UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE
Facultat de Ciències Econòmiques i Empresarials
Facultad de Ciencias Económicas y Empresariales

DOBLE GRADO EN DERECHO Y ADMINISTRACIÓN DE EMPRESAS

CURSO ACADÉMICO 2022 - 2023

BLOCKCHAIN E INTELIGENCIA ARTIFICIAL EN EL SISTEMA DE INFORMACIÓN CONTABLE: LA DISRUPCIÓN DE LA PARTIDA TRIPLE

CARLOS A. WANDEN-BERGHE FAJARDO

TUTOR: JOSÉ LUIS WANDEN-BERGHE LOZANO
DEPARTAMENTO DE ECONOMÍA FINANCIERA Y CONTABILIDAD

San Vicente del Raspeig, mayo de 2023

Abstract

This paper begins with a bibliometric analysis and literature review on the effects of blockchain and artificial intelligence in the field of accounting and auditing in order to identify the lines and research trends in this area. New technologies have made various contributions by enabling the maintenance of distributed and immutable records and facilitating process automation. The combination of these technological resources gives rise to different systems that depend on network configuration, consensus types, and applied cryptographic techniques. In any case, their implementation promises to improve information, overcome the crisis of trust created by financial scandals at the beginning of the century, provide greater transparency, especially important for public accounts, increase the availability of accounting information for auditing and analysis, and serve as a tool to combat corruption and fraud, among other consequences. However, there is no universally accepted system, and the vast majority of applications or proposals are limited to very specific aspects. Therefore, in light of these observations, this paper aims to delve into the functioning and application of blockchain and artificial intelligence in accounting and auditing, with the ultimate goal of designing the foundations for a triple-entry accounting information system, where the third entry would be located in the distributed records of the blockchain, compatible with the insertion of smart contracts to automate processes. Two extreme positions are proposed: an open and transparent system recommended for the management of public funds, and a second system with assured privacy that relies on the zero-knowledge cryptographic protocol. Both would bring significant advantages in terms of security, trust, transparency, cost reduction in information preparation and review, increased immediacy and analysis, potentially leading to continuous auditing becoming a reality. However, they also face obstacles and difficulties that are equally addressed in the paper.

Keywords

Accounting, Auditing, Blockchain, Artificial Intelligence, Transparency, Fraud, Corruption, Internal controls, Accounting information system, Triple-entry, Distributed databases

Resumen

El trabajo parte de un análisis bibliométrico y una revisión bibliográfica sobre los efectos de blockchain y la inteligencia artificial en el área de contabilidad y auditoría con el fin de detectar las líneas y tendencias de investigación al respecto. Las nuevas tecnologías han hecho contribuciones de distinta índole y alcance al permitir mantener registros distribuidos de forma inmutable, así como por posibilitar automatizar procesos. La combinación de estos recursos tecnológicos da lugar a diferentes sistemas que dependen de la configuración de la red, de los tipos de consenso y de las técnicas criptográficas que se apliquen. De cualquier forma, su implantación promete mejorar la información, superar la crisis de confianza que los escándalos financieros de principios de siglo han traído consigo, mayor transparencia especialmente importante para las cuentas públicas, mayor disponibilidad de la información contable para su auditoría y análisis, así como, ser instrumento para luchar contra la corrupción y el fraude, entre otras consecuencias. Sin embargo, no existe un único sistema generalmente aceptado y la gran mayoría de las aplicaciones o propuestas realizadas se limitan a aspectos muy concretos. De ahí que ante tales observaciones el trabajo se ha dirigido a profundizar sobre el funcionamiento y la aplicación de blockchain y la inteligencia artificial en la contabilidad y la auditoría con el objetivo último de diseñar las bases de un sistema de información contable de partida triple, en donde la tercera entrada se ubicaría en los registros distribuidos de la cadena de bloques, compatibles con la inserción de smart contracts para automatizar procesos. Se plantean dos posiciones que son extremas: Un sistema abierto y transparente recomendable para la gestión de fondos públicos y un segundo sistema con privacidad asegurada que recurre al protocolo criptográfico de conocimiento cero. Ambos traerían consigo grandes ventajas en cuanto a seguridad, confianza, transparencia, reducción de costes en la elaboración de la información y su revisión, mayor inmediatez y análisis, pudiendo llevar a que la auditoría continua sea una realidad, pero también cuenta con obstáculos y dificultades que son tratados de igual manera en el trabajo.

Palabras Clave

Contabilidad, Auditoría, Blockchain, Inteligencia Artificial, Transparencia, Fraude, Corrupción, Control interno, Sistema de información contable, Triple entrada, Partida triple, Bases de datos distribuidas

ÍNDICE

I. Introducción 6
II. Estudio bibliométrico. Estado de la investigación y práctica contable 8
III. Qué es y cómo funciona la tecnología blockchain 13
1. Qué es 13
2. Funcionamiento 16
3. Tipos de Redes 21
3.1 Blockchain pública 21
3.2 Blockchain privada 23
3.3 Blockchain Híbridas, de consorcio y federadas 24
3.4 Redes tokenizadas o no tokenizadas 25
4. Tipos de consenso 25
5. Plataformas blockchain 29
IV. Aplicación a la contabilidad y auditoría 31
1. Contabilidad de Partida Triple (o Triple Entrada) 34
1.1 Operatividad de un sistema de contabilidad de partida triple 37
2. Incorporación de la Inteligencia Artificial 38
2.1 Smart Contracts 39
3. Sistemas contables con aplicación de blockchain 43
4. Operatividad en un sistema simple sin privacidad asegurada 46
5. Sistema contable de privacidad asegurada 49
V. Impacto de Blockchain y la Inteligencia Artificial en contabilidad y auditoría 52
1. Impacto de la Aplicación de Blockchain e IA en la Contabilidad 52
1.1 Automatización de los procesos y cumplimiento de acuerdos 53
1.2 Intervención de intermediarios 54
1.3 Registro contable confiable 54
1.4 Transparencia 55
1.5 Trazabilidad y control de inventarios 55
1.6 Cuadro resumen de implicaciones positivas en el área contable 56
1.7 Riesgos y desafíos de su aplicación 57
2. Impacto de la Aplicación de Blockchain e IA en la Auditoría 58
2.1 Auditoría integral y continua 59
2.2 Eficiencia 59
2.3 Cuadro resumen de las implicaciones en la auditoría 60
2.4 Retos y desafíos 60
3. Escenarios futuros: ¿Hacia un ecosistema de información compartida? 61
VI. Conclusiones 64
VII. Referencias Bibliográficas 66

