existido, si es una persona o un grupo de personas, todo lo cual acrecienta la leyenda que rodea a *bitcoin*.

[1] Personaje libertario de la novela *La Rebelión de Atlas* de Ayn Rand.

Antes del *bitcoin* hubo muchos intentos de llevar a cabo una moneda exitosa pero, en general, fracasaban precisamente porque nunca se había logrado una tecnología que eliminara ese "tercero de confianza".

Como mencionábamos, fue Satoshi Nakamoto quien implementa, por primera vez, "una moneda descentralizada, combinando tecnologías primitivas ya establecidas para la gestión de la propiedad, a través de la criptografía de clave pública, más un algoritmo de consenso para llevar la cuenta de quién es el dueño de las monedas, conocido como 'prueba de trabajo'". (Ethereum Whitepaper. Traducción recuperada de: https://goo.gl/XDppik)

> El mecanismo detrás de la prueba de trabajo fue un gran avance, ya que resuelve simultáneamente dos problemas. En primer lugar, proporciona un algoritmo de consenso simple y moderadamente eficaz, permitiendo que los nodos de la red, se pongan de acuerdo colectivamente, en un conjunto de actualizaciones perfectas del estado actual del libro contable de *Bitcoin*. En segundo lugar, proporciona un mecanismo para permitir la entrada libre en el proceso de consenso, resolviendo el problema político de decidir quién va a influir en el consenso, y evitando al mismo tiempo los ataques de tipo Sybil. Lo hace mediante la sustitución de dos barreras: la barrera formal para participar, es decir, el requisito de estar registrado como una entidad única en una lista particular, y la barrera económica, el peso de un solo nodo en el proceso de votación por consenso es directamente proporcional a la potencia de cálculo de la que el nodo dispone. Desde entonces, se ha propuesto un enfoque alternativo, llamado prueba de participación (*proof of stake*), en donde el peso de un nodo debe ser proporcional a su posesión de moneda y no a sus recursos computacionales. (https://goo.gl/GFp7dy).

No es el objetivo de este trabajo desentrañar la identidad del creador o los creadores del *bitcoin*, sino entender la tecnología en que se sustenta para que ustedes cuenten con herramientas propias de análisis y decisión, por esa razón vamos a dejarlo hablar a Satoshi para tratar de entender cuál fue su propósito y el plan que diseñó para lograrlo.

2.1.2 *Peer to peer* para eliminar los costos de intermediación

En palabras de Satoshi, el bitcoin es "… una versión completamente *peer to peer* de efectivo electrónico que permitiría pagos en línea, los cuales se enviarán directamente de una parte a otra sin pasar por una institución financiera" (https://goo.gl/MqyCW7).

Aquí tenemos un objetivo claro para impulsar la creación del *bitcoin*: eliminar la intermediación (bancaria o estatal) en las transacciones que impliquen pagos.

La tecnología de firma digital[2] es muy usual en las transacciones bancarias y en los sistemas de pagos en general. Satoshi entiende y enfatiza su utilidad; sin embargo, en el sistema transaccional actual, implica un doble gasto al requerir de un tercero de confianza. El sistema *peer to peer* elimina los costos de requerir intermediarios.

En Internet, las instituciones financieras actúan como "terceros de confianza" y si bien eso funciona bastante bien, hay problemas sistémicos que hacen necesario revisarlo para resolver algunas cuestiones que encarecen aún más todo el mecanismo de validación de transacciones.

Por ejemplo, la mera posibilidad de que una transacción, una vez realizada, se revierta implica la necesidad de aumentar los costos de *enforcement*.

Otro de los objetivos del *bitcoin,* entonces, es realizar transacciones irreversibles para bajar los costos generales del sistema transaccional. "Con la posibilidad de reversión, la necesidad de confianza se extiende. Los comerciantes deben desconfiar de sus clientes, molestándolos por más información de la que de otra manera necesitarían."

El sistema transaccional previo a las criptomonedas acepta un cierto porcentaje de fraude como inevitable. "Estos costos e incertidumbres de pago se pueden evitar en persona mediante el uso de moneda física, pero no existe ningún mecanismo para realizar pagos a través de un canal de comunicaciones sin un tercero de confianza."

El documento referido propone un sistema de pago electrónico basado en pruebas criptográficas en lugar de terceros de confianza. O lo que hemos llamado más arriba, un sistema transaccional *peer to peer*, en el que las

[2] Citar página de este trabajo

personas puedan realizar sus transacciones directamente entre ellas, sin la necesidad de que intervenga el Estado, los bancos u otros agentes identificadores, validadores o certificadores.

> Las transacciones que son impracticables desde el punto de vista informático protegerían a los vendedores contra el fraude, y los mecanismos de custodia de rutina podrían implementarse fácilmente para proteger a los compradores. (Satoshi. https://goo.gl/H7ykek.)

2.1.3 La privacidad de las transferencias

Otro objetivo del sistema *blockchain* de *bitcoin* es la privacidad. En el sistema bancario actual, se logra cerrando la información impidiendo el acceso a terceros. Con *blockchain*, en cambio, la necesidad de anunciar públicamente todas las transacciones impide este método. La privacidad se asegura, entonces, manteniendo anónimas las claves públicas. Es decir, cualquiera puede ver que alguien está enviando un monto a otra persona, pero no puede vincular la transacción con una persona determinada, sino con la existencia de autorización para que dicha transacción se realice. Las bolsas de valores funcionan de manera similar, se publican detalladamente los movimientos, pero sin señalar a las partes involucradas (Nakamoto en Rivas Villarroya, 2018, https://goo.gl/H7ykek).

