Revista de Derecho UNED, núm. 31, 2023

BLOCKCHAIN Y CANAL INTERNO DE INFORMACIÓN

BLOCKCHAIN AND WHISTLEBLOWING

Carlos Franco Blanco

Abogado y Consultor TIC's. Doctorando en Derecho por la UNED

Resumen: Las utilidades de la incipiente tecnología Blockchain son numerosas en la actualidad y otros están aún por descubrir. En el presente trabajo, en primer lugar se conceptualiza la tecnología blockchain y el canal interno de información para finalizar desarrollando la integración de la citada tecnología en los canales internos de informaciones de las distintas organizaciones como sistema de almacenamiento de las comunicaciones de irregularidades.

Palabras clave: Cadena de bloques, canal interno de información, cumplimiento normativo, Bitcoin.

Abstract: The emerging Blockchain technology utilities are numerous today and others are yet to be discovered. In the present paper, in the first place, Blockchain technology and Whistleblowing are conceptualized to finish developing the integration of the aforemen-

tioned technology in Whistleblowing channels in different organizations as a storage system for communications of irregularities.

Key words: Blockchain, Whistleblowing, Compliance, Bitcoin.

1. TECNOLOGÍA BLOCKCHAIN

1.1. Breve referencia histórica de Blockchain

La tecnología blockchain surge de la mano de Satoshi Nakamoto en una lista de correos electrónicos[1] iniciada el día 31 de octubre de 2008[2] en donde expone su trabajo denominado «Bitcoin: A Peer-to-Peer Electronic Cash System»[3] en el que no existen terceras partes de confianza, se previene el doble gasto, no existencia de casas de moneda, anonimidad de los participantes, creación de monedas desde un sistema de *proof of work* similar al Hashcash[4], entre otros.

Satoshi Nakamoto es el pseudónimo escogido por el programador (o programadores) que compartió con el mundo su brillante visión y el código para construir Bitcoin (BTC), así como la tecnología subyacente a dicha criptomoneda, el Blockchain.

De hecho, no fue hasta el día 16 de agosto de 2010[5] cuando Satoshi acuñó por primera vez el término «block chain» en el Bitcoin Forum creado posteriormente donde se reunía la comunidad atraída por este nuevo concepto de moneda digital.

---

[1] Se puede acceder a la lista completa a través del siguiente enlace: https://satoshi.nakamotoinstitute.org/emails/

[2] Disponible en: https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

[3] NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 de octubre de 2008. Disponible en: https://bitcoin.org/bitcoin.pdf

[4] La función de coste de CPU hashcash calcula un token que se puede usar como *proof of work*. Se pueden construir variantes interactivas y no interactivas de funciones de coste que se pueden utilizar en situaciones en las que el servidor puede emitir un desafío (protocolo interactivo orientado a la conexión), y donde no puede (donde la comunicación se almacena hacia adelante, u orientado en paquetes) respectivamente. Es decir, el objetivo de HashCash, es requerir un trabajo de computación para que este sea verificado. BACK, A., *Hashcash – A Denial of Service Counter-Measure*, 1 de agosto de 2002. Disponible en: http://www.hashcash.org/papers/hashcash.pdf

[5] Post original disponible en: https://bitcointalk.org/index.php?topic=841.msg9813#msg9813

El primer bloque de Bitcoin fue minado el 9 de enero de 2009[6], obteniendo como recompensa 50 BTC. En cuanto a la primera transacción dentro de la red Bitcoin, fue realizada el día 12 de enero del mismo año, desde la billetera de Satoshi Nakamoto a Hal Finney por valor de 10 BTC[7].

Hal Finney era programador informático, activo miembro del movimiento Cypherpunk[8] y uno de los programadores del código de Bitcoin desde sus inicios. Además, es el primer minero de Bitcoin (Aparte de Satoshi Nakamoto) como él mismo afirma en su publicación de 19 de marzo de 2013 del Bitcoin Forum[9]. Trágicamente, Finney fue diagnosticado con ELA en 2009 y estaba «esencialmente paralizado» cuando escribió esta publicación. Pero parecía estar en paz con su situación e interesado en cómo funcionaría la herencia de Bitcoins, escribiendo: «Mis bitcoins están almacenados en nuestra caja de seguridad, y mi hijo y mi hija son expertos en tecnología. Creo que son lo suficientemente seguros. Me siento cómodo con mi legado»[10]. Finney falleció el 28 de agosto de 2014 siendo criopreservado por Alcor Foundation como su paciente centésimo vigésimo octavo pagado a través de una combinación de su seguro de vida y donaciones de Bitcoins de sus admiradores[11].

Por su parte, la intención de Satoshi Nakamoto era desaparecer del escenario público como creador de Bitcoin con una publicación el

---

[6] Verificable en: https://blockchair.com/bitcoin/block/1 ; https://blockchain.coinmarketcap.com/block/bitcoin/1 ; https://explorer.viawallet.com/btc/block/000000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048?page=1

[7] Transacción con hash: f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16. Verificable en: https://blockchair.com/bitcoin/transaction/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 ; https://blockchain.coinmarketcap.com/tx/bitcoin/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 ; https://explorer.viawallet.com/btc/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

[8] Los cypherpunk son un grupo de personas que se dedican al activismo digital centrándose en proteger la privacidad y la seguridad de los usuarios digitales usando lo mejor que la criptografía puede ofrecer. *Cfr.* BIT2ME, «¿Qué es un Cypherpunk?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-un-cypherpunk/

[9] Disponible en: https://bitcointalk.org/index.php?topic=155054.0

[10] PETERSON, A., «Hal Finney received the first Bitcoin transaction. Here´s how he describes it», *The Washington Post*, 3 de enero de 2014. Disponible en: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?noredirect=on

[11] Más información en: https://www.alcor.org/2014/12/hal-finney-becomes-alcors-128th-patient/

día 12 de diciembre de 2010, en el ya mencionado foro indicando al comienzo que «hay más trabajo que hacer sobre DoS[12]».

Sin embargo, el 6 de marzo de 2014 la conocida revista norteamericana Newsweek publicaba un artículo titulado «The Face Behind Bitcoin»[13] donde se identificaba a Dorian Prentice Satoshi Nakamoto, un hombre japonés-americano residente de California que trabajó como ingeniero de sistemas de proyectos confidenciales de defensa y como ingeniero informático para empresas de tecnología e información financiera. Esta especulación provocó la reacción del supuesto real Satoshi Nakamoto publicando bajo este pseudónimo «I am not Dorian Nakamoto» en un blog titulado «Bitcoin open source implementation of P2P currency foro P2P foundation el día 7 de marzo[14], es decir, un día después de la publicación del artículo[15].

Puesto que Nakamoto y Finney ya no están entre nosotros, Bitcoin no ha tenido ninguna autoridad central o líder que pudiera determinar su dirección o ejercer influencia en el transcurso de su desarrollo. Incluso Gavin Andresen, que mantuvo un estrecho contacto con Nakamoto, y una de las caras más identificables de Bitcoin, ha fracasado repetidas veces en su intento de ejercer influencia sobre la dirección de la evolución de Bitcoin. A menudo se cita en la prensa un correo electrónico como el último enviado por Nakamoto, y que dice: «Estoy trabajando en otras cosas. Está en buenas manos con Gavin y el resto». Andresen ha intentado repetidas veces incrementar el tamaño de los bloques de Bitcoin, pero no ha conseguido consolidar

---

[12] Siglas de Denial of Service (ataque de denegación de servicio). En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio. OFICINA DE SEGURIDAD DEL INTERNAUTA, *¿Qué son los ataques doS y DDos?*, 21 de agosto de 2018. Disponible en: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

[13] GOODMAN, L.M., «The Face Behind Bitcoin», *Newsweek*, 6 de marzo de 2014. Disponible en: https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

[14] Disponble en: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186

[15] Advertir que recientemente, el día 24 de diciembre de 2021, este perfil ha publicado de nuevo lo siguiente: «After 13 years of decentralized payment systems evolution we came where we are now, the NFT epoch. You may find NFT of this post here» adjuntando un enlace a OpenSea, considerado el mercado más grande del mundo de arte digital basado en tecnología NFT. Sin embargo, la comunidad crypto está plenamente convencida de que se trata de un hackeo de esta cuenta personal en tanto que la clave pública de la billetera propietaria del mencionado NFT contiene una cantidad de 0.094710992777087179 Ether y únicamente ha tenido 6 transacciones en los días cercanos a la publicación de este mensaje.

ninguna de sus propuestas entre los operadores de nodos[16], a pesar de ser considerado por parte de la comunidad crypto como la persona más importante para el desarrollo de Bitcoin[17].

Finalmente, la primera transacción comercial de la historia de Bitcoin fue realizada por Laszlo Hanyecz el 22 de mayo de 2010 al intercambiar 10.000 BTC[18] por 2 pizzas cuatro días después de su publicación en el mencionado foro[19] pasando dicha fecha a conocerse como el Bitcoin Pizza Day.

1.2. Conceptos

A pesar de existir numerosas definiciones doctrinales sobre los siguientes conceptos, nos decantamos por los que, a nuestro juicio, se encuentran con un lenguaje sencillo y claro permitiendo su comprensión al lector medio sin conocimientos informáticos o técnicos.

Blockchain: Libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y de seguimiento de activos en una red de negocios. Un *activo* puede ser tangible (una casa, un auto, dinero en efectivo, terrenos) o intangible (propiedad intelectual, patentes, derechos de autor, marcas). Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de blockchain, reduciendo el riesgo y los costes para todos los involucrados[20].

Hash: Un hash es el resultado de una función hash, la cual es una operación criptográfica que genera identificadores únicos e irrepetibles a partir de una información dada[21].

---

[16] AMMOUS, S., *El Patrón Bitcoin. La alternativa descentralizada a los bancos centrales*, Deusto, Barcelona, 2018, p. 332.

[17] SIMONITE, T., «The Man Who Really Built Bitcoin», *MIT Technology Review*, 15 de agosto de 2014. Disponible en: https://www.technologyreview.com/2014/08/15/12784/the-man-who-really-built-bitcoin/

[18] Operación verificable en: https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d ; https://blockchair.com/bitcoin/transaction/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d ; https://explorer.viawallet.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

[19] Disponible en: https://bitcointalk.org/index.php?topic=137.0

[20] IBM, *¿Qué es la tecnología de blockchain?*. Disponible en: https://www.ibm.com/es-es/topics/what-is-blockchain

[21] *Cfr.* BIT2ME, «¿Qué es un hash?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-hash/

Nonce: Número arbitrario que se puede usar una única vez en una comunicación criptográfica[22].

Timestamp: El sellado de tiempo es otro elemento muy importante dentro de los bloques. Es un registro de la fecha y la hora, según el tiempo UTC que nos dice cuándo y a qué hora se generó un determinado bloque.

Criptografía asimétrica: También llamada criptografía de clave pública o criptografía de dos claves, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves solo se pueda generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves[23].