I. Introducción

El objeto de este trabajo es realizar una investigación sobre el impacto de blockchain y la inteligencia artificial sobre los sistemas de información contable y la auditoría con el fin de detectar las propuestas y soluciones tanto en el ámbito de la administración pública, donde la transparencia de la información está tan demandada, como para el diseño de sistemas aplicables en empresas y otras entidades, donde se requiere una mayor privacidad.

Desde distintas perspectivas se puede constatar la trascendencia de implementar la tecnología blockchain y la inteligencia artificial en el sistema de información contable. Diversos informes[1] coinciden en pronosticar el alto crecimiento de las inversiones en tecnología blockchain e inteligencia artificial por parte de instituciones públicas y privadas, así como el aumento de la dimensión del mercado ligado a estas tecnologías. En el contexto europeo, el informe del Banco Europeo de Inversiones (2019) con la colaboración de la Comisión Europea, muestra el efecto de sus aplicaciones en el futuro de Europa y la conveniencia de aprovechar las oportunidades que genera, para lo que formula una serie de propuestas tendentes al despliegue de estas tecnologías disruptivas en la administración de Europa.

En los últimos años, organismos profesionales de contabilidad y auditoría están emitiendo informes y recomendaciones sobre el impacto de las nuevas tecnologías en la profesión y en la administración de los recursos económicos. En algunos casos, se está dando formación a contables y auditores sobre las posibilidades de aplicación de blockchain e inteligencia artificial en especial, y las tecnologías emergentes en general. Con mayor anticipación, las cuatro grandes empresas de auditoría hacen lo propio, multiplicado los desarrollos para realizar sus funciones, así como diseñando soluciones para sus clientes basadas en estas tecnologías. En el ámbito académico, en apenas 5 años han empezado a extenderse investigaciones, análisis y propuestas desde distintas áreas de conocimiento que se encaminan a desarrollos disruptivos sobre el estado actual de la gestión de recursos y de la información para la toma de decisiones. Así mismo, surgen iniciativas y proyectos en la administración pública encaminadas hacia una mayor transparencia y una gestión más eficaz de los fondos públicos y como herramientas para luchar contra el fraude y la corrupción.

[1] En el informe MarketsandMarkets (2023) se estima que el tamaño del mercado Blockchain fue de aproximadamente 7,4 mil millones $ en 2022 y puede pasar a generar ingresos de más de 94,0 mil millones $ para fines de 2027, proyectando una CAGR (tasa de crecimiento anual compuesto) del 66,2% entre 2022 y 2027. Otros informes sobre el crecimiento de estas aplicaciones son Deloitte (2023) e International Data Corporation (2023).

Ante tales observaciones, este trabajo parte de un análisis bibliométrico y una revisión bibliográfica sobre los efectos de blockchain y la inteligencia artificial en el área de contabilidad y auditoría con el ptopódito de detectar las líneas y tendencias de investigación al respecto. El estudio se realiza a través de Scopus si bien ha sido complementado con la revisión a través otras bases de datos como ProQuest y Web of Science. Los resultados se han tratado con VOSviewer y canalizado siguiendo la guía de la declaración PRISMA y evidencian que las nuevas tecnologías permiten mantener registros distribuidos de forma inmutable, así como posibilitan automatizar procesos. La combinación de estos recursos tecnológicos da lugar a nuevos sistemas de información contable y prometen transformar el desempeño de las áreas de contabilidad y auditoría en sentido amplio.

De ahí que el siguiente punto del trabajo se dedique a explicar qué es y cómo funciona blockchain, para fundamentar los elementos básicos de la tecnología y su funcionalidad, que dependerá de la configuración de la red, de los tipos de consenso y de las técnicas criptográficas que se apliquen. Por tal motivo, se dedica un espacio a describir los tipos de redes, diferenciando las particularidades de las públicas, privadas e híbridas y mostrando las ventajas e inconvenientes de cada una de ellas. Ha interesado resaltar que existen redes tokenizadas, propias de las criptomonedas, y redes sin tokenizar. Por otra parte, la operatoria de blockchain está condicionada por la forma en que se realiza el consenso, por lo que se hace un recorrido por las distintas opciones para cerrar este punto con las plataformas más importantes que sirven de soporte en los desarrollos realizados.

La aplicación de blockchain y la inteligencia artificial en la contabilidad y la auditoría es objeto del siguiente bloque del trabajo, siendo su máxima expresión la partida triple o contabilidad de tercera entrada. Un sistema de información contable de partida triple no es rupturista con los planteamientos de la partida doble, pero tener el complemento de un tercer registro distribuido y compartido sugiere una nueva era con importantes cambios sobre la situación actual. Esta tercera entrada se ubicaría en los registros distribuidos de la cadena de bloques, con la posibilidad de inserción de smart contracts para automatizar procesos. La incorporación de la inteligencia artificial en la red y la gran contribución que los smart contracts ofrecen con su programación autoejecutable suman potencialidad al sistema y centran la atención en este trabajo.

