UNIVERSIDAD DE CANTABRIA

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

CURSO ACADÉMICO 2020-2021

TRABAJO FIN DE GRADO

Mención en finanzas

Initial Coin Offerings: Análisis de Blockchain y estrategia de financiación basada en emisión de tokens

Initial Coin Offerings: Blockchain analysis and financing strategy based on token issuance

AUTOR: WALTER ALEJANDRO ESPINOZA VARGAS

DIRECTORA: PATRICIA CERECEDO SANDOVAL

SANTANDER, 2 DE DICIEMBRE DE 2020

INITIAL COIN OFFERINGS: ANÁLISIS DE BLOCKCHAIN Y ESTRATEGIA DE FINANCIACIÓN BASADA EN EMISIÓN DE TOKENS

Índice de contenidos

RESUMEN

En 2009 se creó la primera Blockchain, una tecnología de red descentralizada para el intercambio de datos virtuales. Fue creada bajo el proyecto Bitcoin, la primera moneda virtual descentralizada. En los siguientes años comenzaron a asentarse y desarrollarse otras plataformas como Ethereum y la posibilidad de diseñar programas automatizados dentro como los Smart Contracts. La emisión de tokens o criptomonedas, también llamadas ICO (Initial Coin Offering), aparecieron de la proliferación de nuevos proyectos como forma de poder financiarlos. Actualmente existen miles de iniciativas relacionadas al Blockchain moviendo grandes sumas de dinero. A pesar de esto, existe cierto desconocimiento de los aspectos técnicas que la conforman. Así como incertidumbre con respecto a aquellos proyectos fuertemente relacionados. Con este trabajo se busca estudiar sus bases fundamentales y otros aspectos clave de la revolucionaria tecnología. Además de analizar los riesgos y métodos de la emisión de tokens de cara a una startup o PYME.

El trabajo se estructura en tres partes: las fuentes de financiación tradicional, el nuevo ecosistema de Blockchain y la emisión de tokens (ICO). La primera mostrando los métodos de financiación más recurrentes actualmente. La segunda se centra en profundidad en las características y clasificaciones de las propias Blockchains. Incluyendo las DAO, organizaciones descentralizadas que operan a través de Smart Contracts y cuyas decisiones son tomadas por consenso. La última está dedicada específicamente a las ICO. Mostrando su funcionamiento como método de financiación de proyectos, así como sus semejanzas a otras vías ya existentes como el Crowdfunding o las Ofertas Públicas de Venta. La problemática que acarrea determinar su valor, tanto si hablamos del proyecto en sí como de los tokens que lo respaldan. El riesgo y las ventajas existentes desde la óptica de la inversión, como son las posibles estafas o la escasa regulación. Finalmente se incluirá las consideraciones de la legislación española respecto a ICOs.

In 2009 the first Blockchain was created, a decentralized network technology for the exchange of virtual data. It was created under the Bitcoin project, the first decentralized virtual currency. For the following years, other platforms such as Ethereum and the possibility of designing automated programs such as Smart Contracts began to settle and develop. The issuance of tokens or cryptocurrencies, also called ICOs (Initial Coin Offering), appeared from the proliferation of new projects to finance them. Currently there are thousands of initiatives related to Blockchain moving large sums of money. Despite this, there is some ignorance of the technical aspects that make it up. As well as uncertainty regarding those strongly related projects. This work seeks to study its fundamental bases and other key aspects of the revolutionary technology. In addition to analyzing the risks and methods of issuing tokens for a startup or SME.

The work is structured in three parts: traditional financing sources, the new Blockchain ecosystem and the issuance of tokens or ICOs. The first showing the most recurring financing methods today. The second focuses in depth on the characteristics and classifications of the Blockchains themselves. Including DAOs, decentralized organizations that operate through Smart Contracts and whose decisions are made by consensus. The last one is dedicated specifically to ICOs. Showing its operation as a method of financing projects, as well as its similarities to other existing channels such as Crowdfunding or Initial Public Offering. The problems involved in determining its value, whether we talk about the project itself or the tokens that support it. The existing risks and advantages from the investment perspective, such as possible scams or poor

regulation. Finally, the considerations of the Spanish legislation regarding ICOs will be included.

LISTA DE ABREVIATURAS

DAICO	Decentralized Autonomous Initial Coin Offering
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technologies
EVM	Ethereum Virtual Machine
ICO	Initial Coin Offerings
P2P	Peer-to-Peer
SEC	U.S. Securities and Exchange Commission

INITIAL COIN OFFERINGS: ANÁLISIS DE BLOCKCHAIN Y ESTRATEGIA DE FINANCIACIÓN BASADA EN EMISIÓN DE TOKENS

INTRODUCCIÓN

Internet ha permitido varios cambios en nuestra sociedad y las empresas no iban a quedarse atrás. Recientemente han aparecido nuevas oportunidades relacionadas con este nuevo mundo digital que resultan atractivas tanto a emprendedores como a empresas. En 2009 se puso en marcha la primera moneda virtual descentralizada, así nacía Bitcoin. En aquel momento también nace Blockchain, tecnología con un gran potencial. Desde la trazabilidad de productos hasta la validación de todo tipo de información. Y como no podía faltar, también como nueva vía de financiación.

El objeto de este trabajo es entender mejor este nuevo ecosistema. Y para ello hay que entender a mayor profundidad que opciones se tiene actualmente para obtener recursos, el funcionamiento de una red Blockchain y de las Initial Coin Offerings o emisión de tokens. Estructuraremos la información en tres partes. El primero nos centraremos exclusivamente en las fuentes de financiación más comunes. El segundo se dedicará específicamente a la tecnología Blockchain, indagando en la historia y el funcionamiento de estas plataformas. En el último profundizaremos en las ICO, tanto en su origen como en la problemática legal y poder estimar su perspectiva de cara al futuro.

1. FINANCIACIÓN TRADICIONAL

Para cualquier actividad empresarial se deberá disponer de recursos suficientes que puedan llevarla a cabo. Las fuentes de financiación permiten el acceso a estos recursos, garantizando la supervivencia y continuidad de las empresas. Por ello resulta conveniente detallar las diversas fuentes de financiación o liquidez que una empresa puede aprovechar, así como sus características propias (Pérez del Barrio 2012).

1.1. FINANCIACIÓN BANCARIA

1.1.1. FINANCIACIÓN A CORTO PLAZO

Crédito: Una entidad financiera facilita fondos con un límite determinado. Es común su utilización para cubrir desfaces puntuales en la tesorería o en la movilización de créditos comerciales. Es proclive a exigir garantías adicionales y comisiones relativamente altas.

Crédito comercial: El aplazamiento en la exigencia de pago que una empresa concede, por lo general en transacciones comerciales, a sus clientes. Este desfase de tiempo en el desembolso agiliza las operaciones comerciales y ajustes en tesorería, por lo que tiene un carácter más espontaneo. Se diferencian dos tipos, los procedentes de proveedores u acreedores y los proveedores de administraciones públicas.

Descuento comercial: La empresa cede a una entidad financiera sus créditos comerciales a clientes no vencidos, deduciéndose el interés correspondiente. La entidad se encargará del cobro al librado.

Factoring: Se cede la cartera de clientes pendientes de cobrar a una sociedad externa, también denominada factor, quien gestionará dicho cobro. Se podrá solicitar el anticipo del total o de parte del monto al factor. Esta operativa estará sujeta a comisiones e intereses derivados de los importes anticipados. Puede contratarse con recurso o sin

recurso, donde el riego inherente permanece en la empresa o se traslada a la empresa externa respectivamente.

Confirming: Se subcontrata a una entidad financiera para la gestión del pago a proveedores. Se acuerda un límite al crédito en dicha concesión del que los proveedores podrán cobrar anticipadamente deudas pendientes a cargo de la empresa.

1.1.2. FINANCIACIÓN A LARGO PLAZO

Préstamo: Una entidad financiera presta una cantidad de dinero establecida durante un periodo de tiempo determinado y a cambio de un interés estipulado. Puede haber diferenciación por el tipo de interés, las garantías exigidas u otras condiciones.

Leasing: Arrendamiento financiero donde una entidad financiera, adquirente de un determinado bien en las condiciones establecidas por el cliente, se arrienda mediante una cuota que comprende parte del capital, los intereses y el IVA. Se clasifica como leasing financiero u operativo si existe obligatoriedad o no de ejercer opción de compra respectivamente.

Renting: Arrendamiento operativo donde el propietario de un determinado bien, mueble o inmueble, cede los derechos de uso al contratante a cambio de una cuota fija. Esta puede incluir el mantenimiento necesario por un periodo de tiempo determinado.

1.2. SISTEMAS ALTERNATIVOS DE FINANCIACIÓN

Capital semilla público: Entidades públicas invierten en empresas en fase inicial o de creación para ayudarlas en estas etapas. En general, se pretende la reactivación de ciertos sectores particularmente relevantes.

Sociedades de garantía recíproca: Sociedades mercantiles que tienen como objetivo otorgar garantías personales a sus socios en aquellas operaciones financieras que realicen con entidades de crédito. El criterio de avalar un proyecto empresarial estará fuertemente influenciado por la viabilidad de este. Gran parte de los socios son PYMES que únicamente responden al capital aportado, además de prestarse asistencia y asesoramiento.

Sociedades de capital riesgo: Sociedades que invierten de forma temporal sus propios recursos en pequeñas y medianas empresas con expectativas de crecimiento. Durante ese periodo de tiempo las apoyan de forma más activa, normalmente en forma de asesoramiento. Generalmente no intervienen en la gestión operativa o el control de la empresa.

Business Angels: Particulares que aportan capital a empresas en crecimiento o recién formándose. Existen redes de Business Angels donde la confianza es crucial para la selección de buenos proyectos. Dichas redes se enfocan en dos sentidos básicos, la oferta y la demanda de capital. Esto resulta interesante de cara al emprendedor por la oportunidad de presentar su proyecto a posibles inversores interesados, además de recibir asesoramiento especifico y facilitándole contactos.