El anonimato se pierde si se revela quién es el propietario de una determinada clave pública.

> Como si se tratara de un firewall adicional, se debe usar un nuevo par de claves para cada transacción para evitar que se vinculen con un propietario común. Algunos enlaces aún son inevitables con las transacciones de múltiples entradas, que necesariamente revelan que sus entradas fueron propiedad del mismo propietario. Sin embargo, si se revela el propietario de una clave, la vinculación podría revelar otras transacciones que pertenecieron al mismo propietario. (Nakamoto en Rivas Villarroya, 2018, https://goo.gl/H7ykek).

2.1.4 Seguridad de *Bitcoin*: sobre los incentivos

El sistema para transacciones electrónicas que describimos no requiere de validación de confianza para funcionar. Comenzó con el marco habitual de monedas hechas con firmas digitales, lo cual proporciona un fuerte control de la propiedad, pero está incompleto sin una forma de evitar el doble gasto. Con el fin de resolver esto, se propuso una red *peer to peer* utilizando pruebas de trabajo para registrar un historial público de transacciones (las cuales rápidamente se vuelven imprácticas, desde el punto de vista computacional, para que un atacante cambie si los nodos honestos controlan la mayoría del poder de la CPU). La red es robusta a pesar de su aparente simplicidad desestructurada. Los nodos funcionan todos al mismo tiempo, con poca coordinación. No es necesario identificarlos, ya que los mensajes no se envían a ningún lugar en particular. Los nodos pueden salir y unirse a la red a voluntad, aceptando la cadena de prueba de trabajo como constatación de lo que sucedió mientras ellos no estaban. Votan con el poder de su CPU, es decir, expresan la validación de los bloques con el solo hecho de aceptar trabajarlos y, de esta manera, en extenderlos; caso contrario, lso bloques inválidos son rechazados. Todas las reglas e incentivos necesarios se pueden aplicar con este mecanismo de consenso.

2.1.6 *Ethereum Blockchain* 2.0

> *Ethereum no pretende ser el final de toda innovación de criptomonedas, tiene la intención de ser el comienzo.*
> *Vitalik Buterin*

La fecha oficial de nacimiento de la red *Ethereum* es el 30 de julio de 2015, día en el cual se graba el bloque génesis. Un largo e intenso trabajo de alrededor de un año de un importante equipo de desarrolladores echaba a rodar.

A diferencia de lo que pasaba con *bitcoin* (BTC), el creador de *Ethereum* existe, y se llama Vitalik Buterin, un joven que a los 20 años había juntado más de quince millones de dólares (26.000 BTC en agosto de 2014). Este muchacho, nacido en Rusia, se mudó a Canadá a los seis años y a los diez ya había escrito el código de su propio *Space invaders*. Colaboraba escribiendo

para el blog *Bitcoin Weekly,* y le pagaban 5 BTC por artículo (cuando el precio de la unidad se cotizaba en U$S 3,75). Por problemas con su visado no pudo entrar a trabajar en Ripple. A esa altura, y habiendo decidido dedicarse a los *bitcoins*, dado que no tenía tiempo para trabajar mientras estudiaba, decide dejar el curso avanzado de ciencias de la computación de la Universidad de Waterloo.

2.1.7 Contratos autoejecutables

Buterin será reconocido por varias cosas, pero especialmente como "el padre de los *smart contracts*", a los que define sencillamente como un programa de computación en *blockchain*, que controla activos digitales de manera directa.

Una conceptualización más extensa de los *smart contracts* (contratos inteligentes) señala que facilitan el intercambio de dinero, propiedades, acciones, contenidos o cualquier cosa de valor (Davidson, 2017). Cada grupo de estas transacciones, como ya sabemos, se denomina bloque.

El *blockchain* de *Ethereum* es un contrato que se ejecuta a sí mismo y que puede manejar *enforcement*, administración, *performance* y pagos por sí mismo. Cuando estos códigos corren en *blockchain*, el sistema se convierte en una computadora auto-operable que se ejecuta sola cuando determinadas condiciones se cumplen.

En *Blockchain 2.0*, los libros de contabilidad distribuidos han añadido un nivel lógico en la forma de contratos inteligentes. Este código existe junto con la información de la base de datos.

Los *smart contracts* funcionan igual que los programas "tokenizados". A pesar de tener claves públicas como cualquier otra cosa en la red, poseen código y pueden llevar a cabo, por ejemplo, un procedimiento almacenado. Ofrecen una gran cantidad de promesas para crear sistemas inteligentes con contratos de auto-ejecución para permitir que los procesos de negocio funcionen de forma independiente.

Blockchain 2.0 y 1.0 difieren en cómo las cosas son "tokenizadas" y se tramitan. Un *smart contract* es esencialmente un registro de sí mismo en el libro distribuido. Existen activos de "tokenización" dentro de *smart contracts*. Las "entidades tokenizadas" son para el sistema como personas, organizaciones,

activos, mercancías. Las aplicaciones o contratos que trabajan con esos elementos son "validados" en sistemas basados en *smart contract*.[3]

2.1.8 *Ethereum*: mucho más que *smart contracts*

Ethereum es un *blockchain* con un lenguaje de programación incorporado, que permite a cualquier persona programar cualquier aplicación que use *blockchain*.