Llegados a este punto, se revisan los sistemas contables de triple entrada propuestos y se observa que no existe un único sistema generalmente aceptado y la gran mayoría de las

aplicaciones en esta línea se limitan a aspectos muy concretos. Por tal motivo, el trabajo se ha dirigido a presentar dos sistemas extremos. En primer lugar, un sistema sin privacidad asegurada que es indicado para la gestión de fondos públicos donde la transparencia es una necesidad y, en segundo lugar, un sistema con privacidad asegurada que sería el deseable en entidades que requieren una privacidad por cuestiones de estrategia o de confidencialidad de datos. Para tal pretensión existen diversas soluciones, optando este trabajo por emplear la criptografía avanzada de la prueba de conocimiento cero.

Con independencia de la variante de blockchain que se adopte, promete contribuir de manera determinante en mejorar la información y ayudar a superar la crisis de confianza que los escándalos financieros de principios de siglo han traído consigo. Por tanto, el siguiente punto del trabajo se dedica al impacto de estos sistemas en la contabilidad y auditoría. Ello lleva consigo grandes ventajas en cuanto a seguridad, confianza, transparencia, reducción de costes en la elaboración de la información y su revisión, mayor inmediatez y análisis, haciendo posible que la auditoría continua sea una realidad, y, en un proceso más avanzado, llegar a conformar un ecosistema de información compartida entre los diferentes grupos de interés. La mayor transparencia en las cuentas públicas, ligada a la mejora en la disponibilidad de la información contable para su auditoría, seguimiento y análisis, es un instrumento para luchar contra la corrupción y el fraude, entre otras consecuencias. Pero también, estas aplicaciones cuentan con obstáculos y dificultades tanto en cuestiones técnicas como de regulación legal que son tratados de igual manera en el trabajo. Por último, el trabajo sintetiza su contenido con unas conclusiones.

II. Estudio bibliométrico. Estado de la investigación y práctica contable

Tomar el pulso del estado de la investigación y práctica contable con la aplicación de blockchain y la inteligencia artificial es fundamental para sentar las bases de este trabajo. Para ello se realiza un estudio bibliométrico que se complementa con una revisión bibliográfica para detectar las tendencias actuales y localizar los elementos clave de investigación y las prácticas realizadas, así como apuntar hacia donde se dirigen las líneas de investigación en el área de contabilidad.

La metodología utilizada ha partido de la consulta de otras revisiones bibliográficas y estudios bibliométricos en materia contable (Massaro et al., 2016; Schmitz el al., 2019; Bartolacci et al., 2020; Fragoso et al., 2020; Secinaro et al., 2021; Lombardi et al., 2020) con el fin de abordar el análisis con la mayor garantía científica. Se ha seguido la guía de la declaración PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) de Page et al. (2021) para documentar la revisión sistemática y aplicar los métodos para identificar, seleccionar, evaluar y sintetizar el estudio.

La revisión sistemática se ha dirigido a responder las preguntas de investigación que centran el tema, son objeto de la investigación y definen el alcance de esta. Son las siguientes:

- RQ1: ¿Cuál es el estado actual de la investigación y práctica en contabilidad y auditoría con la aplicación de blockchain?
- RQ2: ¿Cuáles son las implicaciones de blockchain en la contabilidad y auditoría?
- RQ3: ¿Cuáles son las líneas futuras de aplicación de blockchain en el área de contabilidad y auditoría?

La búsqueda de los trabajos se realiza de forma combinada a partir de las bases de datos Scopus, ProQuest y Web of Science. El estudio bibliométrico se ha realizado a través de Scopus si bien ha sido complementado con la revisión a través de las otras bases de datos, y los resultados se han tratado con VOSviewer.

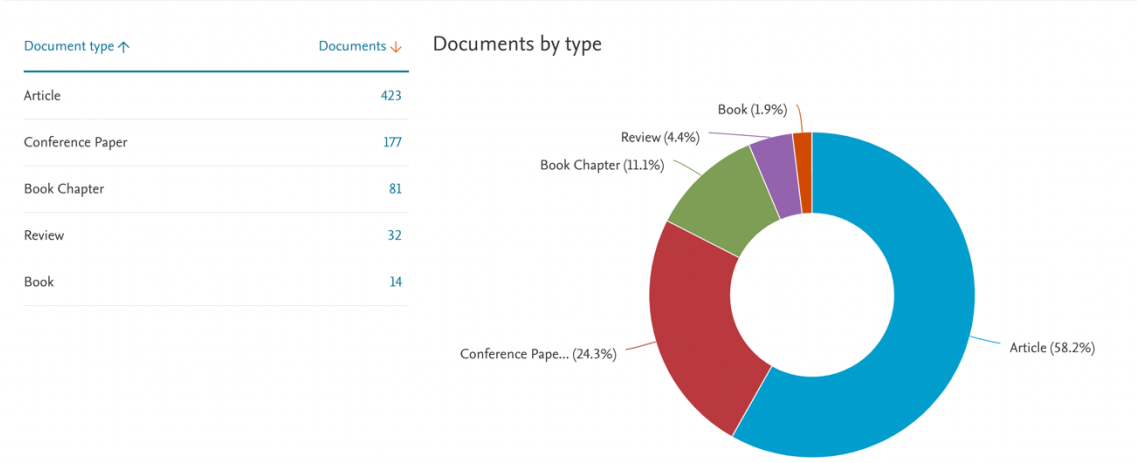
Como se ha indicado, el primer acercamiento a las búsquedas bibliográficas se realizó en Scopus. En el inicio, el intento fue con las palabras claves de blockchain y contabilidad, dando un único resultado, mientras que cruzando “blockchain” y “accounting” se obtuvieron 594 documentos. Ante tal evidencia y diversas búsquedas con comportamiento equivalente, se optó por proceder a hacer las consultas con palabras claves en inglés. Así, “artificial intelligence” y “accounting” mostró 1784 artículos; “blockchain” y “audit*” 1.870 sin ningún tipo de filtro y, posteriormente, se prosiguió realizando cruces con palabras claves como crypto* o smart contract, optando finalmente por realizar el estudio bibliométrico a través de la siguiente secuencia de búsqueda avanzada de Scopus, por ser la más apropiada para el alcance de la revisión:

(TITLE-ABS-KEY (blockchain OR crypto*) AND TITLE-ABS-KEY (account* OR audit*)) AND PUBYEAR > 2007 AND (LIMIT-TO (SUBJAREA , "BUSI")) AND (LIMIT-TO (DOCTYPE , "ar") OR

LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ch") OR LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "bk"))

Las palabras claves de blockchain o crypto* se cruzaron con account* o audit* y se limitó la búsqueda a partir de la aparición de las criptomonedas (2008), así como al subárea de "negocios, administración y contabilidad". Las fuentes elegidas son artículos, comunicaciones a congresos, capítulos de libros, opiniones (reviews) y libros, esto es, una búsqueda completa por ser una temática relativamente reciente pero no se indexan otras fuentes que no reúnen las exigencias de fiabilidad científica. El 18 de abril de 2023 se obtuvieron 727 documentos, una vez eliminadas las duplicidades y descartados los trabajos irrelevantes para la investigación, tal como se muestra en la figura XX, en donde el 58,2% de los documentos son artículos que están sujetos a revisiones.

Figura 01: Tipos de documentos

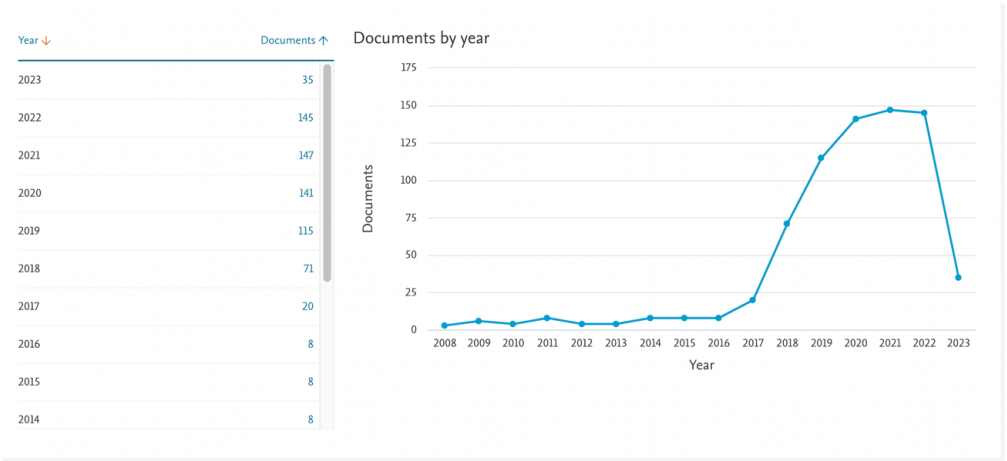


Al atender a los documentos por años de publicación, se observa el creciente interés de la investigación en blockchain en el periodo comprendido entre 2017 y 2020, desde donde se mantiene en las cotas altas de producción anual de forma estable. Como resulta obvio, la caída que se produce en el gráfico en 2023 es porque contiene solo una parte del año.

La figura 01 recoge el mapa de coocurrencia de palabras claves en donde se visualizan las conexiones entre las palabras claves de los documentos. En aras de despejar el mapa se incluyeron palabras claves con 6 o más apariciones en el conjunto de las publicaciones. De esta forma se puede visualizar el "estado del arte" y se identifican conjuntos de documentos que vienen a responder a nuestras preguntas de investigación. Un primer conjunto se dedica a explicar la tecnología blockchain, otro conjunto se centra en aplicaciones de la cadena de

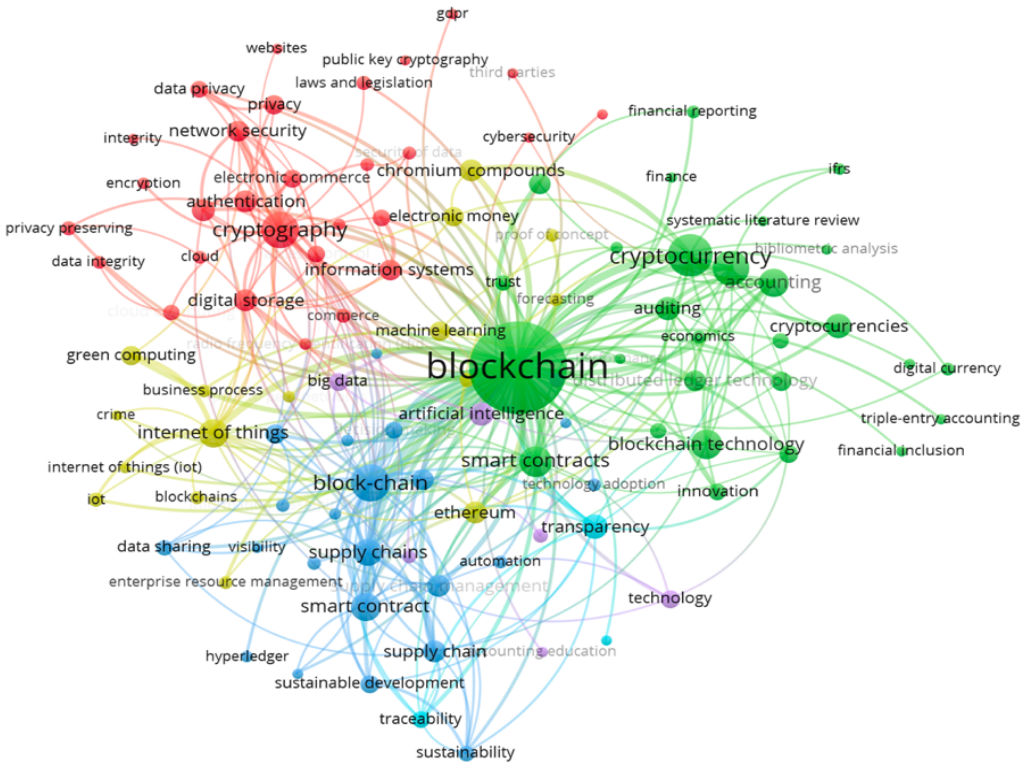
bloques, el siguiente a las implicaciones y, finalmente hay un último conjunto, el más reducido en número, que realiza propuestas de sistemas o modelos a aplicar en el futuro, que va a atraer especialmente nuestra atención.