Nodo: La definición de un nodo puede variar significativamente según el contexto en el que se utiliza. Cuando se trata de redes informáticas o de telecomunicaciones, los nodos pueden ofrecer fines distintos, ya sea como un punto de redistribución o un punto final de comunicación. Por lo general, un nodo consiste en un dispositivo de red físico, pero hay algunos casos específicos en los que se usan nodos virtuales.

En pocas palabras, un nodo de red es un punto en el que se puede crear, recibir o transmitir un mensaje[24].

Aplicación descentralizada (DApp): Aplicación cuyo funcionamiento se basa en una red descentralizada de nodos interactuando unos con otros, de modo que las decisiones son tomadas por la comunidad y no por una organización central[25].

---

[22] SOLÉ, R., «Blockchain: una tecnología más allá de Bitcoin», *Profesional review*, 10 de julio de 2021. Disponible en: https://www.profesionalreview.com/2021/07/10/que-es-blockchain/#Caracteristicas_de_la_tecnologia_blockchain

[23] https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

[24] https://academy.binance.com/es/articles/what-are-nodes

[25] Autores como BARRIO ANDRÉS se posicionan en contra de esta nueva tecnología afirmando lo siguiente: «Si la tecnología *blockchain* se consolida, puede que tengamos que preguntarnos si preferimos vivir en un mundo en el que la mayoría de nuestras transacciones económicas e interacciones sociales están ordenadas por las normas jurídicas –que son generales y sometidas al control judicial pero también más flexibles y ambiguas y, por lo tanto, presentan defectos y a veces lagunas– o si preferimos rendirnos a las normas del código y al imperio de los algoritmos. Las aplicaciones descentralizadas basadas en blockchain pueden liberarnos de la tiranía

Contrato Inteligente (Smart Contract): Aplicaciones que operan como programas informáticos y se ejecutan a través del mecanismo de la cadena de bloques de forma descentralizada. Estos programas ejecutan acuerdos registrados entre dos o más partes, descentralizando la gestión de las partes involucradas, que no requieren un tercero para validarse. Consisten en un código de programación con el que las partes definen el objeto del contrato, las acciones que se pueden realizar sobre él y sus cláusulas de aplicación, que normalmente incluyen transacciones financieras. Éste se autoejecuta cuando se cumplen las condiciones previamente especificadas por acuerdo entre las partes[26].

1.3. Características de la tecnología Blockchain

Seguridad: Toda transacción se encuentra fuertemente encriptada, en el caso de Bitcoin por el sistema SHA-256[27], que protege y codifica la información garantizando su integridad. Las funciones hash son otro de los elementos que proporcionan seguridad a la cadena de bloques. Estos permiten generar identificadores únicos del contenido de los bloques[28].

Asimismo, toda transacción debe ser verificada por los nodos de la red Blockchain de forma que si se pretende realizar una transacción

---

de los intermediarios centralizados y de los Estados, pero esta liberación podría venir al precio de una amenaza mucho mayor, la de caer bajo el yugo de la tiranía del código y del algoritmo». BARRIO ANDRÉS, M., «'Blockchain': la amenaza de la tiranía del código y del algoritmo», *El País*, 19 de abril de 2018. Disponible en: https://elpais.com/retina/2018/04/17/tendencias/1523966659_640333.html

[26] MORALES BARROSO, J., *¿Qué es Blockchain?*, en GARCÍA MEXÍA, P., (Dir.), *Criptoderecho. La regulación de Blockchain*, Wolters Kluwer, Madrid, 2018, p. 59.

[27] Se trata de una función hash iterativa y unidireccional que puede procesar datos de entrada, como una cadena de texto o un archivo, para producir una representación condensada de longitud fija llamada digest. Este algoritmo determina de la integridad de los datos de entrada, es decir, cualquier cambio en los datos de entrada producirá un digest diferente. Esta propiedad es útil en la generación y verificación de firmas digitales y códigos de autenticación de mensajes, así como la generación de números aleatorios o bits. Los puntos que vienen a continuación detallan cada uno de los elementos que forman parte del algoritmo empleado en la función hash SHA-256, tales como variables, constantes y funciones, y también el desarrollo y explicación de las operaciones de lógica proposicional, ´algebra y operaciones con bits que se utilizan para obtener el mensaje digest adecuado. DOMÍNGUEZ GÓMEZ, J., *Criptografía: Función SHA-256*, agosto 2018. Disponible en: https://estudiobitcoin.com/wp-content/uploads/2020/09/Criptography_SHA_256_es.pdf

[28] *Cfr.* TECH ESPAÑA, «Características del blockchain», *School of engineering*, 29 de julio de 2022. Disponible en: https://www.techtitute.com/ingenieria/blog/las-caracteristicas-del-blockchain

falsa, no será aceptada ni subida a la red resultando fallida la operación. Es decir, si alguien pretende corromper la red, deberá modificar todos los datos almacenados en la mayoría de los nodos de la red. Podría haber millones y millones de personas, donde todos tengan la misma copia del registro. Acceder y hackear millones de computadoras es casi imposible y costoso[29].

De hecho, el coste de hardware para poder revertir cualquier operación en la red Bitcoin, a fecha de redacción del presente trabajo[30], sería de 32.439.250.205 Dólares americanos, consumiendo 446.039.690 kWh diarios equivalente a 22.301.985 Dólares por día[31]. Este fenómeno es el llamado ataque del 51%.

Trazabilidad: Es posible recorrer la cadena de bloques y trazar todas las operaciones que se han realizado sobre una determinada dirección; o retroceder en el tiempo y revisar las transacciones que se hicieron en una fecha determinada explorando todos los bloques generados en la fecha indicada.

Anonimidad: Las direcciones Blockchain no están ligadas a las identidades de las personas que las controlan. Para poder operar en una Blockchain pública es necesario disponer del par de claves pública y privada que permiten controlar la correspondiente billetera[32].

Transparencia: La transparencia en Blockchain se consigue publicando las reglas con las que se define su funcionamiento. Esto se logra haciendo público el código del software necesario para ejecutar Blockchain y generando una comunidad de nodos y desarrolladores que siguen este principio de transparencia.

---

[29] *Cfr.* RODRÍGUEZ, N., «6 Características Clave De La Tecnología Blockchain Que Debes Conocer!», *101 Blockchains*, 9 de enero de 2019. Disponible en: https://101blockchains.com/es/caracteristicas-tecnologia-blockchain/

[30] 19 de agosto de 2022.

[31] GOBITCOIN.IO, *Cost of a 51% attack*, 2022. Más información en: https://gobitcoin.io/tools/cost-51-attack/

[32] Recientemente, el Parlamento Europeo, a través de un comunicado de prensa, en el marco de su política de prevención de blanqueo de capitales y financiación del terrorismo, ha iniciado la tramitación parlamentaria para rastrear y eventualmente bloquear las transferencias sospechosas de aquél delito. Sin embargo, este bloqueo solamente será posible de realizar a través de entidades centralizadas y nunca en operaciones *onchain* como protocolos de finanzas descentralizadas (DEX) o conexiones *peer to peer* (P2P) debido a la naturaleza *permissionless* de Bitcoin y resto de criptomonedas en las redes blockchain. EUROPEAN PARLIAMENT, «Crypto assets: new rules to stop illicit flows in the EU», *News*, 31 de marzo de 2022. Disponible en: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

Inmutabilidad: La base tecnológica de la inmutabilidad se basa en el uso de algoritmos criptográficos que nos permiten garantizar y verificar la integridad de un conjunto de datos, es decir que dicho conjunto de datos no ha sido alterado desde su creación. Estos algoritmos tienen como objetivo crear una huella digital de un contenido, pero en ningún caso ocultar su información. Aplicados sobre un conjunto idéntico de datos, obtendrán siempre el mismo resultado, sin embargo, el más mínimo cambio variará por completo su huella. En otras palabras, una vez introducida la información dentro de la red blockchain nunca podrá borrarse. En caso de error, modificación o actualización, deberá emitirse una nueva operación posterior, integrándose en dicho libro de contabilidad dejando constancia plena de ello[33].

1.4. Los protocolos de consenso más utilizados en la actualidad

Proof of Work (PoW): También llamado protocolo de Prueba de Trabajo, es el más conocido y antiguo protocolo de consenso que consiste en que las partes de una red realicen con éxito un trabajo computacionalmente costoso para acceder a los recursos de dicha red. Este protocolo funciona bajo el concepto de requerir un trabajo al cliente, que luego es verificado por la red. Normalmente el trabajo solicitado, consiste en realizar complejas operaciones de cómputo.

Estas operaciones luego son verificadas por la red. Una vez que son aprobadas, se da acceso al cliente para que use los recursos de la misma. Con ello se busca impedir que clientes maliciosos puedan consumir todos los recursos de forma incontrolada. Una situación que puede acabar por denegar el servicio prestado al resto de clientes de la red.

Es el protocolo de consenso utilizado por la red Bitcoin y cada transacción se remite al resto de miembros de la red (nodos) para que sea verificada. Sin embargo, este proceso es muy costoso energéticamente hablando, teniendo en cuenta que el volumen de transacciones de la red Bitcoin no ha sido inferior a los 20 mil millones de dólares diarios en el último año. Este gasto en electricidad supone el 0.59% de la electricidad consumida en todo el mundo según un estudio rea-

[33] *Cfr.* FRANCO BLANCO, C., «¿Hacia un nuevo estándar democrático basado en la tecnología «Blockchain»?», *Confilegal*, 24 de diciembre de 2021. Disponible en: https://confilegal.com/20211224-hacia-un-nuevo-estandar-democratico-basado-en-la-tecnologia-blockchain/#_ftn3

lizado por la Universidad de Cambridge[34]. Ello ha provocado que la Unión Europea valorase las posibilidades de prohibir este tipo de protocolo de consenso debido a su contaminación[35], aunque finalmente, la Comisión de Asuntos Económicos y Monetarios (ECON) eliminó dicha prohibición[3637].

Sin embargo, desde nuestra opinión, gastar energía en asegurar y hacer funcionar un sistema de pago no es ninguna pérdida de tiempo. Como cualquier otro sistema de pago, el uso de Bitcoin conlleva costes de procesamiento. Servicios necesarios para el correcto funcionamiento de las monedas más extendidas mundialmente como los bancos, tarjetas de crédito y vehículos acorazados también necesitan mucha energía. Al contrario que Bitcoin, ese consumo de energía no es transparente y no puede ser medido.

El minado de Bitcoin fue diseñado para que se vuelva más optimizado con el tiempo debido a hardware especializado que consume menos energía, y así los costes operativos del minado deberían continuar siendo proporcionales a la demanda[38] De hecho, se estima que el 60% de la minería de Bitcoin utiliza energías renovables[39]

Proof of Stake (PoS): También conocido como Prueba de Participación, es un protocolo de consenso creado para reemplazar al conocido Proof of Work aportando una mejor seguridad y escalabilidad a las redes que lo implementen.

