Tecnología Blockchain, una nueva era para la empresa

LUZ PARRONDO TORT
UPF Barcelona School of Management

Resumen

Desde 2009, blockchain ha servido como una tecnología de registros potencialmente transformadora que se espera sea tan revolucionaria como Internet. Originalmente desarrollada como una metodología para registrar transacciones de criptomonedas, la funcionalidad de Blockchain ha evolucionado en una gran cantidad de aplicaciones, tales como banca, mercados financieros, contabilidad, cadenas de suministros, sistemas de votación y servicios gubernamentales. Este documento tiene como objetivo explicar en qué consiste la tecnología blockchain a la vez que proporcionar una discusión inicial sobre cómo blockchain podría permitir un ecosistema de empresarial en tiempo real, verificable y transparente. Además, blockchain tiene el potencial de crear empresas digitales a través de contratos inteligentes que permiten automatizar y democratizar la toma de decisiones.

Clasificación JEL: O33

PALABRAS CLAVE

Blockchain, Red de Registros Distribuidos, tecnología, empresa

Abstract

Since 2009, blockchain has served as a potentially transformative record technology that is expected to be as revolutionary as the Internet. Originally developed as a methodology for registering cryptocurrency transactions, Blockchain's functionality has evolved into a large number of applications, such as banking, financial markets, accounting, supply chains, voting systems and government services. This document aims to explain blockchain technology while providing an initial discussion on how this innovation could allow a real-time, verifiable and transparent business ecosystem. In addition, blockchain has the potential to create digital companies through intelligent contracts that allow automation and democratization of decision making.

Clasificación JEL: O33

KEYWORDS

Blockchain, Distributed Ledger Technology, technology, business

---

1. Introducción

La tecnología blockchain es la base tecnológica de Bitcoin, descrita por primera vez por su misterioso autor Shatoshi Nakamoto, en el libro blanco “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008). Es una base de datos distribuida donde cada nodo o usuario en la red ejecuta y registra las mismas transacciones agrupándolas en forma de bloques. Es una forma segura, transparente y descentralizada de registrar transacciones que no se limita únicamente a las monedas digitales, a pesar de que saltó a la fama cuando Bitcoin en 2013 experimentó una subida del 1000%. La capacidad de blockchain de registrar **todo tipo de transacciones** persona-a-persona de manera eficiente, segura, verificable e inmutable significa que puede aplicarse a tareas no financieras como la contabilidad o la trazabilidad de productos en la cadena de suministros. Podría ayudar a resolver finalmente el problema de piratería de música y

video, permitiendo que los medios digitales sean legítimamente comprados, vendidos y heredados. Desde una vertiente social, puede ser utilizada en la transmisión de votos, para ayudar a certificar si un producto es de origen ético, si la ropa se fabrica en talleres legales o si las donaciones llegan al destino esperado. También presentan oportunidades en todo tipo de servicios públicos, como pagos de la salud y el bienestar e incluso para la verificación documental en el registro de la propiedad. Todo ello de forma transparente, segura y prescindiendo de intermediarios que validen la identidad de las partes, la titularidad de los activos o la validez en una transacción.

La crisis de 2007 destruyó la confianza en los intermediarios financieros y fue el detonante para desarrollar una tecnología con capacidad de desplazar el control de las operaciones desde los bancos a los usuarios, reduciendo así la necesidad de un intermediario validador. Esta desintermediación podría significar mayor transparencia y mayor democratización de los sistemas financieros, económicos e incluso políticos. Sin embargo, no hemos de desmerecer el poder de los gobiernos y los gigantes financiero-económicos, que actualmente están invirtiendo en esta tecnología para situarse en la vanguardia de la nueva era.

La segunda derivada de esta tecnología sin embargo puede significar una revolución para la innovación empresarial y los medios de financiación de nuevos proyectos. La cadena de bloques tiene la capacidad de incorporar sobre su estructura aplicaciones como los contratos inteligentes o "smart contracts" y las aplicaciones distribuidas o DApps[1]. Los contratos inteligentes no solo definen las reglas y sanciones en torno a un acuerdo de la misma manera que lo hace un contrato tradicional, sino que también hacen cumplir automáticamente esas obligaciones. Permiten automatizar mecanismos empresariales como pagos, acuerdos y registros allanando el camino para la implementación de las Organizaciones Autónomas Descentralizadas (DAO). Una DAO es un contrato inteligente complejo que da origen a una organización digital carente de jefes o empleados, en la que las decisiones se toman de forma descentralizada y las acciones se ejecutan de forma automática, transparente y sin necesidad de intervención humana.

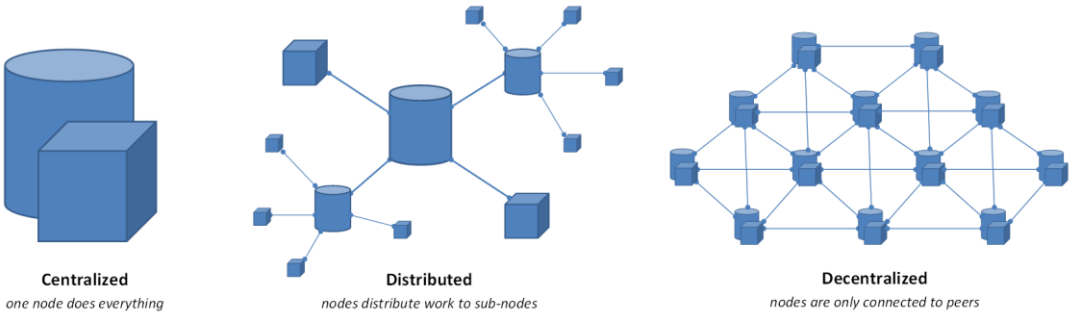
[1] Una DApp es muy similar a una aplicación web tradicional. La interfaz usa la misma tecnología para renderizar la página. La única diferencia fundamental es que en lugar de una API que se conecta a una base de datos, tiene un contrato inteligente que se conecta a una cadena de bloques.

Este artículo proporciona una aproximación accesible para aquellos empresarios que estén interesados en aprender más sobre el desarrollo de blockchain y su potencial impacto en la empresa, la economía y la sociedad. La sección dos presenta una introducción sobre cómo funciona la tecnología blockchain. La sección tres analiza el impacto en la estructura empresarial, en áreas como la contabilidad, la auditoría, la cadena suministros y la financiación. En la sección cuatro se explica en qué consisten las DAO y finalmente, la sección cinco concluye y anima a la reflexión y el debate sobre esta controvertida tecnología que ha apretado el acelerador en los dos últimos años.