Ethereum evidencia las ventajas que implica la articulación de las tres tecnologías que Satoshi Nakamoto combinó con maestría para crear el *bitcoin*[4] y pretende dar a *blockchain* una nueva dimensión. Ha establecido un nuevo *standar* transaccional. Una nueva Ley.

Blockchain 2.0 viene a ser una evolución, una mejora en el sentido de un mejor y más extenso aprovechamiento, o en todo caso, mejores posibilidades de escalabilidad para el sistema.

Vitalik Buterin explica en varios artículos de qué se trata el *Blockchain 2.0*, pero sobretodo plantea que Bitcoin tiene un problema de escala, por haber sido diseñado para ser una criptomoneda.

> (…) esto es lo que Ethereum intenta arreglar. Ethereum no tiene la intención de ser un protocolo de navaja suiza con cientos de características para satisfacer todas las necesidades; en su lugar, Ethereum pretende ser un protocolo fundacional superior y permitir que otras aplicaciones descentralizadas construyan sobre él en lugar de Bitcoin, proporcionándoles más herramientas para trabajar y permitiéndoles obtener los beneficios completos de la escalabilidad y eficiencia de Ethereum. (https://goo.gl/CFpDpP)

Bitcoin es una criptomoneda basada en *blockchain*, mientras que Ethereum es un *blockchain* programable y autoejecutable. Es

[3] Proyecto Blechtley Microsoft.
[4] Blokchain, DLT y tragedia de los comunes.

> (…) una plataforma descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares. Cualquier desarrollador puede crear y publicar aplicaciones distribuidas que realicen contratos inteligentes. Ethereum también provee una ficha de criptomoneda que se llama 'ether'. Se puede intercambiar ether entre cuentas diferentes y también compensar a los nodos participantes los esfuerzos computacionales realizados. (https://goo.gl/nr4DmS)

Ethereum[5] es una plataforma descentralizada que ejecuta contratos inteligentes tal como se programaron sin posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros.

> Estas aplicaciones se producen en una cadena de bloques personalizada, una infraestructura global compartida, enormemente poderosa, que puede mover el valor y representar la titularidad de la propiedad. Esto permite a los desarrolladores crear mercados, almacenar registros de deudas o promesas, mover fondos, en consonancia con las instrucciones dadas en el pasado (como un testamento o un contrato de futuros), entre otras posibilidades. Todo sin un intermediario de confianza (https://goo.gl/MSRLuf).

El proyecto fue iniciado mediante una preventa de 'ether' en agosto de 2014 por aficionados de todo el mundo. En su página oficial se presenta de la siguiente manera:

> El objetivo de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas, proporcionando un conjunto diferente de posibilidades que creemos va a ser muy útil para este tipo de aplicaciones, con especial énfasis en situaciones donde son importantes: un tiempo de desarrollo rápido, la seguridad en aplicaciones pequeñas y que rara vez se utilizan, y la capacidad de que aplicaciones diferentes interactúen de manera muy eficiente. Ethereum hace esto mediante la construcción de lo que es esencialmente una capa abstracta funcional definitiva: una cadena de bloques con un lenguaje de programación integrado del tipo Turing-completo, que permite que cualquiera pueda escribir contratos inteligentes y aplicaciones descentralizadas que pueden crear sus propias reglas para la gestión de la propiedad, los formatos de transacción y las funciones de transición de estados. Una versión escueta de Namecoin se puede escribir en dos líneas de código,

> y otros protocolos como monedas y sistemas de reputación se pueden construir con menos de veinte. Los contratos inteligentes, las "cajas" criptográficas que contienen un determinado valor y que sólo se desbloquean si se cumplen ciertas condiciones, también puede ser incorporadas en la parte superior de la plataforma, con mucho más poder que el que ofrece el lenguaje de secuencias de comandos de Bitcoin, debido a los potencia añadida del Turing-completo, el valor-conocimiento (value-awareness), el blockchain-conocimiento (blockchain-awareness) y el estado. (https://goo.gl/uow5v3).

2.1.9 *Solidity*: el lenguaje de programación de *Ethereum*

El principal aporte de Vitalik Buterin y su equipo al sistema de *blockchain*, es el lenguaje de programación que se dio en llamar *solidity*.

Los lenguajes de programación son herramientas que permiten a los programadores dar instrucciones precisas a una máquina. En su evolución histórica, fueron la consecuencia de la necesidad de lograr programaciones automáticas para ahorrar tiempo (Carranza Torres, 2014).

Como todo lenguaje, el de programación es cultural y la forma que adopta cada uno para comunicarse con la máquina tiene mucho que ver con la filosofía de resolución de problemas que tenga su creador. Todo lenguaje de programación es un lenguaje exclusivamente escrito, al menos por ahora, ya que la máquina solo comprende el sistema binario. El circuito de cada procesador le permite a la computadora entender un conjunto de instrucciones dado. Estas instrucciones están codificadas en el lenguaje binario de la máquina, en la forma de unos y ceros.