A los nodos que minan en PoS se les llama validadores. La decisión sobre qué nodo ha de validar un bloque se hace de forma aleatoria,

---

[34] *Cfr.* UNIVERSITY OF CAMBRIDGE, «Cambridge Bitcoin Elecrícity Consumption Index», *Centre for Alternative Finance*». Disponible en: https://ccaf.io/cbeci/index/comparisons

[35] SZALAY, E., «EU should ban energy-intensive mode of crypto mining, regulator says», *Financial Review*, 19 de enero de 2022. Disponible en: https://www.afr.com/world/europe/eu-should-ban-energy-intensive-mode-of-crypto-mining-regulator-says-20220119-p59plk

[36] *Cfr.* EUROPEAN PARLIAMENT, «Committee on Economic and Monetary Affairs», *Multimedia Centre*, 14 de marzo de 2022. Disponible en: https://multimedia.europarl.europa.eu/en/webstreaming/committee-on-economic-and-monetary-affairs_20220314-1345-COMMITTEE-ECON

[37] *Cfr.* HELMS, K., «EU Parliament Committee votes Against Proof-of-Work Ban, Supports Alternative Amendment on Crypto Assets», *Bitcoin.com*, 14 de marzo de 2022. Disponible en: https://news.bitcoin.com/eu-parliament-committee-votes-against-proof-of-work-ban-supports-alternative-amendment-on-crypto-assets/

[38] https://bitcoin.org/es/faq#que-es-bitcoin

[39] VENEGAS, E., «El Consejo Minero de Bitcoin señala que el 60% de la minería de BTC utiliza energías renovables», *Beincrypto*, 20 de julio de 2022. Disponible en: https://es.beincrypto.com/consejo-minero-bitcoin-senala-60-mineria-btc-utiliza-energias-renovables/

dando mayor probabilidad a quienes cumplan una serie de criterios. Entre estos criterios podemos mencionar la cantidad de moneda reservada (stake) y el tiempo de participación en la red, aunque pueden definirse otros. Una vez establecidos, se inicia el proceso de selección de nodos de forma aleatoria. Una vez terminado el proceso de selección, los nodos elegidos podrán validar transacciones o crear nuevos bloques. Los validadores son responsables de lo mismo que los mineros en la Proof of Work: ordenar transacciones y crear nuevos bloques para que todos los nodos puedan ponerse de acuerdo sobre el estado de la red.

La prueba de participación viene con una serie de mejoras en el sistema de prueba de trabajo: mejor eficiencia energética, no necesita usar muchos bloques de extracción de energía, barreras de entrada más bajas, requisitos de hardware reducidos al no necesitar hardware de élite para tener la oportunidad de crear nuevos bloques, mayor inmunidad a la centralización toda vez que debería conducir a más nodos en la red, mayor soporte para cadenas de fragmentos, etc[40].

En este sentido, la red Blockchain de Ethereum, actualmente la más grande y desarrollada del mundo cuya criptomoneda Ether (ETH) tiene una capitalización de mercado superior a 200 mil millones de Dólares, y recientemente ha sustituido su protocolo de consenso de Proof of Work a Proof of Stake a través de su actualización conocida como «The Merge» que representa la unión de la capa de ejecución existente de Ethereum con su nueva capa de consenso de Proof of Stake, la llamada Beacon Chain[41], reduciendo drásticamente la inflación de dicha criptomoneda.

En segundo lugar, PoS elimina el inmenso consumo de energía y el desperdicio de hardware asociado con PoW. Los investigadores estiman que el uso de energía de Ethereum se reducirá hasta en un 99,95%. Una pequeña fracción del hardware básico regular reemplazará el conjunto actual de ASIC y GPU que actualmente ejecutan el consenso de Ethereum. Estos dos efectos conducirán a un conjunto de participantes en el consenso más eficiente energéticamente, diverso, distribuido geográficamente y antifrágil.

En tercer lugar, Ethereum PoS prepara el escenario para la fragmentación, un cambio de protocolo igualmente significativo que se-

[40] *Cfr.* WACKEROW, P., «Proof-of-Stake», *Ethereumv Docs*, 26 de enero de 2022. Disponible en: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[41] *Cfr*. ETHEREUM, «The Merge», *Upgrades*, 18 de agosto de 2022. Disponible en: https://ethereum.org/en/upgrades/merge/#main-content

parará la cadena en muchos subprocesos concurrentes. El sharding[42] potencia los esfuerzos de escalamiento de L2 al aumentar el espacio de bloques disponible para la disponibilidad y liquidación de datos.

En cuarto lugar, las tarifas de prioridad de ETH que anteriormente iban a los mineros ahora se dirigen a una dirección controlada por validador en la capa de ejecución. Esto significa que el ETH es inmediatamente líquido. Dado que los retiros completos de ETH apostado (staked) solo se implementarán en la actualización de Shanghái a finales del próximo año, esta es una mejora significativa para los validadores con capital bloqueado[43].

Delegated Proof of Stake (DPoS): También llamado Prueba de Participación Delegada, es un protocolo de consenso diseñado para redes Blockchains altamente escalables.

Todos los participantes de la red eligen por votación, una serie de «delegados». Los delegados definen una rotación de líderes. Esto significa que cada delegado, tiene un turno dentro de la rotación para producir un bloque. Gracias a esta acción, dicho delegado puede generar un bloque y cobrar una recompensa por ello. Si el delegado no está disponible cuando llega su turno, debe esperar a uno nuevo.

El poder de voto de cada participante de la red es proporcional a su participación en la misma. Esta característica, es parte de su relación con el protocolo de consenso de Prueba de Participación. Para favorecer la descentralización, es habitual que las redes basadas en DPoS sometan a votación decisiones relacionadas con su funcionamiento. Temas como las recompensas, la cantidad de delegados el comportamiento ante bifurcaciones de la red y otras. Además de que

[42] Sharding es un mecanismo que se utiliza para particionar una red blockchain u otro tipo de red informática o base de datos. Su propósito es distribuir la carga de trabajo computacional y de almacenamiento de la red en un conjunto más amplio de dispositivos, o nodos, para aumentar el rendimiento y la velocidad de transacción de todo el sistema. Cada nodo solo mantiene información relacionada con su fragmento o partición específicos, y dado que cada nodo solo es responsable de procesar una fracción de la carga transaccional de la red general, las capacidades de procesamiento y la resiliencia generales de la red se pueden mejorar enormemente. Como resultado, las mayores velocidades de transacción que se hicieron posibles a través de la fragmentación han permitido que muchas redes basadas en blockchain sean exponencialmente más rápidas, más seguras y más adecuadas para el uso empresarial generalizado. GEMINI, «Sharding», *Cryptopedia*. Disponible en: https://www.gemini.com/cryptopedia/glossary#sharding

[43] https://trent.mirror.xyz/82eyq_NXZzzqFmCNXiKJgSdayf6omCW7BgDQIneyPoA

permiten penalizar a los delegados si no se comportan de acuerdo a lo esperado[44].

Las ventajas de este protocolo de consenso son, entre otros, que las monedas DPoS son mucho más escalables que las criptomonedas POW, ya que nunca comienzan a requerir una gran potencia informática y, en general, son accesibles para los usuarios con equipos deficientes; Las cadenas de bloques DPoS demostraron ser más rápidas que las cadenas de bloques basadas en PoW y PoS; Las monedas DPoS son más democráticas e inclusivas que sus alternativas; DPoS vs PoS ofrece más poder de gobierno a los usuarios con participaciones pequeñas, DPoS vs PoW no requiere tanto poder de cómputo y, por lo tanto, no es tan exigente financieramente para el usuario; Como el umbral para ingresar es muy bajo, DPoS se considera en gran medida como el enfoque más descentralizado para el mecanismo de consenso; DPoS es energéticamente eficiente y respetuoso con el medio ambiente; Las redes DPoS tienen una fuerte protección contra ataques de doble gasto[45].

1.5. Algunos casos de uso

Reserva de valor

En primer lugar, Bitcoin ha sido reconocido por la doctrina mayoritaria como una suerte de oro digital. Pero la comparación con el oro fue solo hasta cierto punto para explicar por qué Bitcoin terminó atrayendo tanta atención. Cada lingote de oro siempre ha existido independientemente de cualquier otro lingote. Los Bitcoins, por otro lado, fueron diseñados para vivir dentro de una red descentralizada inteligentemente construida, al igual que todos los sitios web del mundo existen solo dentro de la red descentralizada conocida como Internet. Al igual que Internet, la red Bitcoin no estaba a cargo de ninguna autoridad central. En cambio, fue construido y sostenido por todas las personas que conectaron sus computadoras a él, lo que cualquiera en el mundo podría hacer. Con Internet, lo que conectaba a todos juntos era un conjunto de reglas de software, conocido como el protocolo de Internet, que gobernaba cómo se movía la información.

[44] *Cfr.* BIT2ME, «¿Qué es DPoS?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-dpos/

[45] *Cfr.* BITCOINWIKI, *DPoS*. Disponible en: https://en.bitcoinwiki.org/wiki/DPoS

Bitcoin tenía su propio protocolo de software: las reglas que dictaban cómo funcionaba el sistema[46].

Por otro lado, se sitúa la naturaleza deflacionaria de este activo. Independientemente del número de usuarios de la red, del valor que llegue a alcanzar y de los avanzados que sean los equipos empleados para su producción, sólo pueden existir 21 millones de Bitcoins. No hay posibilidad técnica de incrementar la oferta para hacer frente al aumento de la demanda. De haber más gente interesada en Bitcoin, la única manera de responder a la demanda consiste en la revalorización de la oferta existente. Dado que un BTC es divisible en 100 millones de satoshis[47], hay margen de sobra para el crecimiento de Bitcoin mediante el uso de unidades cada vez más pequeñas a medida que aumenta su valor[48].

Los Bitcoin son creados durante la creación de cada bloque a una tasa fija y decreciente. Cada bloque, generado en promedio cada 10 minutos, contiene Bitcoins completamente nuevos, creados de la nada. Cada 210.000 bloques, o aproximadamente cada cuatro años, la tasa de emisión de divisas se reduce en un 50% (Halving). Durante los primeros cuatro años de funcionamiento de la red, cada bloque contenía 50 Bitcoins nuevos.

El 28 de noviembre de 2012, la nueva tasa de emisión de Bitcoins se redujo a 25 Bitcoins por bloque[49]. El 9 de julio de 2016 se redujo nuevamente a 12,5 Bitcoins por bloque[50]. El último halving hasta la fecha de publicación del presente trabajo tuvo lugar en el bloque 630.000 reduciendo la recompensa a la mitad nuevamente a los 6,25 Bitcoin[51]. La tasa de nuevas monedas disminuye así exponencialmente en 32 halvings hasta el bloque 6.720.000 (minado aproximadamente en el año 2137), cuando alcanza la unidad monetaria mínima de 1 satoshi. Finalmente, después de 6,93 millones de bloques, en aproximadamente 2140, se emitirán casi 2.099.999.997.690.000 satoshis, o casi 21 millones de Bitcoin. A partir de entonces, los bloques no con-

[46] POPPER, N., *Digital Gold. Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*, Harper, New York, 2016, p. 10.

[47] El satoshi es la unidad de cuenta más pequeña de Bitcoin. Por lo tanto, la fracción mínima de un único BTC es de ocho decimales, es decir, 0,00000001 BTC.

[48] AMMOUS, S., *El Patrón… Op. Cit.,* pp. 262 – 263.