2. Qué es la tecnología blockchain

Antes de intentar comprender cómo funcionan las redes blockchain, vale la pena analizar las redes tradicionales. Durante siglos, las organizaciones han utilizado bases de datos para registrar transacciones e información, y los gobiernos las han usado para mantener registros públicos, como por ejemplo la propiedad de la tierra. Hasta ahora siempre ha sido necesaria la presencia de una autoridad central, el banco o la oficina gubernamental, que gestione los cambios en las transacciones, para identificar quién posee qué en un momento dado. Esto les permite comprobar si las nuevas transacciones son legítimas, que los mismos 10€ no se gastan dos veces y que el vendedor de una casa es el propietario. Dado que los usuarios confían que el intermediario verifica las transacciones correctamente, las personas pueden intercambiar activos entre sí a pesar de no conocerse. La función de estos intermediarios es la de proveer la confianza necesaria entre las partes y la de controlar el acceso a la información en el registro oficial. Estos registros centralizados y privados presentan, a pesar del impulso que supuso la tecnología digital, ineficiencias en tiempo y costes así como una opacidad incapaz de frenar la proliferación fraudes y crisis de confianza.

Blockchain substituye a la entidad central en la legitimación de las transacciones. Esta función es posible gracias a su arquitectura distribuida (ver figura 1) y a un sistema de algoritmos e incentivos llamado minería que asegura una única verdad registral.

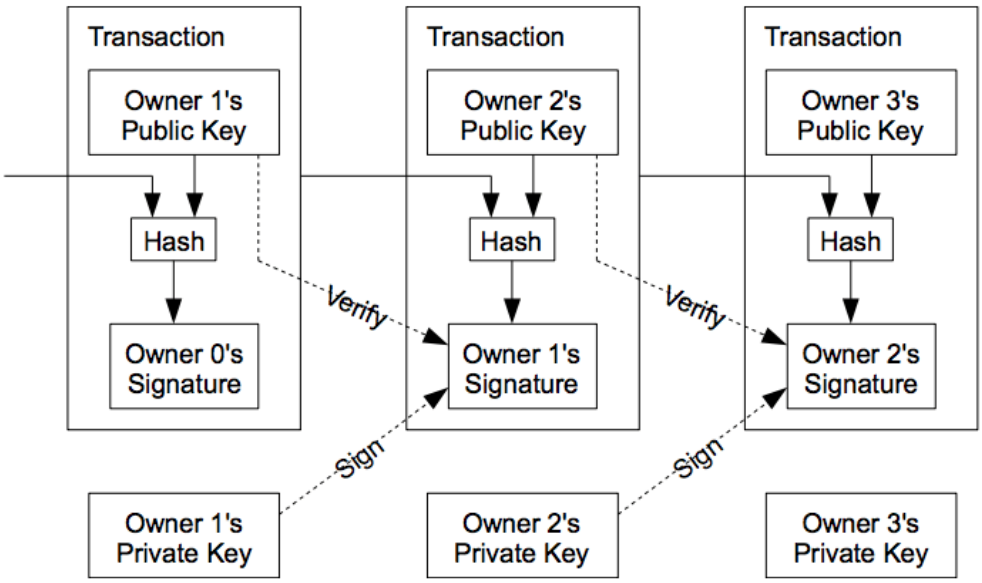


Fuente: "Mesh World P2P Simulation Hypothesis" by Eric Grange

Figura 1. Tipos de sistemas

Blockchain tiene su origen en las criptomonedas, específicamente en Bitcoin. Satoshi Nakamoto, en su libro blanco sobre Bitcoin, define la moneda electrónica como una cadena de firmas digitales. El propietario de una moneda puede transferirla a otra persona añadiendo al final de la cadena la firma digital del código de la transacción anterior y la llave pública del nuevo propietario (ver Figura 2). El reto de este sistema es la verificación de la propiedad y la no duplicidad de las transacciones. La única forma de verificar que la moneda pertenece al transmisor y que éste no la ha gastado previamente es conocer todas las transacciones anteriores. Blockchain ofrece un sistema en el que las transacciones son públicas y los participantes confirman que sólo existe una verdad. Esta verdad está codificada en una cadena en forma de bloques que no está almacenada en un servidor sino distribuida en todos los nodos de la red. Cualquier nodo en el sistema puede solicitar que se agregue una transacción a la cadena de bloques, pero las transacciones solo se aceptan si todos los usuarios validan su legitimidad. Este proceso de verificación se llama minería[2] o "mining". Cada participante verificador o minero valida que la solicitud proviene de la persona autorizada. Certifica que el transmisor es el propietario y que la moneda no ha sido transmitida con anterioridad. El poder de esta tecnología reside en su extensa aplicabilidad. Además de monedas, la cadena puede transmitir cualquier otro activo, desde acciones y bonos a votos o registros de propiedad.

[2] Minería es el proceso de consenso descentralizado que se produce en la red p2p con el objeto de validar las transacciones de los usuarios y evitar que las de doble gasto se incluyan en la cadena de bloques, los nodos de la red son recompensados con bloques de monedas digitales. Se puede pensar de esto como un pago al nodo a cambio del servicio de crear un bloque en la cadena de consenso.



Fuente: "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008
Figura 2. Tipos de sistemas

Una vez añadido el nuevo bloque en la cadena ningún usuario puede eliminarlo. La inviolabilidad de este sistema está garantizada por el hecho de que la información no se encuentra centralizada en un único custodio o intermediario, sino distribuida entre todos los usuarios del sistema. "Hackear" estos registros implica un ataque simultáneo a todos los nodos del sistema. No puede haber un 'red de registros falsa' porque todos los usuarios tienen su propia versión original para contrastar.