Figura 02: Documentos por años



Year	Documents
2023	35
2022	145
2021	147
2020	141
2019	115
2018	71
2017	20
2016	8
2015	8
2014	8

Figura 03: Mapa de coocurrencia de palabras claves



A medida que se avanza en el desarrollo de este trabajo, se citarán los principales estudios en cada conjunto identificado. Antes de ello, interesa mostrar el análisis por países y por patrocinadores de los trabajos. Por países, es Estados Unidos claramente quien reúne más trabajos de investigación, concretamente son 176 documentos, un número muy superior al resto probablemente beneficiado por tener más revistas indexadas y ser las palabras claves de búsqueda en inglés, seguidos por el Reino Unido con 72 documentos. Tras ellos está China y la India (67 y 64 documentos respectivamente). Por patrocinadores, National Natural Science Foundation of China es la entidad que más documentos financia, sin embargo, agrupando entidades de forma geográfica, la Unión Europea es quien destina fondos a más investigaciones.

Figura 04: Documentos por países

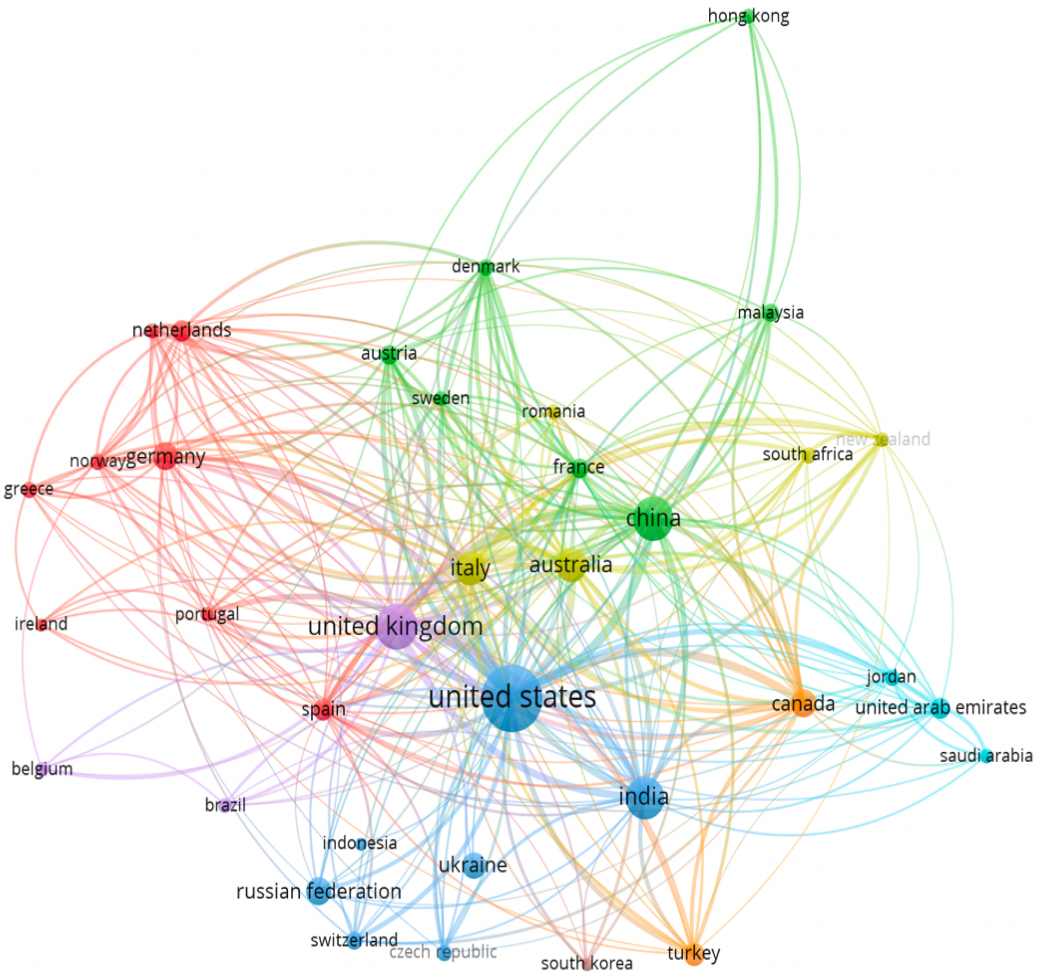
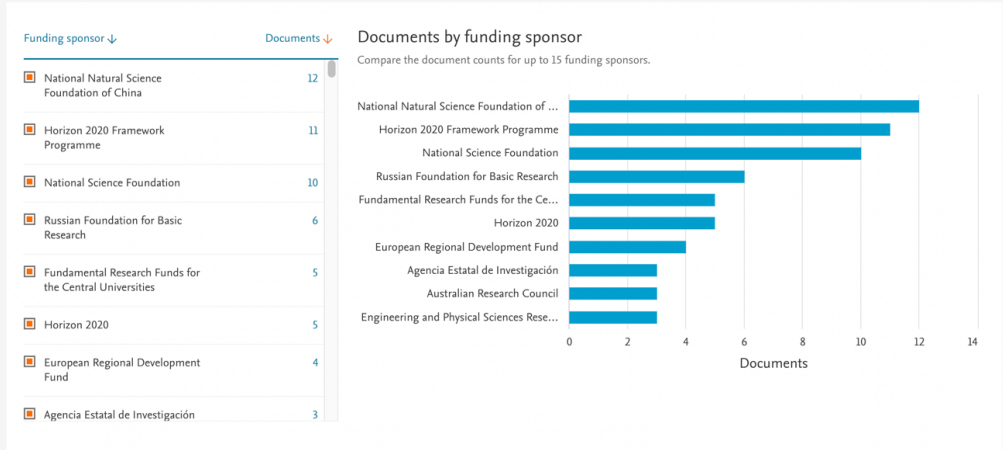