2. IRRUPCIÓN DE LAS DISTRIBUTED LEDGER TECHNOLOGIES

Las Distributed Ledger Technologies o DLT hace referencia a toda tecnología que permite el registro compartido y replicado de datos digitales, pudiendo estar simultáneamente distribuidos en distintos puntos geográficos, países e instituciones. Se crea pues una red entre iguales para la transmisión de información, no siendo necesaria una figura que la centralice.

Esta categoría englobaría las Blockchains, siendo redes que registran información en cada usuario que las conforman de forma paralela. Confiriendo seguridad al poseer mismas copias en cada nodo (usuario) de la red, reduciendo la probabilidad de falsificación.

2.1. BLOCKCHAIN

“Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for the model transactions, it still suffers from inherent weakness of trust-based model. […] What is needed is an electronic payment based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”

(Nakamoto 2008)

2.1.1. ORIGEN: NACIMIENTO DE BITCOIN

En noviembre del 2008 se publicó un informe en el dominio bitcoin.org con el título “Bitcoin: A Peer-to-Peer Electronic Cash System” y bajo la autoría de Satoshi Nakamoto. Un seudónimo de la persona o equipo creador de Bitcoin, la primera criptomoneda con base en las DLT.

Fue durante los comienzos de la crisis financiera del 2008, tras las medidas gubernamentales por salvar a grandes corporaciones, donde nace Bitcoin. Las políticas adoptadas del “too big to fail” destinaban recursos hacia entidades financieras afectadas por la crisis. Afectando gravemente la confianza en instituciones y bancos centrales, augurando inestabilidad en el sistema financiero (Padilla 2020).

El primer bloque de la cadena (Genesis Block) se generó a principios del 2009. Se incluyó una cita del diario The Times que referenciaba los rescates bancarios transcurridos en aquel periodo.

“The Times 03/Jan/2009 Chancellor on brink of second bailout for Banks”

La idea tras bitcoin era la creación de una moneda virtual que operase a través de una base de datos descentralizada que conformase una red criptográfica en un paralelismo a un libro de asientos contables, donde el registro de entradas o salidas producidas son las transacciones realizadas.

Las bases de Bitcoin, así como Blockchain, no eran nuevos en el momento de su creación. Inspiraciones como B-money o el sistema antispamming de HashCash ya habían creado sistemas de pago y seguridad previamente. Aunque mayor peso tuvo Real Proof of Work (Finney 2004), siendo el mecanismo de consenso que regiría Bitcoin.

Otras figuras relevantes fueron Nick Szabo o Vitalik Buterin, denominados a sí mismos como Cypherpunks.

El movimiento anarcocapitalista tecnológico que defendía la privacidad y el anonimato en la red ante la centralización de la información, conocido como Cypherpunk, tuvo fuerte influencia en la propuesta de Nakamoto.

A diferencia de redes que operaban a través de un sistema cliente-servidor, la red de Bitcoin funciona por los propios usuarios a través de un sistema Peer-to-Peer o P2P. Facilitando el registro gracias a la descentralización de la información almacenada. La verificación de dicha información se consigue mediante el consenso entre usuarios. El mecanismo de consenso Proof-of-Work consiste en nodos computarizados en la red de Bitcoin, comúnmente llamados mineros, que validan nuevos bloques de información a través de la resolución de una prueba criptográfica que determina la recompensa y el tiempo medio para resolverlo. Actualmente, la expansión de la red de Bitcoin ha hecho que se requiera una gran cantidad de tiempo y poder computacional para llegar a esta respuesta (Champagne 2014).

2.1.2. ARQUITECTURA: LAS BASES DEL BLOCKCHAIN

Las bases conceptuales que conforman Blockchain se han mantenido para cada nueva generación de estas: (Champagne 2014)

Libro mayor o Ledger: Semejante a la contabilidad de carácter público y el funcionamiento de asientos contables, donde las operaciones o transacciones realizadas son registradas en bloques de la cadena. Para ello debe existir un emisor, un receptor y el activo intercambiado, siendo tokens o criptomonedas. La variación en sus saldos, así como la cantidad intercambiada, quedará guardada e inmutable.

Algoritmo criptográfico: La red Blockchain opera bajo un sistema de cifrado asimétrico que crea dos tipos de claves, una pública y otra privada. Las claves privadas dirigen el cifrado de información, de ellas se derivan sus correspondientes claves públicas. Mientras, las claves publicas controlan el descifrado puesto que es computacionalmente inviable su desencriptación sin utilizar su respectiva clave privada.

Hash criptográfico: Complejo algoritmo que transforma texto en una combinación alfanumérica aleatoria. Cualquier mínimo cambio en el texto original generaría un hash completamente diferente, imposibilitando la manipulación en cualquier punto de la cadena de información. De igual forma es aprovechado por el cifrado asimétrica para la creación de claves, volviendo inviable falsificar o duplicar claves privadas y sus correspondientes claves públicas.

Red distribuida de nodos: La unión de varios sistemas con capacidad computacional, como ordenadores o servidores. Se encargarán de la contabilización, regulación y autorización de las transacciones u operaciones realizadas, siendo necesario superar una prueba de consenso para poder incluirlas como un nuevo bloque de la cadena. Generalmente teniendo que acertar aleatoriamente el valor hash del bloque predecesor, volviendo complejo su resolución. Por ende, se necesitaría la capacidad computacional de más de la mitad de la red para llegar a falsear las transacciones. Dependiendo del tamaño de la red puede ser prácticamente imposible.

Las redes Blockchain poseen ciertas características comunes, aunque podrán ser ajustadas según la intensión y objetivo de los programadores. Estas características serian: (Vilar 2020)

Descentralización: El desarrollo de redes P2P permite trasladar la confianza que antes recaía sobre terceros a la misma tecnología (Zheng 2018). El sistema tradicional cliente-servidor obliga a centralizar acuerdos y transacciones para poder validarlos, lo que termina por incurrir en riesgos de seguridad, manipulación de datos y otros costes derivados de la ineficiencia. Tener una red descentralizada permite obviar estos problemas volviendo la intermediación de una organización o industria innecesaria, y resultando en un ahorro económico y de tiempo.

Inmutabilidad: La estructura de cadena de bloques no permite la alteración de la información, siendo altamente improbable. Haciendo que cada bloque sea único y representativo de la realidad de las transacciones que la conforman. A medida que se van incorporando bloques a la cadena disminuye exponencialmente posibles prácticas fraudulentas, además de fortalecerse ante desviaciones en la cadena principal (Folk). Mejor ejemplificado en una distribución de Poisson que pierde consistencia de forma geométrica a medida que aumentan los nodos de la red (Nakamoto 2008).

Anonimidad: El método común con respecto a la privacidad es limitar la información a aquellas partes implicadas o terceros de confianza. Difiere de la conseguida por Blockchain en donde la información reside en una firma pública encriptada a la que solo pueden acceder aquellos que posean la firma privada. Esta configuración limita el poder alcanzar una privacidad total, estando vinculada la firma pública a una dirección de cartera, pero no a una persona. Comparativamente hablando es similar a como funciona la bolsa de valores, donde son hechos públicos el tiempo y tamaño de las operaciones, pero no la identidad de quienes operan.

Verificabilidad: Las transacciones realizadas son validadas con un sellado de tiempo (Timestamp). Detallando el momento en que se validó y las partes involucradas, y emitiendo públicamente un nuevo hash. Se incluye dentro del nuevo hash el Timestamp del anterior, encadenando y reforzando así las transacciones anteriores.

2.1.3. TRANSACCIONES

El Problema del Doble Gasto plantea el riesgo de que un único usuario intercambie continuamente un mismo recurso. Esto implicaría, como solución, evitar que dicho recurso pueda ser duplicado. Para conseguirlo sin que los participantes cedan parte de la confianza a terceros se propone que las transacciones se anuncien públicamente en un sistema con un historial, y un orden temporal, que permita su trazabilidad (Castellanos 2017).

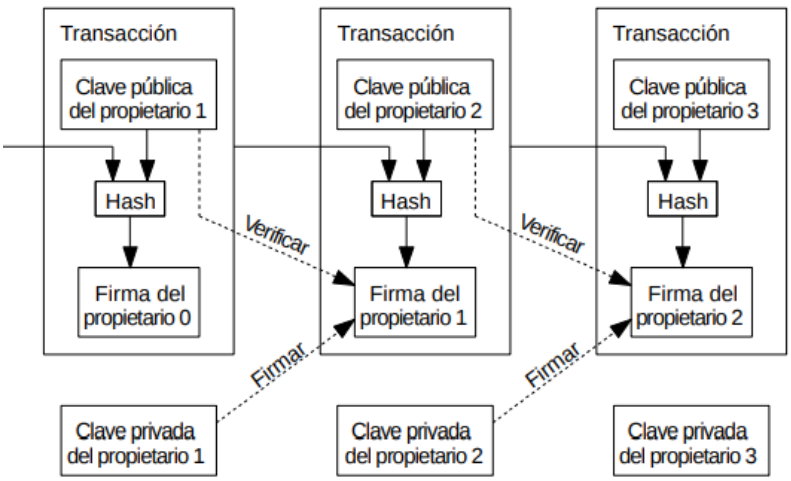

Imagen 2.1: Cadena de firmas digitales

(Fuente: Satoshi Nakamoto para Whitepaper de Bitcoin)

El funcionamiento de una red Blockchain es, como su nombre indica, a través de una estructura en cadena de bloques. Esto significa que cada bloque, y su información interna, se enlazará a los bloques anteriores por medio de valores hash hasta llegar al primer bloque o Genesis Block (Nakamoto 2008). Esto genera, además, un registro temporal donde es fácilmente comprobable la integridad de cada bloque. Dependiendo del Blockchain dicha información será el intercambio de activos, criptomonedas o la realización de contratos ejecutables automáticamente (Smart Contracts).