Estas redes de registros se describen como *sin permiso* o "permissionless", porque no existe una autoridad que pueda negar el permiso para participar en la verificación, adición y visión de las transacciones (Pass & Shi). A pesar de la evidente controversia de esta característica, sus defensores le atribuyen valores sociales y políticos como la transparencia, la redistribución del poder y el incremento de la democracia. Posteriormente, y por exigencias en muchos casos empresariales, ciertas plataformas han configurado redes *autorizadas*, donde un grupo limitado de participantes tiene la capacidad de acceder, verificar y agregar transacciones en la cadena de registros. Los detractores de esta opción advierten que va en contra de la idea original por la que

Shatosi Nakamoto[3] la creó, ya que permite a los intermediarios, como los bancos y los gobiernos, perpetuar el control.

Clases de las redes

Basándonos en el acceso a los datos almacenados, podemos clasificar las redes como públicas o privadas. En la primera, no hay ninguna restricción para la lectura de datos por parte de los usuarios; en cambio, en la segunda, la lectura se limita a participantes determinados.

Por otro lado, basándose en la capacidad para generar y agregar nuevos bloques, las redes se dividen en "sin permisos" o "permisionless" y "con permisos" o "permissioned". En las primeras no hay restricciones para poder realizar transacciones y crear nuevos bloques, de modo que se ofrecen monedas o activos digitales (tokens[4]) nativos de la red como recompensa a los usuarios que quieran realizar la función de mineros. Son redes descentralizadas y un ejemplo es la famosa plataforma Bitcoin. Las segundas son desarrolladas por entidades generalmente privadas, en muchos casos para uso interno, y los usuarios de éstas necesitan permisos por parte de los administradores de la red para interactuar con el protocolo. Son centralizadas, es decir, controladas por la entidad y no por los usuarios y el proceso de verificación no se basa en un sistema de recompensas, ya que los permisos se concentran en un una sola organización.

Dadas estas posibles características, podríamos dividir blockchain en tres tipos fundamentales:

- *Blockchain pública*: una Blockchain pública es una red a la que cualquier persona puede acceder, puede crear bloques y puede participar en el proceso de consenso o proceso de validación. Como ya hemos explicado, el proveedor de confianza en estas redes públicas es la minería, una combinación de incentivos económicos y verificación criptográfica utilizando mecanismos como "Work of Proof" (WoP) o "Work of Stake" (WoS), siendo esta última más eficiente en

[3] "Bitcoin: A Peer-to-Peer Electronic Cash System"

[4] El token es un activo o valor generado por las empresas para diferentes propósitos. Se asimilan a las acciones o los bonos pero también pueden ser utilizados para adquirir productos o servicios y por lo tanto como cupones de fidelización, por ejemplo. Para más información ver sección 4, apartado "Financiación" de este artículo.

términos de coste energético y computacional (Dispenza, Garcia, & Molecke, 2017). Estos mecanismos se basan en el principio de que el poder de validación es proporcional a la cantidad de recursos económicos que pueden aportar. Estas cadenas de bloques generalmente se consideran "totalmente descentralizadas". Bitcoin, Ethereum, Litecoin, Namecoin son ejemplos de redes públicas.

- *Blockchain de consorcio:* una Blockchain de consorcio es una cadena de bloques donde el proceso de consenso es controlado por un conjunto de nodos preseleccionados; por ejemplo, uno podría imaginar un consorcio de 15 organizaciones, cada una de las cuales opera un nodo y 10 deben firmar para que el bloque sea válido. La lectura puede ser pública o restringida a los participantes. Estas cadenas de bloques se pueden considerar "parcialmente descentralizadas".

- *Blockchain privada*: una Blockchain totalmente privada es una cadena de bloques donde los permisos de escritura se mantienen centralizados en una organización. Los permisos de lectura pueden ser públicos o restringidos de forma arbitraria. Las posibles aplicaciones incluyen administración de bases de datos o auditoría internas a una sola empresa, por lo que la lectura pública puede no ser necesaria en muchos casos. Hyperledger es uno de los proyectos que más apoyo ha suscitado para crear blockchains privadas transversales. Hyperledger está formado por decenas de miembros asociados que pretenden desarrollar una plataforma común y universal para blockchains privadas. Empresas como IBM, Intel, Cisco, JP Morgan, Wells Fargo, State Street, el London Stock Exchange Group o Accenture, forman parte de este conglomerado.

Parce probable que en el futuro habrán muchas Blockchains públicas y millones de Blockchains privadas diseñadas para mercados específicos. Todas ellas variarán en protocolos pero usarán la tecnología de cadena de bloques común. Sería comparable a la existencia de diferentes sistemas operativos: por ejemplo Android y GNU/Linux comparten una pequeña parte de su código, el núcleo, pero son sistemas operativos totalmente diferentes. Sus librerías son diferentes, lo que hace que las aplicaciones de ambos sistemas se desarrollen de forma totalmente distinta, y que por lo tanto las de uno no sean compatibles con el otro. Asimismo, cada blockchain tendrá un mecanismo de

consenso diferente, un lenguaje de contrato inteligente específico y unas características únicas.

Terminología

Los términos que aluden a esta tecnología suelen ser tres: Blockchain, Tecnología de Registros Distribuidos (DLT) y Tecnología Bitcoin, por haber sido su impulsor.

Blockchain puede aludir tanto a la tecnología en su conjunto como a las plataformas que la implementan. Acompañar la palabra con "tecnología" suele ser lo adecuado para aludir a la tecnología un contexto amplio, y este, a su vez, es un término que suele usarse en las cadenas públicas. Existe cierta polémica en si se debería o no llamar 'Blockchain' a las plataformas privadas. No obstante, este uso no es limitativo, pues muchos bancos lo utilizan para referirse a sus pruebas y, en general, es el más utilizado por todos los desarrolladores y usuarios.

Tecnología de Registros Distribuidos o "Distributed Ledger Technology" es sinónimo a tecnología blockchain. Suele usarse, sin embargo, en el ámbito del desarrollo privado y más bien alejada de Bitcoin como criptomoneda. A diferencia de 'blockchain' no posee doble significado, pues sólo es capaz de aludir a la tecnología de forma completa.

Por último, Tecnología Bitcoin es el término más ambiguo de los tres. Puede hacer referencia a tres conceptos: la DLT en su conjunto, la blockchain de Bitcoin en particular o incluso los protocolos que han permitido el desarrollo de todas las criptomonedas. Debido a esto, no suele utilizarse demasiado.