[49] Verificable en: https://blockchair.com/bitcoin/block/210000

[50] Verificable en: https://blockchair.com/bitcoin/block/420000

[51] Verificable en: https://blockchair.com/bitcoin/block/630000

tendrán nuevos Bitcoins y los mineros serán recompensados únicamente a través de las tarifas de transacción[52].

Pagos internacionales instantáneos

Otra utilidad de la tecnología Blockchain, a través de las distintas criptomonedas, es la posibilidad de realizar pagos internacionales, sin tener que pagar elevadas comisiones por cambio de divisa, sin la necesidad de autorización de un tercero y de forma instantánea evitando retrasos de las entidades bancarias que pueden ser de incluso semanas. Para ello solamente sería necesario un dispositivo conectado a internet.

Un ejemplo de ello es RippleNet[53] que ha creado la única red global de bancos que envían y reciben pagos a través de la tecnología financiera distribuida de Ripple proporcionando mensajería instantánea, compensación y liquidación de transacciones. RippleNet es una red descentralizada basada en un acuerdo entre participantes de Ripple y de la red, todos los cuales utilizan la misma tecnología y adherirse a un conjunto consistente de reglas y estándares de pago. Los bancos de RippleNet se benefician de la conectividad sólida, la tecnología estandarizada y los datos adjuntos enriquecidos con cada pago. La tecnología financiera distribuida de Ripple supera la infraestructura actual al reducir los costes, aumentar las velocidades de procesamiento y brindar visibilidad integral de las tarifas de pago, el tiempo y la entrega[54].

También recientemente en el contexto de la guerra entre Rusia y Ucrania, hemos observado la utilidad de las criptomonedas basadas en tecnología blockchain como herramienta para realizar donaciones en Bitcoin, Ether, USDT y DOT a través de la red Ethereum y Polkadot[55] al estado ucraniano con la finalidad de recaudar fondos para apoyar a sus civiles y tropas[56].

---

[52] ANTONOPOULOS, A.M., *Mastering Bitcoin. Programming the Open Blockchain*, O'Reilly, California, 2017, p. 215.

[53] Más información en: https://ripple.com/#

[54] RIPPLE, *Solution Overview*. Disponible en: https://ripple.com/files/ripple_solutions_guide.pdf

[55] Disponible en: https://twitter.com/Ukraine/status/1497594592438497282

[56] *Cfr.* SARKAR, A., «Ucrania acepta donaciones en Bitcoin, Ethereum y USDT en medio de la guerra», *Cointelegraph*, 27 de febrero de 2022. Disponible en: https://es.cointelegraph.com/news/ukraine-accepts-bitcoin-ethereum-usdt-donations-to-fund-ongoing-war

Votaciones electrónicas:

Otros usos que se pueden beneficiar del Blockchain serían la votación electrónica, dado que queda garantizado el anonimato por medio de la criptografía de clave pública y resultaría imposible alterar el voto[57].

De igual modo se respetarían los principios de sufragio universal, libre, igual, directo y secreto gracias a las inherentes funcionalidades de la tecnología Blockchain de manera que cada persona sería propietario único de un token de gobernanza intransferible con el que se le otorgue el derecho a votar cuestiones como la elección de candidatos políticos a las Cortes o su postura sobre la toma de decisión en cuanto al desarrollo de una DApp, entre otras, desde cualquier lugar del mundo con un dispositivo que cuente con acceso a internet[58].

En este apartado también podemos hablar de las DAOs (*Decentralized Autonomous Organization*) u organizaciones autónomas descentralizadas como una forma efectiva y segura de trabajar con personas de ideas afines en todo el mundo.

Se trata de una especie de negocio nativo de Internet que es propiedad y está administrado colectivamente por sus miembros. Tienen fondos incorporados a los que nadie tiene la autoridad para acceder sin la aprobación del grupo. Las decisiones se rigen por propuestas y votaciones para garantizar que todos en la organización tengan voz.

Ejemplos de DAOs son una organización benéfica que puede aceptar membresía y donaciones de cualquier persona en el mundo y el grupo puede decidir cómo quiere gastar las donaciones; Una red de trabajadores independientes que puede crear una red de contratistas que reúnan sus fondos para espacios de oficina y suscripciones de software o; La creación de un fondo de riesgo que reúna el capital de inversión. El dinero reembolsado podría luego redistribuirse entre los miembros de la DAO[59].

---

[57] *Cfr.* PUYOL MONTERO, J. y FRANCO BLANCO, C., *Libro de test Delegado de Protección de Datos (DPO) Dominio III*, Tirant lo Blanch, Valencia, 2020, p. 102.

[58] *Cfr.* FRANCO BLANCO, C., «¿Hacia un nuevo estándar democrático basado en la tecnología «Blockchain»?», *Confilegal*, 24 de diciembre de 2021. Disponible en: https://confilegal.com/20211224-hacia-un-nuevo-estandar-democratico-basado-en-la-tecnologia-blockchain/

[59] *Cfr.* ETHEREUM, «Decentralized autonomous organizations (DAOs)», *Use Ethereum*. Disponible en: https://ethereum.org/en/dao/

Registro y almacenamiento de datos

Blockchain abre un nuevo paradigma respecto al intercambio y almacenamiento de los registros, construyendo un sistema en el que la información se descentraliza y los participantes comparten información al mismo nivel. Se asegura un intercambio de datos confiable, evitando que nadie sea el dueño del sistema[60].

A modo de ejemplo, ciertos países como Alemania, Reino Unido, Brasil o Japón, están avanzando en la implementación del registro de la propiedad a través de tecnología Blockchain, lo cual podría permitir solucionar problemas de trasparencia y, sobre todo, de ajuste real de lo que acontece en la realidad física y lo reflejado en la práctica registral. El objetivo sería contar con un registro de la propiedad cuya información estuviera sincronizada con la realidad física.

La tecnología Blockchain permite la tokenización de nuestros activos, es decir, la creación de un reflejo digital a través del cual operaríamos, incluso con nuestros bienes inmuebles mediante un contrato inteligente encargado de verificar automáticamente la titularidad de los inmuebles, ejecutar el pago y el registro del mismo a nombre del nuevo propietario[61].

Esta nueva posibilidad es actualmente posible gracias a la tecnología de los *Non Fungible Tokens* (NFT) donde los Registradores de la propiedad tendrán un papel vital en la verificación de la titularidad real de las propiedades. De este modo, a los NFTs, se les asigna una especie de certificado digital de autenticidad, una serie de metadatos incrustados en una red Blockchain que no se pueden modificar garantizando su autenticidad, registrando el valor de partida y todas las adquisiciones o transacciones que se hayan hecho, y también a su autor. Esto quiere decir que la compraventa de un contenido digital

[60] LARRAÑAGA PIEDRA, U., «Blockchain como solución a los problemas de trazabilidad y logística», *Izertis*, 22 de febrero de 2018. Disponible en: https://www.izertis.com/es/-/blog/blockchain-como-solucion-a-los-problemas-de-trazabilidad-y-logistica

[61] Aunque existen opiniones dispares en la doctrina que afirman que lo más probable es que el Blockchain termine siendo utilizado exclusivamente en el ámbito notarial como mecanismo tecnológico para el depósito público de escrituras, pero no para sustituir por completo a los Registros Públicos, desde nuestro punto de vista, nada obsta para una (necesaria) modificación normativa que digitalice a través de la tecnología Blockchain los Registros Públicos. *Cfr.* PERETE RAMÍREZ, C., *Blockchain, privacidad y protección de datos de carácter personal*, en GARCÍA MEXIA, P., (Dir.), *Criptoderecho. La regulación de Blockchain*, Wolters Kluwer, Madrid, 2018, pp. 196-197.

tokenizado con NFT, habrá constancia en todo momento del primer valor que tuvo, así como el valor de las sucesivas transmisiones[62].

Por lo tanto, coincidimos con GARCÍA-VALDECASAS RODRÍGUEZ DE RIVERA al afirmar que la figura del fedatario público no puede, ni debe, desaparecer toda vez que sigue habiendo cuestiones formales, procedimentales y notoriedad pública, que no pueden ser obviadas ni automatizadas a través de meras operaciones tecnológicas[63].

Desde un punto de vista técnico, Protocol Labs ha creado el denominado esquema de red de almacenamiento descentralizado (DSN[64]). Los DSN agregan almacenamiento ofrecido por múltiples proveedores de almacenamiento independientes y se coordinan a sí mismos para proporcionar almacenamiento y recuperación de datos a los clientes. La coordinación es descentralizada y no requiere partes de confianza toda vez que la operación segura de estos sistemas se logra a través de protocolos que coordinan y verifican las operaciones realizadas por partes individuales[65].

Otro ejemplo lo encontramos en Sia[66] como una plataforma de almacenamiento en la nube descentralizada que pretende competir con las soluciones de almacenamiento existentes, tanto a nivel P2P como empresarial. En lugar de alquilar almacenamiento de un proveedor centralizado, los pares de Sia alquilan almacenamiento entre sí. La propia Sia almacena solamente los contratos de almacenamiento formados entre las partes, definiendo los términos de su acuerdo[67].

2. CANAL DE INTERNO DE INFORMACIÓN

2.1. Definición

Atendiendo al origen etimológico del *whistleblowing*, podemos remontarnos a la práctica de los oficiales de policía británicos que

[62] FERNÁNDEZ, Y., «Qué son los NFT y cómo funcionan», *Xataka Basics*, 31 de marzo de 2022. *Cfr. https://www.xataka.com/basics/que-nft-como-funcionan*

[63] *Cfr*. GARCÍA-VALDECASAS RODRÍGUEZ DE RIVERA, P, *Blockchain y automatización de procedimientos en la Administración Pública*, Wolters Kluwer, Madrid, 2022, pp. 186 – 187.

[64] Acrónimo de *Decentralized Storage Network*.

[65] PROTOCOL LABS, *Filecoin: A Decentralized Storage Network*, 19 de julio de 2017, p. 8. Disponible en: https://filecoin.io/filecoin.pdf

[66] Más información en: https://sia.tech/

[67] VORICK, D. y CHAMPINE, L., *Sia: Simple Decentralized Storage*, 29 de noviembre de 2014, p. 1. Disponible en: https://sia.tech/sia.pdf

hacían sonar sus silbatos (*whistle*) soplando (*blow*), cuando presenciaban la comisión de un delito[68].

El concepto de *whistleblowing* surge de la mano de NADER definiéndolo como «*aquel acto de un hombre o una mujer que, creyendo que el interés público es superior al interés de la organización a la que sirve, toca el silbato que alerta de que la organización está realizando actividades corruptas, ilegales, fraudulentas o perjudiciales*»[69].

QUICK define el *whistleblowing como la divulgación por antiguos o actuales miembros de la organización de prácticas ilegales, ilegítimas o inmorales a personas o autoridades con la capacidad de tomar medidas correctivas para abordar dichas irregularidades*[70].

Por su parte, VAGADIA señala que *whistleblowing* es el término utilizado cuando un empleado eleva una preocupación sobre un posible fraude, crimen, peligro u otros riesgos serios que pueden amenazar a los clientes, compañeros de trabajo, accionistas, el público o la propia reputación de la organización[71].