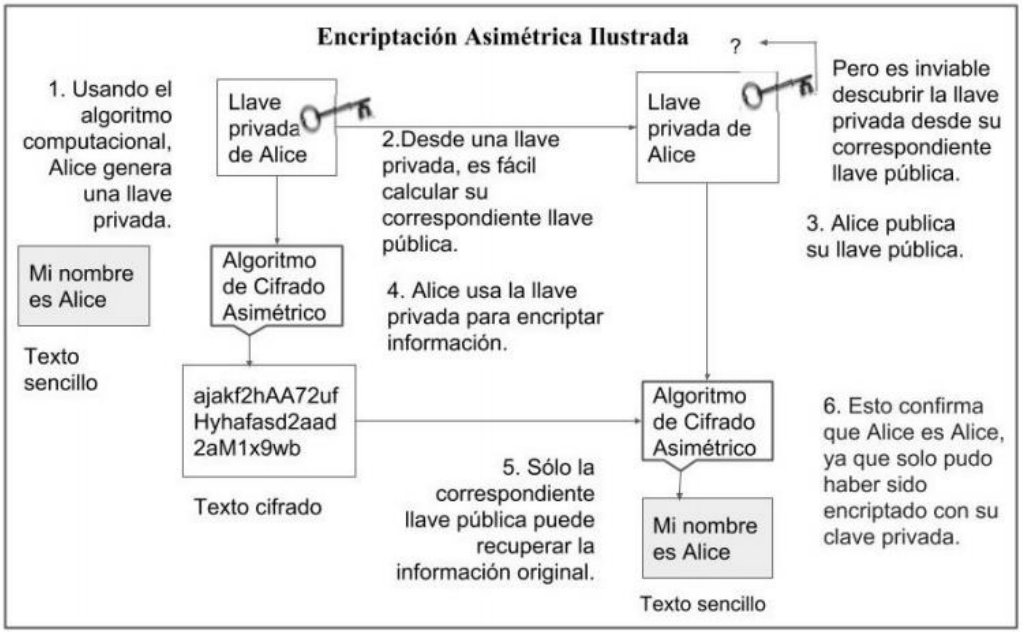

Imagen 2.2: Encriptación Asimétrica Ilustrada

(Fuente: Phil Champagne para “El Libro de Satoshi: La colección de escritos del creador de Bitcoin Satoshi Nakamoto”)

Se puede describir también a una Blockchain como una cadena de firmas digitales, donde el cifrado asimétrico permite al usuario generar una llave privada y otra pública. La llave privada del emisor firmará el hash del bloque previo y la llave pública del destinatario, encriptando la información transmitida. El receptor podrá desencriptarlo con su llave pública, generando de paso un nuevo hash al bloque incluido. El valor del nuevo hash coincidirá con el conseguido por uno de los nodos tras realizar la prueba de consenso, validando el traspaso de información en la red Blockchain.

2.1.4. CLASIFICACIÓN Y REDES P2P

El funcionamiento particular de cada red Blockchain permite distinguir dos grandes grupos con claras diferencias entre sí: (Padilla 2020)

Blockchain permissionless o **públicas:** Aquellas de acceso libre y abierto a quien desee pertenecer o mantener el Ledger, ejemplo de ellas son Bitcoin o Ethereum. Son la expresión más pura del concepto de Blockchain al ser accesibles, distribuidas, descentralizadas y parcialmente anónimas. Cualquier individuo puede formar parte de la red sin necesidad de solicitar permiso o revelar su identidad y marcharse de igual forma, lo que entraña ciertos riegos. La probabilidad de nodos maliciosos dentro de la red aumenta, además de propiciar actividades ilícitas como lavado de capitales o financiación de actividades criminales.

Blockchain permissioned o **privadas:** Delimitan el número de nodos participantes dentro de la red, quienes se encargarán de validar los cambios en el Ledger. El acceso y la permisibilidad a ellas estará regido por una autoridad centralizada, aunque de quererse se podría seguir manteniendo el anonimato parcial. Esto permite reducir los riesgos operacionales asociados a las Blockchain públicas, puesto que un sistema cerrado dificultaría la existencia de nodos maliciosos u otras actividades indeseables. El limitado número de participantes reduce el tiempo de validación, al ser menos los nodos que deban llegar a un consenso, mejorando así la eficiencia en las operaciones.

Existen otro tipo, **Blockchain hibrida** o **de consorcio.** Mantienen el Ledger abierto o semiabierto, siendo visible las operaciones de la red, unido a la existencia de nodos previamente seleccionados. Se pretende de esta forma aprovechar los beneficios de seguridad y eficiencia de ambos sistemas.

La arquitectura cliente-servidor es un modelo de software donde se separan responsabilidades entre clientes y servidores. Los servidores centralizarían información o recursos, poniéndolo a disposición de cualquier usuario que lo demandase. Contrariamente, las redes Peer-to-Peer o P2P dividen la carga de trabajo entre los integrantes de la red, compartiendo información y recursos a la vez que colaboran ante tareas específicas. Aunque esta definición dependerá del tipo de red P2P y sus diferentes clasificaciones.

Las redes P2P presentan varias ventajas estructurales que destacarían en el intercambio de archivos o almacenamiento de información, pilares básicos de la tecnología Blockchain. Destaca su escalabilidad puesto que cuantos más nodos conformen la red más recursos se podrán destinar a ejecutar operaciones, teniendo mayor tolerancia a fallos. Distinto de las redes cliente-servidor donde más individuos implica un menor rendimiento. También sobresale su robustez al no centralizar la operabilidad, evitando que exista un único punto de falla que pueda afectar a toda la red (Cardozo y Perdomo 2020).

2.1.5. MECANISMOS DE CONSENSO

El Problema de los Generales Bizantinos, es un planteamiento metafórico sobre un conjunto de sistemas informáticos en una estructura jerárquica y con objetivos comunes. Esta problemática ilustra el desafío que resulta la comunicación entre sistemas en un ambiente de desconfianza, donde uno o varios de ellos puedan estar proporcionando información falsa intencionadamente.

La confianza es una pieza clave dentro de las DLT, incluyendo especialmente Blockchain. Los mecanismos de consenso son la vía en que los distintos nodos pueden validar el estado del Ledger para incluir un nuevo bloque a la cadena, teniendo que llegar a un acuerdo entre ellos. Para ello se tendrá que prever posibles fallas en la comunicación u otras dificultades propias de cada Blockchain. Los objetivos buscados con estos sistemas son que el valor generado, ya sea tokens o criptomonedas, sean generados por un nodo “honesto”. Y que, finalmente, también sean validados por el resto de los nodos honestos (Cardozo y Perdomo 2020).

La aleatoriedad y la anonimidad juegan un papel importante contra la creación de bloques por parte de nodos maliciosos con intención de validar operaciones o transacciones fraudulentas (ataques Sybils). Se busca mantener la confianza dentro de la red evitando la duplicidad de transacciones. En última instancia, determinadas plataformas recompensan aquellos nodos honestos que evitan el fraude con incentivos, ya sea económicos u otros (Narayanan 2016).

Existen varios mecanismos de consenso con distintas características adaptadas a las demandas de cada Blockchain. Algunos de muchos ejemplos son:

pBFT o **practical Byzantine Fault Tolerance**. Mecanismo donde los nodos se ordenan secuencialmente denominando aleatoriamente un líder y al resto como secundarios, llegando al consenso por regla de la mayoría.

dBFT o **delegated Byzantine Fault Tolerance.** Sustituye la figura del líder por diferentes delegados seleccionados dentro de la Blockchain. De entre ellos se elegirá a un orador al azar quien será el responsable de la creación de bloques tras la validación de transacciones.

Otro tipo de mecanismos son los algoritmos basados en pruebas donde los nodos deberán resolver un problema o puzle criptográfico exitosamente para poder validar un bloque e integrarlo a la cadena, pudiendo recibir incentivos por ello. Un ejemplo puede ser **PoW** o **Proof-of-Work** de Bitcoin, como mencionamos anteriormente. Otro sería **PoS** o **Proof-of-Stake**, donde los nodos podrán validar bloques jerárquicamente según la cantidad de tokens o criptomonedas que ellos tengan en posesión.

2.2. BLOCKCHAIN 2.0

“A Next-Generation Smart Contract and Decentralized Application Platform”

(Buterin 2013).

2.2.1. ETHEREUM: EL COMIENZO DE UNA GENERACIÓN

El Whitepaper de Ethereum se publicó en 2013 bajo la autoría de Vitalik Buterin. En el año 2015 se lanzaría la plataforma Ethereum, con unos principios y características definidos.

La trayectoria de Vitalik está activamente relacionada a la divulgación de la tecnología. Desde la aparición de Bitcoin mostró interés en el potencial que esta y las criptomonedas guardaban, no sin remarcar los problemas que aún soportaban. Entró a formar parte de esta comunidad, con aportaciones en blogs y artículos en Bitcoin Magazine, siendo su cofundador. A comienzos de 2014 emprendió un proyecto junto a un equipo de desarrollo, lanzar una plataforma para la creación y desarrollo de aplicaciones descentralizadas soportado en tecnología Blockchain. Esto puso sobre la mesa la idea que Nick Szabo propuso en los años 90, el concepto de las Smart Contracts.

Los principios que mueven la plataforma Ethereum desde sus comienzos son: (Buterin 2013)

Simplicidad: Mantener la simpleza, aun a costa del almacenamiento de datos o ineficiencia de tiempo, potenciando el carácter democratizador y el acceso a todo público.

Universalidad: Proporcionar un lenguaje interno de scripting Turing completo, sin especificaciones concretas. Lo que permite que cualquier usuario pueda programar contratos o transacciones mientras sean definibles matemáticamente.

Modularidad: Las partes del protocolo esta diseñadas lo más modular y separadas posible. Haciendo que la modificación en cierta parte del protocolo no pueda afectar al resto de aplicaciones de la plataforma, siendo en este sentido independientes.

Agilidad: La disponibilidad de realizar modificaciones si suponen una mejora sustancial en la escalabilidad o la seguridad, extremando la prudencia. Estos cambios pueden ser en el protocolo, Ethereum Virtual Machine (EVM), etc.

No discriminación y no censura: No se intenta restringir o prevenir categorías concretas de uso. Los mecanismos reguladores están pensados para prevenir el daño, no para oponerse a aplicaciones específicas.