Cripotomonedas y tokens

La creación de Bitcoin precipitó la expansión de un ecosistema de monedas y tokens, todos ellos considerados criptomonedas aun cuando no todos entran dentro de la definición formal de "moneda". Una moneda representa técnicamente (1) **una unidad de cuenta**, (2) **una reserva de valor** y (3) **un medio de cambio**, y dado que este ecosistema fue iniciado a partir de la creación de Bitcoin, que cumple con las tres características, todas se consideran criptomonedas a pesar de que la mayoría no lo son.

A la hora de distinguir entre criptomoneda y token, podemos reducirlo en términos generales a que una moneda digital es solo eso, una moneda, o medio de pago, mientras

que un token tiene una funcionalidad más amplia. Pero en la práctica, la línea entre las monedas y los tokens no es tan nítida y en muchas ocasiones se utilizan ambas palabras de forma confusa e intercambiable. No hemos de olvidar que la palabra token posee múltiples acepciones, desde moneda a ficha e incluso cheque regalo. Tradicionalmente se ha utilizado para referirnos a fichas que se utilizan como moneda de cambio en eventos privados como por ejemplo conciertos. Asimismo en muchas ocasiones nos referimos a Bitcoin como token y confundimos un token con una criptomoneda. A medida que la tecnología criptográfica ha ido avanzando la distinción se ha hecho cada vez más clara y en este momento podemos considerar la siguiente bifurcación: (1) las criptomonedas, que incluye el Bitcoin y las Altcoins[5] cuya función es la de medio de pago y (2) los tokens o "criptovalores" que incorporan funciones adicionales.

La mayoría de altcoins son una variante de Bitcoin, construida utilizando código abierto de Bitcoin con algunos cambios. Pero también existen otras que han creado su propia cadena de bloques y sus propios protocolos generando una moneda nativa. Ejemplos de estas crtyptomonedas incluyen Ethereum, Litecoin, Dash, Ripple, Omni, Nxt, Waves y Counterparty. La minería de Bitcoin requiere un gran poder de cómputo, lo que implica altos costes para los mineros se dedican a esta tarea. El algoritmo creado para el Litecoin permite que casi cualquier sistema de cómputo pueda realizar minería, sin la necesidad de grandes inversiones en hardware. Por otro lado, la altcoin Dash incrementa el anonimato de quienes participan en la red y mejora la velocidad de las transacciones. Una diferencia más entre las diversas criptomonedas con relación a Bitcoin, en un ámbito ya no técnico, es el del propósito de la moneda digital. La altcoin Ripple surgió para servir como intermediario para toda transacción de unidades de valor, es decir, está diseñado para conectar diferentes sistemas de pago. El nicho al que apunta es al del cambio de divisas, un aspecto que el Bitcoin no integra.

Los tokens, por otro lado, son un activo o un valor que se asienta sobre una cadena de bloques determinada. En este caso, las plataformas más frecuentes son Ethereum[6] o Wave. Los tokens pueden representar básicamente cualquier activo que sea fungible y negociable: desde participaciones en proyectos empresariales hasta medios de pago. Un ejemplo de tokens son los Energy Efficiency Coins (EEcoin). Este es un caso que como

---

[5] Altcoins son monedas alternativas al Bitcoin
[6] Ver Ethereum White Paper https://github.com/ethereum/wiki/wiki/White-Paper

hemos mencionado anteriormente puede llevar a confusión. A pesar de que en su denominación aparece la palabra "coin", no hace referencia a una moneda sino a un token a través del cual se puede participar en un ecosistema blockchain de energías renovables votando y proponiendo nuevos proyectos. Los propietarios de tokens, tienen derecho a votar, y pueden comerciar con ellos, pero no tienen los derechos de un accionista, aunque pueda parecer equiparable[7]. La función más habitual de los tokens es la de recaudar fondos para proyectos específicos, algo que nos recuerda mucho más al crowdfunding que a las IPO. Sin embargo, en ocasiones se puede recompensar a los poseedores de tokens con participación en beneficios, o bien pueden utilizar estos tokens para comprar los productos y servicios de la organización.

Crear tokens es un proceso muy sencillo ya que no tiene que modificar los códigos de un protocolo en particular ni crear una cadena de bloques desde cero, todo lo que tiene que hacer es seguir una plantilla estándar en la plataforma blockchain. Esta simplicidad ha potenciado su uso entre las empresas que como explicaremos en secciones posteriores, los utilizan para campañas de fidelización o para recaudación de fondos a través de una oferta inicial de monedas o "Initial Coin Offering" (ICO).

---

3. Impacto en la Empresa

El camino hacia el futuro pasa por acoplar diferentes entidades productivas, la digitalización sustentada en las nuevas tecnologías y la posibilidad de democratizar no sólo la información sino también los activos de valor. La digitalización es la base de la llamada "Industria inteligente", llevada de la mano del IoT, (Internet de las Cosas), la comunicación Machine to Machine (M2M), el Cloud, Big Data, Machine learning, etc.

A todas estas tecnologías ahora se une la tecnología blockchain. Esta cadena de bloques proporciona a las empresas un nuevo universo de comunicación, de interacción y de confianza. La introducción de nuevas aplicaciones industriales requiere un grado

---

[7] El libro blanco de EECoin especifica "EECoin is not a security, future, or share, it is not a guarantee of ownership in a company or any underlying assets, or a claim against any consumer rights as guaranteed by EnLedger. The goal of this structure is to offer the public a way to participate in an energy-efficient blockchain network and to provide capital to renewable energy projects, increasing price competition for renewable energy assets and thereby enabling society to directly provide a market incentive for production of renewable forms of energy as opposed to nonrenewable ones."

creciente de seguridad y protección de la privacidad; la prueba de existencia o de origen y la trazabilidad ganan cada vez mayor importancia. Confiar en los registros temporales y la integridad de los datos puede ser un requisito crucial. Por ello Blockchain tiene el potencial de cambiar la forma en que la empresa digitalizada se aproxima al futuro, con una mayor seguridad y calidad en los datos.

