Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Economía y Empresa

PCEO DERECHO/ADE

TRABAJO FIN DE GRADO

De la tecnología Blockchain y sus aplicaciones económicas

Alumno: César Ramos Gutiérrez

Convocatoria: Extraordinaria segundo semestre

Índice

Introducción

La tecnología Blockchain presenta tantos riesgos como oportunidades. La tecnología actual soporta sistemas y aplicaciones centralizados que operan sujetos a instituciones centralizadas y autoridades las cuales implementan sus propios sistemas internos de reglas, que a menudo ignoran o intentan eludir los sistemas de control tradicionales.

A diferencia de tales construcciones tecnológicas desplegadas actualmente en Internet, los nuevos sistemas descentralizados y aplicaciones pueden regirse casi exclusivamente por las reglas del código. Internet ya había planteado una disyuntiva fundamental entre el estado de derecho de la ley, basado en las fronteras geográficas y la regla del código. La regulación del ciberespacio se encuentra en la intersección entre estos dos sistemas normativos, que pueden cooperar o competir entre sí, según las circunstancias. Con el código, la gente podría implementar sus propios sistemas de reglas, aplicados por una construcción tecnológica que opera más allá de cualquier jurisdicción legal. Esto es lo que inspiró a una serie de activistas tecnológicos a creer que el ciberespacio era un espacio no regulable que los gobiernos no tenían el derecho o la capacidad de controlar. Deseosos de eludir las políticas de cierre y control promulgadas por los gobiernos y las empresas, estos grupos creían que Internet fomentaría nuevos sistemas normativos que facilitarían el libre flujo de información y promoverían la autonomía política y cultural. Es aquí donde entraría en juego el potencial de la tecnología Blockchain.

Abstract

Blockchain technology presents as many challenges as opportunities. Modern technology supports systems and modules centralized to the point where they operate dependant to centralized institutions and authorities who implement their own sets of rules, which often ignore or elude traditional security systems. In contrast with those systems actually deployed on the Internet, the new decentralized systems and modules can operate almost solely on code. Internet had already raised fundamental questions about the extent of the rule of law determined by physical borders and the rules of code systems. Thus the regualtion of the cyberspace stands in the crossroads betweeen those two sets of rules, which can cooperate or compete among themselves depending on the circumstances. Thanks to coding, people could create their own sets of digital rules enforced by a technological construct which supersedes any legal jurisdiction. This was the idea which

inspired a new breed of technological activists to believe in a cyberspace defined by the lack of applicable rules from governments without the legitimacy or capacity to do so. Being keen on eluding enclosure policies by governments and corporations, those groups believed in the capacity of the Internet to spawn new sets of rules which would encourage the free flow of information and political autonomy as well as cultural one. It is here where Blockchain technology's potential comes afoot.

1. Blockchain e Internet, un prólogo histórico al mundo digital

Antes del origen del Internet, los ordenadores trabajaban de forma aislada. En cierto modo, eran ínsulas incapaces de conectarse entre sí, excepto mediante el uso de cables. Todo eso cambió a fines de la década de 1950 con el lanzamiento exitoso del Sputnik al espacio por parte de los soviéticos y el aumento de los recelos internacionales de la Guerra Fría, momento en el que los investigadores de Rand Corporation comenzaron a explorar un nuevo paradigma informático, con la esperanza de desarrollar un sistema que pudiera resistir una catástrofe nuclear. (Abbate Janet, 2000). En agosto de 1964, después de años de investigación, Paul Baran, uno de los investigadores de Rand, realizó el esperado avance; basándose en una tecnología llamada conmutación de paquetes, Baran pudo enviar fragmentos de información de una computadora a otra y hacer que estos fragmentos se ensamblasen de nuevo (Baran, 1964). Armada con la investigación de Baran, la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de los Estados Unidos de América crea la primera red de ordenadores, ARPAnet, más tarde rebautizada como DARPAnet después de que se agregara "Defense" al comienzo del nombre de la agencia, ayudando a investigadores y académicos a compartir archivos e intercambiar recursos entre sí.

En el transcurso de las siguientes décadas, el poder de esta nueva red creció, a medida que se desarrollaron capas adicionales de tecnología, como TCP/IP (Programa de control de transmisión y Protocolo de Internet) y servicios de nombres de dominio (DNS), para hacer más fácil la identificación de los ordenadores en la red y garantizar que la información se encauzase adecuadamente. Atrás quedaba la insularidad informática, dando paso a la

unión mediante capas de código. A medida que DARPAnet despegaba, se gestaba una segunda revolución. Los nuevos algoritmos criptográficos estaban creando nuevos medios para que las personas y las máquinas intercambien mensajes, archivos y otra información de forma segura y autentificada.

En 1976, Whitfield Diffie y Marty Hellman, dos criptógrafos de la Universidad de Stanford, inventaron ingeniosamente el concepto de "criptografía de clave públicoprivada", resolviendo uno de los problemas fundamentales de la criptografía, la necesidad de una distribución segura de claves, mientras que al mismo tiempo establecían una base teórica para las firmas digitales autentificadas (Diffie, 1976). Antes del advenimiento de la clave público-privada cifrada, el envío de mensajes privados era difícil. Los mensajes cifrados viajaban por canales inseguros, lo que los volvía vulnerables a la intercepción. Para enviar un mensaje encriptado, el mensaje debe codificarse mediante el uso de una clave (también conocida como cifrado), lo que da como resultado una cadena de texto impenetrable. Cuando el mensaje codificado llegaba a su destino previsto, el destinatario usaba la misma clave para decodificar el texto cifrado, revelando el mensaje subyacente (Castiglioni Maldonado, 2018).

Una limitación importante de estos primeros sistemas criptográficos era la relevancia de la clave a la hora de mantener la confidencialidad del mensaje enviado. Las partes que usaban estos sistemas tenían que acordar una clave antes de intercambiar mensajes, o la clave tenía que comunicarse de alguna manera a la parte receptora. Debido a estas limitaciones, las claves podrían verse comprometidas fácilmente. Si un tercero obtuviera acceso a la clave, podría interceptar la comunicación y decodificar el mensaje encriptado (Davies, 1997).

La criptografía de clave público-privada resolvió este problema al permitir el envío de mensajes encriptados sin necesidad de una clave compartida. Según el modelo de Diffie y Hellman, ambas partes acordarían una clave pública compartida que sería descifrada por una clave privada. La clave privada actuaba como una contraseña secreta, que las partes no necesitaban compartir, mientras que la clave pública servía como un punto de referencia que podía comunicarse libremente. Al combinar la clave pública con la clave privada de una de las partes y luego combinar el resultado con la clave privada de la otra parte, Diffie y Hellman se dieron cuenta de que era posible generar una clave secreta compartida que podía usarse tanto para cifrar como para descifrar mensajes (Davies, 1997).

En 1978, poco después de que Diffie y Hellman publicaran su innovador trabajo, un equipo de criptógrafos del MIT (Ron Rivest, Adi Shamir y Len Adleman) se basaron en la investigación de Diffie y Hellman y desarrollaron un algoritmo, conocido como el algoritmo RSA (nacido de las últimas iniciales de los desarrolladores), para crear un conjunto de claves públicas y privadas vinculadas matemáticamente y generadas al multiplicar dos números primos grandes. Estos criptógrafos se dieron cuenta de que era relativamente sencillo multiplicar dos números primos grandes, pero excepcionalmente difícil, incluso para ordenadores potentes, calcular qué números primos se usaban (un proceso llamado factorización prima) (Tapscott, 2016). Al aprovechar esta peculiaridad matemática, el algoritmo RSA hizo posible que las personas transmitieran ampliamente sus claves públicas, sabiendo que sería casi imposible descubrir las claves privadas subyacentes (Diffie, 1976), (Castiglione, 2018). Por ejemplo, si Juan quisiera enviar información confidencial a Pedro, podría cifrar la información usando su propia clave, la clave pública de Pedro y publicar públicamente el mensaje cifrado. Con el algoritmo RSA, y debido al uso de la factorización prima, solo la clave privada de Pedro podría descifrar el mensaje.

La aplicación de la criptografía de clave pública y privada se extendió más allá del cifrado de mensajes. Como Diffie y Hellman reconocieron, mediante la construcción de nuevos criptosistemas en los que "el cifrado y el descifrado se regían por claves distintas", la criptografía de clave pública y privada podría sustentar firmas digitales seguras y autentificadas que fueran altamente resistentes a la falsificación, reemplazando así la necesidad de firmas escritas que requieren instrumentos y contratos en papel (Diffie, 1976). Por ejemplo, mediante el uso del algoritmo RSA, una parte emisora podría adjuntar a un mensaje una “firma digital” generada al combinar el mensaje con la clave privada de la parte remitente (Castiglioni Maldonado, 2018). Una vez enviado, la parte receptora podría usar la clave pública de la parte emisora para verificar la autenticidad e integridad del mensaje. Mediante el uso de cifrado de clave público-privada y firmas digitales, si Juan quisiera enviar un mensaje privado a Pedro, podría cifrar el mensaje usando su propia clave privada y la clave pública de Pedro y luego firmar el mensaje usando su clave privada. Pedro podría entonces usar la clave pública de Juan para verificar que el mensaje se originó en el ordenador de Pedro y no se modificó durante la transmisión. Pedro podría entonces descifrar el mensaje de forma segura utilizando su clave privada y la clave pública de Juan (Piper, 2002). El cifrado de clave público-privada despertó la imaginación

de una nueva generación de académicos, matemáticos e informáticos, que comenzaron a imaginar nuevos sistemas que podrían construirse utilizando estas nuevas técnicas criptográficas. Basándose en la criptografía de clave pública-privada y las firmas digitales, se hizo teóricamente posible construir dinero electrónico, reputación seudónima y sistemas de distribución de contenido, así como nuevas formas de contratos digitales (Delfs H., 2002).

El Internet comercial y las redes estaban a punto en los años posteriores al nacimiento de Internet y la invención de la criptografía de clave público-privada. Con el coste de los ordenadores disminuyendo rápidamente, estas máquinas extrañas consideradas al alcance de unos pocos pasaron de los sótanos de las grandes corporaciones y agencias gubernamentales a escritorios y hogares. Después de que Apple lanzara su icónico ordenador personal, el Apple II, una amplia gama de ordenadores de bajo coste inundó el mercado. Aparentemente de la noche a la mañana, los ordenadores aparecieron en la vida diaria. A mediados de la década de 1990, Internet había entrado en una fase de rápida expansión y comercialización. DARPAnet había crecido más allá de su entorno académico inicial y, con algunas actualizaciones, se transformó en el Internet moderno. Impulsados por una constelación de proveedores privados de servicios de Internet (ISP), millones de personas en todo el mundo estaban explorando los límites del ciberespacio, interactuando con nuevos protocolos de software que permitían a las personas enviar mensajes electrónicos (a través del protocolo de transferencia de correo simple, SMTP), transferir archivos (a través del protocolo de transferencia de archivos, FTP) y distribuir y vincular medios alojados en los ordenadores de otros (a través del protocolo de transferencia de hipertexto, HTTP). En cuestión de años, Internet había pasado de ser una herramienta del mundo gubernamental y académico a una nueva forma de infraestructura.