Figura 05: Documentos por patrocinador de financiación



Para concluir este estudio y mostrar la incipiente investigación en sistemas de información contable basados en blockchain e inteligencia artificial, cabe indicar que la consulta cruzada de la búsqueda anterior con la "inteligencia artificial" o "smart contract", se redujo a 172 resultados, que van a centrar especialmente la atención en este trabajo y a los que se hará referencia en los siguientes apartados. Esta es la secuencia de búsqueda avanzada que se ha utilizado:

(TITLE-ABS-KEY (blockchain OR crypto*) AND TITLE-ABS-KEY (account* OR audit*) AND TITLE-ABS-KEY ("artificial intelligence" OR "smart contract")) AND PUBYEAR > 2007 AND (LIMIT-TO (SUBJAREA , "BUSI")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ch") OR LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "bk"))

III. Qué es y cómo funciona la tecnología blockchain

1. Qué es

La tecnología blockchain ha trascendido a la idea para la que fue creada inicialmente —el facilitar las transacciones de criptomonedas (Nakamoto, 2008)— y dada la naturaleza de este trabajo es necesario explicar su dinámica para comprender en profundidad las implicaciones y beneficios que podría aportar a los ámbitos de la contabilidad y la auditoría.

Blockchain, como indica su nombre, es una cadena compuesta por bloques que funciona como un libro de contabilidad digital inmutable, seguro y distribuido que se basa en el consenso de los participantes y que almacena información. Como señala Bashir (2018) hay que contemplar blockchain desde una doble perspectiva para conocer su particularidad. Desde una perspectiva comercial, es una plataforma de intercambio de transacciones de valor entre pares participantes de tal forma que es la propia tecnología quien gestiona los registros sin necesitar la intermediación de ninguna autoridad central. Pero no se limita a tal fin, sino que desde una perspectiva técnica, se contempla como un libro mayor distribuido, peer to peer, criptográficamente seguro, inmutable y que solo se puede modificar por consenso o acuerdo entre pares. Precisamente, es muy frecuente esa asociación entre blockchain y libro mayor distribuido, tan propio del método contable, donde se registran transacciones y hechos organizados en bloques que son ordenados cronológicamente y mantenidos en diversos ordenadores conectados a la red (Maffei, 2021; Dai & Vasarhelyi, 2017). Además, dicha información es transmitida entre los integrantes de la red sin necesidad de la intervención de un intermediario y se encuentra protegida criptográficamente en un entramado entre pares o peer to peer donde todos los participantes — nodos u ordenadores — están conectados y no necesitan confiar plenamente entre ellos.

Interesa resaltar que en un inicio la cadena de bloques fue creada para hacer posible las transacciones con criptomonedas sin intermediación, pero es una tecnología que ha evolucionado y no se puede asociar exclusivamente a las criptomonedas o a la tokenización de activos, pues es un libro mayor distribuido que recoge una lista de registros que puede involucrar cualquier valor, bienes, propiedades, expedientes, incluso votos, es decir, cualquier información. Está generalmente aceptado que blockchain está en su cuarta etapa de madurez. La primera surge con la aparición de bitcoin y el despliegue de criptomonedas, dando lugar a aplicaciones relacionadas con transferencias, remesas o sistemas de pago digitales (Swan, 2015). Desde esa fase inicial, se extiende a Blockchain 2.0 en donde se abordan aspectos de privacidad, contratos inteligentes y el uso de tokens, siendo un ejemplo de esta etapa la plataforma Ethereum o la hyperledger de IBM (Schuster, 2018; Wass, 2018). La siguiente etapa está protagonizada por las dApp o aplicaciones que se ejecutan en la red descentralizada que permiten compartir o subcontratar actividades y, por tanto, puede conducir a modificaciones en la estructura y en el enfoque de la administración de las entidades. Finalmente, Blockchain 4.0 representa el uso integral de blockchain y la inteligencia artificial de forma conjunta. En este punto cabe contemplar sistemas de bases de datos distribuidas que en algunos aspectos

puedan tomar decisiones y actuar sobre ellas sin necesidad de interferencia humana directa. Con ello, tienen capacidad de realizar una función de registro o gestión, programando una serie de parámetros, emitiendo juicios y posteriormente ejecutarlos independientemente de la supervisión. Sin embargo, hay que destacar que cada etapa de blockchain comprende un conjunto de funcionalidades encaminadas a satisfacer las necesidades de servicio. La prioridad, por tanto, está en implementar la etapa adecuada de la tecnología para cubrir las necesidades de información y gestión de la entidad, en lugar de buscar los niveles tecnológicos más altos (Angelis & Ribeiro da Silva, 2019).

Sin necesidad de llegar a este último y máximo desarrollo por la observación indicada, toda cadena de bloques se caracteriza con una serie de rasgos que hacen a esta tecnología especialmente atractiva (Ducas & Wilner, 2017; Ahmad et al., 2019; O'Leary, 2017; Schmitz & Leoni, 2019; Zheng et al., 2018; Du et al., 2019), cuya conexión entre ellos le otorga una mayor fortaleza, aunque cada uno de ellos por si solos sugieren oportunidades aprovechables en los sistemas de información:

- Transparencia: La información es compartida por todos los participantes de la cadena de bloques distribuida y almacenada en diferentes ordenadores conectados a una red.