Para traducir el lenguaje humano a una sucesión de unos y ceros comprensible por la máquina es necesario, primero, escribir las instrucciones en un lenguaje de programación, que es una manera más precisa de expresar las instrucciones, con estrictas reglas sintácticas y gramaticales que eviten la ambigüedad y vaguedad del lenguaje humano común.

Esto se conoce como "programa fuente", que podríamos definir como un lenguaje alternativo, utilizado para articular ideas con mayor precisión que con el lenguaje tradicional, y que instruye a los programadores sobre cómo llevar a cabo su tarea.

Para que la computadora entienda las órdenes que le damos, necesitamos un "programa objeto", el cual puede ser definido como una extensa combinación de unos y ceros destinados a ser leídos por la computadora y que implican una serie instrucciones específicas a ser ejecutadas por esta. Su característica saliente es su "intercambiabilidad" con el hardware, en el sentido de que un dispositivo electrónico conectado a una computadora puede lograr el mismo resultado que si fuera inducido por el código objeto, razón por la cual muchas veces los programas de computación reciben el nombre de "máquinas virtuales" (Halpern, 2000).

Lo que transforma un programa fuente en un programa objeto (legible por la computadora) se llama "compilador", el cual puede ser caracterizado como un "programa que traduce instrucciones escritas en un lenguaje que los seres humanos pueden entender, a códigos binarios que las computadoras pueden ejecutar" (Ceruzzi, 2003).

Dicho de forma más simple, el compilador es una suerte de "traductor" que lleva el mundo de los humanos al mundo de las máquinas, es el "intérprete" que le dice a la máquina que haga lo que el humano ordenó en otro programa que este pueda entender.

Compilador es, entonces, el traductor de un lenguaje de alto nivel, como Fortran o C++, a lenguaje de máquina (el lenguaje del procesador). Los compiladores permiten que las personas escriban los programas en un lenguaje inteligible, sin que sea necesario que el procesador lo entienda.

En definitiva, los lenguajes de programación sirven para que seres humanos hagan tareas como diagramar sentencias con sujeto, verbo y predicado, empleando las distintas categorías gramaticales pero puestos en forma de árbol, de acuerdo a las posibilidades que ofrezca el lenguaje en cuestión, proceso conocido como parsing (Shasha & Lazere, 1998).

> *Solidity* es un lenguaje de alto nivel orientado a contratos cuya síntesis es similar a JavaScript y ha sido diseñado para la máquina virtual Ethereum. Solidity es de tipado estático, soporta herencias, librerías y complejas definiciones de tipos de usuario, entre otras características. (https://goo.gl/sPQFfg).

Unidad 2: Accesibilidad a la infraestructura blockchain

2.2.1 Centralización vs. Descentralización

En esta unidad, estamos ante uno de los temas más relevantes del fenómeno *blockchain*: la accesibilidad.

Internet es una red pública, en el sentido de que es accesible a cualquier persona, tiene una arquitectura y un diseño de protocolos que enfatiza y promueve la accesibilidad pública, masiva, irrestricta. Podríamos afirmar que los pocos límites a la accesibilidad de Internet que existen en el mundo tienen que ver con los esfuerzos de algunos países por censurar contenidos o por apropiarse de riqueza ajena, no con la intención gubernamental de garantizar acceso a la información a toda su población o agrandar las fronteras del conocimiento y de la libertad.

La comunidad de Internet, ha resistido con mano firme, los reiterados y persistentes intentos de que se estatice. Internet sigue siendo una red pública, de acceso irrestricto y libre para cualquier individuo del mundo, gracias a que se mantiene privado, en el sentido de no estatal.

Internet es una infraestructura de comunicación, un hito de la cultura humana, que ha contribuido a la paz y a la prosperidad mundial, mucho más que cualquier religión, que cualquier ideología y que cualquier gobierno.

Blockchain tiene la misma arquitectura abierta y colaborativa que Internet, es un paso evolutivo posterior, que enfatiza y resuelve los aspectos transaccionales de la revolución comunicacional que significó su predecesora.

Blockchain es un mojón de la evolución de nuestra especie, un verdadero símbolo de esta época en la que la razón humana prosigue su alocada carrera para escapar de la catástrofe malthusiana. Es la infraestructura de las transacciones privadas entre personas libres, negociando su riqueza de manera voluntaria, sin intermediación.

Blockchain, igual que el ADN de los seres vivos, es una infraestructura de información transaccional y de transmisión de dicha información. Es una nueva manera de interactuar para los seres humanos.

Hasta hace pocos meses, la lucha de las empresas globales estaba centrada en la obtención de datos personales para transformar en oro lo que el público entregaba a precio de baratijas: los datos personales. La tecnología *blockchain* es un giro de transparencia hacia esa tendencia que parecía irrefrenable.

Con el tiempo veremos cómo evoluciona, si cumple lo que hoy promete. El futuro de *blockchain* depende de la interacción espontánea y libre de millones de personas que interactuarán en esa infraestructura en el futuro y que administrarán su información de la manera en que su conocimiento, sus creencias y su cultura lo incentiven a hacerlo. Pero no hay ninguna duda de que, una vez que este cambio empiece, el ritmo será vertiginoso y los cambios que traerá aparejados serán exponenciales.