Al principio, los servicios de Internet se estructuraron predominantemente usando un modelo de cliente-servidor. Los servidores, propiedad de las primeras empresas "punto com", alojan los sitios web y proporcionan diversos tipos de aplicaciones, a las que los usuarios de Internet pueden acceder a través de sus clientes. Por lo general, la información fluía en una sola dirección: de un servidor a un cliente. Los servidores podían compartir sus recursos con los clientes, pero los clientes a menudo no podían compartir sus recursos con el servidor u otros clientes conectados al mismo servicio de Internet (Abbate Janet, 2000). Estos primeros sistemas cliente-servidor eran relativamente seguros, pero a menudo actuaban como cuellos de botella. Cada servicio en línea tenía que mantener

servidores con considerables costes de configuración y operación. Si un servidor administrado de forma centralizada se apaga, todo un servicio podría dejar de funcionar y, si un servidor recibiera demasiadas solicitudes de los usuarios, podría sobrecargarse, incapacitando temporalmente el servicio.

A principios del siglo XXI, nuevos modelos habían surgido para la prestación de servicios en línea. En lugar de depender de un servidor centralizado, las partes comenzaron a experimentar con redes peer-to-peer (P2P), que dependían de una infraestructura descentralizada en la que cada participante en la red (normalmente llamado "peer" o "nodo") actuaba como ambos, un proveedor y consumidor de recursos informativos (Tapscott, 2016). Las nuevas redes peer-to-peer, como Gnutella y BitTorrent, permitieron a las personas compartir información sobre archivos ubicados en sus ordenadores personales. Con la llegada de estas redes peer-to-peer descentralizadas de segunda generación, había comenzado a solidificarse un nuevo modo para la entrega de contenido, liberando el intercambio de información de los grandes operadores en línea. Estas redes descentralizadas carecían de un centro discernible y atraían a un número menor de intermediarios (Castiglioni Maldonado, 2018). Es en este momento cuando, finalmente, se disponía de las herramientas adecuadas y se habían eliminado los principales obstáculos para concebir e implementar un nuevo sistema de transferencia digital.

2. Surgimiento de las cadenas de bloques

La idea de redes de igual a igual descentralizadas y seguras resonó en un grupo de criptógrafos y otros tecnólogos fascinados con los avances en la criptografía de clave pública y privada, que se dieron cuenta del poder de las redes peer-to-peer y el cifrado, considerando ambos como herramientas para contrarrestar la vulneración de la libertad personal. Estos creían que sin los controles y contrapesos adecuados, el despliegue de la tecnología afectaría la privacidad, lo que daría como resultado una vigilancia gubernamental y corporativa generalizada (Piper, 2002). La tecnología Blockchain supondría pues la piedra de toque sobre la que se implementarían las primeras iteraciones criptográficas de sistemas de intercambio de valor en clave digital.

La tecnología Blockchain, como se muestra en la siguiente figura, es un libro mayor centralizado, donde una o más partes registran las transacciones en una base de datos central que actúa como el libro mayor, mientras que en un libro mayor descentralizado

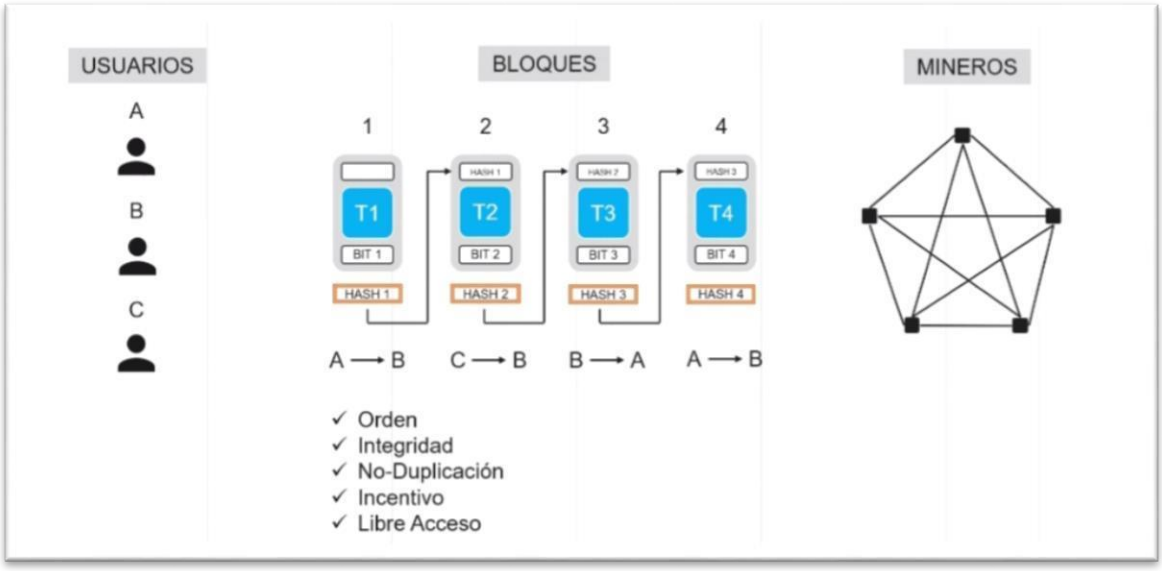
cada parte tiene su propia copia de las transacciones del libro mayor que está sincronizada con toda la red, es decir, el libro mayor de cada parte es exactamente el mismo que el de todos los demás (Tapscott, 2016).

A medida que las transacciones ocurren en la red descentralizada y cada transacción se valida, esa transacción se agrega al libro mayor de todos los participantes. Los libros de contabilidad centralizados pueden ser susceptibles de alteraciones, ya que normalmente son propiedad de una sola parte. Una vez que se ha registrado una transacción en la cadena de bloques, se vuelve inmutable; no se puede cambiar sin que la mayoría de la red de la cadena de bloques acepte el cambio (Mukhopadhyay, 2018). Esto garantiza la seguridad de los datos de las transacciones en la cadena de bloques y en toda la red. Además de la descentralización, otra característica de las cadenas de bloques es la persistencia, donde los datos se registran en todos los nodos de la cadena de bloques, que conduce a la inmutabilidad, lo que garantiza que los datos no se corrompan. La persistencia también proporciona tolerancia a fallas donde la pérdida de cualquier nodo en la red Blockchain no lo inutilizará.

La auditabilidad y la transparencia son otras características importantes, teniendo en cuenta que cada transacción se registra en la cadena de bloques, que luego se puede auditar más tarde, y es transparente en el caso de las cadenas de bloques sin permiso, que están abiertas para que cualquiera pueda ver las transacciones (Cottrill, 2017).

Podría proporcionar una infraestructura de trazabilidad en línea que se encargue del almacenamiento permanente y el intercambio de los elementos clave a lo largo de cadena, y el hecho de que ya sea un libro de contabilidad digital lo hace adecuado para registrar transacciones de productos entre los actores de la cadena de suministro. En el siguiente gráfico se muestran las características principales de una red pública basada en esta tecnología.

Gráfico 2. Arquitectura de una cadena de bloques



Fuente: Lánský, 2017

Las cadenas de bloques se componen de numerosos nodos (participantes) en una red, y cada nodo contiene una copia exacta del libro de contabilidad digital. Estos nodos pueden contarse por miles y existir en todo el mundo. Los algoritmos de consenso son clave para el funcionamiento de las redes Blockchain y son responsables de mantener la integridad y seguridad de la red. Estos algoritmos garantizan que se sigan las reglas del protocolo Blockchain, que todos los nodos de la red estén sincronizados entre sí y que sean clave para evitar que una sola entidad controle la red Blockchain. La prueba de trabajo (PoW) y la prueba de participación (PoS) son dos de los principales algoritmos de consenso en uso (Chris, 2013):

Prueba de trabajo (PoW): fue el primer algoritmo de consenso implementado en una cadena de bloques y se utiliza en la cadena de bloques de Bitcoin. Requiere nodos, conocidos como mineros, en la red para competir resolviendo un problema matemático complejo, cuya solución se conoce como valor hash. Un valor hash no es más que una combinación de caracteres de longitud fija que hace referencia a una cantidad de datos previamente convertida por un algoritmo en tal combinación; matemáticamente, 4+5 sería la información previa y 9 el valor hash que a ella se refiere, de forma que poseyendo la información original resulta sencillo obtener el valor hash, pero poseyendo únicamente el valor hash (9 en este ejemplo) es significativamente más complejo obtener la información a la que se refiere (la combinación específica 4+5). Volviendo al tema que nos ocupa, una vez que un minero encuentra el valor hash correcto, los nodos de la red lo verifican antes de ejecutar la transacción y agregarlo a la cadena de bloques. El minero que encuentre el valor hash correcto recibirá una recompensa, conocida como recompensa en bloque.

Debido a los cálculos que realizan los mineros para lograr el valor hash correcto, PoW utiliza mucha energía para confirmar transacciones en la cadena de bloques. Esto está diseñado para mejorar la seguridad de este algoritmo de consenso (Jensen, 2019).

Prueba de participación (PoS): es una alternativa a PoW donde se elige un nodo, conocido como validador para confirmar un bloque en función de su participación económica (número de tokens) en la red junto con una función de aleatorización. Un token es una unidad de valor emitida por Blockchain, cuya función consiste en representar bienes tradicionales, intercambiables exclusivamente por la criptomoneda en la cual operan; por ejemplo, si una vivienda es intercambiable por euros en el mundo real, un token representando una vivienda es intercambiable por bitcoins en el mundo digital. La gran mayoría de los tokens operan en la red Ethereum. Retomando la función de aleatorización evita la centralización y la posibilidad de que el validador con mayor interés económico siempre valide las transacciones. En lo referente al sistema poS, el validador no está incentivado a acciones maliciosas porque una parte de su participación estará en riesgo. Al igual que con PoW, el validador recibe una recompensa y PoS se considera una mejor opción que PoW porque usa mucha menos energía para confirmar las transacciones (Yong, 2020).

3. Monedas digitales y sistemas de pago descentralizados

En los siguientes puntos se analiza el surgimiento de las monedas digitales como consecuencia del desarrollo de los sistemas Blockchain. Debe mencionarse que la proliferación de criptomonedas y productos financieros relacionados ha generado preocupación sobre las consecuencias para los inversores (Mukhopadhyay, 2018). Los bancos centrales y otros reguladores, sorprendidos por la popularidad de los criptoactivos entre los inversores, han estado luchando en la retaguardia debido a la falta de claridad sobre si las regulaciones existentes se aplican a estos productos no tradicionales.