Las principales ventajas de esta tecnología son:

- Intercambio sin intermediación de terceros: Es posible el intercambio de activos entre dos partes sin la supervisión de terceros, reduciendo riesgos considerablemente.
- Inviolabilidad: Blockchain puede resistir ataques maliciosos mejor, ya que carece de punto central débil, al utilizarse redes descentralizadas.
- Transparencia: Los datos bajo Blockchain están globalmente disponibles, son verificables y se transmiten en tiempo real.
- Control del usuario: Los usuarios pueden controlar todas sus transacciones e información.
- Inmutabilidad: Cada transacción es inmutable; no puede ser eliminada o modificada.
- Simplificación del sistema contable: Al añadir cada transacción a una simple contabilidad pública, reducimos la complejidad de múltiples contabilidades.
- Transacciones eficientes: Blockchain otorga mayor seguridad, rapidez y eficacia. Esta productividad hace que se reduzcan gastos generales y costes intermediarios innecesarios, al requerir menos seguimiento y control.

El impacto de esta aplicación tecnológica puede abarcar todas áreas de una empresa desde la contabilidad, pasando por la cadena de suministros, la innovación, la financiación e incluso la fidelización de clientes.

Contabilidad y auditoría

No sería la primera vez que una nueva forma de registrar transacciones cambia el mundo. En sus inicios la contabilidad se basaba en registros de una única entrada. Con el desarrollo del comercio este sistema resultó obsoleto. Alrededor del año 1400 en el norte de Italia surgió una nueva técnica de contabilidad, más tarde conocida como contabilidad de doble entrada. Fue un gran paso en el desarrollo de la empresa y la economía modernas. Este avance tecnológico permitió el acceso y el seguimiento de la

información financiera a toda parte interesada más allá del propietario. Puede parecer un hecho irrelevante, pero Werner Sombart, un sociólogo alemán que murió en 1941, argumentó que la doble entrada contable marcó el nacimiento del capitalismo. Después de 500 años sin grandes cambios la contabilidad vuelve a mostrarse obsoleta (The End of Accounting and the Path Forward for Investors and Managers, 2016).

El esperado cambio que la comunidad contable estaba esperando llega de la mano de esta revolucionaria tecnología. Si la doble entrada rescató a la información contable de la cabeza del comerciante, la cadena de bloques la libera de los confines de una organización. Por definición, Blockchain es un libro de registros distribuido, o en otras palabras un libro mayor distribuido (Distribuded Ledger Tecnology). El hecho de que la firma digital sea criptográfica le confiere al registro una poderosa fuerza probatoria y en la práctica elimina el problema contable de la veracidad o la existencia registral. Este problema se resuelve compartiendo los registros: cada uno de los nodos del sistema tiene una copia original. Lo que conduce a dos pares de entradas dobles conectadas por la lista central de recibos; tres entradas para cada transacción (Dai & Vasarhelyi, 2017).

El registro distribuido representa un enorme desafío para la contabilidad más allá de la triple entrada y la mayor visibilidad que este libro mayor distribuido proporciona (Ijiri, 1989). La capacidad de blockchain para registrar múltiple transacciones en tiempo real es increíblemente poderosa. A esto se le une la posibilidad de añadir contratos inteligentes para automatizar los procesos empresariales, como los de pagos y los seguimientos de control. Por ejemplo se podría emitir una orden de compra contra ese contrato, facturas contra esa orden de compra, pagos contra esas facturas, etc., rastreando cualquier problema que surja en el camino. Habría una identificación única relacionada con el contrato, la orden de compra o las facturas en esa cadena que uniría en único bloque informativo todas las piezas independientes.

Tener un libro de contabilidad que muestre fácilmente toda la cadena de transacciones relacionadas no solo proporcionaría excelentes registros de auditoría, sino que también permitiría a ambas partes de una transacción tener actualizaciones de estado en tiempo real. Cada vez que se actualiza el blockchain con un nuevo registro, ambas partes de la transacción pueden ver la actualización de inmediato.

Cadena de suministros o "supply chain"

Otro aspecto importante dentro del mundo empresarial y el comercio es la cadena de suministro. La escala y complejidad de estos procesos conduce a altos costes transaccionales, desajustes frecuentes y errores manuales. Las "cadenas de custodia" completas, que prueban los orígenes de cada producto o material, aún están fragmentadas en todas las organizaciones y son vulnerables al fraude y al error, incluso entre las empresas certificadas. Las aplicaciones basadas en Blockchain tienen el potencial de mejorar las cadenas de suministro al proporcionar infraestructura para registrar, certificar y rastrear a bajo costo los bienes transferidos entre partes distantes, que están conectadas a través de una cadena de suministro pero que no necesariamente confían entre sí. Todos los productos se identifican de forma única a través de registros transferidos desde su origen hasta su destino final a través de blockchain. Cada transacción es verificada y marcada con el tiempo en un proceso cifrado pero transparente dando visibilidad a las partes implicadas como proveedores, transportistas o compradores. Los términos de cada transacción permanecen irrevocables e inmutables, abiertos a inspección para todos o para los auditores autorizados. Aquí también los contratos inteligentes podrían implementarse para ejecutar automáticamente pagos y otros procedimientos. Existen ya empresas que utilizan esta tecnología en su cadena de suministros. Everledger permite a las empresas y compradores rastrear la procedencia de los diamantes desde las minas a las joyerías y combatir el fraude de seguros o documentación. La empresa social Provenance, ha desarrollado una plataforma de datos en tiempo real que reúne y verifica el origen de un activo asignándole un 'pasaporte digital' que puede rastrearse a lo largo de toda la cadena de suministro hasta que llega a su destino. El gigante Wal-Mart está probando Blockchain para la seguridad alimentaria. Se espera que un registro preciso y actualizado basado en Blockchain pueda ayudar a identificar el producto, el envío y el proveedor, por ejemplo cuando ocurre un brote, y de esta manera obtener detalles sobre cómo y dónde se cultivaron los alimentos y quién los inspeccionó.

Nuevas vías para los negocios

Muchas son las empresas que ven en las criptomonedas utilidades que van más allá del simple medio de pago. Chanticleer Holdings Inc., empresa matriz de varias franquicias de comida rápida en Estados Unidos (BGR, Little Big Burger y American Burger, Just Fresh y algunos restaurantes Hooters), utilizará la tecnología blockchain para implementar un programa de recompensas por lealtad para los clientes de sus cadenas

de comida. El cliente recibiría criptomonedas nativas llamadas Merits, las cuales podría intercambiar con otros clientes o utilizarlas para consumir sus productos y servicios. Transforma las recompensas tradicionales del consumidor en algo que el consumidor puede controlar.