Como hemos visto, la visión de Ethereum es de una computadora mundial descentralizada, imparable, resistente a la censura, capaz de sostenerse por sí misma. Para ello deberá poder calcular, almacenar datos y comunicarse entre sí. Y necesitará poder conseguir esas tres cosas de manera bastante eficiente y sólida (Kehrli 2016).

Aunque anteriormente ya existían plataformas donde se podían añadir scripts en los bloques, fue con Ethereum cuando se abrió la posibilidad de creación y desarrollo de aplicaciones descentralizadas basadas en tecnología Blockchain. Se clasifica como "Turning-complete programming language" al poder soportar cualquier lenguaje de programación en que se quiera ejecutar. Esto dista de Bitcoin, por ejemplo, quien presenta grandes limitaciones relacionados a la interpretación de código sin contar con sus obvias diferencias estructurales.

La Ethereum Virtual Machine es un ordenador universal que permite la ejecución de código en la red Ethereum. El Ether o ETH es la criptomoneda aceptada en la red y funciona como el medio de intercambio en las operaciones o transacciones realizadas. Tanto desarrolladores como mineros serán recompensados con estas por dotar de lógica y complejidad a Smart Contracts dentro de la red, así como incluir nuevos bloques a la cadena (Vilar 2020).

2.2.2. SMART CONTRACTS

Nick Szabo introdujo en 1996 el concepto de Smart Contract. Este abogado y científico computacional propuso la posibilidad de codificar software de tal forma que se asemejase a una cláusula contractual vinculante entre sus partes, minimizando la posibilidad de incumplimiento.

Los Smart Contracts son un programa informático almacenado en una red Blockchain. Una de las partes interesadas la programará y ejecutará de forma que cumpla con determinadas acciones automáticamente y bajo unas condiciones prefijadas. El mismo alojamiento en la Blockchain supone mayor seguridad en el contrato ya que impide las falsificaciones o modificaciones no deseadas. Aunque está alejado del concepto tradicional de contrato como fuente de obligaciones vinculantes, más bien siendo un mecanismo de ejecución de dichas obligaciones. Dichas líneas de código pretenden ser más eficientes que los contractos actuales, evitando fraudes y suponiendo un ahorro en tiempo y dinero

Pero estos nuevos "contratos" no están libres de problemas. Errores de origen humano en el momento de su programación o posibles comportamientos maliciosos pueden degenerar en conflicto entre las partes, aunado a la inmutabilidad de la información dentro de la Blockchain que dificulta su corrección. Actualmente algunas plataformas permiten mayor flexibilidad en este sentido, permitiendo actualizar los contratos. La actualización consiste en desplegar un nuevo contrato con las acciones modificadas y deshabilitar el contrato anterior, ya que resulta inviable borrarlo de la Blockchain (De Biase y Mayor 2018).

2.2.3. ORACLE

En plataformas que soportan y ejecutan Smart Contracts resulta imprescindible la información en vigor, siendo necesario interactuar con el mundo real. Los Oracles proveen diferentes tipos de datos e información externa a la Blockchain, lo que permite enlazarla a Smart Contracts. Los distintos agentes dentro de un contrato tendrán que confiar que los datos transmitidos a la red son fieles a la realidad. Podrán consensuar la asignación de esta tarea a una entidad externa o usar un servicio Oracle descentralizado. Ejemplo de esto último es Oraclize, una red Blockchain que media entre Smart Contracts y las webs convencionales (webs API) (Solomon 2018).

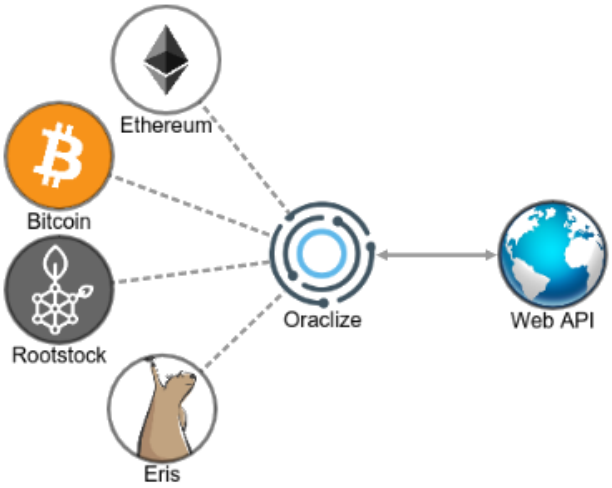

Imagen 2.3: Oraclize

(Fuente: Matt Solomon para medium.com/coinmonks)

Una buena construcción de Oracles es vital para Smart Contrants. Podrá ocupar esta función una entidad, persona o algoritmo. En el caso de una persona o entidad, se tendrá que asegurar por los medios legales la veracidad y precisión de la información. Se tiene que prever posibles problemas con los Smart Contracts. Y si llegase el caso, los medios legales tradicionales pueden ser la única solución (Czarnecki 2016).

Se puede clasificar a los Oracles según su especialidad siendo estos **de hardware**, **de software** y **de consenso**. Otra clasificación se centra más en su relación con la información: (Cardozo y Perdomo 2020)

Oracles inbound: Permiten incluir información externa a la Blockchain.

Oracles outbound: Permiten informar a una entidad externa a la Blockchain de un suceso ocurrido dentro de ella.

2.3. DECENTRALIZED AUTONOMOUS ORGANIZATION

El concepto de DAO hace referencia a una organización regida por Smart Contracts, reglas codificadas dentro de programas informáticos. El registro de sus transacciones y reglas programadas se mantienen en una Blockchain, lo que incrementa la transparencia a costa de la seguridad (Chohan 2017).

También se entiende como una forma más compleja de Smart Contract, siendo el conjunto de varios y donde se definen de antemano las reglas que dominarán la

organización. Al mismo tiempo fijará unos objetivos y expectativas propias de su naturaleza, ya sea empresarial o no.

2.3.1. ¿UN NUEVO PARADIGMA ORGANIZACIONAL?

Por lo general, las organizaciones tradicionales son propiedad de aquellas partes interesadas y cuyas operaciones están centralizadas, adoptando estructuras jerárquicas. De esta forma se sigue una dinámica de roles, con determinada capacidad de toma de decisiones y responsabilidades o tareas establecidas. Por el contrario, los participantes de un DAO tienen los mismos derechos en la toma de decisiones, no existiendo privilegios dentro de su gestión.

Este campo exige un mayor desarrollo en los conceptos que engloban a estas nuevas formas de organización. Buterin (2014) extendió la terminología en su blog, relacionando la existencia de capital interno, automatización y participación humana (Calderón y Tovar Gutiérrez 2018).

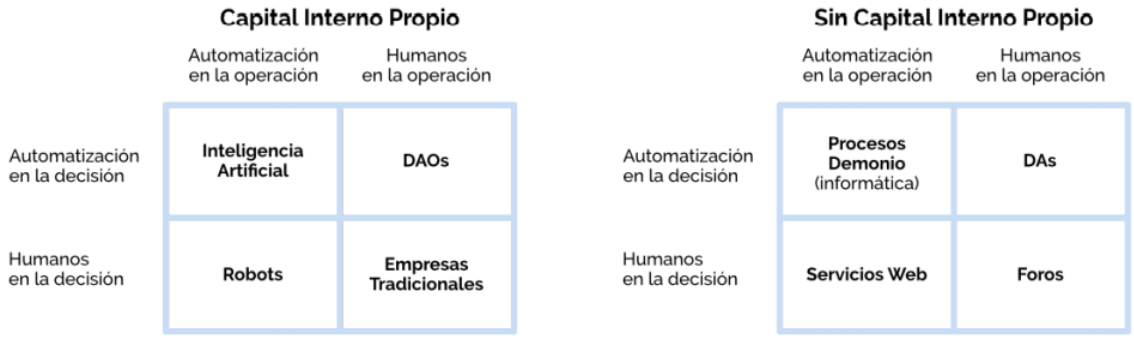

Imagen 2.4: Ilustración de actividades y organizaciones de acuerdo con el capital interno, y el nivel de automatización y participación humana.

(Fuente: “Comunidad Blockchain”, tomado del blog de Vitalik Buterin)

Agentes Autónomos: Se localizan en el espectro más especializado de la automatización, donde no existe intervención humana. Aunque es verdad que puede existir intervención en la construcción del hardware de su ejecución, posterior a esto es completamente independiente. Un Agente Autónomo completo, o inteligencia artificial completa, sería capaz teóricamente de adaptarse a las irregularidades de su entorno.

DAs o **Decentralized Applications:** Similares a Smart Contracts con la salvedad que tienen una capacidad ilimitada para incluir a varias partes contratantes o participantes, no necesariamente siendo aplicaciones financieras. Generalmente se pueden segmentar dos categorías dentro de su amplio espectro; aquellas que permiten el total anonimato de los integrantes, y las que se basan en la reputación de dichos integrantes y su participación en el mantenimiento del sistema.

DOs o **Decentralized Organizations:** Plantea la sustitución de la estructura jerárquica dentro de las organizaciones por una estructura descentralizada en donde los miembros interactúen entre sí bajo un protocolo especificado en el código, y dentro de una Blockchain. La diferencia entre una DO y una DAO radica en la automatización de la toma de decisiones interna, confiriéndole su categoría de “autónomo”. Aunque se discute aún el carácter autónomo debido a la necesidad actual de un equipo de desarrollo detrás.

DAC o **Decentralized Autonomous Corporations:** Una subclase de DAO donde la principal característica que los diferencia es el pago de dividendos entre los miembros, aquellos poseedores de tokens.

2.3.2. CARACTERÍSTICAS E IMPLEMENTACIÓN

Una de las propiedades más destacadas de las DAO es la autonomía. El uso de Smart Contracts convierte en innecesaria la intervención manual a la vez que fija los protocolos de actuación. El hecho que esté integrada en una Blockchain confiere seguridad y confianza, al ser toda operación o transacción transparente e incorruptible (Diallo et al. 2018).