3.1. Surgimiento de las monedas digitales

Según el criptógrafo David Chaum, fundador de la Asociación Internacional para la Investigación Criptológica, la tecnología informática, con el tiempo, privaría a las personas de su capacidad para monitorizar y controlar su información, permitiendo a los gobiernos y corporaciones recopilarla y usarla “en detrimento de los estilos de vida, hábitos, desfiles y asociaciones de las personas a partir de los datos recopilados en las

transacciones ordinarias de los consumidores" (Delfs H., 2002). Para contrarrestar estos riesgos percibidos, abogaron por el despliegue masivo de herramientas criptográficas, socavando al mismo tiempo la hegemonía de los gobiernos de todo el mundo. Buscaron democratizar el acceso a la criptografía, creando sistemas de mensajería segura, contratos digitales. El sustrato esencial era el efectivo anónimo y otros sistemas de pago imposibles de rastrear. A partir de 1983, los criptógrafos comenzaron a explorar el uso de la criptografía de clave pública y privada para construir nuevos sistemas monetarios. Ese año, Chaum propuso un sistema para permitir la creación y transferencia de efectivo electrónico que no requeriría que los usuarios entregaran información personal (Chaum D, 1983).

Este sistema finalmente se convirtió en DigiCash, una empresa que Chaum lanzó en 1994. DigiCash se basaba en criptografía de clave pública y privada para emitir una moneda digital, utilizando un sistema de firma digital inventado por Chaum (llamado firmas ciegas) para validar las transacciones entre las partes. La empresa actuó como una cámara de compensación central, fijando el suministro de dinero y procesando las transacciones de DigiCash. Sin embargo, DigiCash tenía una limitación técnica. Operaba a través de un modelo cliente-servidor, que requería que la empresa de Chaum verificara y validara cada transacción en la red. El éxito de DigiCash estuvo íntimamente ligado al destino de la empresa y dependía por completo de él. Cuando esa empresa quebró en 1998, DigiCash se derrumbó con ella (Chaum D. F, 1989). Sin embargo, la idea de crear una moneda digital anónima encendió una llama inmarcesible en el imaginario colectivo. A raíz de DigiCash, un número creciente de personas, incluidos Hal Finney, Wai Dai y Nick Szabo, se embarcaron en una búsqueda de una década para construir una moneda digital anónima que careciera de control centralizado (Tapscott, 2016).

La moneda digital es solo una serie de bits almacenados en la memoria de una o más máquinas. A diferencia de los billetes de papel o las monedas de metal, no tiene una representación física. Por lo tanto, como cualquier otro recurso digital, una unidad de moneda digital puede copiarse y reproducirse sin cesar. Debido a estas características inherentes, las monedas digitales crean vías obvias para el fraude. La solución fue la utilización de la tecnología Blockchain y su capacidad para realizar pagos seguros utilizando solo identidades digitales (claves públicas y privadas), presentando métodos para garantizar la integridad de grandes cantidades de información de transacciones y permitir su verificación (Castiglioni Maldonado, 2018). Pero estos elementos no son

suficientes para establecer un sistema de pago fiable y de confianza. Sin una cámara de compensación central o cualquier otro intermediario capaz de validar transacciones y actualizar los saldos de las cuentas, cualquier persona en posesión de una unidad de efectivo digital tendría la capacidad de enviar fondos a dos partes simultáneamente, creando un problema de "doble gasto" (Castiglioni Maldonado, 2018). Por ejemplo, Si Pedro poseyera 5 euros en moneda digital, podría transferir esa cantidad tanto a Juan como a Pablo al mismo tiempo, gastando ilegítimamente un total de 10 euros. Cualquier sistema de pago descentralizado necesitaría resolver este problema de doble gasto y tendría que hacerlo de una manera que no dependiera de ningún intermediario centralizado. El monto total de la moneda en circulación en un momento dado tendría que ser fijo o controlado por un protocolo de software, a fin de evitar que las personas devalúen la moneda generando fondos adicionales no autorizados (Lansky, 2018). El sistema también tendría que crear un registro integrado de transacciones para realizar un seguimiento de toda la moneda digital que fluye a través del sistema. Sin estas características esenciales, sería imposible validar quién poseía qué cantidad de moneda digital en un momento dado sin depender de una autoridad o cámara de compensación de confianza.

A fines de 2008, uno o más desarrolladores anónimos llamados Satoshi Nakamoto resolvieron este problema fusionando criptografía de clave pública y privada, firmas digitales y tecnologías punto a punto para crear una nueva base de datos distribuida, que se conoció como cadena de bloques. Usando una cadena de bloques, Nakamoto construyó una moneda digital descentralizada que podía operar sin la necesidad de un intermediario centralizado. A diferencia de DigiCash de Chaum, que dependía de un operador centralizado, el sistema de Nakamoto, descrito en un breve artículo de nueve páginas titulado "Bitcoin: un sistema de efectivo electrónico punto a punto", (Nakamoto, 2008) dependía de una red de ordenadores para validar y mantener un registro de todas las transacciones de Bitcoin. Según este modelo, las transacciones se registraban en un almacén de datos común y el software subyacente de Bitcoin controlaba el suministro de la moneda digital y coordinaba la validación de transacciones, eliminando así la necesidad de un control centralizado.

Desde su lanzamiento en 2009, Bitcoin se ha convertido en uno de los sistemas de pago más grandes del mundo y, sin embargo, sus fundamentos técnicos son, para muchos, tan misteriosos como su fundación. Una forma de conceptualizar cómo funciona Bitcoin es pensar en el correo electrónico. Hoy en día, una dirección de correo electrónico nos

permite enviar y recibir mensajes electrónicos de cualquier persona conectada a Internet en tan solo unos segundos. Las direcciones de correo electrónico a menudo no están vinculadas a nuestra identidad individual; pueden ser seudónimos y actuar como punto de referencia para recibir mensajes electrónicos. Si muchos usuarios confían en operadores externos para administrar el correo electrónico, el protocolo subyacente para enviar y recibir mensajes es un protocolo gratuito, abierto e interoperable que se puede usar sin tener que pedir permiso a nadie. El acceso a una bandeja de entrada de correo electrónico se mantiene mediante una contraseña única, lo que permite a las personas controlar sus cuentas de correo electrónico, ya sea a través de una interfaz web como Gmail o mediante un cliente de correo electrónico como Microsoft Outlook o Thunderbird. Bitcoin es similar. Al igual que con el correo electrónico, Bitcoin es un protocolo abierto e interoperable que no está controlado centralmente por ninguna de las partes (Nakamoto, 2008).

Bitcoin se basa en la criptografía de clave pública privada para permitir que las personas creen seudónimos, identidades digitales separadas de sus credenciales reales. Con una cuenta de Bitcoin, las personas pueden recibir y enviar bitcoins a cualquier persona en todo el mundo, en cuestión de minutos, ejecutando y firmando digitalmente una transacción de Bitcoin con una clave privada. Una vez firmada una transacción, los miembros de la red de Bitcoin verifican que la transacción sea válida y, posteriormente, actualizan los saldos de las cuentas de Bitcoin relevantes. Las personas generalmente interactúan con la red Bitcoin mediante el uso de una billetera. Al igual que un cliente de correo electrónico, las billeteras de Bitcoin ayudan a las personas en la red de Bitcoin a administrar sus cuentas. Un elemento crucial que sustenta al Bitcoin es el mecanismo para validar transacciones de manera descentralizada, sin una autoridad central o de confianza involucrada, y con un registro inmutable de transacciones. Esta es una de las innovaciones más atractivas para aquellos que prefieren no depositar su confianza en una institución financiera pública o privada.

La solución de Bitcoin para los problemas de validación e inmutabilidad es utilizar un mecanismo de consenso público administrado a través de una red entre pares que alerta a los participantes en una red sobre cada transacción casi en tiempo real. Una red peer-to-peer es esencialmente una gran red de ordenadores (nodos), ninguno de los cuales tiene un estado especial, estando vinculados a través de Internet y no requiriendo un servidor

central para distribuir información a otros miembros (Antonopoulos, 2018). La red no es administrada ni controlada por ninguna entidad oficial o privada.

Los propietarios de monedas digitales las almacenan en billeteras Bitcoin. Estas son billeteras digitales construidas por un programa de software y que residen en la red (no necesita ejecutar un nodo de igual a igual para tener una billetera) (Tapscott, 2016). Cada billetera de Bitcoin está asociada con un par de claves: una clave pública, un identificador digital público de esa billetera, y una clave privada, una clave secreta conocida solo por el propietario de la billetera que se requiere para realizar transacciones financieras.

Bitcoin utiliza un protocolo PoW para lograr sus objetivos de validación e inmutabilidad. Para que la red logre esto sin un tercero, cada bloque de transacciones debe ser validado por alguien, y toda la red debe aceptarlo como un bloque de transacciones válido: este es el significado del consenso público.

El privilegio de crear un bloque válido recae en los creadores de bloques, más conocidos como mineros. El protocolo de Prueba de trabajo requiere que los mineros usen su poder computacional para resolver un problema criptográfico generado aleatoriamente que involucra hash. Estos problemas son generados automáticamente por el algoritmo de Bitcoin, sin intervención humana. Los problemas son acertijos matemáticos cuyo nivel de dificultad es medible y que solo pueden resolverse utilizando potencia informática bruta. La naturaleza de los problemas, que implica encontrar una entrada que (usando la función hash SHA-256) produzca un hash que satisfaga ciertas condiciones, es tal que no existen herramientas analíticas que puedan resolverlos de manera más eficiente (Mukhopadhyay, 2018).

En esencia, una computadora tiene que averiguar la solución de un problema hasta que encuentre una que funcione: los ordenadores más rápidos con más poder de cómputo pueden acelerar el proceso de adivinación, pero la fuerza bruta es la única forma de resolver los acertijos. Los ordenadores más potentes pueden adivinar millones de posibles soluciones por segundo, por lo que los problemas deben ser realmente difíciles de resolver, lo cual acarrea un coste energético exponencialmente mayor cuantos más problemas se van resolviendo. Esto también ha llevado a la creación de las famosas granjas de ordenadores, principalmente situadas en la frontera septentrional china; en ellas se instalan grandes cantidades de procesadores y tarjetas gráficas de última generación cuya única función es el minado de criptomonedas, dado que el actual estado de la minería

digital requiere de una gran potencia para volverse rentable, de la misma forma que el minado de metales preciosos hoy día únicamente es económicamente viable para las grandes empresas que pueden permitirse el equipamiento especializado necesario para minar a gran escala.

Debido a que no hay otra forma que no sea usar la potencia informática en bruto para descifrar estos acertijos, resolverlos demuestra la prueba del trabajo (computacional). Una vez que un nodo resuelve el problema asignado, esa solución es transmitida y confirmada por otros nodos. Este es un proceso muy rápido: una vez que se conoce la solución, verificar que sea la correcta es trivial, ya que esto simplemente implica asegurarse de que el hash de la solución cumpla con la condición requerida (Castiglioni Maldonado, 2018). La red también verifica que las transacciones en el bloque sean válidas, es decir, que correspondan a saldos legítimos no gastados en billeteras de Bitcoin. El bloque de transacciones validadas luego se agrega a la cadena.