- Descentralización y desintermediación: Permite evitar la intervención de un actor central que proporcione confianza, pues la propia tecnología es quien la genera. Al ser una red peer to peer con pruebas criptográficas, elimina el problema de que la confianza recaiga en un tercero para la verificación y, por derivación faculta la desintermediación.

- Inmutabilidad: Una vez que un bloque se añade a la cadena, dicha información permanecerá inmutable. La única posibilidad de modificar el contenido de un bloque es insertar otro bloque que revierta la situación, y ello no podrá realizarse sin el consenso de todos los participantes.

- Verificabilidad: Terceras partes podrían comprobar que una transacción entre dos partes es lícita y se ha llevado a cabo en un momento determinado.

- Confiabilidad: La consecuencia de las características anteriores hacen que sea un registro seguro, en bloques encadenados en orden cronológico, protegidos criptográficamente y distribuidos en servidores diferentes de manera inalterable, por lo que dan como resultado que la información sea confiable.

- Accesibilidad: La tecnología es de bases de datos distribuidas conectadas y accesibles, si bien puede permitir diferentes niveles de accesibilidad.

No obstante, estos rasgos característicos de toda cadena de bloques pueden estar graduados atendiendo a la mayor o menor restricción que haya tanto al acceso como a las diferentes funciones dentro de la cadena, es decir, la configuración de la cadena puede acentuar sus componentes según estemos ante redes abiertas o restringidas, dependiendo del tipo de consenso que se realice y de los protocolos y pruebas[2] criptográficas que se apliquen.

Teniendo presente todo ello, se puede terminar este apartado con la síntesis de la tecnología blockchain indicando que se trata de un libro mayor distribuido que aporta confianza y eficiencia al permitir que las transacciones y datos se registren de manera idéntica en los diversos nodos que componen la red (cada uno de los participantes cuenta con una copia), todo lo relativo al registro de una transacción u otro tipo de información, con la seguridad de que los datos no se han modificado ni alterado: una vez validado — consensuado o minado — un bloque, este se añade a la cadena sin posibilidad de que pueda ser alterado y queda protegido adicionalmente por la criptografía.

2. Funcionamiento

En términos generales, la tecnología blockchain permite el registro de información en bases de datos distribuidas que, además, es compartida e inalterable. Ahora bien, dicha idea no es más que la síntesis de una compleja tecnología cuyo funcionamiento genérico se describe a continuación.

Una red blockchain está formada por una serie de participantes que pueden interactuar en ella de diversas formas: realizar propuestas, anotar información, participar en el consenso necesario para la formación y registro del bloque, consultar los datos ya registrados…. Estos participantes pueden actuar libremente o con permiso dependiendo del tipo de red y, en el caso de estar en una red restringida tendrían que ser seleccionados o cumplir ciertas condiciones para formar parte de misma o para asumir determinado rol. En cualquier caso, se persigue registrar las operaciones producidas entre ellos en una cadena de bloques que contaría con las características ya expuestas de transparencia, inmutabilidad, descentralización, verificabilidad, confiabilidad

[2] Los protocolos criptográficos son procedimientos que utilizan la criptografía para lograr objetivos de seguridad específicos, como la autenticación o el intercambio seguro de información. Por otro lado, las pruebas criptográficas son métodos matemáticos utilizados para demostrar la seguridad de los algoritmos y protocolos

y accesibilidad. Sin embargo, es obvio que el registro requiere un proceso para su funcionamiento que lleva aparejado el empleo de elementos criptográficos indispensables para la seguridad e inmutabilidad de la cadena. Siguiendo a Desplebin et al. (2018), se pueden distinguir cinco fases para explicar el funcionamiento de blockchain:

- En primer lugar, el agente A registra una petición en el registro de blockchain (transacción financiera, registro contable, contrato, entrega, expediente, transferencia de propiedad, etc.). Para ello, el agente A utiliza un software en internet que transmite la solicitud a los usuarios de una red.

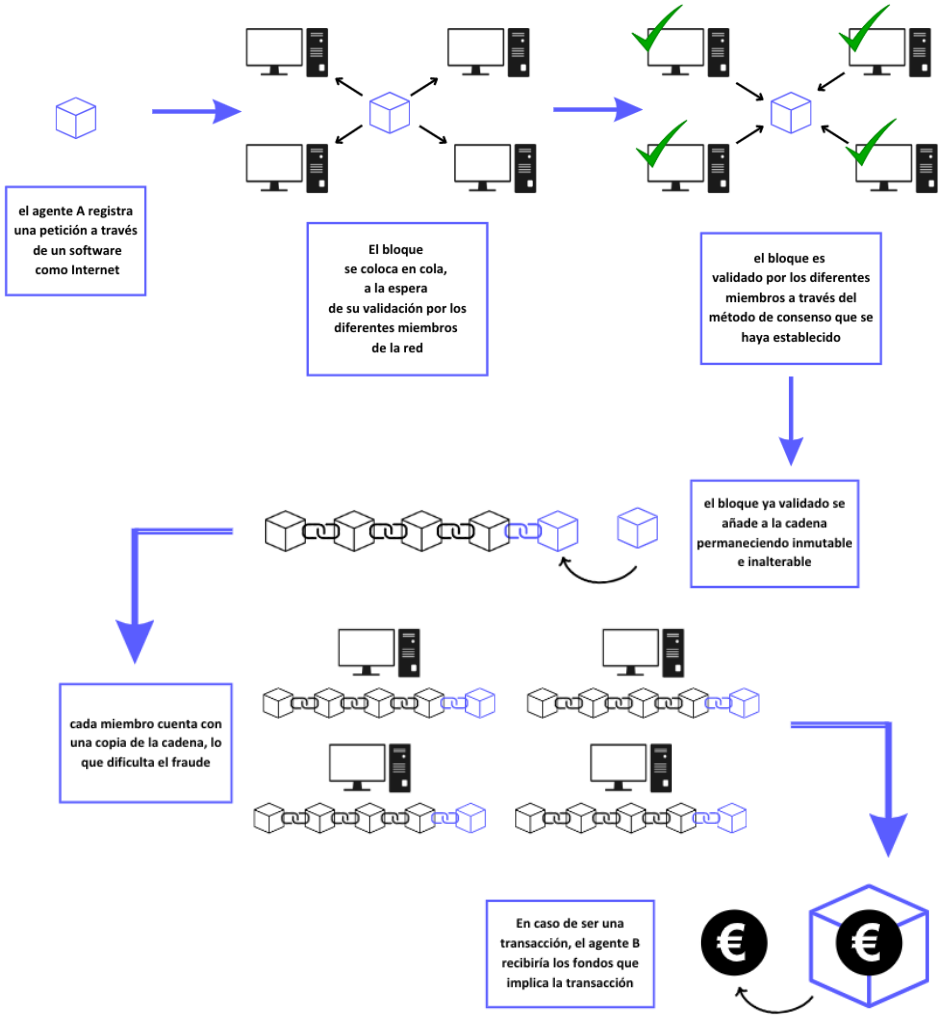
- En la fase siguiente, la solicitud del agente A se agrega a un bloque de información que reúne todas las solicitudes registradas en blockchain por diferentes usuarios de la red. Se puede decir que ese bloque se coloca "en una cola".