Un inconveniente de este sistema de recompensas es su fragmentación y su segmentación que provoca ineficiencias y rigideces. Hemos de recordar que tanto las criptomonedas como los puntos de lealtad tradicionales suponen una deuda para las empresas y por lo tanto incrementan su pasivo. La solución a este problema pasa por sustituir los sistemas de lealtad privados por sistemas universales. Elements coin es una criptomoneda con base en código abierto aceptada por varias organizaciones y de uso universal. Este modelo, los Elements se pueden intercambiar por dinero fiduciario y por otras monedas digitales reduciendo así la deuda de las empresas e incrementando el control de los usuarios. Cabe destacar también que estos usuarios poseerán toda la información sobre sus transacciones y las organizaciones tendrán los datos de sus respectivas interacciones con los consumidores. El potencial de esta información en manos de las plataformas es inagotable.

Financiación

Es evidente que las empresas no han desaprovechado el potencial de las criptomonedas y lo han hecho desde diversos enfoques. Uno de los sectores donde las empresas han explotado más este potencial, es el sector financiero. Al margen de la euforia despertada por Bitcoin, y su gran boom especulativo, las empresas han visto en esta tecnología una nueva forma de financiación empresarial más flexible y veloz. Especialmente ahora que aún se encuentra poco regulada comparada con los medios de financiación convencionales.

La oferta inicial de monedas, también conocida como ICO (Initial Coin Offering) es un mecanismo de recaudación de fondos en el que los nuevos proyectos empresariales se financian a través de la venta de tokens criptográficos a cambio de dinero o moneda digital (Venegas, 2017). La creación de tokens es muy sencilla, se hace posible mediante el uso de plantillas en plataformas Blockchain como Ethereum y de contratos inteligentes autoejecutables que no que necesitan ningún tercero para operar. Los tokens se crean y distribuyen al público a través de una ICO para financiar el desarrollo de un proyecto específico.

Las ICO se han comparado con dos formas tradicionales de financiación: (1) las Ofertas Públicas Iniciales (IPO) en la que los inversores compran acciones de una empresa, y (2) el modelo crowdfunding donde, como en las ICO, la financiación está ligada a un proyecto determinado. En ambos casos las diferencias son significativas y muy ligadas a la regulación y a la protección del inversor.

La principal diferencia entre el modelo ICO e IPO es la supervisión regulatoria. En una IPO las empresas deben incluir un documento legal declarando su finalidad, además de cumplir ciertos estándares de transparencia. En segundo lugar, una empresa sólo puede emitir las acciones si cumple una serie de requisitos, como un mínimo de ganancias o un buen historial. Ninguna de estas dos condiciones es necesaria en las ICO. En tercer lugar, las acciones otorgan propiedad sobre las ganancias futuras de la empresa, los tokens no otorgan propiedad sobre el proyecto al que van ligados. Hay muchas formas en que los propietarios de tokens pueden obtener beneficios futuros, y eso depende de cómo esté estructurada la moneda. Algunas monedas generan valor al tener participación en los ingresos futuros de los proyectos, mientras que otras tienen el valor de su uso dentro del ecosistema; cuanto mayor sea el uso, mayor será su valor. Finalmente, la duración de la oferta es mayor en las IPO, y el acceso a los inversores es limitado, mientras que en las ICO está abierto a cualquier persona. Estas son importantes diferencias que un inversor debería tener en cuenta antes de adquirir tokens (ver Crypto ICO vs. Stock IPO: What is the difference? (2017).

Respecto a su comparación a crowdfunding es mucho más acertada. A pesar de que podríamos considerar las ICO como el crowdfunding 2.0, merece la pena tener en cuenta algunas diferencias. Cuando se introduce un producto en plataformas de crowdfunding como Indiegogo, los inversores y compradores saben exactamente qué esperar cuando el proyecto acabe. Por ejemplo, cuando el Tablero impulsado con monopatín eléctrico o el reloj inteligente Pebble iniciaron sus campañas de financiación colectiva, los inversores pudieron decir inmediatamente si el producto valía una cierta cantidad de dinero comparando los productos con otros en el mercado. Por el contrario, es prácticamente imposible predecir el resultado de una ICO, especialmente si los usuarios no entienden la operativa y las implicaciones de su inversión. Las ICO en sí mismas no se basan en ningún valor de mercado en el mundo real, lo que lo hace difícil su valoración. El "producto" asociado a este crowdfunding 2.0 es el token en sí mismo. La empresa a través de su buena gestión puede revalorizar los tokens y así proporcionar

plusvalías a su propietario en el mercado criptográfico. Del mismo modo, la mala gestión puede desplomar el valor del token a cero. Tampoco existe regulación que impida a la empresa desaparecer con todo el dinero recaudado[8]. Muchos son los que advierten de los peligros de invertir en tokens. A pesar de estas advertencias este mercado está creciendo exponencialmente. La razón es sencilla: a mayor riesgo, mayor beneficio (pero no olvidemos que también mayor pérdida). La simplicidad a la hora de generar los tokens así como la falta de regulación y las grandes expectativas de los inversores entorno a un fenómeno altamente asociado al Bitcoin ha ayudado a disparar la emisión de estas ICO. Algunos ven en ellas la oportunidad de recaudar una cantidad injustificada y posiblemente fraudulenta de capital, mientras que otros argumentan que es una innovación en el modelo tradicional de financiación de riesgo. Algunas de estas ICO han sido exitosas, pero otras han sido fraudulentas, o excesivamente opacas llevando a sus compradores a pérdidas millonarias (Zetzsche, Ross P. Buckley1, & Föhr, 2017).

La decisión de la SEC puede haber proporcionado cierta claridad sobre el estado de los tokens de utilidad versus seguridad; sin embargo, todavía hay trabajo por hacer en el ámbito legal. Por ahora, y hasta que se impongan límites legales adicionales, las empresas se continuarán aprovechando este nuevo fenómeno. En septiembre de 2017, China amenazó con declarar las ICO ilegales. El Banco Popular de China advirtió que castigaría estrictamente las nuevas ofertas y que penalizaría las infracciones legales de las ya finalizadas. El regulador ordenó a las empresas devolver la recaudación, aunque no especificó cómo se les retornaría el dinero a los inversionistas.