3.2. Limitaciones del Bitcoin y el surgimiento de nuevas criptomonedas

Parecía que Bitcoin podría cambiar el mundo de las finanzas, o al menos revolucionar la tecnología de pago. Se suponía que proporcionaría costes de transacción bajos, anónimos, transparencia en tiempo real, propiedad e intercambio sin confianza y sin participación del gobierno e inmunidad de los problemas heredados del sistema bancario. Sin embargo, a medida que pasaba el tiempo, las deficiencias de Bitcoin se volvieron patentes. En primer lugar, no se podía garantizar que una moneda de emisión privada sin respaldo mantuviera un valor estable. En segundo lugar, el mecanismo descentralizado para validar transacciones no se pudo ampliar para transacciones minoristas de gran volumen. En tercer lugar, Bitcoin no pudo cumplir con el atractivo de un sistema de pago digital que ofrece un verdadero anonimato. Sin embargo, en lugar de crear desilusión con las criptomonedas, los defectos de Bitcoin generaron una gran variedad de criptodivisas alternativas que tenían como objetivo solucionar cada uno de estos problemas. Con esto vino el reconocimiento de que ninguna de ellas por sí sola podía hacer todo lo que Bitcoin aspiraba a hacer (Chris, 2013).

La disputa entre nuevos productos y servicios, que podría enmascarar diversas formas de artimañas financieras, cuando no un fraude total, y las aprensiones de los reguladores sobre los riesgos para los inversores y la estabilidad del sistema financiero se manifiestan de diversas formas en diferentes países.

La popularidad de Bitcoin, combinada con sus mencionadas limitaciones, ha generado una gran cantidad de criptomonedas alternativas. Algunos de los ejemplos más interesantes que veremos se han diseñado para solucionar problemas específicos mediante el desarrollo de mejores protocolos de consenso, asegurando una valoración más estable, proporcionando un anonimato más completo y ampliando la funcionalidad de la cadena de bloques. El coste y la ineficiencia de los protocolos de prueba de trabajo han motivado el desarrollo de mecanismos de consenso alternativos que son necesarios para validar las transacciones que tienen lugar en una cadena de bloques sin la participación de un tercero de confianza. El más popular de estos es la PoP, que utiliza un proceso diferente para llegar a un consenso.

En la prueba de participación (PoP), el privilegio de validar transacciones en un nuevo bloque se asigna en función de cuánto han apostado varios nodos competidores. La apuesta se basa en la cantidad de monedas que tiene el propietario de un nodo en la cadena de bloques correspondiente. Para ganar la oportunidad de validar transacciones, el usuario debe colocar monedas en una billetera digital específica. Esta billetera congela temporalmente las monedas, ya que no se pueden usar en transacciones mientras se usan para apostar en la red. Donde la Prueba de trabajo requeriría que sus mineros resolvieran un acertijo matemático, compitiendo sobre la base de la potencia informática, los protocolos de Prueba de participación eligen a los ganadores potenciales al azar, con la probabilidad de ser elegidos según la cantidad apostada (Castiglioni Maldonado, 2018).

Algunos cálculos criptográficos brutos aún están involucrados en este proceso, pero son mucho más simples de ejecutar, por lo que el poder de cómputo bruto por sí solo ya no confiere una ventaja. En la prueba de participación, los nodos que participan en la validación se denominan falsificadores o acuñadores (o, de manera más genérica, validadores) porque forjan o acuñan nuevos bloques para agregarlos a la cadena de bloques. Este proceso es menos exigente desde el punto de vista informático que la minería con Prueba de trabajo y no hay una recompensa en bloque.

Si bien Bitcoin otorga una recompensa por bloque y una tarifa de transacción cada vez que se valida un nuevo bloque, cualquier persona que contribuya al sistema de Prueba de participación generalmente solo gana una tarifa de transacción. La prueba de participación generalmente adopta una estructura lineal, con el porcentaje de bloques que un

falsificador puede validar aumentando como una proporción constante de la participación de ese falsificador en la criptomoneda.

3.3. Stablecoins

Las criptomonedas reconocen que un medio de intercambio viable necesita un valor estable más que el anonimato absoluto o un mecanismo de validación totalmente descentralizado, surgiendo en consecuencia varias criptodivisas centradas en atajar esta cuestión. Convenientemente, estas criptomonedas, que aparentemente mantienen un valor estable en relación con las monedas fiduciarias, se conocen como monedas estables. Las monedas estables utilizan tecnología criptográfica para brindar cierto grado de anonimato al usuario, pero la validación y liquidación de transacciones están a cargo del emisor de la moneda o de una parte autorizada.

Las monedas estables pueden estar respaldadas por monedas fiduciarias o por activos como el oro y otras materias primas. Incluso hay monedas estables respaldadas por reservas de criptodivisas destacadas como Bitcoin y Ether, aunque esto parecería una contradicción en los términos. Tales monedas estables respaldadas por criptomonedas tienen como objetivo mantener un valor estable manteniendo una canasta de criptodivisas, en lugar de una criptomoneda en particular en reserva, manteniendo un mayor stock de dichas reservas que lo estrictamente necesario para respaldar las monedas.

La noción de reducir la volatilidad mediante la diversificación de precios tiene sentido; donde tiene menos sentido es al tratar con la realidad de que los precios de las principales criptomonedas generalmente se mueven bastante juntos. El punto más importante es que el deseo de usar criptomonedas sin abandonar la estabilidad ha generado muchas nuevas estrategias que representan una amplia gama de enfoques para garantizar valores estables (Reed, 2017).

Una de las primeras monedas estables, Realcoin, se lanzó a principios de 2014. En noviembre de 2014, Realcoin se renombró como Tether para evitar ser asociado negativamente con Altcoins, que en ese momento estaban siendo criticadas como criptodivisas más débiles y menos confiables que Bitcoin. Supuestamente, Tether está respaldado por reservas de dólar estadounidense y diseñado para mantener un valor estable a la par con el dólar estadounidense. Por lo tanto, el precio de esta criptomoneda está permanentemente atado a la moneda fiduciaria.

Conceptualmente, la moneda fiduciaria en reserva se transforma en un token que se puede negociar en la plataforma, llamada Omni, utilizada por esta criptodivisa. El modelo comercial de Tether se basa en una tarifa de aproximadamente el 0,1 por ciento de todas las transacciones que involucran la conversión de divisas a criptomonedas o viceversa, así como una tarifa de 150 dólares por configurar una cuenta (Castiglioni Maldonado, 2018).

3.4. Restaurar el anonimato

Las criptomonedas como Bitcoin y Ethereum proporcionan privacidad, pero ahora se entiende bastante bien que esta es una promesa limitada sobre el verdadero anonimato. Cualquiera que use estas criptodivisas de forma extensiva deja un rastro digital que, a través de sus interacciones con el mundo real en forma de compras o ventas de bienes y servicios físicos, permite vincular identidades físicas y digitales. Tal desenmascaramiento de usuarios no es trivial de lograr, pero es factible utilizando el registro público de transacciones asociadas con la identidad digital de cada usuario.

El uso de múltiples identidades digitales ayudaría a enmascarar la verdadera identidad de un usuario, pero incluso estas podrían, en principio, vincularse a través del registro público de transacciones entre usuarios en la red de una criptodivisa.

Hay nuevas criptomonedas que intentan resolver este problema con tecnologías de enmascaramiento más sofisticadas (Narayanan, 2016). Monero y Zcash, dos criptodivisas que fueron diseñadas para ser verdaderamente anónimas en el sentido de que ninguna información asociada con una transacción en particular estaría disponible públicamente en sus redes.

Monero se diferencia de la configuración Bitcoin-Ethereum en tres aspectos. Primero, Monero usa direcciones de un solo uso para las transacciones, de modo que ninguna transacción individual se puede asociar con un usuario individual. Esto se llama desvinculación. En segundo lugar, Monero utiliza firmas de anillo para ocultar el historial de transacciones de un usuario, de modo que los fondos que una parte recibe de una transacción anterior no puedan ser rastreados más tarde por el remitente en esa transacción anterior. En tercer lugar, Monero utiliza transacciones confidenciales en anillo, que funcionan como una extensión de las firmas en anillo, para ocultar (en el registro público de la cadena de bloques) la cantidad de fondos transferidos en una transacción. Esta descripción sugiere que Monero ofrece un anonimato mucho más fuerte que Bitcoin. Las

transacciones basadas en Monero tienen las siguientes características: no se pueden vincular a ninguna identidad fija, flujos de fondos imposibles de rastrear y tamaños de transacción ocultos (Morabito, 2017).

4. Contratos Inteligentes como contratos legales

Con la creciente adopción de Bitcoin y otros sistemas basados en Blockchain, ha habido un interés renovado y una mayor experimentación en la transformación de acuerdos legales en código. Los protocolos avanzados basados en Blockchain como Ethereum proporcionan la tecnología necesaria para implementar algunas de las ideas descritas por Nick Szabo hace más de veinte años, tales como los protocolos de comercio informático o el sistema Bit Gold (Szabo, 1994). Mediante el uso de contratos inteligentes basados en Blockchain, las partes pueden entablar una relación comercial vinculante, ya sea total o parcialmente regida mediante código, y utilizar software para gestionar el desempeño contractual. En suma, el contrato inteligente no es más que un programa informático programado para ejecutar automáticamente las diferentes cláusulas contractuales que en él se integren, sin necesidad de acudir a un tercero. En muchos sentidos, los contratos inteligentes no son diferentes a los acuerdos escritos actuales. (Antonopoulos, 2018).

En el caso de un conflicto legal, las partes pueden renegociar el acuerdo subyacente o solicitar una reparación a un tribunal o panel de arbitraje para revertir los efectos del contrato inteligente. Donde los acuerdos legales tradicionales y los contratos inteligentes comienzan a diferir está en la capacidad de los contratos inteligentes para hacer cumplir las obligaciones mediante el uso de código autónomo. Más bien, estas obligaciones se establecen en el código de un contrato inteligente utilizando un lenguaje de programación estricto y formal (como Solidity de Ethereum). Por ejemplo, en un contrato con aval ya no sería necesario acudir al avalista y requerir el aval en caso de incumplimiento, sino que el programa que gestionase el contrato realizaría un requerimiento automático al sistema bancario del avalista, realizando de inmediato el desembolso.

El código de contrato inteligente se ejecuta de forma distribuida por todos los nodos que soportan la red subyacente basada en Blockchain, sin depender necesariamente de ningún operador intermediario o intermediario de confianza. Debido a que los contratos inteligentes son autónomos por naturaleza, las promesas registradas en un contrato inteligente son, por defecto, más difíciles de rescindir que las cláusulas tradicionales.

Es posible que no haya forma de detener la ejecución de un contrato inteligente después de que haya sido activado por las partes pertinentes, porque éstas no controlan la ejecución de una cadena de bloques. Una vez que se pone en marcha un contrato inteligente, los términos incorporados en el código pueden ejecutarse y no pueden detenerse a menos que las partes hayan incorporado una lógica en el contrato inteligente para detener la ejecución del programa (Tapscott, 2016).