GÓMEZ MARTÍN y TURIENZO FERNÁNDEZ entienden que el canal de cumplimiento normativo, o líneas de *whistleblowing*, representan el medio por excelencia a través del cual los integrantes de la corporación van a informar al responsable del modelo de prevención delictiva acerca de aquellas circunstancias presuntamente delictivas alertadas. La organización debería ocuparse de asegurar que a todos los integrantes de la corporación les alcance la máxima «si ves algo, di algo»[72].

---

[68] *Cfr.* PÉREZ BASTARDO, S., «Creación de un canal de denuncias y cumplimiento de la normativa vigente en materia de protección de datos», *Legal Today*, 20 de septiembre de 2021. Disponible en: https://www.legaltoday.com/opinion/blogs/nuevas-tecnologias-blogs/blog-prodat/creacion-de-un-canal-de-denuncias-y-cumplimiento-de-la-normativa-vigente-en-materia-de-proteccion-de-datos-2021-09-20/

[69] NADER, R., (Ed.), *Whistleblowing. The report of the Conference on Professional Responsibility*, Penguin Group Incorporated, USA, 1974, pp. 174 y ss.

[70] QUICK, R., *Whistleblowing*, en IDOWU, S.O., CAPALDI, N., FIFKA, M.S., ZU, L. y SCHMIDPETER, R., (Eds.), *Dictionary of Corporate Social Responsibility. CSR, Sustainability, Ethics and Governance*, Springer, Cham, Heidelberg, New york, Dordrecht, London, 2015, p. 579.

[71] VAGADIA, B., *Enterprise Governance. Driving Enterprise Performance Through Strategic Alignment*, Springer-Verlag Berlin Heidelberg, 2014, p. 233.

[72] *Cfr.* GÓMEZ MARTÍN, V. y TURIENZO FERNÁNDEZ A., *Elementos esenciales de los modelos de prevención de delitos,* en CORCOY BIDASOLO, M. y GÓMEZ MARTÍN, V., (Dirs.), *Derecho penal económico y de empresa. Parte general y parte especial. Doctrina y jurisprudencia con casos solucionados. Tomo 2,* Tirant lo Blanch, Valencia, 2020, p. 182.

Otros autores como ENSEÑAT DE CARLOS lo definen como un canal de comunicación directo para que los empleados, clientes o proveedores puedan denunciar el incumplimiento tanto de normas internas como de otras regulaciones que rigen la actividad de la organización, y constituye la mejor forma de hacer efectivo su gobierno corporativo[73].

SIMÓN CASTELLANO indica que la denuncia de irregularidades se diseña como un mecanismo de control adicional para que los empleados informen de malas conductas de manera interna, evitando «males mayores» para todas las partes implicadas[74].

Acorde a la anterior conceptualización aborda el término la INTERNATIONAL ORGANIZATION FOR STANDARDIZATION[75] en su norma ISO 37002:2021[76] definiendo la denuncia de irregularidades en su capítulo 3.10 como aquella *información sobre sospechas de irregularidades o irregularidades reales aportadas por un denunciante*.

La Directiva *whistleblower* realiza una distinción entre la denuncia interna, que será aquella comunicación verbal o por escrito de información sobre infracciones dentro de una entidad jurídica de los sectores privado o público, y externa que la define como la comunicación verbal o por escrito de información sobre infracciones ante las autoridades competentes.

Finalmente, desde nuestra perspectiva podemos entender el canal interno de información como aquel mecanismo interno de una organización, pública o privada, que permite a su personal y a toda persona vinculada a ella (*stakeholders*), trasladar a los órganos encargados de velar por el cumplimiento normativo las posibles irregularidades e incumplimientos de la legislación o normativa interna en el marco de su actividad.

2.2. Situación actual

La Unión Europea comenzó a preocuparse seriamente de los canales de denuncia en el año 2015 y por medio de la figura del Defensor

[73] ENSEÑAT DE CARLOS, S., *Manual del Compliance Officer. Guía Práctica para los responsables de Compliance de habla hispana,* Thomson Reuters Aranzadi, Cizur Menor, 2016, p. 49.

[74] SIMÓN CASTELLANO, P., «Canales de denuncia: Entre la obligación y la oportunidad», *Font Advocats*, 20 de noviembre de 2020. Disponible en: https://www.fontadvocats.com/articulo-canales-de-denuncia-entre-la-obligacion-y-la-oportunidad/

[75] Más información en: https://www.iso.org/home.html

[76] Disponible en: https://www.iso.org/obp/ui/#iso:std:iso:37002:ed-1:v1:en

del Pueblo Europeo[77]. Aunque no es hasta el año 2019 en que el Parlamento Europeo y el Consejo, después de casi cuatro años, promulgan la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, también denominada Directiva *whistleblower*, en la que se garantiza, entre otras cuestiones, un alto nivel de protección para los denunciantes de violaciones de la legislación de la Unión Europea.

En este sentido, los Estados miembros tienen libertad para ampliar estas normas a otros ámbitos. La Comisión alienta a los Estados miembros a que establezcan amplias estructuras basadas en los mismos principios en materia de protección de los denunciantes de infracciones. En el ámbito interno, y tras un largo periplo parlamentario[78], el legislador español ha elaborado la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión donde se constituyen los siguientes extremos:

— Amplio ámbito material: El ámbito objetivo de la Directiva *whistleblower*, se incorporan todas aquellas acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.

— Procedimientos y obligaciones de información claros para los empleadores: las nuevas normas establecen un sistema de cauces de denuncia seguros dentro de las propias organizaciones y en el contexto de la comunicación con las autoridades públicas.

— Cauces seguros de comunicación: se anima a los informantes a que comuniquen primero a nivel interno si la infracción que desean revelar puede tratarse de manera eficaz dentro de su propia organización y siempre y cuando no estén expuestos a represalias. También pueden informar directamente a las au-

[77] Más información en: https://www.ombudsman.europa.eu/es/make-a-complaint

[78] La tardanza en la publicación de la citada norma ha supuesto que la Comisión Europea ha notificado en fecha 27 de enero de 2022 la apertura del expediente INFR(2022)0073 al estado español por el incumplimiento de la transposición de la Directiva *Whistleblower* en atención a lo dispuesto en los artículo 258 y 260 TFUE. *Cfr.* COMISIÓN EUROPEA, «La Comisión Europea decide llevar a ocho Estados miembros ante el Tribunal de Justicia de la UE en relación con la protección de los denunciantes de irregularidades», *Comunicado de prensa*, 15 de febrero de 2023. Disponible en: https://ec.europa.eu/commission/presscorner/detail/ES/IP_23_703

toridades competentes si lo consideran oportuno, en función de las circunstancias del caso. Además, si tras la denuncia a las autoridades no se toman las medidas oportunas o si existe peligro inminente o manifiesto para el interés público, o cuando la denuncia a las autoridades no surta efecto, debido, por ejemplo, a que dichas autoridades se hallan en connivencia con el autor de la irregularidad, los informantes pueden divulgar la información, también a los medios de comunicación.

— Prevención de represalias y protección eficaz: las normas protegerán a los informantes frente al despido, la degradación y otras formas de represalia. También exigirán a las autoridades nacionales que informen a los ciudadanos sobre los procedimientos de denuncia de infracciones y la protección a la que pueden acogerse. Los informantes también gozarán de protección en los procedimientos judiciales[79].

— Creación de la Autoridad Independiente de Protección del Informante: entre cuyas funciones se encuentra la gestión del canal externo de comunicaciones, la adopción de las medidas de protección al informante, la elaboración de informes preceptivos en los anteproyectos y proyectos de disposiciones generales que afecten a su ámbito de competencias, la tramitación del procedimiento sancionador y la imposición de sanciones y, finalmente, el fomento y la promoción de la cultura de la información.

— Régimen sancionador aplicable tanto para el sector público como privado: Una de las cuestiones que nos ha llamado gratamente la atención consiste en la posibilidad de imposición de sanciones a la Administración Pública. De este modo se está inculcando una cultura de *Compliance* a través del conocido *Tone at the top*[80].

— Ausencia de recompensas económicas a favor del informante: A pesar que se trataba de una posibilidad remota tomada del Derecho comparado[81], sí que se ha incluido una suerte de pro-

[79] https://www.cissCompliancefiscal.com/documento.php?id=EX0000143344_20190326.html

[80] El *tone at the top* es un componente básico del marco de control interno COSO 2013, y su importancia ha sido destacada por recientes fracasos comerciales de alto perfil y fraudes perpetrados por la alta dirección. *Cfr.* ONWURA NZECHUKWU, P., *Internal Audit Practice from A to Z*, Taylor & Francis Group, Boca Ratón, 2017, p. 78.

[81] Véase la *False Claims Act*, la *Dodd-Frank Act* o la *IRS Whistleblower Law* estadounidenses que establecen una recompensa a los informantes de entre el 10 y el 30 por ciento de las sanciones monetarias recuperadas.

grama de clemencia en su artículo 40 que permite la exención o atenuación de las sanciones administrativas que hubiesen cometido los informantes.

Por otro lado, desde las Comunidades Autónomas se han elaborado distintas Leyes que, bajo el pretexto de combatir el fraude y la corrupción, han creado canales de denuncia propios como por ejemplo la Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears, la Ley 11/2016, de 28 de noviembre, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, la Ley Foral 7/2018, de 17 de mayo, de creación de la oficina de buenas prácticas y anticorrupción de la Comunidad Foral de Navarra, la Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés, del Principado de Asturias o la más reciente Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante.

2.3. Características y elementos esenciales del canal interno de información

Según la Directiva *whistleblower* ya citada, se crean tres tipos de mecanismos para denunciar hechos ilícitos de los que una persona tenga constancia en el seno de una organización. Se trata de un triple nivel de denuncia (interno —art. 7 y ss.—, externo —art. 10 y ss.—, y de revelación pública —art. 15—) que, aunque no puede evitar el carácter universalmente público de poner los hechos punibles en conocimiento de Jueces, Fiscales y Policías (arts. 7.2 Directiva whistleblower y arts. 259 y 262 LECrim), acentúa el nivel de exigencia en los realizados tanto por las entidades jurídicas privadas como en las públicas[82].

Desde el ámbito interno, la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción sigue el esquema establecido por la Directiva, diferenciando entre el sector público y privado respecto del canal de denuncias interno, el canal de denuncias externo que será competencia exclusiva de la eventual Autoridad Independiente de Protección del Informante, o las autoridades inde-

[82] VELASCO NÚÑEZ, E., *10 años de responsabilidad penal de la persona jurídica (análisis de su jurisprudencia)*, Aranzadi, Cizur Menor, 2020, p. 141.

pendientes que se constituyan al efecto en las distintas Comunidades Autónomas[83].