Un miembro de la DAO puede lanzar una propuesta para un cambio en la organización. Cualquier cambio se validará por medio de una votación entre los miembros, siendo necesario tokens. La cantidad de estos determina el peso del voto. Los tokens serán la representación del valor dentro de la empresa y un método de recompensa a los miembros. Resulta común requerir de empleados cualificados que se encarguen del mantenimiento y desarrollo del código interno, siendo estos también elegidos por consenso.

Las relaciones en una DAO son más complejas que simples Smart Contracts. No son dos únicas entidades vinculadas sino varias, con objetivos distintos e incluso contrarios. También se abre la posibilidad de agregar nuevas entidades. Su fácil constitución y su apertura global permite el acceso a cualquier persona o entidad, como se observa en el siguiente cuadro (Czarnecki 2016).

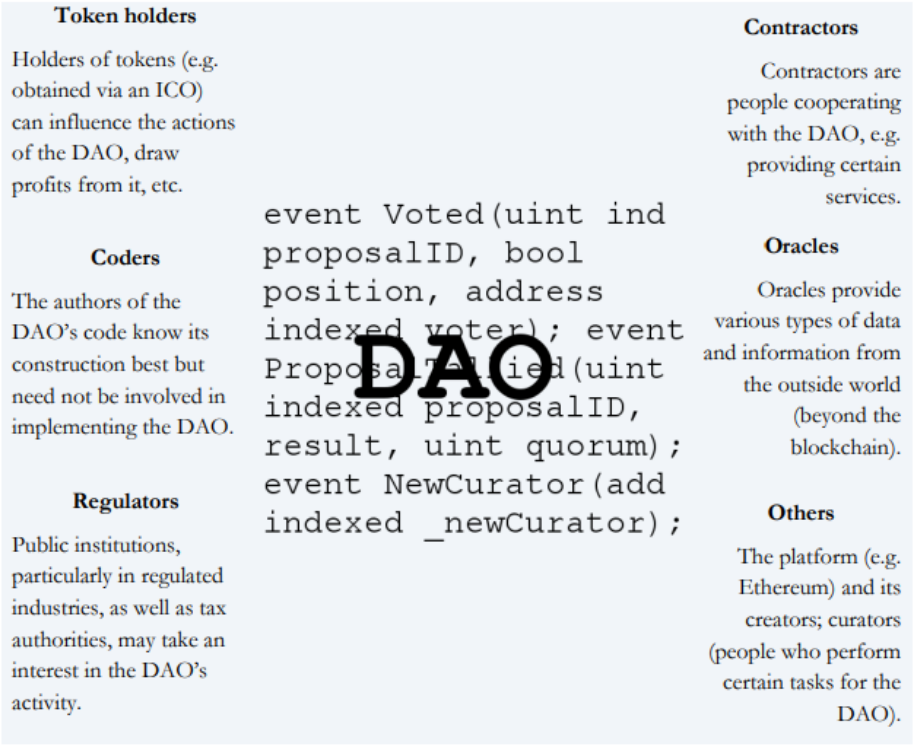

Imagen 2.5: Stakeholders de las DAO

(Fuente: Jacek Czarnecki para "Blockchain, smart contracts and DAO")

A la hora de implementar una DAO desde cero, lenguajes como Solidity, web3 y algunas interfaces de programación de aplicaciones como Angular o React son utilizados. Por otro lado, existen frameworks que ofrecen una estructura que facilita la implementación. Estas plataformas incentivan la creación de organizaciones y aplicaciones descentralizadas además de ser un marco de referencia para desarrollar, a partir de ellas, proyectos que quieran incursionar en una nueva economía descentralizada. Algunos ejemplos serían: (González, Guevara y Fernández 2020)

DAOstack: Plataforma creada para la gobernanza descentralizada permitiendo a colectivos la auto gobernanza bajo valores y objetivos comunes.

Colony: Proyecto que busca promover la creación de organizaciones digitales. Esta utilizaría la Blockchain de Ethereum, además que primaría un sistema de reputación basado en méritos conseguidos.

Aragon: Iniciativa española que también fomenta la gobernanza descentralizada. Aunque cuenta con componentes que la han vuelto interesante en el desarrollo de aplicaciones descentralizadas (DAs o Dapps), así como otros protocolos fundamentados en la criptografía.

2.3.3. LIMITACIONES E INCERTIDUMBRE LEGAL

Hay cierta problemática dentro del entorno de las DAO que han estado presente desde sus inicios. La falta de compromiso y participación por parte del grueso de la comunidad, poseedores de tokens, en las votaciones de las DAO debido al desconocimiento del valor e influencia de estos. Aunado a la existencia de dificultades para corregir desperfectos o errores en el código puesto que se necesitaría ser aprobadas por la mayoría. Todo ello incrementa actitudes oportunistas o ralentiza la adaptabilidad de la propio DAO.

Otro factor importante es la legalidad. Es difícil determinar dentro de que marco legal entran estas organizaciones teniendo en cuenta que también existen contradicciones con la propia tecnología Blockchain o las criptomonedas. El mejor ejemplo de estos conflictos sería “The DAO”, un proyecto que buscaba un nuevo modelo organizacional específicamente en fondos de inversión. Sería la comunidad quien decidiese donde invertir los fondos de la propio DAO. Una vulnerabilidad en el código produjo el movimiento indeseado de un tercio del patrimonio a cuentas anónimas. Finalmente, se decidió por votación devolver a la red a un estado anterior a lo ocurrido (hard fork), afectando gravemente a la confianza en ella (González, Guevara y Fernández 2020).

3. INITIAL COIN OFFERINGS

“Instead, citizens may one day prefer virtual currencies, since they potentially offer the same cost and convenience as cash—no settlement risks, no clearing delays, no central registration, no intermediary to check accounts and identities.”

(Lagarde, 2017)

3.1. NACIMIENTO DE UN NUEVO MÉTODO DE FINANCIACIÓN DIGITAL

Para empresas jóvenes la captación de financiación resulta crucial, pero existen limitaciones en las vías tradicionales propias de su naturaleza. Internet y las nuevas tecnologías han abierto la puerta a nuevas formas de financiación alternativa, propiciando la internacionalización y avance de proyectos de toda índole. Métodos como el Crowdfunding o las ICO son otros ejemplos de lo que actualmente se denomina como “Cryptoeconomics”.

Las Initial Coin Offerings o ICO son un método de financiación donde los interesados emiten criptomonedas de un proyecto basado en Blockchain a un precio fijado. El

objetivo detrás de esto es proveerles de capital inicial para empezar el desarrollo del proyecto.

3.1.1. ORIGEN: EL ASCENSO DEL TOKEN

Tras las restricciones al crédito bancario derivada de la crisis financiera de 2008, fueron pocos los emprendimientos que podían acceder a nuevo crédito. Un motivo fue la incapacidad de cumplir con las exigencias mínimas requeridas. De esta situación surgieron diversas soluciones, entre ellas las ICO.

En un inicio se planteó las ICO como un mecanismo de apoyo a nuevas ideas y emprendimientos dentro de la comunidad Blockchain. Pero con el tiempo fue adquiriendo mayor relevancia, lo que proponía ser una nueva vía para fines más amplios y con cantidades superiores. En 2013 tuvo lugar la primera ICO por parte de Mastercoin reuniendo 5 millones de dólares en bitcoins. Pocos años después saldrían las ICO de Ethereum y The DAO, siendo estas considerablemente mayores.

En 2018 se registró más de 2200 ICOs mundialmente, recaudando 11,4 mil millones de dólares. Según García-Ramos Lucero y Rejas Muslera (2020), la falta de estandarización en el proceso resulta ventajosa para los startups por lo que, desde 2017, más de ellas optan por ICOs buscando evitar las rigurosas regulaciones. Este crecimiento exponencial ha sido tan pronunciado que en años anteriores ha superado en recaudación al capital riesgo del mercado Blockchain, al menos hasta finales de 2017.

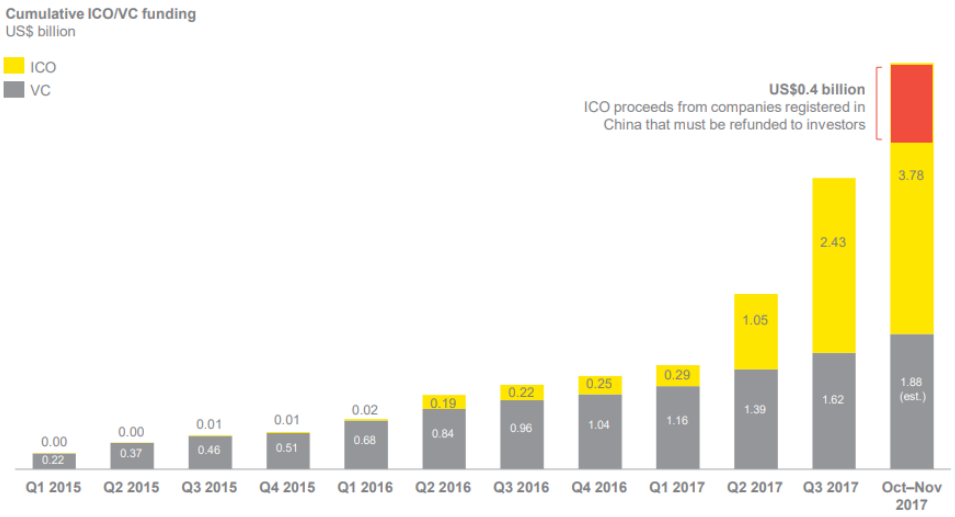

Gráfico 3.1: Los ingresos totales de ICO se acercan a los 4 mil millones USD y han superado las inversiones de capital de riesgo en proyectos de blockchain

(Fuente: EY research: initial coin offerings (ICOs) December 2017)

El token o criptomoneda es una unidad, monetaria o no, virtual que funciona como método de intercambio de valor dentro de una red Blockchain u otros sistemas de transacciones. Actualmente no existe un consenso claro en lo referente a su clasificación, siendo este una de las cuestiones que mayor controversia traen a nivel legal.

El investigador Mougayar (2017) propone una clasificación de las partes que conforman los tokens. Estos se compondrían de tres partes; un role, un propósito y una serie de características propias de cada role.