Los oráculos, así denominados por la conexión que realizan entre el mundo digital y el real, son programas que almacenan y transmiten información desde el mundo exterior, proporcionando así un medio para que los sistemas basados en Blockchain interactúen con personas del mundo real y potencialmente reaccionar a eventos externos. Por ejemplo, los oráculos se pueden conectar a una fuente de datos de un tercero que transmite la última tasa de oferta interbancaria de Londres (LIBOR), o se pueden vincular a sensores que transmiten la temperatura exterior, la humedad u otros datos relevantes sobre un lugar en particular. Con los oráculos, los contratos inteligentes pueden responder a las condiciones cambiantes casi en tiempo real. Las partes de un contrato pueden hacer referencia a un oráculo para modificar los flujos de pago o alterar los derechos y obligaciones codificados según la nueva información recibida. Los oráculos también permiten determinar o actualizar las obligaciones de rendimiento específicas de los contratos inteligentes basándose en el juicio subjetivo y arbitrario de los individuos. De este modo, las partes pueden confiar en la ejecución determinista y garantizada de los contratos inteligentes para las promesas objetivas que son fácilmente traducibles en código. Al mismo tiempo, pueden asignar a un oráculo de base humana la tarea de evaluar las promesas que no pueden codificarse fácilmente en un contrato inteligente, ya sea porque son demasiado ambiguas o porque requieren una evaluación subjetiva de los acontecimientos del mundo real (Ortolani, 2016).

Desde el lanzamiento de Ethereum, se ha producido la aparición de una gama cada vez mayor de contratos inteligentes ligados a esta criptomoneda para gestionar acuerdos comerciales. Los contratos inteligentes se están diseñando para gobernar la transferencia de monedas digitales o tokens que representan activos tangibles o intangibles, así como para controlar el acceso a datos u otros recursos informativos referenciados en una red basada en Blockchain. Los contratos inteligentes también están ayudando a las personas a realizar transacciones entre sí en mercados de comercio electrónico descentralizados como eBay o Craigslist para apoyar y coordinar la venta de bienes (Open Bazaar, 2022).

Estos servicios se basan en la tecnología Blockchain y en los contratos inteligentes para gestionar el pago de los bienes, y utilizan oráculos humanos para resolver los posibles problemas que puedan surgir en el curso del comercio.

En estos mercados descentralizados, los vendedores pueden poner a la venta un producto registrando información en una cadena de bloques, como una descripción del bien y su precio. Los compradores interesados pueden enviar dinero a una cuenta virtual de depósito en garantía implementada a través de un contrato inteligente (a menudo denominada cuenta multifirma), que controla y gestiona de forma autónoma los fondos depositados (Arvind Narayanan, 2016). Si todo va según lo previsto y el comprador recibe el bien en cuestión, el comprador envía un mensaje basado en la Blockchain firmado digitalmente a la cuenta de depósito en garantía, que entonces libera el importe del precio de compra al vendedor. Por el contrario, si surge una disputa sobre la calidad del bien o si el producto simplemente nunca se entrega, un oráculo basado en humanos interviene para analizar los hechos del caso y determinar quién debe recibir los fondos en custodia (Triantis, 2002). Al igual que otros programas informáticos, los contratos inteligentes también ofrecen ventajas comparables en cuanto a claridad, precisión y personalización. A pesar de las mejores intenciones, los contratos legales suelen estar mal redactados. Los términos incoherentes se incorporan en los acuerdos complejos especialmente en los redactados con calendarios muy ajustados nublando la intención real de las partes (Posner, 2004). Cuando se enfrentan a cuestiones de interpretación de los contratos, los tribunales se han esforzado por aplicar normas coherentes.

Durante décadas, los académicos han reconocido que la lógica simbólica, como el código de software, puede reducir la ambigüedad contractual al convertir las promesas en reglas técnicas objetivamente verificables. Dado que los contratos inteligentes no son más que porciones de enunciados lógicos ejecutados de forma determinista, pueden disminuir la posibilidad de interpretaciones erróneas en los casos en que las partes pueden identificar de forma fiable obligaciones de ejecución objetivamente verificables. Al igual que otros códigos, los contratos inteligentes también son intrínsecamente modulares y pueden dividirse en porciones discretas, que pueden ensamblarse fácilmente y los programadores o los abogados pueden crear bibliotecas de código de contratos inteligentes diseñadas específicamente para implementar ciertas funcionalidades que aparecen habitualmente en los contratos legales. Por ejemplo, las bibliotecas de código de contratos inteligentes

podrían escribirse para regular la transferencia de pagos durante períodos de tiempo específicos, con o sin intereses.

Estas bibliotecas podrían incorporarse a una serie de acuerdos, incluidos los pagarés, así como los acuerdos de empleo, de servicios, de contratistas y de despido. Si las bibliotecas de código de contratos inteligentes se estructuran bajo licencias de código abierto como muchas bibliotecas de software podrían ser mejoradas por una comunidad de expertos legales. En última instancia, esto podría conducir a la aparición de un conjunto de disposiciones estándar basadas en contratos inteligentes que pueden ser utilizadas, reutilizadas y progresivamente refinadas gracias al escrutinio público y a los comentarios (Geis, 2008). De forma similar al desarrollo de los lenguajes de programación, que se han multiplicado y simplificado desde la llegada de la informática, el código de contratos inteligentes podría, con el tiempo, ser más fácil de manipular e incorporar en una serie de relaciones contractuales. A medida que la tecnología Blockchain madure, estas bibliotecas podrían aumentar su complejidad, otorgando a las partes la capacidad de redactar contratos inteligentes como si se tratara de ensamblar bloques de Lego, con porciones de código de contrato inteligente añadidos para tener en cuenta una serie de posibles contingencias, creando acuerdos legales más complejos, completos y sofisticados.

Dado que los contratos inteligentes son informáticamente legibles, también podrían ser utilizados por dispositivos autónomos e inteligencia artificial (IA). Mediante los contratos inteligentes, los dispositivos conectados a Internet pueden realizar transacciones de máquina a máquina, controlando cuentas de moneda digital y celebrando acuerdos para la compra de bienes o servicios. Por ejemplo, una máquina expendedora podría detectar automáticamente cuándo se ha quedado sin refrescos o barras de caramelo y enviar una solicitud a un proveedor a través de un contrato inteligente para que reponga la máquina a cambio de una pequeña tarifa. Del mismo modo, un coche con conducción automática podría pagar autónomamente el combustible o la electricidad mediante un contrato inteligente, sin necesidad de intervención humana. Aunque los contratos inteligentes tienen ciertas ventajas, también presentan una serie de inconvenientes en términos de privacidad, formalización de contratos y riesgos de excesiva estandarización.

Los contratos inteligentes presentan un grado de transparencia que puede resultar poco atractivo para las partes contratantes. Cuando las partes celebran un acuerdo escrito en lenguaje legal, generalmente tienen la opción de mantener los términos de su acuerdo en

privado. Sin embargo, debido a la transparencia de las cadenas de bloques, todas las acciones ejecutadas a través de un contrato inteligente, así como el código del contrato inteligente se propagan a través de una red de pares, haciéndolas públicamente visibles para los nodos de la red. Esto crea riesgos de privacidad, especialmente cuando las cuentas de las partes que realizan transacciones en una cadena de bloques están asociadas a entidades conocidas. Incluso cuando las partes que realizan las transacciones no están identificadas, ya que la mayoría de las cadenas de bloques se basan en cuentas seudónimas en lugar de puramente anónimas, se pueden utilizar técnicas de identificación como las descritas anteriormente para discernir las identidades de las partes que realizan transacciones con un contrato inteligente concreto (Ahmed Kosba, 2016). Aunque no se puede garantizar el éxito de estas técnicas, a medida que se realizan más y más transacciones en una cadena de bloques, las partes pueden tener dificultades para ocultar su identidad. Una vez que la identidad de una parte ha sido determinada, todas las operaciones realizadas con la misma cuenta pueden asociarse a la misma identidad. Aunque en los últimos años han surgido cadenas de bloques que preservan la privacidad como Zcash y Monero, estas redes no admiten el despliegue de contratos inteligentes robustos como los disponibles en Ethereum. Por lo tanto, las cuestiones de privacidad enturbian los contratos inteligentes y, en última instancia, pueden limitar la adopción de la tecnología. Por otra parte, debido a su dependencia de los lenguajes de programación formales, los contratos inteligentes tampoco serán probablemente útiles para los acuerdos con visiones de futuro inciertas.

Por su diseño, los contratos inteligentes facilitan la creación de obligaciones contractuales, regidas por reglas estrictas basadas en código informático. Son especialmente adecuados para crear acuerdos en los que las partes pueden delinear las obligaciones de una manera objetiva y predecible y no acuerdos en los que tales obligaciones no estén definidas con precisión en el momento de la contratación. De hecho, no todos los contratos regulan relaciones comerciales cuidadosamente definidas. Los acuerdos contractuales a menudo quedan abiertos porque las partes no pueden prever o delinear las obligaciones de ejecución en el momento de la redacción.

Las partes celebran habitualmente acuerdos con condiciones abiertas que se modifican continuamente para tener en cuenta las circunstancias imprevistas o la relación cambiante de las partes. Los contratos inteligentes no son especialmente adecuados para dar cabida a acuerdos jurídicos de naturaleza relacional. Para aplicar un contrato inteligente, las

partes deben definir con precisión las obligaciones de rendimiento y, si se basan en oráculos humanos, los casos en los que se requiere la visión humana. En el caso de ciertos acuerdos legales, esto podría ser fácilmente evidente. Sin embargo, en muchas transacciones comerciales, las obligaciones serán probablemente imprevisibles, y los contratos inteligentes no podrán proporcionar a las partes la flexibilidad necesaria para estructurar sus relaciones contractuales en curso. Incluso si los contratos inteligentes se utilizan para modelar obligaciones legales predecibles y objetivamente verificables, sigue habiendo dudas sobre el grado en que los contratos inteligentes pueden memorizar con precisión la intención de las partes.

El proceso de creación de un contrato inteligente implicará decisiones sustantivas sobre el significado, el contenido y la aplicabilidad de los acuerdos de las partes contratantes. Los programadores tendrán que hacer juicios subjetivos, interpretaciones y decisiones sustantivas sobre eventos futuros potencialmente inciertos al redactar el código de los contratos inteligentes, lo que podría enmascarar o distorsionar la intención de las partes. La naturaleza autónoma de los contratos inteligentes también crea complicaciones en los acuerdos comerciales que implican a partes seudónimas. Una vez que se ha puesto en marcha un contrato inteligente, las partes seudónimas tendrán una capacidad limitada para afectar a una transacción de contrato inteligente, incluso si hay un error en el código subyacente (Levy, 2017). Todo ello debe hacernos ver que estos contratos inteligentes suponen un mero avance en el plano legal, no una solución holística que elimine permanentemente al componente humano, como muestra la necesaria existencia de los oráculos humanos una vez alcanzadas las limitaciones computacionales de estos programas.