Como bien expone la STS 35/2020, de 6 de febrero,[84] citando la Directiva *whistleblower*, *los canales de denuncia deben permitir que las personas denuncien por escrito y que lo puedan hacer por correo, a través de un buzón físico destinado a recoger denuncias o a través de una plataforma en línea, ya sea en la intranet o en internet, o que denuncien verbalmente, por línea de atención telefónica o a través de otro sistema de mensajería vocal, o ambos.... Los procedimientos de denuncia interna deben permitir a entidades jurídicas del sector privado recibir e investigar con total confidencialidad denuncias de los trabajadores de la entidad y de sus filiales (en lo sucesivo, «grupo»), pero también, en la medida de lo posible, de cualquiera de los agentes y proveedores del grupo y de cualquier persona que acceda a la información a través de sus actividades laborales relacionadas con la entidad y el grupo.*

En cuanto a los elementos esenciales de un canal interno de información enmarcamos los siguientes:

La comunicación

Evidentemente, todo procedimiento a través de un canal interno de información debe comenzar con este acto fundamental por el cual se pondrán de manifiesto al órgano competente en materia de cumplimiento normativo la comisión de hechos irregulares. Las comunicaciones podrán ser confidenciales o anónimas a elección exclusiva del informante y, en caso de que no se disponga nada, será confidencial por defecto.

Como ya se ha expresado, los medios mínimos por los que se puede informar son el correo electrónico o postal, página web (intranet), llamada telefónica, aplicación móvil (en su caso), sistemas de grabación de voz y presencialmente. La presentación de la denuncia a través de una DApp se considera como adicional pero no imprescindible.

[83] En este sentido, reviste particular importancia la Ley 3/2023, de 16 de marzo, de medidas fiscales, financieras, administrativas y del sector público para el 2023 de Cataluña que, en su disposición adicional séptima asigna a la Oficina Antifraude de Cataluña las funciones de protección de los informantes, el ejercicio de la potestad sancionadora así como proceder a la ejecución forzosa de las resoluciones sancionadoras.

[84] Roj: STS 272/2020 - ECLI:ES:TS:2020:272.

Análisis preliminar

Tras la interposición de la comunicación inicial, el órgano competente deberá adoptar alguna de las siguientes posibilidades:

— Inadmitir la comunicación, en el supuesto de que los hechos carezcan de toda verosimilitud, no sean constitutivos de infracción del ordenamiento jurídico, carezca manifiestamente de fundamento o existan indicios de que la información comunicada se ha obtenido mediante la comisión de un delito y cuando la comunicación no contenga información nueva y significativa.

— Admitir a trámite la comunicación y proceder a la investigación de los hechos.

— Remitir, con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito.

— Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación.

La investigación

Una vez superado ese análisis preliminar, será imprescindible realizar una investigación sobre los hechos comunicados con el fin de corroborar aspectos procedimentales, como la competencia, legitimación o procedimiento adecuado, así como cuestiones de fondo que verifiquen los hechos irregulares. Asimismo y como no puede ser de otro modo, durante todo el procedimiento deberán respetarse los derechos fundamentales de los intervinientes según establece la doctrina *Drittwirkung*[85], en particular, el derecho de defensa del denunciado, su presunción de inocencia y confidencialidad de las actuaciones[86].

[85] La doctrina Drittwirkung se trata de un concepto originario del Derecho constitucional alemán que ejemplifica la idea de que la constitución implica obligaciones legales sobre las interacciones de Derecho privado de las personas privadas en sus relaciones *inter se*. *Cfr.* ENGLE, E., «Third Party Effect of Fundamental Rights (*Drittwirkung*), *European Law / Europarecht*, 2009, p. 165.

[86] *Cfr.* PUYOL MONTERO, J., *El funcionamiento práctico del canal de compliance «whistleblowing»,* Tirant lo Blanch, Valencia, 2017, pp. 56 – 59.

Conclusión del procedimiento

El expediente que contenga la investigación realizada, deberá darse traslado al órgano competente para su resolución. Las resoluciones podrán consistir en el archivo de las actuaciones, sanción disciplinaria laboral, despido disciplinario o traslado de las actuaciones al Ministerio Fiscal con el objeto de que inicie su propia investigación poniendo a su disposición todos los recursos de la organización para el completo esclarecimiento de los hechos indiciariamente delictivos.

Tras la emisión de la resolución, será primordial realizar una monitorización de las decisiones adoptadas de modo que se garantice el cumplimiento de las medidas, así como un proceso de mejora continua tal y como se establece en los apartados 9 y 10 de la UNE-ISO 37002 relativa a los sistemas de gestión de la denuncia de irregularidades[87].

Protección del informante

El temor a las represalias está a menudo bien fundado. La encuesta de *Global Business Ethics Survey* de 2016[88] realizada a más de 10 000 trabajadores en los sectores privado, público y sin ánimo de lucro en trece países arrojó que el 33% de los trabajadores habían tenido conocimiento de faltas; el 59% de ellos las denunciaron, y el 36% de éstos sufrieron represalias. Además de las represalias deliberadas y acciones laborales adversas, los informantes han experimentado la aparición de impactos colaterales informales como el estrés y el aislamiento[89].

Una mejor protección de los informantes puede resultar beneficiosa para la vida diaria y el bienestar de todos los ciudadanos europeos al ayudar a prevenir riesgos graves para el interés público que pueden extenderse más allá de las fronteras nacionales.

Por su sólida y extensa base empírica, cabe destacar el trabajo de campo liderado por la Universidad de Griffith de Queensland centra-

[87] UNE-ISO 37002. Sistemas de gestión de la denuncia de irregularidades. Directrices, octubre 2021, pp. 42 – 47.

[88] ETHICS & COMPLIANCE INICIATIVE, *Global Business Ethic Survey, Measuring Risk and Promoting Workplace Integrity*, 2016. Disponible en: http://www.boeingsuppliers.com/2016_Global_Ethics_Survey_Report.pdf

[89] *Cfr.* BROWN, A.J., LAWRENCE, S.A. y OLSEN, J., *Why protect whistleblowers? Importance versus treatment in the public & private sectors*, en BROWN, A.J., (Ed.), *Whistleblowing: New Rules, New Policies, New Vision.,* Griffith University, Brisbane, 2018, p. 45.

do en el ámbito territorial de Australia y Nueva Zelanda. Este estudio abarca el periodo 2016-2018 y se basa en un total de casi 18.000 respuestas individuales sobre *whistleblowing* en organizaciones públicas, privadas y del tercer sector. Entre sus hallazgos más significativos destaca que prácticamente el 82% de los informantes han sufrido consecuencias negativas derivadas de sus revelaciones. La mayoría provienen de sus superiores (en menor medida de los compañeros), prevaleciendo las de carácter informal tales como el estrés o el aislamiento. El estudio revela, igualmente, un patrón consistente en que quienes sufren más las consecuencias negativas de ser alertadores son los empleados de base frente a los de mayor rango jerárquico[90].

En relación a este aspecto, la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión engloba en su Título VII las medidas de apoyo a los informantes que podrán consistir en asesoramiento integral sobre procedimientos y recursos disponibles, asistencia efectiva frente a represalias y apoyo financiero y psicológico aunque solamente de forma excepcional tras la valoración de las circunstancias del caso. También se establece un programa de clemencia por el que facultativamente y mediante decisión motivada por el Juez, se podrá eximir al informante del cumplimiento de la sanción administrativa que le correspondiera.

3. TECNOLOGÍA BLOCKCHAIN APLICADA AL CANAL INTERNO DE INFORMACIÓN

El uso de la criptografía y mecanismos de consenso distribuido Blockchain proporciona la combinación única de mantenimiento de registros permanentes y a prueba de manipulaciones, transparencia y auditabilidad de transacciones automatizadas con *Smart contracts*, y la reducción de una autoridad centralizada y propiedad de la información dentro de sus procesos. Estas propiedades hacen de Blockchain una tecnología emergente de alto potencial para abordar la investigación de irregularidades en toda organización pública o privada[91].

[90] PARRAMÓN BREGOLAT, L. y ROCA SAFONT, Ó., *Alertadores de la corrupción… Op. Cit.*, pp. 126 – 127.

[91] *Cfr.* WORLD ECONOMIC FORUM, *Exploring blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*, Cologny/Geneva, 2020, p. 4.

La aplicación de la tecnología Blockchain al ámbito del canal interno de información de una organización puede realizarse de dos maneras aunque, desde nuestro punto de vista, solamente una de ellas es viable económica y técnicamente:

Crear una red Blockchain

En primer lugar, desde nuestro punto de vista la creación de una red Blockchain comporta un desproporcionado gasto de recursos humanos, técnicos y financieros a la organización.

Por otro lado, el eje fundamental de las redes Blockchain consiste en su descentralización de modo que permita operaciones sin autorización de una tercera parte. En el caso de la creación de una red blockchain propia de una única organización, surge el problema de quiénes van a ser los nodos validadores de las transacciones que, en el caso de estar comprendidos en la organización, poco diferiría de los servidores centralizados actuales.

Desarrollar una aplicación descentralizada en una red Blockchain

A modo introductorio, este tipo de aplicaciones tienen su código de backend (contratos inteligentes) ejecutándose en una red descentralizada y no en un servidor centralizado. Utilizan la cadena de bloques para el almacenamiento de datos y contratos inteligentes para su lógica de aplicaciones.

Un contrato inteligente es como un conjunto de reglas que viven en cadena para que todos vean y ejecuten exactamente de acuerdo con esas reglas. Imagine una máquina expendedora: si le suministra suficientes fondos y hace la selección correcta, obtendrá el artículo que desee. Y al igual que las máquinas expendedoras, los contratos inteligentes pueden mantener fondos de la misma manera que su billetera. Esto permite que el código medie en acuerdos y transacciones.

Una vez que las DApps están desplegadas en la red Blockchain, no puede cambiarlas. Las DApps pueden descentralizarse porque están controladas por la lógica escrita en el contrato, no por un individuo o por una empresa.

Tras lo expuesto, es evidente que la creación de una aplicación descentralizada es la única opción factible de uso de tecnología Blockchain en el canal interno de información desde el punto de vista de

la organización, siempre y cuando se desarrolle adecuadamente con los propósitos pretendidos.

3.1. Principales ventajas

Cero tiempo de inactividad: Una vez que el contrato inteligente esté implementado en el núcleo de la aplicación y sobre la Blockchain, la red como conjunto siempre será capaz de servir a los usuarios que pretendan interactuar con el contrato interponiendo una comunicación. Por lo tanto, los actores maliciosos no pueden lanzar ataques de denegación de servicio (DDoS) dirigidos hacia las DApps individuales.

Resistencia a la censura: Ninguna entidad en la red u organización puede bloquear a los usuarios a la hora de enviar transacciones y comunicaciones o leer los datos desde la Blockchain.

Integridad completa de los datos: Los datos almacenados en la Blockchain son inmutables e indisputables, gracias a las primitivas criptográficas. Los actores maliciosos, como los denunciados, no pueden falsificar las transacciones, hechos comunicados u otros datos que ya se hayan hecho públicos.

Informática sin confianza/Comportamiento verificable: Los contratos inteligentes se pueden analizar y están garantizados para ejecutarse de manera predecible, sin la necesidad de confiar en una autoridad central. Esto no se aplica en los modelos tradicionales; por ejemplo, cuando utilizamos un servicio de almacenamiento en la nube, tenemos que confiar en que las organizaciones que prestan estos servicios no utilizarán nuestra información, manipularán nuestros registros o nos atacarán[92].