4. Nuevas formas de organización: las DAO

DAO es el acrónimo en inglés de Organización Autónoma Descentralizada, que es un nuevo tipo de organización, que podría ser comparable con una sociedad digital, pero sin ningún tipo de entidad legal adscrita. Fue propuesta originariamente por Vitalik Buterin en (2014), quien luego pasaría a ser el cofundador de Ethereum. Esta organización está creada con código informático, es decir, es una entidad que sólo existe en el blockchain y que además está controlada directamente por los propietarios

[8] La mayoría de las ICOs se ejecutan con un descargo de responsabilidad que no garantiza el retorno a los inversores, si el precio del token asociado cae a cero por negligencia o acciones maliciosas del equipo de desarrollo, es probable que no haya mucho recurso legal al que acudir.

(poseedores de tokens), sin necesidad de que exista una dirección centralizada (Jentzsch, 2017). La DAO es en sí misma un contrato inteligente complejo basado en código fuente autónomo, que automatiza todas las funciones dentro de una organización, y sus directrices sólo pueden modificarse si un tanto por ciento de los miembros están de acuerdo. Además, lleva consigo una participación comunitaria, de tal forma que no son únicamente los (inexistentes) directores los que tienen poder de decisión, sino que toda la comunidad en posesión de tokens participa en las votaciones o introducen propuestas para ser votadas (Venegas, 2017).

El operativo funciona de la siguiente manera. Los desarrolladores de código escriben los contratos inteligentes que ejecutará la organización. Hay un período de financiación inicial, en el que los inversores agregan fondos al DAO mediante la compra de tokens que representan la "propiedad": esto se denomina crowdsale, o una oferta inicial de monedas (ICO). Cuando finaliza el período de financiación, la DAO comienza a funcionar. Los titulares de tokens pueden hacer propuestas sobre cómo invertir los fondos y votar para aprobar o denegar propuestas. Los requisitos para participar en un DAO son escasos, pueden reducirse a tener conexión a internet. A pesar de que algunos países, como EE. UU. protegen fuertemente a los inversores y obligan a los compradores de tokens a cumplir ciertos requisitos, la mayoría de los países no disponen de esta protección. Las DAO carecen de directores o empleados, y no tienen un objetivo empresarial específico. La simplicidad en las decisiones, el anonimato, la seguridad y la reducción de costes son sus grandes pilares. Los defensores de este tipo de organizaciones alegan que fomentan la innovación y la profesionalidad al basar las decisiones en el valor de los proyectos y no el interés personal de los individuos y sus luchas de poder.

Algunos ejemplos de DAO son SuperDAO o Solar DAO (Solodukha, 2017). El proyecto SuperDAO tiene como objetivo crear productos y servicios disruptivos a través de la cooperación virtual de innovadores sin limitaciones geográficas a través de software de código abierto. Solar DAO por el contrario tiene un objetivo específico. Opera como un fondo de inversión para construir plantas solares fotovoltaicas. Vende tokens a los usuarios, los cuales pueden mantenerlos para obtener dividendos[9] o pueden

[9] Solar DAO white paper: 'Solar DAOtoken ownership will allow users to: 1. Invest in solar plants worldwide efficiently by circumventing issues related to ownership, audits and selection of contractors 2. Take part in PV plant construction, starting from as low as $1 3. Own assets (tokens) safely and

comerciar con ellos en los mercados criptográficos. A través de los contratos inteligentes los pagos se hacen automáticos sin revelar la identidad del propietario del token.

5. Conclusiones y debate

Es innegable que el año 2017 ha sido el año de las criptomonedas, especialmente del Bitcoin y parece probable que en los próximos sean los años del Blockchain. Hasta el momento, muchas son las compañías que se han revalorizado al incluir alguna innovación relacionada con blockchain o con criptomonedas. Por ejemplo, las acciones de la empresa Chanticleer se dispararon un 50% tras el anuncio de su programa de recompensas con blockchain, y su capitalización de mercado se elevó de 8 millones a 12 millones de dólares. Recientemente, las acciones de Long Island Iced Tea (una compañía fabricante de té helado) se revalorizaron más de 500% después de haber cambiado su nombre a Long Blockchain Corp. Algo semejante experimentaron algunas compañías de Israel dedicadas a la minería de metales preciosos, energía solar, y tabaco respectivamente, luego de haber anunciado su integración al ecosistema blockchain.

Sin embargo, hay razones para ser cauteloso. La confianza entre los participantes depende de la confianza en la tecnología blockchain, pero esto no está completamente libre de vulnerabilidades, incluidos los errores accidentales y los ataques maliciosos en las aplicaciones que se asientan sobre la cadena de bloques. La automatización tampoco eliminará los conflictos de interés o la corrupción. A pesar de que los defensores y de Blockchain promulgan su inviolabilidad, nadie está exento de fallos. La primera iniciativa de DAO promulgada por Ethereum recibió un duro golpe al ser víctima del robo de más de 150.000 ethers, 30 millones de dólares (ver https://www.coindesk.com/understanding-dao-hack-journalists) y dio origen a un gran debate ideológico que dividió a la comunidad Ethereum en dos. En un lado se situaron los defensores de aceptar el robo y no hacer nada cumpliendo así con las directrices originarias de inmutabilidad del código (“code is law”). Por otro lado lo hicieron los defensores de retrotraer la cadena hasta el bloque previo a la función que permitió la sustracción. Es importante remarcar que el error de codificación estaba en la DAO y no

---

anonymously 4. Receive dividends from the investments made and profit from the value increase of tokens 5. Sell tokens on the exchange market as needed

en la cadena de bloques subyacente. Sin embargo, muchos pueden argumentar que esta diferencia no afecta el hecho de que la aclamada inviolabilidad queda totalmente en entredicho. Finalmente, los fundadores y otros colaboradores de Etherum decidieron retrotraer el código, dando lugar a dos cadenas de bloques paralelas (ver Figura 4). Las dos cadenas persistieron. La cadena que conservó las normas antiguas, se bautizó como Ethereum Classic[10] (ETC), y la nueva cadena que se creó a partir de la retroacción se llamó simplemente Ethereum (ETH).