Si un contrato inteligente se utiliza para determinar un acuerdo entre partes con identidades conocidas, las obligaciones de rendimiento embebidas en el contrato inteligente pueden ser modificadas mediante la participación en una segunda transacción para deshacer o modificar los efectos de cualquier código inicialmente ejecutado. Al igual que con cualquier otro acuerdo legal, estas partes también tienen la opción de hacer valer sus derechos contractuales en un tribunal u otro órgano arbitral de toma de decisiones, pudiendo recuperar los daños y perjuicios. Estas oportunidades pueden no estar disponibles en el contexto de los acuerdos basados en contratos inteligentes que implican a partes que no conocen la identidad de la otra. Para presentar una demanda, la parte perjudicada tendrá que conocer la identidad de la parte contraria para cumplir los

requisitos de notificación. Incluso si una parte obtuviera una sentencia condenatoria dictada en rebeldía, la sentencia tendría un efecto práctico limitado a menos que la identidad de la parte condenada en ausencia pudiera establecerse de alguna manera. Debido a estos problemas de ejecución, los acuerdos basados en contratos inteligentes que impliquen a partes en el anonimato probablemente mostrarán una dinámica interna diferente a la de los acuerdos actuales. Por ejemplo, las sólidas doctrinas del derecho consuetudinario y del derecho civil como la desprotección y la incapacitación suavizan el golpe de los contratos que contienen cláusulas asimétricas o desfavorables. (McCluskey, 2016). Sin embargo, en el contexto de los contratos inteligentes utilizados para regir las transacciones entre partes seudónimas, es probable que las partes perjudicadas carezcan de la capacidad de invocar estas defensas, lo que posiblemente fomente el despliegue de acuerdos basados en contratos inteligentes que favorezcan desproporcionadamente a las partes con mayor poder de negociación.

La adopción generalizada de los contratos inteligentes también puede acelerar los cambios en la prestación de servicios jurídicos, lo que dará lugar a un cambio estructural en la profesión jurídica. A medida que los contratos inteligentes se hacen más sofisticados, los individuos podrían confiar menos en el asesoramiento de los abogados, optando por utilizar acuerdos estandarizados, algunos de los cuales incorporan el código de los contratos inteligentes. Si se pone en marcha un servicio de este tipo y se generalizan los acuerdos basados en contratos inteligentes, quienes necesiten ayuda legal podrían renunciar cada vez más a la orientación jurídica directa de un abogado en ejercicio, reduciendo en última instancia el trabajo jurídico transaccional. En la actualidad, ya tendemos a confiar más en los sistemas de recomendación informáticos que en otras fuentes de información, un fenómeno conocido como sesgo de automatización. En lugar de evaluar críticamente la información, se siguen las recomendaciones proporcionadas por los ordenadores y las máquinas, incluso si el consejo es erróneo o da lugar a la comisión de errores. Con la mayor disponibilidad de bibliotecas estandarizadas de códigos de contratos inteligentes o acuerdos híbridos, podrían perderse algunas sutilezas del trabajo jurídico transaccional. Dado que es poco probable que estas bibliotecas se ajusten perfectamente a las especificidades de cada acuerdo comercial y jurídico, las partes contratantes podrían optar por memorizar sus obligaciones utilizando disposiciones por defecto, sin considerar cuidadosamente si estas disposiciones se ajustan con precisión a sus necesidades legales.

5. Contratos inteligentes y derivados

Dado que las monedas digitales y los contratos inteligentes permiten a las partes transferir valor de forma segura y en gran medida irreversible, sin necesidad de un intermediario centralizado, la tecnología Blockchain puede utilizarse para modelar y crear acuerdos financieros digitalizados que se liquiden y compensen de forma bilateral con menos necesidad de administración por parte de terceros. Aunque hay una serie de productos financieros que pueden verse afectados por la tecnología Blockchain, aquí nos centraremos en dos: los valores y los derivados.

Las cadenas de bloques pueden mejorar la liquidación y compensación de valores y derivados y crear potencialmente un sistema financiero más global y transparente. Al mismo tiempo, si no se controlan, las cadenas de bloques pueden crear un panorama financiero más inestable y no regulable, gobernado por un número cada vez mayor de sistemas que dependen de la criptografía. La emisión y venta de los primeros valores a través de una cadena de bloques, aunque sea una transacción pequeña representa uno de los pocos casos de uso de la tecnología de la cadena de bloques y puede marcar el comienzo de un cambio mayor hacia la descentralización financiera. Las operaciones con valores y derivados incluyen varias fases, como la confirmación, la compensación y la liquidación. Una vez que las partes acuerdan una operación, se confirman los términos de esta y se determinan y liquidan las obligaciones. Tras la confirmación y la compensación, la operación se liquida mediante procedimientos que difieren en función del producto financiero. En el caso de las operaciones con valores, la liquidación se produce cuando el vendedor entrega el título de los valores en cuestión y recibe el pago.

En el caso de una transacción de materias primas, la liquidación y compensación puede implicar la entrega de instrumentos financieros, documentos o incluso artículos físicos como trigo, maíz o metales preciosos. Hoy en día, varios intermediarios ayudan en el proceso de liquidación y compensación, sirviendo como infraestructura crítica para el correcto funcionamiento de los mercados de valores y derivados. Por ejemplo, los agentes de bolsa suelen mantener las carteras financieras de particulares, hogares o empresas y realizan operaciones en nombre de sus clientes. A su vez, estos agentes trabajan con otros intermediarios financieros de mayor envergadura, como las bolsas de valores y las contrapartes centrales (CCP) en el caso de los derivados, para facilitar la compensación y la liquidación de las operaciones (Regulatory, 2022). Las bolsas y las contrapartes

centralizadas, como la Bolsa de Nueva York, el Sistema de Cuota Automatizada de la Asociación Nacional de Agentes de Valores (NASDAQ) y la Bolsa Mercantil de Chicago, actúan como centros a través de los cuales operan los bancos o los agentes de bolsa. Estos intermediarios centralizados imponen normas institucionales y definen cómo y en qué circunstancias pueden realizarse las operaciones con valores y derivados. Gestionan el flujo de información sobre las operaciones y nivelan las condiciones de los participantes en el mercado proporcionando una lista actualizada de precios para los valores y los productos derivados.

5.1. El riesgo sistémico de los mercados bursátiles, problema y solución

Las bolsas y las contrapartes centrales suelen mantener también cámaras de compensación estrechamente vinculadas, ayudando a sus miembros a capear las duras tormentas económicas. Cada cámara de compensación exige a sus miembros que presenten garantías y hagan contribuciones a un fondo de garantía antes de unirse a ella, y garantiza el pago si uno de sus miembros incumple, haciéndose legalmente responsable de las operaciones de sus miembros (Kress, 2011). En general, cada bolsa o contraparte central que participa en operaciones de valores o derivados compensadas de forma centralizada mantiene un libro de contabilidad de las operaciones pertinentes, al igual que cada institución financiera participante. La confirmación, la compensación y la liquidación de estas operaciones dependen en gran medida de la actualización y la conciliación de los libros de contabilidad que compiten entre sí a través de un proceso que ha evolucionado a lo largo de los siglos.

Sin embargo, no todos los valores y derivados pasan por los mercados o las contrapartes centralizadas. Algunas operaciones se realizan en mercados extrabursátiles (OTC). Estos mercados son menos formales y, por lo general, dependen de las relaciones comerciales organizadas en torno a los intermediarios que cultivan los mercados de productos financieros específicos. Dado que los mercados OTC giran en torno a los intermediarios, tienden a funcionar con menos transparencia y con menos normas en comparación con los mercados apoyados por intermediarios centralizados. Estos mercados no son públicos y, como las partes suelen negociar las operaciones OTC de forma bilateral, no tienen acceso a la misma información que un intermediario. Tanto si una operación financiera es OTC como si se compensa de forma centralizada, los actuales procesos de liquidación y compensación adolecen de problemas operativos. Por ejemplo, aunque una operación

bursátil se ejecuta en una fracción de segundo en la mayoría de las bolsas reguladas de EE.UU., la liquidación tarda hasta tres días (Christian, 2006).

Estos agentes, a su vez, trabajan con sus bancos depositarios para coordinar la liquidación y facilitar el pago, y también trabajan con la Depository Trust & Clearing Corporation (DTCC) un intermediario que mantiene los certificados físicos de las acciones que se negocian en los mercados estadounidenses para transferir su titularidad. Si bien este riesgo suele ser tolerable a título individual, en caso de incumplimiento de un actor importante en el mercado, las operaciones que no se han liquidado y compensado en su totalidad pueden tener consecuencias catastróficas, creando un efecto dominó en los mercados de capitales que, en última instancia, podría conducir a la quiebra de otras empresas financieras.

Una preocupación similar sobre el riesgo de contraparte se manifiesta en los mercados de derivados, especialmente en los mercados que implican operaciones OTC. A diferencia de las operaciones de valores compensadas de forma centralizada que se liquidan en unos pocos días, los contratos de derivados pueden permanecer pendientes durante meses o incluso años antes de su liquidación, exponiendo a las partes a un prolongado riesgo de contraparte. Para tener en cuenta este riesgo, muchos contratos de derivados exigen que las partes reserven una parte del valor del derivado como garantía (también conocida como margen), que se ajusta periódicamente para reflejar las circunstancias cambiantes o los cambios en las calificaciones crediticias de las partes. Dado que los derivados OTC se negocian y ejecutan de forma bilateral, nadie tiene una visión completa de todos los acuerdos que una parte ha suscrito previamente, lo que hace difícil predecir si una parte ha realizado otras transacciones u operaciones que puedan afectar a su capacidad de pago. Debido a estos problemas, el incumplimiento de una o varias transacciones de derivados puede crear un riesgo sistémico y paralizar la actividad del mercado. De hecho, esto es en gran medida lo que precipitó la crisis financiera que se desarrolló en 2007 y 2008 (Steigerwald, 2014).

Cuando los precios de la vivienda cayeron, las obligaciones contraídas en virtud de estos derivados vencieron, pero estas instituciones financieras carecían de activos suficientes para cumplir su parte del trato. Al carecer de información suficiente, los gobiernos se esforzaron por llegar a un consenso sobre la forma adecuada de gestionar este riesgo imprevisto, optando finalmente por rescatar a las empresas financieras en dificultades con la esperanza de detener el contagio financiero y las olas de impago en cascada. Al igual

que una cadena de bloques sustituye a un banco central en la administración de las transferencias de moneda digital, una cadena de bloques también puede servir como depósito centralizado para facilitar las operaciones de valores.

Utilizando una cadena de bloques, es posible tokenizar una acción de una empresa, un bono del Tesoro de EE. UU., un préstamo sindicado u otros valores, e intercambiar rápidamente el token como si de un bitcoin se tratase. La red de ordenadores que soportan la cadena de bloques subyacente puede verificar y validar una transacción que implique un token, creando un registro transparente, resistente a la manipulación y con sello de tiempo de cada operación. Una vez creado un token, se puede utilizar un contrato inteligente para facilitar el pago y la transferencia del token entre las partes, así como para codificar otros derechos económicos, como el derecho a recibir dividendos, en el caso de las acciones, o pagos periódicos, en el caso de un bono o préstamo. Al basarse en contratos inteligentes, la transferencia de un token, y las obligaciones de pago relacionadas, pueden producirse de forma automática y casi instantánea sin necesidad de terceros para facilitar y supervisar el pago.