3.2. Principales desventajas

Necesidad: El principal problema lo encontramos en la obsesión por la tecnología blockchain, ejemplo actual de la «ciencia del culto a la carga» expuesta por FEYNMAN en los años 70[93]. No existe ninguna necesidad en descentralizar el almacenamiento de datos de las co-

[92] *Cfr.* SMITH, C., «Introducción a las DApps», *Documentos Ethereum*, 8 de febrero de 2022. Disponible en: https://ethereum.org/es/developers/docs/dapps/#benefits-of-dapp-development

[93] FEYNMAN, R.P., «Cargo Cult Science», *Engineering and Science*, june 1974, vol 37, 7, pp. 110 – 13.

municaciones siempre que se tenga en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo[94].

Por ello, una solución centralizada, segura y sencilla en su utilización en el seno de la organización cumplirá eficazmente los objetivos propuestos.

Transparencia: A pesar de la frecuente concepción de las virtudes de la transparencia en los asuntos de utilidad pública, debemos mostrar nuestro rechazo a la misma cuando se dirimen supuestos hechos irregulares e incluso conductas delictivas en el seno de cualquier organización.

De este modo, cualquier persona con acceso a la DApp podría tener conocimiento de los hechos comunicados y del expediente completo de manera que se vulneraría la confidencialidad de las actuaciones, así como la posible revelación de secretos comerciales, entre otras muchas cuestiones.

Cumplimiento normativo: Las redes Blockchain con su propia moneda, existen ortogonalmente a la Ley; no hay casi nada que pueda hacer una autoridad gubernamental para afectar o alterar su funcionamiento[95]. Sin embargo, la creación de una aplicación descentralizada cuyo propósito consista en presentar comunicaciones por irregularidades al amparo de la Directiva *whistleblower*, se topará con la imposibilidad de aplicar los artículos 5.1.b) y e), 17 y 18, entre otros, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), relativos al principio de limitación de la finalidad y plazo de conservación, al derecho de supresión, también llamado derecho

[94] Véase el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, relativo a la seguridad del tratamiento de datos personales.

[95] El presidente de la Reserva Federal de Estados Unidos ha manifestado que carece de autoridad para regular Bitcoin. *Cfr.* RUSSOLILLO, S., «Yellen on Bitcoin: Fed Doesn't Have Authority to Regulate It in Any Way», *The Wall Street Journal*, 27 de febrero de 2014. Disponible en: https://www.wsj.com/articles/BL-MBB-17195

al olvido y la limitación del tratamiento, pues una vez subida la información a la red Blockchain permanecerá inmutable y disponible para sus usuarios. Asimismo, cabe recordar que no existe la figura de responsable ni encargado del tratamiento[96] al tratarse de redes descentralizadas *permissionless*[97].

Del mismo modo, resulta de imposible aplicación lo dispuesto en el artículo 32.4 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, que dispone la obligatoriedad de supresión de los datos del sistema interno de información una vez transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, es decir la propia DApp.

Desde el aspecto constitucional, sería de compleja adecuación la presentación de comunicaciones de hechos irregulares con los artículos 18, 24 de la Constitución Española relativos al derecho a la intimidad y el secreto de las comunicaciones, y el derecho de defensa, así como la presunción de inocencia, respectivamente.

Irreversibilidad: Los pagos, contratos o bases de datos, las denuncias, los errores humanos o de software, en una Blockchain una vez se ha confirmado el bloque y se unen nuevos bloques, sólo será posible revertir alguna de sus transacciones reuniendo el 51% de la capacidad de procesamiento de la red y haciéndola retroceder hasta donde todos estos nodos acuerdan pasarse al mismo tiempo a una blockchain modificada, y esperando que el otro 49% no quiera poner en marcha su propia red y se una a la nueva. Cuanto mayor sea la red, más difícil resulta revertir una transacción incorrecta. Por el contrario, una blockchain que sea alterable es un absurdo ejercicio de sofisticación técnica desde el punto de vista funcional: utiliza un complejo y costoso método de autorización para eliminar a los intermediarios y establecer inmutabilidad, pero luego concede a un intermediario la capacidad de revocar dicha inmutabilidad[98]. Por esta razón, resulta

[96] Excepto en las personas físicas o jurídicas que realicen tratamiento de datos en su propias DApps, siempre y cuando no sea de aplicación lo dispuesto en el artículo 11 RGPD relativo al tratamiento de datos que no requiere identificación.

[97] Véase BLOCKCHAIN BUNDESVERBAND, *Blockchain, data protection, and the gdpr*, Berlin, 2018. Disponible en: https://bundesblock.de/bundesblock-releases-position-paper-on-gdpr-blockchain-and-data-protection/

[98] Sin embargo, debemos traer a colación el caso de Ethereum y The DAO. En julio de 2016, tras advertir un error de programación, un grupo de usuarios consiguieron retirar 11.5 millones de Ether. Este hecho ocasionó una gran controversia en el mundo crypto que desembocó en un *hard fork* de Ethereum aprobado por la mayoría de la comunidad donde se revirtió el ataque y devolvió a los usuarios los fondos robados

habitual referirse en el ciberespacio al código informático como la ley que rige las relaciones de los usuarios[99].

Alternatividad: La creación de una aplicación descentralizada para interponer denuncias internas en una organización no debe impedir la presentación de comunicaciones por otros medios alternativos como, por ejemplo, telefónicamente, a través de la intranet o internet, mediante correo electrónico o postal e incluso presencialmente.

Claves públicas[100]: La taxonomía del cifrado de clave pública, expuesto anteriormente, supone el anonimato del usuario propietario de dicha dirección pública, sin limitación para crear estas direcciones de modo que la organización desconoce por completo quién interpone la comunicación. Ello supone ciertos problemas.

— Las comunicaciones confidenciales o que el informante desee incluir su identidad, estará perdiendo su anonimidad futura con relación a esa dirección.

— Relacionado con el anterior, si una misma dirección pública comunica unos hechos distintos con posterioridad, podría acotarse su ámbito facilitando su identificación.

— Una misma persona, podría utilizar la capacidad de crear múltiples direcciones con el propósito de presentar distintas comunicaciones haciéndose pasar por varias personas.

— La organización no puede otorgar un número limitado de direcciones a los posibles informantes en tanto que, se coartaría la posibilidad de realizar comunicaciones un número superior de veces a las direcciones otorgadas, la organización estaría actuando como intermediario con el riesgo de conocer la identidad detrás de cada billetera y supondría una complejidad desproporcionada para los informantes.

Necesidad de conocimientos informáticos: La creación de una aplicación informática *whistleblower friendly* parte de la concepción

---

en The DAO. De este modo, y aún en la actualidad, existen dos redes blockchain de Ethereum y Ethereum Classic. *Cfr.* ETHEREUM CLASSIC, *Why Ethereum Classic?*, 22 de febrero de 2022. Disponible en: https://ethereumclassic.org/why-classic

[99] LESSIG, L., «Code Is Law. On liberty in Cyberspace», *Harvard Magacine*, 1 de enero de 2000. Disponible en: https://www.harvardmagazine.com/2000/01/code-is-law-html#

[100] Advertir que desde la Comisión Europea, a través de la Recomendación (UE) 2021/946 de la Comisión, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea, se ha propuesto la creación de una Identidad Digital confiable y segura para todos los ciudadanos europeos.

de que el informante tiene conocimientos básicos en tecnologías de la información y comunicación, así como acceso a este tipo de dispositivos cuando la realidad puede ser muy distinta.

Costes de transacción: Tener todas las transacciones registradas con cada miembro de la red es una redundancia muy costosa cuyo único propósito es eliminar la intermediación. Intermediación que no sucede en un sistema de gestión de información interno bien diseñado.

Aun asumiendo dicho gasto por parte de la organización, en la práctica totalidad de redes Blockchain donde se desarrolle la aplicación del canal interno de información siendo necesario para realizar cualquier transacción su criptomoneda nativa, es decir, en el caso de la red de Ethereum es necesario tener Ether (ETH), en la Binance Smart Chain hay que poseer Binance Coin (BNB), en la red Cardano es imprescindible tener ADA, etc.

Por lo tanto, es indispensable que los informantes posean estas criptomonedas para abonar las comisiones de transacción, concluyendo en un claro impedimento a la hora de formular comunicaciones.

La única solución posible[101] consiste que la organización abone una cantidad definida de estas criptomonedas a cada persona legitimada para presentar una comunicación. Ello conllevaría un gasto desproporcionado, una limitación de presentación de comunicaciones, pruebas o alegaciones posteriores hasta el gasto completo de dichas criptomonedas, sin obviar los problemas regulatorios que ello supondría al tener la actual consideración de pago en especie a los trabajadores.

4. CONCLUSIONES

A pesar de que la tecnología Blockchain es una de las principales novedades en el mundo cibernético actual, no debe caerse en la tentación de descentralizar toda la información mediante el uso de dichas redes descentralizadas o distribuidas.

Asimismo, los hechos comunicados en muchos casos deben estar revestidos de las garantías constitucionalmente protegidas como la intimidad, el secreto de las comunicaciones, el derecho de defensa y

[101] La solución de que la organización abone las comisiones de transacción supondría una intermediación de un tercero de confianza echando por tierra los principios fundamentales de la tecnología Blockchain y por lo tanto su utilidad.

asistencia letrada, así como la presunción de inocencia, cuestiones prácticamente imposibles de adoptar en una blockchain pública descentralizada, al menos en la actualidad.

Uno de los principales objetivos de cualquier órgano de cumplimiento normativo de toda entidad pública o privada debe consistir en la promoción de las comunicaciones de irregularidades entre sus *stakeholders* convirtiéndose en una organización *whistleblower friendly*. A través de la adopción de una DApp donde se puedan comunicar estos hechos solo propiciará complejidad y confusión a este proceso interno desembocando en un desinterés de los denunciantes por poner en conocimiento estos hechos.

Finalmente, concluimos que la adaptación de la tecnología Blockchain al *Compliance*, y más concretamente al canal interno de información, en la actualidad no resulta aconsejable debido a sus múltiples desventajas de aplicación, así como problemas regulatorios insalvables que devienen en perjuicio de los derechos fundamentales de las personas físicas, tanto informantes como denunciados.

5. BIBLIOGRAFÍA

Ammous, S., *El Patrón Bitcoin. La alternativa descentralizada a los bancos centrales*, Deusto, Barcelona, 2018.

Antonopoulos, A.M., *Mastering Bitcoin. Programming the Open Blockchain*, O'Reilly, California, 2017.

Back, A., *Hashcash. A Denial of Service Counter-Measure*, 1 de agosto de 2002. Disponible en: http://www.hashcash.org/papers/hashcash.pdf

Barrio Andrés, M., «'Blockchain': la amenaza de la tiranía del código y del algoritmo», *El País*, 19 de abril de 2018.