Dentro de esta clasificación nos encontramos con seis roles diferentes:

Right: La posesión del token implica ciertos derechos dentro del ecosistema del mismo proyecto.

Value Exchange: Los tokens se relacionan con el intercambio de valor dentro del ecosistema. Desarrollando un sistema económico interno que se crea y mantiene individualmente.

Toll: La adquisición de tokens facilita al propietario el acceso a funcionalidades, servicios o beneficios del propio proyecto.

Function: Los propietarios de los tokens podrán enriquecer su experiencia de usuario dentro de los límites que el proyecto permita.

Currency: Los tokens representan una unidad de medida del valor intercambiable tanto dentro como fuera del ecosistema del proyecto.

Earnings: Se centra en los inversores, permite una distribución equitativa del valor creado por el proyecto u otros beneficios financieros relacionados.

Lejos de las propiedades de los tokens, sigue existiendo discrepancias en la categorización. Particularmente, según su diseño y uso por parte de los usuarios. El legislador de Suiza, el Swiss Financial Market Supervisory Authority (FINMA), aprovecha la siguiente clasificación aplicando ciertas particularidades propias de su legislación:

Payment tokens: Usados para adquirir bienes y servicios o la realización de transferencias. Es la comunidad quien las acepta como medio de pago y la que determina su valor, siendo esta su principal utilidad. El ejemplo más claro sería los bitcoins.

Utility tokens: La propiedad de estos tokens permite el futuro acceso a productos o servicios del proyecto en vías de desarrollo. De ahí su denominación como tokens de usuario o App Coins. Su naturaleza difiere de los modelos de inversión, asemejándose más a un prepago.

Investment o **security tokens:** Proveen a sus poseedores un derecho patrimonial que se traduce en potenciales beneficios futuros tras la implementación y desarrollo del proyecto. Estos tokens poseen un remarcado carácter de inversión por lo que pueden considerarse un valor negociable.

Hybrid tokens: Aquellos que acumulan características propias de los tokens antes mencionados, lo que implica ajustarse a los aspectos y regulaciones propias de estos.

3.1.2. LANZAMIENTO DE UNA ICO

El lanzamiento de una ICO puede resultar complejo debido a factores como la confianza en los promotores o en las expectativas de crecimiento. A diferencia de negocios más establecidos y comparables donde existen flujos de caja o cuota de mercado, en las ICO son las expectativas de crecimiento las que ayudan a aproximar su valor y posteriormente su precio.

Determinar qué características pueden clasificar a un token como valor negociable entraña cierta dificultad ya que en una ICO no siempre las ganancias son seguras o pueden demorar varios años en afianzarse como negocio. El regulador estadounidense, el U.S. Securities and Exchange Commission (SEC), aplica un sistema de evaluación creada y puesta en marcha por la Corte Suprema llamado Howey Test. Aclarando si una determinada transacción realizada dentro del territorio puede ser considerada una inversión, debiendo cumplir aspectos como la entrega de una cuantía monetaria,

expectativas de beneficio por dicho desembolso y efectuándose a través de terceros especializados (Common Enterprise). El Howey Test se aprovecha como guía y marco de referencia ante las ICO, aunque finalmente es cada jurisdicción quien fija los límites y condiciones en relación con tokens dentro de su territorio.

La disparidad de proyectos unido a la falta de estandarización de información obstaculiza poder establecer pautas o métodos claros en los lanzamientos de criptomonedas. No obstante, abre la puerta a nuevas soluciones. Entre ellas las que plantea Ciucci (2017) al automatizar, a través de Smart Contracts, la verificación de tokens y el cumplimiento de los objetivos del proyecto por parte del equipo promotor. Otro enfoque sería establecer reglas de buena conducta que busquen consensuar la creación de mejores prácticas de lanzamientos de ICOs en este nuevo ecosistema. En Europa ha habido iniciativas, especialmente relacionado al Crowdfunding, que pretenden asentar nuevas pautas de la mano del marco jurídico ya existente (European Crowdfunding Network 2016).

A pesar de lo anterior, la realidad muestra patrones específicos en la emisión de ICOs: (De Biase y Mayor 2018)

Los promotores que concibieron el proyecto anuncian la emisión de una ICO para recaudar fondos a través de foros especializados como Bitcoin Talk o Cryptocointalk, unido a un resumen ejecutivo.

Posteriormente se elabora una memoria llamada Whitepaper donde se detalla todo el plan de negocio como la información de los promotores u otros aspectos técnicos. Será indispensable la claridad y detalle en la información de la estrategia de inversión para los fondos percibidos. En ocasiones se incluye un documento con las especificaciones técnicas detrás del proyecto denominado Yellowpaper.

En la primera etapa o pre-sale es común ofertar preliminarmente a cientos de inversores, generalmente empresas relacionadas a la tecnología o inversores institucionales. Posterior a esto, se anuncia el lanzamiento públicamente con sus correspondientes actividades publicitarias. En este punto el inversor minoritario es libre de adquirir los tokens o criptomonedas. Tanto promotores como asesores del proyecto suelen reservar tokens como contraprestación por el trabajo realizado.

Se fijará un límite máximo de tokens en circulación, pudiendo ser ampliado en caso de cumplirse dicho limite en un determinado periodo de tiempo. Tras ser emitidos entre los inversores iniciales los tokens podrán ser negociados en mercados digitales alternativos e intercambiados por monedas de curso real u otras criptomonedas. En estos mercados secundarios, la oferta y demanda marcará el precio, estando fuertemente influenciado por el buen desempeño del proyecto y del equipo promotor.

3.2. ¿PROBLEMAS DE VALORACIÓN?

El nuevo ecosistema Blockchain, más concretamente las ICO, plantean ciertos dilemas en lo que respecta a financiación e inversión. Por parte de promotores, en como determinar el precio de sus tokens y cuantos inversores cualificados pueden suscribirse sin que perjudique la expansión de la red. Y por parte del inversor, en como estimar el valor de proyectos como estos. Por lo que resultará interesante tratar los aspectos y características más destacables de las ICO.

3.2.1. SEMEJANZA A OTRAS FUENTES DE FINANCIACIÓN

La llamada “tokenización” cada vez está teniendo una mayor presencia en ámbitos alejados de la búsqueda de financiación, aunque en estos últimos se percibe cierto estancamiento en la captación de fondos. Una posible razón estaría en las estafas

(Scam) existentes en proyectos de esta índole. El nivel de confianza por parte de inversores y la misma comunidad hacia el equipo de desarrollo puede determinar el éxito o fracaso de una ICO.

Por lo que resulta interesante comparar las ICO con otras fuentes de similares características para determinar que opciones tendría una empresa emergente dentro del vasto entorno: (Carcedo Coello de Portugal, 2019)

Capital Riesgo: Está fuertemente vinculado con las ICO. Los fondos de capital riesgo suscriben criptomonedas en la fase inicial de preventa, aunque es común que los startups tomen la iniciativa en colaborar. Los beneficios percibidos van más allá del capital captado, existiendo sinergias como el conocimiento o la red de contactos que ayudan al progreso del proyecto. A pesar de esta complementariedad entre ambas vías, las ICO destacan en la liquidez al permitir tokens negociables en mercados secundarios. Contrario a las inversiones en Capital Riesgo donde se espera una rentabilidad económica a medio plazo, haciéndolas poco liquidas.

Existe mayor prevalencia de financiación por ICOs en detrimento del Capital Riesgo en aquellas inversiones que presenten una alta volatilidad, quienes necesitarían un mayor rendimiento para cubrir su elevada exposición. Las ICO destacarían en aquellos negocios donde existiesen mayor presencia de riesgos intrínsecos (Coin Bureau, 2017).

Oferta Pública de Venta: En términos generales, tanto las OPV como las ICO buscan financiarse a través de la emisión de determinados derechos vinculados, ya sean acciones o tokens. Mientras que las OPV se realizan en una fase de maduración avanzada, las ICO buscan financiación inicial y se concentran en PYMES o startups. Los fondos captados en las OPV son considerablemente mayores, además de estar altamente regulados y siendo común la realización de varias rondas de financiación. Por el contrario, la falta de regulación en las ICO genera una mayor exposición al riesgo y, por ende, mayor volatilidad de precios. La posibilidad de comercializar fracciones de tokens beneficia al inversor minorista, unido a sus altas expectativas de crecimiento.

Crowdfunding: El paralelismo entre ambas es claramente destacable. Ambas vías permiten la financiación de PYMES y startups por medios on-line. Las plataformas de Crowdfunding dan soporte a la publicación de proyectos, recayendo la confianza sobre ellas. Esto implica la necesidad de mantener la fiabilidad del público, limitando proyectos de dudosa reputación. Desde el punto de vista del inversor, el Crowdfunding basado en acciones está motivado por el rendimiento financiero obtenido, mientras que el basado en recompensas se aleja de ello como objetivo último para buscar el apoyar un proyecto o la pertenencia a una comunidad. Por el contrario, en las ICO se elimina dicha intermediación, la confianza recae únicamente en el propio proyecto y su red Blockchain. Comparativamente hablando estas últimas recaudan mayores fondos y no sufren de restricciones en la publicidad realizada al no haber, de momento, regulaciones concretas.

3.2.2. VENTAJAS ASOCIADAS A LAS ICO

Una de las más destacables ventajas que presenta las ICO es la democratización del entorno de inversión frente a otras fuentes de financiación. Su carácter global permite el acceso de una mayor población que, de otra forma, hubiera sido altamente improbable. Las ICO o el Crowdfunding permite este alcance abriendo la puerta a nuevos proyectos respaldados por una creciente comunidad. Anteriormente era común la brecha entre emprendimientos que no lograban obtener financiación temprana e inversores que no llegaban a financiar. Además, existen límites de información debido al reducido número de inversores cualificados, con grandes patrimonios y perspectivas a largo plazo, provocando ineficiencias en cuestión de tiempo o criterios de valoración sesgados (Bellón Núñez-Mera, de los Ríos Sastre y Sáenz-Díez Rojas 2018).