Un *blockchain* es una base de datos que ofrece muchas ventajas. Tiene una estructura descentralizada sin punto único de falla y los datos allí almacenados son completamente inviolables.

Además, una vez almacenados los datos en una cadena de bloques siempre se almacenarán allí y todos los detalles de la transferencia y el procesamiento estarán visibles para todas las personas conectadas a la red y para cualquier persona no conectada a la red que desee verificar dichos detalles.

Es posible que todavía no alcancemos a entender la tremenda importancia de algo tan sencillo.

2.2.2 *Blockchain* público

En una cadena de bloques pública, cualquiera puede leer y escribir los datos almacenados allí, ya que es accesible para todo el mundo. Una persona puede convertirse en miembro de la red *blockchain* y puede almacenar, enviar y recibir datos luego de descargar el software requerido en su dispositivo.

Un *blockchain* público está completamente descentralizado ya que los permisos para leer y escribir datos en *blockchain* se comparten por igual entre todos los usuarios conectados, que llegan a un consenso antes de que se almacenen en la base de datos. Un *blockchain* público se basa en un sistema completamente libre de terceros de confianza en el que ningún usuario tiene privilegios especiales en ninguna decisión.

Las implementaciones más comunes de un *blockchain* público son *bitcoin* y *ethereum*, donde la naturaleza pública de *blockchain* permite a los usuarios de diversos entornos acceder a una plataforma común para realizar transacciones directas eliminando la necesidad de proveedores externos.

Como es descentralizado, un *blockchain* público también es matemáticamente muy difícil de piratear ya que el costo es demasiado alto para un sistema donde todos los nodos conectados se sincronizan con la base de datos *blockchain* y, más importante, una vez que se descubre un *hack*, el valor de las monedas pirateadas disminuirían exponencialmente, lo que provocaría enormes pérdidas para el pirata informático (que tuvo que invertir una gran cantidad de hardware para superar el hash de la red).

Como todas las transacciones en un *blockchain* público deben ser verificadas por miles de usuarios, el proceso de verificación de la transacción puede consumir mucho tiempo. Los usuarios pagan una tarifa mayor en comparación con cadena de bloques privada y autorizada.

2.2.3 *Blockchain* privado

En una cadena de bloques privada, los permisos para escribir datos están controlados por una organización en la que los demás usuarios confían. Esta organización puede no permitir que los usuarios tengan acceso, ya que la legibilidad pública puede no ser necesaria en la mayoría de los casos. En algunas situaciones, la organización podría querer que el público audite los datos. Los permisos de lectura limitados o restringidos también proporcionan un mayor nivel de privacidad a los usuarios, una función que no está disponible en los *blockchains* públicos.

La organización de control tiene el poder de cambiar las reglas de un *blockchain* privado y rechazar transacciones basadas en reglas y regulaciones establecidas.[6]

En un *blockchain* privado, las transacciones son más rápidas, ya que se puede verificar que sea una pequeña cantidad de dispositivos. Por lo tanto, los usuarios pagan tarifas menores ya que el número de personas que verifica la transacción es menor que en un *blockchain* público.

[6] Ver Gobierno de blockchain en el módulo 4.

Además, los dispositivos están muy bien conectados y cualquier falla puede ser arreglada por intervención humana y aprobada fácilmente por los usuarios ya que estos confían en la organización única que controla *blockchain*.

2.2.4 *Blockchain* autorizado

Es un tipo de *blockchain* privado y comparte con estas muchas características. Proporciona un híbrido entre la 'baja confianza' provista por los *blockchains* públicos y el modelo de 'entidad altamente confiable' de los *blockchains* privados. Conocido popularmente como consorcio de *blockchain*, es aquel en el que, en lugar de permitir que una persona con conexión a Internet participe en la verificación del proceso de transacción o permita que una sola compañía tenga control total, algunos nodos seleccionados están predeterminados.

Por ejemplo, un consorcio de diez compañías, donde cada una de las cuales opera un dispositivo conectado a la red *blockchain*. Si la empresa A solo comercializa y comparte sus facturas con B, C y D, no es necesario que las otras empresas tengan los permisos para leer los datos compartidos.

> Aunque se mantiene cierto grado de descentralización en su estructura, los participantes tienen el poder de otorgar permisos de lectura / escritura a otros participantes, lo que lleva al diseño 'parcialmente descentralizado' de *blockchains* autorizados.
>
> Las transacciones se verifican rápidamente en una cadena de bloques autorizada, ya que hay un puñado de verificadores, con la tarifa de transacción minúscula, lo que aumenta la eficiencia general de las transacciones. Al igual que los *blockchains* privados, los *blockchains* autorizados mantienen la privacidad de los datos de un usuario, sin consolidar el poder con una sola organización. (https://goo.gl/D5sWN8).