Bitcoinwiki, *DPoS*. Disponible en: https://en.bitcoinwiki.org/wiki/DPoS

BIT2ME, «¿Qué es un Cypherpunk?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-un-cypherpunk/

BIT2ME, «¿Qué es DPoS?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-dpos/

BIT2ME, «¿Qué es un hash?», *Academy*. Disponible en: https://academy.bit2me.com/que-es-hash/

Blockchain Bundesverband, *Blockchain, data protection, and the gdpr*, Berlin, 2018. Disponible en: https://bundesblock.de/bundesblock-releases-position-paper-on-gdpr-blockchain-and-data-protection/

Brown, A.J., Lawrence, S.A. y Olsen, J., *Why protect whistleblowers? Importance versus treatment in the public & private sectors*, en Brown, A.J., (Ed.), *Whistleblowing: New Rules, New Policies, New Vision.*, Griffith University, Brisbane, 2018.

Domínguez Gómez, J., *Criptografía: Función SHA-256*, agosto 2018. Disponible en: https://estudiobitcoin.com/wp-content/uploads/2020/09/Criptography_SHA_256_es.pdf

Engle, E., «Third Party Effect of Fundamental Rights (*Drittwirkung*), *European Law / Europarecht*, 2009.

Enseñat de Carlos, S., *Manual del Compliance Officer. Guía Práctica para los responsables de Compliance de habla hispana,* Thomson Reuters Aranzadi, Cizur Menor, 2016.

Ethereum, «Decentralized autonomous organizations (DAOs)», *Use Ethereum*. Disponible en: https://ethereum.org/en/dao/

Ethereum, «The Merge», *Upgrades*, 18 de agosto de 2022. Disponible en: https://ethereum.org/en/upgrades/merge/#main-content

Ethereum Classic, *Why Ethereum Classic?*, 22 de febrero de 2022. Disponible en: https://ethereumclassic.org/why-classic

Ethics & Compliance Iniciative, *Global Business Ethic Survey, Measuring Risk and Promoting Workplace Integrity*, 2016. Disponible en: http://www.boeingsuppliers.com/2016_Global_Ethics_Survey_Report.pdf

European Parliament, «Committee on Economic and Monetary Affairs», *Multimedia Centre*, 14 de marzo de 2022. Disponible en: https://multimedia.europarl.europa.eu/en/webstreaming/committee-on-economic-and-monetary-affairs_20220314-1345-COMMITTEE-ECON

European Parliament, «Crypto assets: new rules to stop illicit flows in the EU», *News*, 31 de marzo de 2022. Disponible en: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

Fernández, Y., «Qué son los NFT y cómo funcionan», *Xataka Basics*, 31 de marzo de 2022. *Cfr. https://www.xataka.com/basics/que-nft-como-funcionan*

Feynman, R.P., «Cargo Cult Science», *Engineering and Science*, vol. 37, 7, june 1974.

Franco Blanco, C., «¿Hacia un nuevo estándar democrático basado en la tecnología «Blockchain»?», *Confilegal*, 24 de diciembre de 2021. Disponible en: https://confilegal.com/20211224-hacia-un-nuevo-estandar-democratico-basado-en-la-tecnologia-blockchain/#_ftn3

García-Valdecasas Rodríguez de Rivera, P, *Blockchain y automatización de procedimientos en la Administración Pública*, Wolters Kluwer, Madrid, 2022.

Gemini, «Sharding», *Cryptopedia*. Disponible en: https://www.gemini.com/cryptopedia/glossary#sharding

Gobitcoin.Io, *Cost of a 51% attack*, 2022. Más información en: https://gobitcoin.io/tools/cost-51-attack/

Gómez Martín, V. y Turienzo Fernández A., *Elementos esenciales de los modelos de prevención de delitos,* en Corcoy Bidasolo, M. y Gómez Martín, V., (Dirs.), *Derecho penal económico y de empresa. Parte general y parte especial. Doctrina y jurisprudencia con casos solucionados. Tomo 2,* Tirant lo Blanch, Valencia, 2020.

Goodman, L.M., «The Face Behind Bitcoin», *Newsweek*, 6 de marzo de 2014. Disponible en: https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

Helms, K., «EU Parliament Committee votes Against Proof-of-Work Ban, Supports Alternative Amendment on Crypto Assets», *Bitcoin.com*, 14 de marzo de 2022. Disponible en: https://news.bitcoin.com/eu-parliament-committee-votes-against-proof-of-work-ban-supports-alternative-amendment-on-crypto-assets/

IBM, *¿Qué es la tecnología de blockchain?. https://www.ibm.com/es-es/topics/what-is-blockchain*

Larrañaga Piedra, U., «Blockchain como solución a los problemas de trazabilidad y logística», *Izertis*, 22 de febrero de 2018. Disponible en: https://www.izertis.com/es/-/blog/blockchain-como-solucion-a-los-problemas-de-trazabilidad-y-logistica

Lessig, L., «Code Is Law. On liberty in Cyberspace», *Harvard Magacine*, 1 de enero de 2000. Disponible en: https://www.harvardmagazine.com/2000/01/code-is-law-html#

Morales Barroso, J., *¿Qué es Blockchain?*, en García Mexia, P., (Dir.), *Criptoderecho. La regulación de Blockchain*, Wolters Kluwer, Madrid, 2018.

Moreno, R., Una nueva ley sancionará con hasta un millón de euros a quien tome represalias contra el alertador de corrupción», *Confilegal*, 4 de marzo de 2022. Disponible en: Disponible en: https://confilegal.com/20220304-una-nueva-ley-sancionara-con-hasta-un-millon-de-euros-a-quien-tome-represalias-contra-el-alertador-de-corrupcion/

Nader, R., (Ed.), *Whistleblowing. The report of the Conference on Professional Responsibility*, Penguin Group Incorporated, USA, 1974.

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 de octubre de 2008. https://bitcoin.org/bitcoin.pdf

Oficina de Seguridad del Internauta, *¿Qué son los ataques doS y DDos?*, 21 de agosto de 2018. Disponible en: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Onwura Nzechukwu, P., *Internal Audit Practice from A to Z*, Taylor & Francis Group, Boca Ratón, 2017.

Pérez Bastardo, S., «Creación de un canal de denuncias y cumplimiento de la normativa vigente en materia de protección de datos», *Legal Today*, 20 de septiembre de 2021. Disponible en: https://www.legaltoday.com/opinion/blogs/nuevas-tecnologias-blogs/blog-prodat/creacion-de-un-canal-de-denuncias-y-cumplimiento-de-la-normativa-vigente-en-materia-de-proteccion-de-datos-2021-09-20/

Peterson, A., «Hal Finney received the first Bitcoin transaction. Here´s how he describes it», *The Washington Post*, 3 de enero de 2014. Disponible en: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?noredirect=on

Popper, N., *Digital Gold. Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*, Harper, New York, 2016.

Protocol Labs, *Filecoin: A Decentralized Storage Network*, 19 de julio de 2017. Disponible en: https://filecoin.io/filecoin.pdf

Puyol Montero, J., *El funcionamiento práctico del canal de compliance «whistleblowing»*, Tirant lo Blanch, Valencia, 2017.

Puyol Montero, J. y Franco Blanco, C., *Libro de test Delegado de Protección de Datos (DPO) Dominio III*, Tirant lo Blanch, Valencia, 2020.

Quick, R., *Whistleblowing*, en Idowu, S.O., Capaldi, N., Fifka, M.S., Zu, L. y Schmidpeter, R., (Eds.), *Dictionary of Corporate Social*

Responsibility. CSR, Sustainability, Ethics and Governance, Springer, Cham, Heidelberg, New york, Dordrecht, London, 2015.

Ripple, *Solution Overview*. Disponible en: https://ripple.com/files/ripple_solutions_guide.pdf

Rodríguez, N., «6 Características Clave De La Tecnología Blockchain Que Debes Conocer!», *101 Blockchains*, 9 de enero de 2019. Disponible en: https://101blockchains.com/es/caracteristicas-tecnologia-blockchain/

Russolillo, S., «Yellen on Bitcoin: Fed Doesn't Have Authority to Regulate It in Any Way», *The Wall Street Journal*, 27 de febrero de 2014. Disponible en: https://www.wsj.com/articles/BL-MBB-17195

Sarkar, A., «Ucrania acepta donaciones en Bitcoin, Ethereum y USDT en medio de la guerra», *Cointelegraph*, 27 de febrero de 2022. Disponible en: https://es.cointelegraph.com/news/ukraine-accepts-bitcoin-ethereum-usdt-donations-to-fund-ongoing-war

Simonite, T., «The Man Who Really Built Bitcoin», *MIT Technology Review*, 15 de agosto de 2014. Disponible en: https://www.technologyreview.com/2014/08/15/12784/the-man-who-really-built-bitcoin/

Smith, C., «Introducción a las DApps», *Documentos Ethereum*, 8 de febrero de 2022. Disponible en: https://ethereum.org/es/developers/docs/dapps/#benefits-of-dapp-development

Simón Castellano, P., «Canales de denuncia: Entre la obligación y la oportunidad», *Font Advocats*, 20 de noviembre de 2020. Disponible en: https://www.fontadvocats.com/articulo-canales-de-denuncia-entre-la-obligacion-y-la-oportunidad/

Solé, R., «Blockchain: una tecnología más allá de Bitcoin», *Profesional review*, 10 de julio de 2021. Disponible en: https://www.profesionalreview.com/2021/07/10/que-es-blockchain/#Caracteristicas_de_la_tecnologia_blockchain

Szalay, E., «EU should ban energy-intensive mode of crypto mining, regulator says», *Financial Review*, 19 de enero de 2022. Disponible en: https://www.afr.com/world/europe/eu-should-ban-energy-intensive-mode-of-crypto-mining-regulator-says-20220119-p59plk

Tech España, «Características del blockchain», *School of engineering*, 29 de julio de 2022. Disponible en: https://www.techtitute.com/ingenieria/blog/las-caracteristicas-del-blockchain

UNE-ISO 37002. Sistemas de gestión de la denuncia de irregularidades. Directrices, octubre 2021.

University of Cambridge, «Cambridge Bitcoin Elecrícity Consumption Index», *Centre for Alternative Finance*». Disponible en: https://ccaf.io/cbeci/index/comparisons

Vagadia, B., *Enterprise Governance. Driving Enterprise Performance Through Strategic Alignment*, Springer-Verlag Berlin Heidelberg, 2014.

Velasco Núñez, E., *10 años de responsabilidad penal de la persona jurídica (análisis de su jurisprudencia)*, Aranzadi, Cizur Menor, 2020.

Venegas, E., «El Consejo Minero de Bitcoin señala que el 60% de la minería de BTC utiliza energías renovables», *Beincrypto*, 20 de julio de 2022. Disponible en: https://es.beincrypto.com/consejo-minero-bitcoin-senala-60-mineria-btc-utiliza-energias-renovables/

Vorick, D. y Champine, L., *Sia: Simple Decentralized Storage*, 29 de noviembre de 2014. Disponible en: https://sia.tech/sia.pdf

Wackerow, P., «Proof-of-Stake», *Ethereumv Docs*, 26 de enero de 2022. Disponible en: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

World Economic Forum, *Exploring blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*, Cologny/Geneva, 2020.