La expansión del apoyo a cada vez más número de emprendimientos no está libre de críticas. Una de las dudas planteadas es acerca del incremento de nuevos recursos, y si no sería a costa de otras fuentes de financiación ya establecidas. Sobre este tema Estrin, Gozman y Khavul (2018) entrevistó a inversores en Equity Crowdfunding o basado en acciones. La mayoría no había realizado ningún tipo de inversión relacionada con anterioridad lo que podría sugerir que parte de los recursos captados con estas nuevas vías sí son complementarias a las tradicionales.

3.2.3. RIESGOS IMPLÍCITOS

Al igual que otros métodos de inversión, las ICO entrañan problemáticas propias del negocio o la situación. Además de nuevos riesgos y desafíos comparados con sus predecesores. Aunque existen propuestas que pretenden mejorar estos aspectos aún es relativamente pronto, sobre todo de cara a la inversión.

El riesgo de posible conflicto entre las partes está muy presente. Por lo general, son muy pocas las ICO que otorgan derechos de voto en la toma de decisiones, lo que da muy poco poder a los tenedores de tokens. Añadido al hecho de que la emisión de criptomonedas se realiza con un número determinado de ellas, lo que imposibilita una financiación más escalonada. Distinto de las OPV, por ejemplo, teniendo varias rondas de financiación. A esto último, existen posibles soluciones como la que ofrece las DAICO (Bellón Núñez-Mera, de los Ríos Sastre y Sáenz-Díez Rojas 2018).

Poder acceder a un mayor número de usuarios también genera dificultades. La capacidad de investigar a fondo un negocio (Due diligence) que poseen los grandes inversores cualificados se disipa en un inversor individual al ser incapaz de asumir los costes inherentes de esa labor. Por tanto, la asimetría de información entre la empresa y los inversores minoritarios es mucho mayor.

En los comienzos de las ICOs se proporcionaba el código fuente completo lo que respaldaba el proyecto detrás. Con el tiempo se fue generalizando mucho más las ICO, desembocando en el apoyo a proyectos en fases más tempranas y con el código fuente aún sin terminar. Esto puede degenerar en comportamientos fraudulentos. Según Adhami, Giudici y Martinazzi (2017), el 57% de las 253 ICOs analizadas no disponían del código fuente, el 16% no presentaban Whitepaper del proyecto y el 69% de los que sí presentaban Whitepaper no especificaban la finalidad que se daría a los fondos captados.

Otra cuestión de riesgo es la relacionada a la legalidad. Como ya se ha mencionado, no existe consenso a la hora de categorizar aquellos proyectos que se pueden considerar inversión. Cada legislación aplica sus propias medidas, que en muchos casos resultan poco claras debido a su inmadurez. Habiendo también incertidumbre con respecto a la protección de los inversores no acreditados.

3.2.4. DECENTRALIZED AUTONOMOUS INITIAL COIN OFFERING

“If the voters are very unhappy with the development team’s progress, they can always vote to shut the DAICO down entirely and get their money back”

(Buterin 2018)

En enero de 2018 Vitalik Buterin publicó en su foro el concepto de DAICO. Una idea que planteaba mejorar el modelo ICO mediante los beneficios que aportaban las DAO, pero de manera que se minimice la complejidad y el riesgo. La intención era limitar la concentración de poder por parte de los promotores de las ICO en favor de los poseedores de los tokens, aunque fuese en menor medida (Calderón y Tovar Gutiérrez 2018).

Imagen 3.2: Explicación de las DAICOs

(Fuente: Blog de Vitalik Buterin)

Aplica características de la DAO como no depender de equipos centralizados o aprovechar la inteligencia colectiva para favorecer una mayor democratización del ecosistema. Y al igual que cualquier ICO, tiene un periodo de contribución para adquirir los tokens y uno posterior donde pueden llegar a ser negociables en mercados secundarios.

La principal diferencia es que los votantes, poseedores de los tokens, pueden decidir y fijar un presupuesto temporal razonable y no demasiado elevado de los fondos captados. A medida que se demuestra la competencia del equipo de desarrollado cumpliendo con los objetivos marcados dentro del presupuesto existente, los votantes podrán decidir liberar otra parte mayor de estos fondos.

La liberación y consenso por fases favorece incluso si existe descontento por el progreso del proyecto, pudiendo votar para cerrar por completo el DAICO y recuperar el capital. Esto permite asegurarse ante riesgos como ataques en el 51% de la red, sobornos u otras vulnerabilidades, así como riesgos propios de las ICO como la irresponsabilidad de los promotores o posibles proyectos fraudulentos.

3.2.5. POSIBLES SOLUCIONES DESCENTRALIZADAS

Determinar el valor de una ICO difiere en diversas soluciones que bien podrían seguir desarrollándose de cara al futuro. Actualmente existen dos campos de estudio con perspectivas altamente ligadas al nuevo ecosistema que Blockchain plantea, estos serían la Inteligencia Artificial y la Inteligencia Colectiva.

Inteligencia Artificial: Se proponen diversas iniciativas relacionadas con la inversión. Generalmente la valoración realizada no sería pública puesto que esta se extrae de variables internas y gracias a su propio rendimiento computacional pudiendo incluso, con los resultados obtenidos, ser capaz de adaptarse.

Inteligencia Colectiva: Se encuentra relacionado con el campo de los Mercados Predictivos. Esta metodología aprovecha el conocimiento y análisis de la población mayoritaria de un colectivo para la evaluación y valoración de ICOs, así como para su gestión descentralizada.

Actualmente existen diversos proyectos enfocados en la valoración con inteligencia colectiva como son Augur o Gnosis. Un ejemplo destacable es Wings, al ser su principal objetivo la valoración de ICOs.

Wings es una DAO cuya principal función es la evolución y promoción de ICOs. A través de un sistema de recompensas dentro de la comunidad se premia aquellos nodos, los usuarios, con las predicciones más acertadas con relación a la valoración o recaudación obtenida. Un equipo promotor le resultará interesante los servicios de Wings a la hora de especificar el valor de los tokens que ponen en emisión (Bussutil y Rubio 2018).

3.2.6. SITUACIÓN JURÍDICA EN ESPAÑA

La complejidad implícita obliga a una revisión constante de los criterios. La CNMV (2018) actualmente califica a los tokens como valores negociables siempre que cumplan ciertos criterios como atribuir derecho o expectativas de participación en la rentabilidad potencial o de revalorización. En general, derechos semejantes a los propios de las acciones, obligaciones u otros instrumentos financieros incluidos en el artículo 2 del TRLMV. Además de incluirse si se ofrecen junto con expectativas de beneficio para el inversor, ya sea implícita o explícitamente. Se excluyen aquellas donde sea incierta una correlación razonable entre las expectativas de revalorización o rentabilidad y la evolución del proyecto.

Se remitirá al art. 35.3 de la LMV la necesidad y alcance de intervención de las entidades autorizadas en emitir y comercializar ICOs. Como mínimo, deberán supervisar el proceso y validar la información siendo clara, imparcial, no engañosa, refiriéndose las características y riesgos, así como la situación jurídica y económico-financiera del emisor para su apropiada valoración de inversión. Con relación a la intermediación y custodia no será necesaria la intervención generalizada de dichas entidades excepto cuando la actividad se realice “con carácter profesional o habitual”. Además, las ICO se someterán a la necesidad de representación mediante anotaciones en cuenta y la participación de un depositario central de valores según el art. 8.3 de la LMV. Por último, la mayoría de dichas operaciones cumplen con las condiciones de no obligatoriedad de publicar folleto informativo recogido en el art. 35.2 de la LMV. Aunque la CNMV aseguró mantener el principio de proporcionalidad en los casos donde sea necesario publicar folleto, intentando adaptarse a las situaciones concretas de cada emisor (Pérez Carrillo 2018).

CONCLUSIONES

A lo largo del trabajo se ha ido observando el avance de la tecnología Blockchain, acompañado de su capacidad para generar valor. Desde el punto de vista empresarial, la posibilidad para una mayor captación de fondos es amplia, especialmente para startups o pequeñas empresas.

Dentro de los métodos de financiación convencionales, los procedentes de entidades bancarias suelen estar reservados a empresas ya establecidas o en mercados maduros, indiferentemente del plazo establecido. Por el contrario, sistemas alternativos de financiación como los Business Angels estarán más predispuestos en invertir en PYMES o startups, asumiendo el riesgo inherente a ellos.

Por su parte, las ICO han sufrido un crecimiento exponencial a lo largo de los años. Desde un punto de vista práctico, es una opción de captación de fondos viable para empresas emergentes. Hay indicios que señalan un mayor emprendimiento dentro de estas comunidades, unido a los esfuerzos en adaptar mejor la ley por parte de la administración.

Ahora bien, esto último no las libra de serios inconvenientes. La aún poco regulada legislación y la falta de estándares concretos no solo las vuelven inciertas sino arriesgadas. La volatilidad de precios en mercados secundarios es considerablemente alta, lo que dista de la aparente estabilidad presentada en otros activos tecnológicos comparables. En parte se explicaría por la tendencia a la especulación en la adquisición de criptomonedas. Esta situación mermaría la confianza del público general e incentivaría los fraudes en proyectos, no necesariamente buscando solo el capital captado sino la revalorización de sus tokens.

Para finalizar, y de cara a futuras indagaciones, es conveniente mencionar el potencial de la tecnología Blockchain en campos muy dispares, más allá de únicamente la financiación. Instituciones como los bancos centrales están barajando la posibilidad de emitir sus propias criptomonedas (Belinchón 2020). A fecha de publicación del trabajo el Banco Central Europeo se encuentra en fase de investigación. Por otro lado, la proliferación de Smart Contracts agilizaría procesos en sectores como los seguros o la negociación internacional, automatizando fases intermedias o mediando la desconfianza entre partes. Las Blockchains privadas podrían mejorar la contabilidad interna de grandes multinacionales, mayormente dispersas, creando una única contabilidad segura e inmutable.