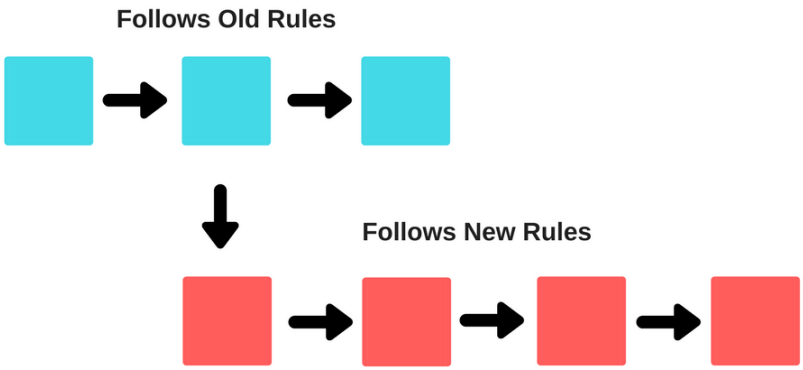


Figura 3. Escisión de la plataforma: Ethereum (rojo) y Ethereum Classic (azul)

Esta decisión también ataca otro de los pilares fundamentales de blockchain, la inmutabilidad del código. Si bien no es posible para los hackers modificar el código ya que no pueden acceder a todos los nodos simultáneamente, parece que es posible para las plataformas alterar la cadena.

Desde un enfoque más conceptual, aquellos que ven en la tecnología una forma de democratizar la creación de valor eliminando a los intermediarios junto con sus abusos e imperfecciones pueden verse decepcionados. Una primera tentativa fue la economía colaborativa, desgraciadamente este ecosistema está empezando a mostrar señales de fracaso en su objetivo inicial. En lugar de eliminar o reducir intermediarios oligopolistas, éstos están siendo substituidos por gigantes como Uber, que no necesariamente mejoran la situación inicial. Blockchain, para muchos puede ser

[10] En el libro blanco de Ethereum Classic se lee: "Ethereum 'Classic' is the original unmolested Ethereum block chain of the Ethereum platform. We believe in decentralized, censorship-resistant, permissionless blockchains. We believe in the original vision of Ethereum as a world computer you can't shut down, running irreversible smart contracts. We believe in a strong separation of concerns, where system forks are only possible in order to correct actual platform bugs, not to bail out failed contracts and special interests. We believe in censorship-resistant platform that can be actually trusted - by anyone."

finalmente la solución a este problema. Un sistema no sólo descentralizado, sino distribuido, en el que los intermediarios ya no son necesarios y las reglas del juego no vienen marcadas por la decisión arbitraria de un organismo interesado. La idea es válida, pero quien nos garantiza que esta opción no va a presentar los mismos errores que su predecesora. Los bancos han sido el primer objetivo de este plan de desintermediación, iniciado a partir de la crisis financiera de 2007-2008[11]. Como reacción, este sector está utilizando la propia tecnología blockchain para perpetuar su dominio en las transacciones financieras. Fintech es la forma en que se denomina a la tecnología aplicada a las finanzas. En agosto de 2017, por ejemplo, Barclays, Credit Suisse, Banco Imperial Canadiense de Comercio (CIBC), HSBC, Banco MUFG y State Street Bank, seis de las mayores entidades financieras del mundo, se unieron para crear una moneda digital basada en la tecnología blockchain. La resistencia no sólo se produce en el sector financiero. Plataformas como Hyperledger crean cadenas privadas adaptadas a las necesidades de las organizaciones y no al contrario. Redes cerradas, con permisos y controladas por un grupo de participantes que no difieren en gran medida del actual concepto de intermediación.

Por otro lado, si bien Blockchain promete un mundo en el que los intermediarios que conocemos no son necesarios, aún pueden ser posibles. Por ejemplo, a partir de la creación de internet las agencias de viajes no eran necesarias. Cualquiera puede reservar vuelos, hoteles y viaje completos sin necesidad de ellas pero esto no implica que desaparezcan. El hecho de que podamos hacer un contrato directamente no implica que tengamos los conocimientos o el tiempo necesario para llevarlo a cabo. Estos costes incentivan el uso de intermediarios a pesar de no ser necesarios. Incluso en el supuesto de eliminar antiguos intermediaros, estos probablemente serían sustituidos por nuevos. Un posible candidato serían las plataformas blockchain, como Ethereum o Hyperledger que al igual que Uber en la economía colaborativa, no necesariamente mejorarían la situación.

Como reflexión final cabe remarcar el hecho de que a pesar de que blockchain no consiga revolucionar la economía y la sociedad, es indudable que tendrá un impacto sustancial en muchas áreas y es necesario estar preparados para los desafíos y oportunidades que presenta.

---

[11] Satoshi Nakamoto lanzó su "Bitcoin paper" en 2009, tras la crisis financiera de 2007-2008

Bibliografía

Aziz. (2017). Crypto ICO vs. Stock IPO: What's the Difference? *Available at https://masterthecrypto.com/crypto-ico-vs-stock-ipo/.*

Buterin, V. (2014). *A Next Generation Smart Contract & Decentralized Application Platform (White Paper).* http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems, 31*(3), 5-21.

Dispenza, J., Garcia, C., & Molecke, R. (2017). Energy Efficiency Coin (EECoin) A Blockchain Asset Class Pegged to Renewable Energy Markets. *Available at https://www.enledger.io/Energy_Efficiency_Coin_Whitepaper_v1_0.pdf.*

Ijiri, Y. (1989). Momentum accounting and triple-entry bookkeeping : exploring the dynamic structure of accounting measurements. *American Accounting Association* .

Jentzsch, C. (2017). *Decentralized Autonomous Organization to Automate Governance.* file:///C:/Users/LUZ/Downloads/WhitePaper%202.pdf.

Lev, B., & Gu, F. (2016). *The End of Accounting and the Path Forward for Investors and Managers.* ISBN: 978-1-119-19109-4.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper*.

Pass, R., & Shi, E. (sense data). Hybrid consensus: Efficient consensus in the Permissionless Model. *DOI: 10.4230/LIPIcs.DISC.2017.39 URL: http://drops.dagstuhl.de/opus/volltexte/2017/8004/*.

Solodukha, D. (2017). *Solar DAO (White Paper).* https://solardao.me/files/wpeng.pdf.

Venegas, P. (2017). Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Markets . *Available at SSRN: https://ssrn.com/abstract=3012238*.

Zetzsche, D. A., Ross P. Buckley1, D. W., & Föhr, L. (2017). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. . *University of Luxembourg Law Working Paper No. 11/2017; UNSW Law Resear*.