Para enriquecer el debate al respecto, tomamos los aportes de Collin Thompson, quien explica que “A medida que las instituciones financieras comienzan a explorar las posibilidades de la tecnología *blockchain*, están creando sistemas que complementan sus modelos de negocios existentes.” Entonces, una plataforma *blockchain* privada o de consorcio permitirá conservar el control y la privacidad mientras que reduce sus costos y velocidades de transacción. Añade Thompson:

> Los puristas de Blockchain no están impresionados. Una plataforma privada efectivamente mata a su parte favorita de esta tecnología naciente: la descentralización. Ven el advenimiento de los sistemas privados de blockchain como poco más que un intento furtivo de los grandes bancos para mantener su control de los mercados financieros. En cierto modo, están en lo correcto. Aunque la narrativa de la trama malvada es demasiado. Si los grandes bancos pueden utilizar una forma de tecnología de cadena de bloques que revoluciona las finanzas, y si están dispuestos y son capaces de transferir estos beneficios a sus clientes, entonces difícilmente se trata de un plan malvado. Es solo un buen negocio. (https://goo.gl/TnSkTH).

Por su parte, Vitalik Buterin plantea que ambas categorías (público y privado) tienen ventajas y desventajas. *Blockchain* fue diseñado para eliminar al intermediario en cualquier escenario de intercambio de activos y esto lo lleva a cabo configurando un bloque de transacciones punto a punto. Es decir que cada transacción se verifica y sincroniza con cada nodo afiliado al *blockchain* antes de que se escriba en el sistema. Hasta que esto ocurra, la próxima transacción no puede avanzar.

> Cualquier persona con una computadora y conexión a Internet puede configurarlo como un nodo que luego se sincroniza con todo el historial de *blockchain*. Si bien esta redundancia hace que el *blockchain* público sea extremadamente seguro, también lo hace lento y derrochador. La electricidad necesaria para ejecutar cada transacción es astronómica y aumenta con cada nodo adicional. El beneficio es que cada transacción es pública y los usuarios pueden mantener el anonimato. Un *blockchain* público es más apropiado cuando una red necesita ser descentralizada. También es excelente si se desea obtener la transparencia total del libro mayor o el anonimato individual. Los costos son más altos y las velocidades son más lentas que en una cadena privada, pero aún más rápidas y menos costosas que los sistemas y métodos contables utilizados en la actualidad. Esta es una buena compensación para una criptomoneda como *bitcoin*. La seguridad es clave para sus usuarios, una red descentralizada es el corazón del proyecto y sus competidores en la industria financiera son significativamente más caros y lentos que una red de *blockchain* pública a pesar de su lentitud en comparación con una cadena de bloques privada. (Buterin. https://goo.gl/WAqCK5)

En relación con *blockchain* privado, Buterin señala que se permite al intermediario volver a entrar pero con limitaciones. Si bien existe mayor eficiencia y velocidad ya que la compañía escribe y verifica cada transacción, no ofrece la misma seguridad descentralizada que su contraparte pública. La compañía, además, puede elegir quién tiene acceso a las transacciones de su *blockchain*, lo que permite una mayor privacidad que una cadena de bloques pública.

> Un *blockchain* privado es apropiado para los modelos comerciales y de gobierno más tradicionales, pero eso no es malo. El hecho de que sea poco probable que revolucione nuestro mundo no significa que no pueda desempeñar un papel para mejorar el mundo.
>
> La competencia es clave para desarrollar los productos más útiles. Las instituciones financieras tradicionales han mantenido durante mucho tiempo un monopolio, técnicamente, un oligopolio, sobre la industria. Sus productos y servicios obsoletos son el resultado directo de este poder. Usar una versión privada de la tecnología blockchain puede llevar a estas organizaciones al siglo XXI. Varias de nuestras instituciones de gobernanza son antiguas y obsoletas también. Al igual que las finanzas, nuestro gobierno no está sujeto a la competencia. La adopción y la integración probablemente serán más lentas en este sector, pero si se adoptan las tecnologías blockchain, se eliminarán miles de millones de dólares de gastos tras bastidores. Imagine un sistema de votación en línea verdaderamente seguro. No más trabajadores electorales, mesas de votación, boletas de papel, mostradores pagados u organizadores con sueldos cómodos. Además, las barreras para votar se reducirán en gran medida y es probable que veamos un aumento en la participación. Esto podría lograrse con un diseño público, pero es poco probable que la mayoría de los gobiernos descentralicen el control y la seguridad, por lo que un sistema privado aprobado aumenta en gran medida las posibilidades de adopción. (Buterin. https://goo.gl/WAqCK5)

Un consorcio *blockchain* es parcialmente privado. Para entender en qué difiere con un sistema totalmente privado, Buterin proporciona la siguiente definición:

> (…) el primero proporciona un híbrido entre el 'low-trust' proporcionado por blockchains públicos y el modelo de 'entidad de alta confianza única' de blockchains privados, mientras que este último puede describirse con mayor precisión como un sistema centralizado tradicional con un grado de auditabilidad criptográfica adjunto. (Buterin. https://goo.gl/WAqCK5)

Entonces, si bien ambas modalidades comparten muchos beneficios (eficiencia y privacidad de las transacciones, por ejemplo), la diferencia radica en que una plataforma de consorcio no concentra el poder en una sola compañía.

> Las plataformas de *blockchain* del consorcio tienen muchas de las mismas ventajas de una cadena de bloques privada, pero operan bajo el liderazgo de un grupo en lugar de una sola entidad. Esta plataforma sería ideal para la colaboración organizacional. Imagine a los bancos centrales coordinando sus actividades con base en las reglas internacionales de finanzas. O que las Naciones Unidas subcontraten su contabilidad transaccional y su sistema de votación a blockchain, permitiendo que cada país represente un nodo de verificación. (Thompson, https://goo.gl/TnSkTH).