Desde mi punto de vista, y tras esta rigurosa investigación, podemos concluir que en cierta medida el uso de Blockchain mejoraría diversos aspectos de la sociedad, desde el aumento de la eficiencia en ciertos procesos hasta la creación de nuevos emprendimientos o soluciones. A pesar de esto, cabe la duda de si realmente las ICO son la mejor vía de financiación, siendo muy pronto para determinarlo. Dependiendo del tamaño y expectativas, a una empresa emergente puede convenirle o no. Animo a seguir investigando, queriendo que este trabajo sea otro punto de apoyo para aquellos quienes deseen adentrarse en esta apasionante área.

INITIAL COIN OFFERINGS: ANÁLISIS DE BLOCKCHAIN Y ESTRATEGIA DE FINANCIACIÓN BASADA EN EMISIÓN DE TOKENS

BIBLIOGRAFÍA

- ADHAMI, S.; GIUDICI, G. y MARTINAZZI, S. 2017. *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings.* Journal of Economics and Business, Forthcoming. DOI: http://dx.doi.org/10.2139/ssrn.3046209
- ARAGON.ORG. 2020. *Next-Level Communities Run on Aragon*. [online] Disponible en: https://aragon.org/ [Último acceso: 24 noviembre 2020].
- BELINCHÓN, F. 2020. Los bancos centrales estudian crear sus propias criptodivisas. *Cinco Días. El País*, [online] Disponible en: https://cincodias.elpais.com/cincodias/2020/01/03/mercados/1578070851_687433.html [Último acceso: 24 noviembre 2020].
- BELLÓN NÚÑEZ-MERA, C.; DE LOS RÍOS SASTRE, S. y SÁENZ-DÍEZ ROJAS, R. 2018. *Financiación Alternativa para el Emprendedor: Las Initial Coin Offerings a examen*. Informe técnico. Información Comercial Española.
- BUSSUTIL, A. y RUBIO, L. 2018. ¿Cómo Valorar Una ICO O Criptoactivo? En: *Comunidad Blockchain: El futuro de la criptoeconomía descentralizada y las ICO's.* pp.13-30.
- BUTERIN, V. 2018. Explanation of DAICOs. [Blog] *Ethereum Research*, Disponible en: https://ethresear.ch/t/explanation-of-daicos/465 [Último acceso: 22 noviembre 2020].
- BUTERIN, V. 2013. *A Next-Generation Smart Contract and Decentralized Application Platform*. [online] Disponible en: https://ethereum.org/en/whitepaper/ [Último acceso: 22 noviembre 2020].
- CALDERÓN, J. y TOVAR GUTIÉRREZ, M. 2018. DAO: La Empresa Descentralizada En La Tokeneconomía. En: *Comunidad Blockchain: El futuro de la criptoeconomía descentralizada y las ICO's.* pp.31-39.
- CARCEDO COELLO DE PORTUGAL, A. 2019. *Los Icos Como Sistema De Financiación Alternativa Para Start-Ups*. FERNÁNDEZ-TRAPA DÍAZ-OBREGÓN, V. (dir.) Trabajo Fin de Grado, Universidad Pontificia Comillas.
- CARDOZO, G. y PERDOMO, P. 2020. *Comparación De Plataformas Para Smart Contracts Basadas En Blockchain*. Proyecto de Grado. Universidad de la República.
- CASTELLANOS, E. 2017. *CRIPTOMONEDAS, BLOCKCHAIN Y UNA NUEVA VISIÓN DEL MUNDO*.
- CHAMPAGNE, P. 2014. *El Libro De Satoshi (Edición Blockchainespana.com): La Colección de Escritos del Creador de Bitcoin Satoshi Nakamoto*. E53 Publishing LLC.
- CHOHAN, U.W. 2017. *The Decentralized Autonomous Organization and Governance Issues*. Informe técnico. University of New South Wales.
- CIUCCI, F. 2017. ICOs can be fixed with automation, not with guidelines for humans. [Blog] *LinkedIn*, Disponible en: https://www.linkedin.com/pulse/icos-can-fixed-automation-guidelines-humans-fabio-ciucci/ [Último acceso: 22 noviembre 2020].
- COIN BUREAU. 2017. *Managing Cryptocurrency Risk in Your Portfolio: Top Tips*. [online] Disponible en: https://www.coinbureau.com/education/managing-cryptocurrency-risk-your-portfolio-top-tips/ [Último acceso: 22 noviembre 2020].
- COLONY.IO. 2020. *Colony*. [online] Disponible en: https://colony.io/ [Último acceso: 24 noviembre 2020].
- COMISIÓN NACIONAL DEL MERCADO DE VALORES. 2018. *Criterios en relación con las ICOs. https://www.cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf*
- CZARNECKI, J. 2016. What Are Smart Contracts And DAO? En: *Blockchain, smart contracts and DAO.* pp.5-9.

- CZARNECKI, J. 2016. How to design smart contracts and DAO. En: *Blockchain, smart contracts and DAO.* pp.16-18.
- DAOSTACK.IO. 2020. *Daostack*. [online] Disponible en: https://daostack.io/ [Último acceso: 24 noviembre 2020].
- DE BIASE, P. y MAYOR, D. 2018. *Initial Coin Offerings ("Icos"): Un Estudio Sobre Una Nueva Forma De Financiación En La Era Digital*. [online] Disponible en: http://www.incari.org/upload/Anuario2017/Art04_A2017.pdf [Último acceso: 22 noviembre 2020].
- DIALLO, N. [et al.] 2018. *Egov-DAO: A Better Government Using Blockchain Based Decentralized Autonomous Organization*. Informe técnico. University of Houston.
- ESTRIN, S.; GOZMAN, D. y KHAVUL, S. 2018. *The Evolution and Adoption of Equity Crowdfunding: Entrepreneur and Investor Entry into a New Market*. Small Business Economics, pp.1-15.
- ETHEREUM FOUNDATION 2014. *Daos, Dacs, Das And More: An Incomplete Terminology Guide*. Ethereum Blog. [online] Disponible en: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ [Último acceso: 22 noviembre 2020].
- EUROPEAN CROWDFUNDING NETWORK. 2016. *ICO CHARTER*. [online] Disponible en: https://eurocrowd.org/membership/code-of-conduct/ico-charter/ [Último acceso: 22 noviembre 2020].
- EYGM LIMITED. 2018. *EY Research: Initial Coin Offerings (Icos) December 2017*. [online] Disponible en: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf [Último acceso: 23 noviembre 2020].
- FINNEY, H. 2004. *RPOW - Reusable Proofs of Work*. [online] Disponible en: https://nakamotoinstitute.org/finney/rpow/index.html [Último acceso: 21 noviembre 2020].
- GARCÍA-RAMOS LUCERO, M. y REJAS MUSLERA, R. 2020. Balance del régimen jurídico-económico de las ICOs en la financiación de las PYMES. *Derecho Y Cambio Social*, n.º 61, pp.489-501. Disponible en: https://lnx.derechoycambiosocial.com/ojs-3.1.1-4/index.php/derechoycambiosocial/article/view/402
- GONZÁLEZ BLANCO, D.; GUEVARA CARPIZO, A. y FERNÁNDEZ ALONSO, M. 2020. *Organizaciones Autónomas Descentralizadas (Daos) Para Economía Colaborativa Utilizando Blockchain*. COLLADO, S.; VILA, D. y ADROHER, J. (dir.) Trabajo Fin de Grado, Universidad Complutense de Madrid.
- KEHRLI, J. 2016. Blockchain 2.0 - From Bitcoin Transactions to Smart Contract applications. [Blog] *niceideas.ch*, Disponible en: https://www.niceideas.ch/roller2/badtrash/entry/blockchain-2-0-from-bitcoin#sec41 [Último acceso: 22 noviembre 2020].
- LAGARDE, C. 2020. *Virtual Currencies. Better Payment Services?* [entrevista] Central Banking and Fintech—A Brave New World? Disponible en: https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world [Último acceso: 22 noviembre 2020].
- MOUGAYAR, W. 2017. Tokenomics — A Business Guide to Token Usage, Utility and Value. [Blog] *William Mougayar*, Disponible en: https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416 [Último acceso: 23 noviembre 2020].
- NAKAMOTO, S. 2008. *Bitcoin: Un Sistema De Dinero En Efectivo Electrónico Peer-To-Peer*. [online] Disponible en: https://bitcoin.org/es/bitcoin-documento [Último acceso: 22 noviembre 2020].

- NAKAMOTOINSTITUTE.ORG. 2020. *Satoshi Nakamoto Institute*. [online] Disponible en: https://nakamotoinstitute.org/ [Último acceso: 24 noviembre 2020].
- NARAYANAN, A. [et al.] 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- PADILLA SÁNCHEZ, J. 2020. Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*, n.º 39, pp.175-201. DOI: https://doi.org/10.18601/01234366.n39.08.
- PÉREZ CARRILLO, E. 2018. ICO, tokens y aplicación de la Ley de Mercado de Valores. Criterios de la CNMV. [Blog] *Derecho Mercantil. (DerMerUle)*, Disponible en: https://blogs.unileon.es/mercantil/ico-tokens-y-aplicacion-de-la-ley-de-mercado-de-valores-criterios-de-la-cnmv/ [Último acceso: 23 noviembre 2020].
- PÉREZ DEL BARRIO, P. 2012. *Sistemas Alternativos De Financiación Empresarial Para PYMES*. TORRE OLMO, B. (dir.) Trabajo Fin de Grado, Universidad de Cantabria.
- SOLOMON, M. 2018. Using APIs in Your Ethereum Smart Contract with Oraclize. [Blog] *Coinmonks*, Disponible en: https://medium.com/coinmonks/using-apis-in-your-ethereum-smart-contract-with-oraclize-95656434292e [Último acceso: 22 noviembre 2020].
- VILAR PAGÈS, F. 2020. *Tecnología blockchain, smart contracts y caso swap: Descripción, evolución, aplicaciones y tendencias*. PUIG, E. (dir.) Trabajo Fin de Grado, Universitat de Barcelona.
- ZHENG, Z. X. 2018. *Blockchain challenges and opportunities: A survey*. International Journal of Web and Grid Services.