La tecnología de cadenas de bloques ofrece la posibilidad de fusionar la negociación, la compensación y la liquidación en un solo proceso, reduciendo la necesidad de que la transacción pase por múltiples capas de intermediarios financieros mediante la transferencia de representaciones digitalizadas de certificados y créditos de préstamo (Mukhopadhyay, 2018). Mediante el uso de contratos inteligentes, las cadenas de bloques pueden reducir el papel de los intermediarios implicados en la facilitación de los pagos asociados y otros derechos económicos. Con una cadena de bloques, una operación se completa una vez que la red subyacente verifica y valida una transacción basada en tokens. En la medida en que las partes confíen en el mismo sistema basado en la cadena de bloques, las afirmaciones y confirmaciones posteriores a la operación, así como la alineación de los datos de la operación y la liquidación, se vuelven menos necesarias. Al disminuir la necesidad de conciliación de datos, las cadenas de bloques reducen el riesgo de error y el tiempo necesario para liquidar y compensar una operación. Es posible que las partes ya no tengan que esperar días para completar una operación, lo que reduce tanto el riesgo de la contraparte como la posibilidad de disputas. Además de reducir los tiempos de compensación y liquidación, las cadenas de bloques crean un medio para coordinar los mercados de forma más descentralizada, reduciendo el papel de las bolsas centralizadas y aportando potencialmente más transparencia a los mercados OTC. Un grupo de partes

independientes y sin confianza puede utilizar una cadena de bloques como fuente de datos resistente y a prueba de manipulaciones para conciliar los datos de las operaciones. Dado que cualquier persona conectada a una red basada en una cadena de bloques puede ejecutar una transacción relacionada con un valor "tokenizado", los participantes en el mercado pueden realizar operaciones con productos financieros de igual a igual. La información relacionada con el precio y el momento de una operación de valores puede almacenarse directamente en una cadena de bloques, y las partes pueden calcular el precio de un valor en cualquier momento, reduciendo la necesidad de acudir a bolsas centrales para difundir la información de precios a los participantes del mercado en el caso de las bolsas centralizadas, o revelar la información de precios relevante en los mercados OTC.

5.2. Blockchain, alternativa al sistema financiero clásico

A medida que la tecnología Blockchain madura y se adopta de forma más generalizada, la naturaleza directa y transnacional de los blockchains abrirá la posibilidad de crear un sistema unificado y global para la emisión y la mayor parte de las operaciones bursátiles en todo el mundo. En el futuro, podremos ser testigos de la aparición de nuevas bolsas descentralizadas y basadas en códigos que operen sobre un sistema basado en Blockchain (Morabito, 2017). De hecho, los sistemas basados en Blockchain podrían implementar potencialmente las normas específicas de cada jurisdicción relativas a la compra y venta de valores mediante la codificación de estas normas en códigos de contratos inteligentes. Si tienen éxito, estos sistemas basados en la cadena de bloques podrían acabar sustituyendo el actual sistema financiero por nuevos sistemas basados en la cadena de bloques que respeten y cumplan simultáneamente las normas jurisdiccionales específicas.

Al igual que con los valores, las cadenas de bloques también pueden agilizar la creación, ejecución y negociación de derivados. Como se ha descrito anteriormente, los contratos inteligentes pueden utilizarse para memorizar la totalidad o parte de los acuerdos legales, y las partes contratantes pueden confiar en una cadena de bloques para garantizar las obligaciones de cumplimiento. Con una cadena de bloques, las partes pueden memorizar ciertos aspectos de los contratos de derivados utilizando código, de modo que puedan ser procesados y ejecutados automáticamente por una red subyacente basada en la cadena de bloques. Dado que el valor de los derivados negociados en bolsa se basa en acontecimientos futuros, estos contratos pueden incorporar oráculos para ajustar sus condiciones en función de los cambios en los tipos de interés o en los precios de las divisas y las acciones. Las cadenas de bloques también pueden aumentar la transparencia de los

mercados de derivados OTC. La nueva tecnología podría arrojar luz sobre los precios de los derivados y proporcionar un recurso compartido para discernir las posiciones de las partes. Los gobiernos y los organismos encargados de hacer cumplir la ley podrían obtener una mayor capacidad para evaluar el valor y el riesgo de estas transacciones financieras almacenando información transparente, resistente y a prueba de manipulaciones sobre estos acuerdos, incluido el tipo de derivado, el valor nocional de cada contrato de derivados y las obligaciones de garantía de las partes.

Al igual que los valores inteligentes, los contratos de derivados inteligentes podrían incluso estar programados para cumplir con reglas de mercado bien aceptadas y cuidadosamente implementadas. Pensemos en un contrato de futuros altamente estandarizado que se negocie habitualmente en bolsas centralizadas como la Bolsa Mercantil de Chicago. Un futuro "inteligente" podría tener sus condiciones, como la calidad, la cantidad y la entrega, preprogramadas y podría tener codificados los requisitos de margen. Una cadena de bloques podría liquidar automáticamente la operación una vez que el futuro haya expirado, sin necesidad de que una bolsa aplique estas normas (Castiglione, 2018), y podría aplicar normas basadas en contratos inteligentes diseñadas para evitar órdenes excesivas y controlar a las partes que toman grandes posiciones, reduciendo así las posibles perturbaciones del mercado.

Si se emplean adecuadamente, estos mercados serían menos susceptibles de ser manipulados. Sus normas se aplicarían automáticamente mediante una cadena de bloques, dejando a las partes participantes con menos margen de maniobra para eludir las normas codificadas. Aunque las blockchains albergan la esperanza de mejorar la negociación, compensación y liquidación de las transacciones de valores y derivados, el camino hacia la implementación y adopción de la tecnología Blockchain para mejorar los mercados financieros no está exento de peligros.

En muchos sentidos, la tecnología Blockchain devuelve al sistema financiero a sus raíces históricas La historia de los derivados es en gran medida la misma. Mientras que las bolsas reguladas surgieron a mediados del siglo XIX sólo después de la Gran Recesión, los gobiernos de todo el mundo trataron de centralizar la compensación y la gestión de las operaciones de derivados estándar con la esperanza de contener y controlar los riesgos de los derivados OTC. Hasta cierto punto, la centralización ha sido eficaz. Las cámaras de compensación previenen el riesgo de impago de los participantes en el mercado y mejoran la liquidez en ciertas transacciones financieras estandarizadas y de gran volumen. Al

agrupar las garantías y a través del proceso de novación estos intermediarios proporcionan un seguro a las instituciones miembros, haciéndose legalmente responsables de las deudas de los miembros en caso de impago, y absorbiendo el riesgo financiero al actuar como una fortaleza de capital.

La centralización también ayuda a los bancos centrales a aplicar la política monetaria influyendo en los tipos de interés a corto plazo a través de la compra y venta de instrumentos financieros, como los valores del Estado y los préstamos garantizados. Al realizar operaciones a través de mercados estrechamente controlados y ampliamente utilizados, los bancos centrales pueden encontrar contrapartes de forma fiable y garantizar que los efectos de la política monetaria se extiendan amplia y rápidamente por toda la economía.

Si la tecnología Blockchain conduce a una proliferación de mercados descentralizados, puede aumentar el riesgo sistémico del sector financiero. Aunque las cadenas de bloques son excelentes para transferir valores tokenizados y automatizar ciertos aspectos de las operaciones con derivados, no son cámaras de compensación (Bank for International Settlements, 2022). Las cadenas de bloques no proporcionan, por defecto, un seguro a los participantes del mercado. Por lo tanto, si un número cada vez mayor de operaciones con valores y derivados se realiza de igual a igual, sin el uso de una cámara de compensación, el incumplimiento de un gran actor financiero puede paralizar los mercados. Aunque las grandes instituciones financieras podrían poner en común sus recursos para superar este problema o un tercero podría proporcionar un seguro, por el momento, estos mecanismos no existen. Confiar en la tecnología Blockchain para descentralizar el sistema financiero podría crear nuevos riesgos que, en última instancia, requerirían una nueva centralización para garantizar un crecimiento económico más constante y estable. Así, podríamos correr el riesgo de repetir errores del pasado. La naturaleza transparente de las cadenas de bloques también podría limitar su capacidad para apoyar y cultivar un sistema financiero saludable. En el caso de los valores y los derivados, si se utiliza una cadena de bloques para facilitar la ejecución y la liquidación de las transacciones financieras, la información relacionada con esas transacciones corre el riesgo de ser divulgada públicamente.

A diferencia de las empresas de otros sectores, las empresas de servicios financieros no suelen recurrir a las patentes para proteger su propiedad intelectual, ya que la Oficina de Patentes y Marcas de los Estados Unidos (USPTO) sólo ha considerado recientemente que los procesos empresariales son patentables. Al carecer de protección de patentes, las

instituciones financieras se basan principalmente en las leyes de secreto comercial para mantener una ventaja competitiva y para evitar que otros participantes en el mercado hagan ingeniería inversa de sus estrategias patentadas. Por ejemplo, un fondo de cobertura dedicado a una estrategia de acciones largo-corto en la que el fondo tomó posiciones largas en acciones que creía que iban a aumentar de valor y posiciones cortas en acciones que se preveía que iban a disminuir. Si todas las acciones relevantes dependen de una bolsa de valores basada en Blockchain, el fondo de cobertura corre el riesgo de revelar públicamente su estrategia al participar en la negociación, otorgando a los competidores la capacidad de analizar las transacciones y, si es rentable, participar en una estrategia similar para limitar la ganancia financiera potencial del fondo de cobertura. También es preocupante el hecho de que la transparencia de una cadena de bloques podría disminuir la capacidad de los activistas y reformadores para tomar el control de las empresas y realizar cambios de política corporativa (Beckerman-Rodau, 2002).

En general, dada la mayor transparencia de las redes basadas en Blockchain y su incapacidad para asegurar los riesgos de impago, los beneficios producidos por un sistema basado en Blockchain se verían compensados por la aparición de un sistema financiero más arriesgado caracterizado por empresas con prácticas de gobierno corporativo más débiles. Independientemente de que las tecnologías Blockchain sean empleadas por las instituciones financieras existentes, plantean una serie de nuevos retos en la medida en que pueden utilizarse para apoyar transacciones financieras y comerciales ilícitas. Las cadenas de bloques pueden construirse para ser opacas y facilitar el comercio de instrumentos financieros a escala mundial. También pueden combinarse con contratos inteligentes para construir nuevos sistemas financieros que dependan en gran medida de esta tecnología (Morabito, 2017).

En Estados Unidos, el acceso a los mercados públicos de capitales ha estado muy controlado desde el siglo XX. El gobierno estadounidense trató de prevenir futuros *cracks* obligando a las empresas a revelar más información sobre sus operaciones y la inversión ofrecida al público. La esperanza era que, a través de la divulgación afirmativa, los directivos de las empresas se comportarían de forma más honesta, por miedo a las represalias públicas o a la vergüenza (huelga mencionar el éxito de esta disuasión). Las divulgaciones reducirían los costes necesarios para que los titulares de las acciones se protegieran contra la mala conducta de los directivos y permitirían a los inversores tomar decisiones de inversión más racionales al reducir las asimetrías informativas e igualar las

condiciones de los participantes en el mercado (Vargo, 2007). Sin embargo, desde que se aprobaron estas leyes para vender valores al público, las empresas deben preparar documentos como declaraciones de registro, declaraciones de representación, informes anuales y documentos financieros, que a menudo son largos y complicados. Aunque se han aprobado leyes en Estados Unidos y en otros países que facilitan a las empresas la obtención de dinero sin necesidad de una amplia divulgación, por ejemplo, abriendo oportunidades de inversión a través del *crowdfunding*, la mayoría de los mercados públicos siguen siendo inaccesibles para las pequeñas empresas o las nuevas empresas, a menudo en nombre de la protección de los consumidores.
(Arslanian, 2019).