Los usos de los *blockchain* privados y de consorcio son incipientes. Si su rasgo principal es eliminar al intermediario y permitir las transacciones entre iguales, es comprensible que estos intermediarios opongan resistencia para evitar su desarrollo y consolidación.

Hoy las empresas pugnan por proteger sus modelos comerciales de esta tecnología disruptiva. Las ideas que hacen cosas sin precedentes con esta tecnología, en lugar de solo aplicarla a los modelos existentes, serán donde esta tecnología brille.

Es importante a esta altura recordar que la tecnología que creó *Bitcoin* existía mucho antes de que se diseñara la criptomoneda. Se necesitó un poco de imaginación y mucho trabajo para convertir la tecnología existente en un producto viable.

Buterin conoce la intensidad de las discusiones ideológicas al respecto y no rehuye al debate. A continuación, recuperamos la distinción que realiza entre sistemas totalmente descentralizados y los parcialmente descentralizados como propuesta de innovación en la matriz de *blockchain*.

> (…) en vez de tener una red totalmente pública y no controlada y una máquina de estado protegida por criptoeconomía (por ejemplo, prueba de trabajo, prueba de participación), también

es posible crear un sistema donde los permisos de acceso estén más estrechamente controlados, con derechos de modificar o incluso leer el estado de cadena de bloques restringido a unos pocos usuarios, mientras se mantienen muchos tipos de garantías parciales de autenticidad y descentralización que proporcionan las cadenas de bloques.

(…) una cadena de bloques pública es una cadena de bloques que cualquier persona en el mundo puede leer, cualquier persona en el mundo puede enviar transacciones y esperar verlas incluidas si son válidas, y cualquier persona en el mundo puede participar en el *proceso de consenso* -el proceso para determinar qué bloques se agregan a la cadena y cuál es el estado actual-. Como sustituto de la confianza centralizada o cuasicentralizada, las cadenas de bloques públicas están protegidas por criptoeconomía: la combinación de incentivos económicos y verificación criptográfica utilizando mecanismos como prueba de trabajo o prueba de participación, siguiendo el principio general de que el grado en que alguien puede tener una influencia en el proceso de consenso es proporcional a la cantidad de recursos económicos que pueden aportar. Estas cadenas de bloques generalmente se consideran "totalmente descentralizadas.

(…) blockchain de consorcio es una cadena de bloques donde el proceso de consenso es controlado por un conjunto de nodos preseleccionados; por ejemplo, uno podría imaginar un consorcio de 15 instituciones financieras, cada una de las cuales opera un nodo y de las cuales 10 deben firmar cada bloque para que el bloque sea válido. El derecho a leer el blockchain puede ser público o restringido a los participantes, y también hay rutas híbridas como el hash raíz de los bloques que son públicos junto con una API que permite a los miembros del público hacer un número limitado de consultas y obtener pruebas criptográficas de algunas partes del estado blockchain. Estas cadenas de bloques se pueden considerar "parcialmente descentralizadas". (Buterin, 2015, https://goo.gl/qTdXIA).

Volviendo a las diferencias entre la modalidad pública y la privada, podemos decir que *blockchain* privado, en comparación con las cadenas de bloques públicas, presenta una serie de ventajas.

Prosiguiendo con Buterin (2015), entre las más importantes se cuentan las siguientes:

1) Los validadores son conocidos, por lo que no se aplica ningún riesgo de un ataque del 51% derivado de una colusión de mineros en China.

2) Las transacciones son más baratas, ya que solo necesitan ser verificadas por unos pocos nodos en los que se puede confiar que tienen un poder de procesamiento muy alto, y no necesitan ser verificados por diez mil laptops. Esta es una preocupación muy importante en este momento, ya que las cadenas de bloques públicas tienden a tener tasas de transacción que superan los $ 0.01 por tx, pero es importante notar que puede cambiar a largo plazo con una tecnología *blockchain* escalable que promete reducir los costos de *blockchain* público a dentro de uno o dos órdenes de magnitud de un sistema blockchain privado óptimo eficiente.

3) Se puede confiar en que los nodos están bien conectados y las fallas pueden repararse rápidamente mediante intervención manual, lo que permite el uso de algoritmos de consenso que ofrecen carácter definitivo después de tiempos de bloqueo mucho más cortos. Las mejoras en la tecnología pública de *blockchain*, como el concepto de Ethereum 1.0 y la posterior prueba de estaca, pueden acercar las cadenas de bloques públicas al ideal de "confirmación instantánea" (por ejemplo, ofrecer finalidad total después de 15 segundos, en lugar de 99,999% de finalidad después de dos horas como lo hace *bitcoin*), pero aún las cadenas de bloques privadas siempre serán más rápidas y la diferencia de latencia nunca desaparecerá ya que desafortunadamente la velocidad de la luz no aumenta en 2 veces cada dos años según la ley de Moore.

4) Si los permisos de lectura están restringidos, los *blockchains* privados pueden proporcionar un mayor nivel de privacidad. (https://goo.gl/qTdXIA).