Con las cadenas de bloques, los productos financieros y los mercados pueden diseñarse para evitar las regulaciones financieras existentes, facilitando a las partes la obtención de dinero del público, independientemente de si está permitido por las leyes existentes. Los nuevos sistemas basados en la cadena de bloques permiten ahora a las partes recaudar fondos en línea, reuniendo vastos fondos de moneda digital a través de ventas conocidas como "ventas de fichas" u "ofertas iniciales de monedas" (ICO), si bien cabe mencionar el riesgo inherente a basar la capitalización de una compañía exclusivamente en la creación de una criptomoneda. Las cadenas de bloques y los sistemas basados en contratos inteligentes permiten a las partes confiar en el código para establecer objetivos de recaudación de fondos y recoger dinero de una variedad de personas a través de Internet sin que pase por autoridades de confianza o intermediarios centralizados (Angelov, 2019).

Algunos tokens, generalmente denominados tokens de utilidad, son principalmente de naturaleza funcional o de consumo, y a menudo sirven como medio para acceder a un servicio en línea y medirlo. En algunos casos, estos tokens suelen conferir a sus titulares el derecho a desarrollar o crear características para el servicio, incluido el derecho a votar sobre cómo debe actualizarse o evolucionar el servicio en línea. Otros tokens basados en Blockchain, generalmente denominados tokens de inversión, son diferentes de los tokens de utilidad y no sólo son de naturaleza funcional, sino que proporcionan a los titulares derechos económicos y otros beneficios.

A diferencia de los tokens de utilidad, estos tokens utilizan contratos inteligentes para asignar los beneficios a los titulares de estos tokens o imbuir a los titulares de tokens con derechos económicos expresos. Por ejemplo, uno de los primeros tokens de inversión fue DAO, una organización no constituida que emitió el "token DAO" para representar una

participación en un fondo de capital riesgo. La DAO no tenía un supuesto propietario, y las partes obtenían los tokens de la DAO transmitiendo Ethereum (la criptomoneda en la que operaba el sistema) a un contrato inteligente que gestionaba la DAO. Cualquiera que tuviera un token de la DAO podía solicitar financiación a la DAO presentando una propuesta a través de un contrato inteligente que incluía información como una descripción del proyecto y la cantidad de ether solicitada. Una vez que se presentaba una propuesta válida, el contrato inteligente subyacente de DAO permitía a los poseedores de tokens votar si se financiaba el proyecto. Si los titulares de tokens de la DAO lo aprobaban, el proyecto se vinculaba a DAO a través de otro contrato inteligente, que a su vez remitía los pagos al creador del proyecto si se alcanzaban ciertos objetivos. El mismo contrato inteligente devolvería a DAO cualquier Ethereum ganado por el proyecto, y cualquier beneficio o ganancia se redistribuiría a los titulares de tokens DAO de forma proporcional.

Las partes que están detrás de estas ventas de tokens y ICOs a menudo no cumplen con la normativa legal de las ofertas públicas, debido a la creencia de que los tokens no estarán sujetos a las leyes de valores u otras regulaciones financieras. En su lugar, proporcionan información informal, normalmente en forma de "libros blancos" que esbozan los detalles técnicos del proyecto y sitios web sencillos con información biográfica básica sobre los fundadores y asesores del proyecto. Las partes que venden tokens recurren a las redes sociales y a otros sitios en línea para anunciar la venta, y los partidarios compran estos tokens utilizando moneda digital, a menudo con la esperanza de que el valor de estos tokens se revalorice en los mercados secundarios si el proyecto se pone en marcha. Para facilitar esta nueva economía hay varias bolsas de criptomonedas, y eventualmente bolsas descentralizadas, que no operarán como los mercados de valores regulados u otros mercados tradicionales respaldados por grandes empresas financieras (Liermann, 2019).

Conclusión

La tecnología Blockchain es reconocida universalmente como una nueva oportunidad para la descentralización, percibida como un nuevo medio para que la gente se libere de la tiranía de los gobiernos y las empresas en formas que recuerdan bastante a los primeros días de Internet.

Los gobiernos han ampliado su control exigiendo a los intermediarios que cambien su código para mantener y que mantengan y respeten las leyes jurisdiccionales. Con la llegada de Bitcoin y la tecnología Blockchain en general estamos a punto de asistir a una nueva ola de descentralización y a nuevos llamamientos que el mundo se regirá, una vez más, por la regla del código. Los ecos de la primera ola de Internet impregnan el discurso en torno a las cadenas de bloques, con afirmaciones que la tecnología Blockchain conducirá a una mayor libertad y emancipación individual, como aspiraban inicialmente estos primeros defensores de la tecnología.

Asimismo, ésta facilita la aparición de nuevos sistemas autónomos y autocontenidos. Estos sistemas permiten a las personas comunicarse, organizarse e intercambiar valor de igual a igual, con menos necesidad de operadores intermediarios. Proporcionan a los individuos la oportunidad de crear una nueva capa normativa o un sistema personalizado de reglas basadas en códigos que pueden fácilmente incorporarse al tejido de esta nueva construcción tecnológica, lo que facilita la elusión

La ley basada en la criptografía comparte ciertas similitudes con los medios más tradicionales de regulación por código, sin embargo, se distingue de los regímenes actuales basados en códigos, en que opera de forma autónoma independientemente de cualquier gobierno u otra autoridad centralizada. Si la visión de los defensores de la cadena de bloques se acerca a la realidad, se estaría delegando el poder en construcciones tecnológicas que podrían desplazar los actuales sistemas burocráticos, regidos por la jerarquía y las leyes gobernados por reglas deterministas dictadas por chips de silicio, ordenadores y los que los programan. Estos sistemas podrían mejorar la sociedad de forma demostrable, pero también podrían restringir, en lugar de mejorar, la libertad individual.

Bibliografía

Abbate Janet. (2000). *Inventing the Internet.* MIT Press.

Ahmed Kosba, A. M. (2016). *Preserving Smart Contracts.* IEEE Symposium on Security and Privacy (SP).

Angelov, A. S. (2019). El sistema financiero digital: los nuevos agentes. págs. 1-84. doi:ISSN-e 2172-7856

Antonopoulos, A. M. (2018). *Mastering Ethereum: Building Smart Contracts and Dapps.* Publisher: O'Reilly Media.

Arslanian, H. F. (2019). *The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services* . Springer International Publishing; Palgrave Macmillan.

Arvind Narayanan, J. B. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* . Princeton University Press. Obtenido de Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and

Bank for International Settlements. (28 de 02 de 2022). *Distributed Ledger Technology in Payment, Clearing and Settle.* Obtenido de http://www.bis.org/cpmi/publ/d157.pdf

Baran, P. (1964). *On Distributed Communication.* RAND Corporation .

Beckerman-Rodau, A. (2002). "The Choice between Patent Protection and Trade Secret Protection: A Legal and Business Decision" . *Journal of Patent and Trademark Office Society* , 371–409.

Castiglioni Maldonado, F. (2018). *Introduction to blockchain and ethereum.* Packt Publishing.

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto 82*, 199-203.

Chaum, D. F. (1989). Untraceable Electronic Cash. *CRYPTO '88 Proceedings on Advances in cryptology*, 319-327.

Christian, J. W. (2006). Naked Short Selling: How Exposed Are Investors? *Houston Law Review 43*, 1033–1099.

Davies, D. (1997). *A Brief History of Cryptography.* Information Security.

Delfs H., K. H. (2002). *An Introduction to Cryptography.* Network Associates.

Diffie, W. D. (1976). *New Directions in Cryptography.* Transactions on Information Theory.

Farnsworth, A. E. (1967). Meaning' in the Law of Contracts. *Yale Law Journal*, 939– 965.

Geis, G. S. (2008). Automating Contract Law. *New York University Law Review*, 450500.

Kress, J. (2011). Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity. *Harvard Journal on Legislation*, 49-93. Obtenido de "Credit Default Swaps, Clearinghouses, and Systemic Risk:

Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. *JOURNAL OF SYSTEMS INTEGRATION* , 1-31.

Levy, K. E. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart. *Contracts and the Social Workings of Law*, 1-15.

Liermann, V. (2019). *The Impact of Digital Transformation and FinTech on the Finance Professional* . Springer International Publishing, Palgrave Macmillan.

McCluskey, M. T. (2016). *Regulating Forced Arbitration in Consumer Financial Services: Re-opening the Courthouse Doors to Victimized Consumers.* Center for Progressive Reform.

Morabito, V. (2017). *Business Innovation Through Blockchain.* Springer.

Mukhopadhyay, M. (2018). *Etherum Smart Contract Development.* Packt. Publishing

Nakamoto, S. (2008). *Bitcoin: A peer-to- peer electronic cash system.* Obtenido de https://bitcoin.org/bitcoin.pdf

Open Bazaar. (28 de 02 de 2022). Obtenido de OpenBazaar, https://openbazaar.org/; SafeMarket, https://safemarket

Ortolani, P. (2016). Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin,.

Oxford Journal of Legal Studies , 595–629.

Piper, F. (2002). *Cryptography: A Very Short Introduction.* Oxford University Press.

Posner, R. (2004). The Law and Economics of Contract Interpretation. *Olin Working Paper* , 229.

Reed, J. (2017). *Litecoin: An Introduction to Litecoin Cryptocurrency and Litecoin Mining.* CreateSpace Independent Publishing Platform.

Regulatory, F. I. (02 de 03 de 2022). Obtenido de http://www.shearman.com/~/media/Files/NewsInsights/Publications/2016/02/EU US-Agreement-OnRegulation-Of-Central-Counterparties-FIAFR-021616.pdf

Steigerwald, R. (2014). Transparency, Systemic Risk and OTC Derivatives the G-20 Trade Execution and Clearing Mandates Reconsidered. *Futures & Derivatives Law Report 34*, , 20.

Szabo, N. (1994). *Smart Contracts.* https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literat ur e/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Tapscott, D. (2016). *The Blockchain Revolution.* Penguin Random House.

Triantis, G. G. (2002). The Efficiency of Vague Contract Terms: A Response to the Schwartz-Scott Theory of U.C.C. *Louisiana Law Review*, 1065–1079.

Vargo, S. L. (2007). On A Theory of Markets and Marketing: From Positively Normative to Normatively Positive. *Australasian Marketing Journal (AMJ)*, 53-60.

ANEXO I

DECLARACIÓN RELATIVA AL ARTÍCULO 8.3 DEL REGLAMENTO SOBRE LA ASIGNATURA TRABAJO FIN DE GRADO (*Acuerdo de 5 de marzo de 2020, del Consejo de Gobierno de la Universidad de Oviedo).*

Yo, César Ramos Gutiérrez con DNI 71744942F,

DECLARO

que el TFG titulado **De la tecnología Blockchain y sus aplicaciones económicas** es una obra original y que he citado debidamente todas las fuentes utilizadas.

24 de mayo del 2022