Teniendo en cuenta todo esto, puede parecer que los *blockchains* privados son, sin duda, una mejor opción. Sin embargo, la importancia de las cadenas de bloques públicas radica en la promoción de valores como la libertad, la neutralidad y la apertura. Las ventajas de los *blockchains* públicos -siguiendo con este autor- generalmente se dividen en dos características principales:

1) Los *blockchains* públicos protegen a los usuarios de los desarrolladores, estableciendo que hay ciertas cosas que incluso estos no tienen autoridad para hacer. Desde un punto de vista ingenuo, puede ser difícil entender por qué un desarrollador de aplicaciones querría voluntariamente renunciar a la potencia y

> los músculos isquiotibiales por sí mismos. Sin embargo, el análisis económico más avanzado proporciona dos razones. En primer lugar, si explícitamente le dificulta o le imposibilita hacer ciertas cosas, entonces es más probable que otros confíen en usted y, por lo tanto, empiecen a interactuar. En segundo lugar, si usted está siendo forzado o presionado por otra entidad, puede decir: "No tengo poder para hacer esto aunque quisiera" es una importante moneda de cambio, ya que desalienta a esa entidad de intentar obligarlo a hacerlo. Una gran categoría de presión o coacción que los desarrolladores de aplicaciones están en riesgo es la de los gobiernos, por lo que la "resistencia a la censura" se relaciona fuertemente con este tipo de argumento.
>
> 2) La condición de apertura de las cadenas de bloques públicas implica que intervengan muchas entidades y, en consecuencia, obtengan algunos efectos de red. Por ejemplo, tomemos el caso del depósito en garantía de nombre de dominio. Si A quiere vender un dominio a B, existe un problema estándar de riesgo de contraparte que debe resolverse: si A envía primero, B no puede enviar el dinero, y si B envía primero, A podría no enviar el dominio. Para resolver este problema, se centralizan los intermediarios de depósito en garantía, quienes cobran tarifas de 3% a 6%. Sin embargo, si el sistema de nombre de dominio se encuentra en una cadena de bloques, con la misma moneda, entonces podemos reducir los costos a casi 0 por medio de un contrato inteligente: A puede enviar el dominio a un programa que inmediatamente lo transfiera a la primera persona para mandar dinero al programa (y el programa es confiable porque se ejecuta en una cadena de bloques pública). Para que esto funcione de manera eficiente, dos clases de activos completamente heterogéneos de industrias diferentes deben estar en la misma base de datos, una situación que no puede ocurrir fácilmente con los libros contables privados. (Buterin, 2015, https://goo.gl/qTdXIA)

Como puede verse, dejando de lado las posiciones extremas, siempre es cuestión de conveniencia y habrá que evaluar para cada caso si es apropiado el uso de la red pública o la privada, o de modalidades híbridas o intermedias, tal como menciona Buterin.

Para concluir, recuperamos la posición de Praveen Jayachandran, quien resalta no solo las diferencias entre la cadena de bloques públicos y privados (como ya hemos analizado), sino también sus similitudes. En un artículo publicado en el blog de IBM, las sintetiza de la siguiente manera:

- Tanto los *blockchain* privados como los públicos son redes descentralizadas *peer to peer*, en las que cada participante mantiene una réplica de un libro de contabilidad compartido de transacciones firmadas digitalmente.
- Mantienen las réplicas sincronizadas a través de un protocolo de consenso.
- Brindan garantías sobre la inmutabilidad del libro mayor, incluso cuando algunos participantes son indolentes o malintencionados (Jayachandran, 2017, https://goo.gl/iLCBmE).

Referencias

Buterin, V. (2014). Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. *BitCoin Magazine*. Recuperado de: https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/

Buterin, V. (2015). On public and private blockchains. Recuperado de: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Carranza Torres, M. (2008). *El derecho de la innovación tecnológica. Una historia del tecnotropismo capitalista*. Buenos Aires: Abeledo Perrot.

Carranza Torres, M. (s/d). ¿Son legales las criptomonedas? Recuperado de: http://www.ciiecca.org.ar/wp-content/uploads/2018/01/Legalidad-de-las-criptomonedas.pptx

Ceruzzi, Paul E. (2003). A history of modern computing

Davidson, J. (2017). Ethereum: the new blockchain revolution.

Ethereum Blockchain App Platform (s/f) https://www.ethereum.org/

Ethereum Apps (s/f) http://ethereumdapps.net/

Halpern. (2000). Harmonizing the convergence of medium, expression, and functionality: A study of the speech interest in computer software, Harvard Journal of Law & Technology, Volume 14, Number 1.

Jayachandran, P. (2017). The difference between public and private blockchain. Recuperado de: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Nakamoto, S. (s/d). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de: https://bitcoin.org/bitcoin.pdf

QF4 Technologies (s/f) https://www.qf4tech.com/blockchain_assessment.html

Rivas Villarroya, V. (2018). Declaración Satoshi Nakamoto Bitcoin en Español: Un sistema de efectivo electrónico punto a punto. LinkedIn.

Recuperado de: https://es.linkedin.com/pulse/declaraci%C3%B3n-satoshi-nakamoto-bitcoin-en-espa%C3%B1ol-un-de-v%C3%ADctor

Shasha & Lazere (1998) Out of Their Minds. The Lives and Discoveries of 15 Great Computer Scientist, Copernicus, New York.

Thompson, C. (s/d) The difference between a Private, Public & Consortium Blockchain. Blockchain Daily News. Recuperado de: http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html