- Tras ello, se produce la validación de ese bloque y el registro efectivo de la información que contiene dentro de la cadena. Dicha validación (o, en otros términos, el proceso de minería) requiere el consenso de los usuarios de la red, lo que proporciona una gran confiabilidad en la información registrada. Hay que avanzar en este punto que el proceso de validación y generación del nuevo bloque depende del protocolo de consenso utilizado por la red en concreto y, en cierta forma, del modelo de blockchain que siga la red. Existen diversas opciones de consenso y, atendiendo a los fines de la red, resultará más conveniente aplicar una u otra.

- Por último, una vez que el bloque ha sido agregado y situado a continuación de los ya registrados en la cadena, todos los miembros de la red pueden acceder a dicha información, dado que es un registro distribuido y accesible. No obstante, al igual que se dijo anteriormente, en este punto también hay distintos niveles de visibilidad o privacidad.

Con independencia del diseño de la red blockchain, el bloque es inalterable una vez se produce la adición y a través de recursos criptográficos, entre los que destaca el hash, hacen que el bloque permanezca inmutable de forma segura. Adicionalmente, en caso de una transacción, los fondos derivados de la misma, se transmitirán en, por ejemplo, forma de criptomonedas como sucede en Bitcoin o Ethereum.

Figura 06: Funcionamiento de una blockchain



Fuente: Adaptado a partir del esquema de Maffei et al. (2021)

Este esquema de funcionamiento del proceso de registro que opera en blockchain a través de las fases señaladas, conviene ser complementado con una explicación más concreta sobre cómo se genera la cadena, la estructura del bloque y el enlazamiento que se establece entre ellos que, en esencia es el fundamento por el que esta tecnología aporta seguridad y confiabilidad. Para ello, se ha creado una cadena de tres bloques en la demo de blockchain de Anders Brownworth[3], que se presenta en la Figura 07. En dicha cadena de tres bloques figuran los componentes básicos de todo bloque, si bien existen plataformas blockchain que incluyen campos de información adicionales (Gómez Carpena, 2018; Wanden-Berghe & Fernández Daza, 2018):

[3] https://andersbrownworth.com/blockchain/

- En primer lugar, encontramos el número de bloque, con el único propósito de que este aparezca en el lugar que le corresponde de la cadena de acuerdo con la cronología.

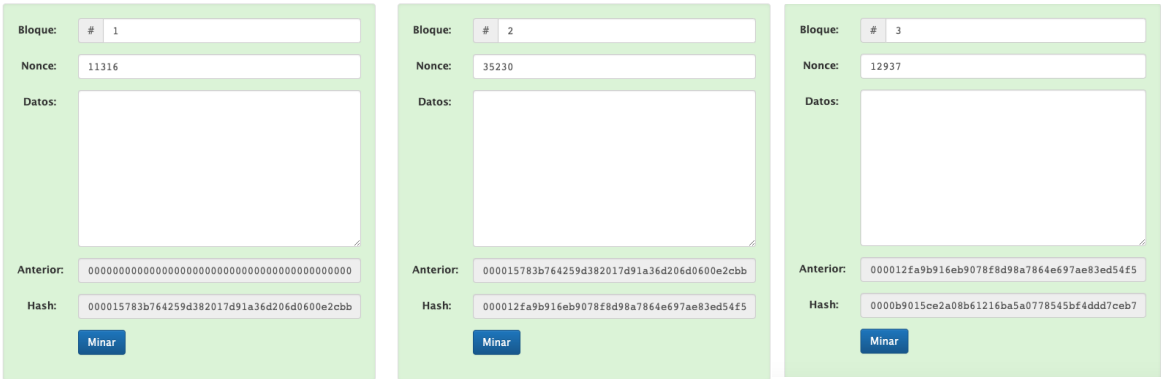
- En segundo lugar, el "nonce" informa de aspectos técnicos y de programación y es resultado de un algoritmo matemático.

- En tercer lugar, figura un apartado destinado a recoger los datos que se registran en dicho bloque, los cuales, aunque fueron diseñados para transacciones de criptomonedas, actualmente podrían ser datos referentes a innumerables aspectos informativos y de registro, como son las anotaciones contables.

- En cuarto lugar, aparece el componente más relevante del bloque para su encadenamiento: el hash. Este representa el contenido del bloque encriptado en un código. A través de él, se identifica cada bloque pues, como se ha dicho, no es más que el resultado de un algoritmo matemático dependiente de los datos registrados en él. Su importancia radica en que, al obtenerse directamente de la información registrada, los bloques de las múltiples copias de la cadena que poseen los participantes de la red tendrán el mismo hash, siendo imposible la alteración de la información. Cualquier incidencia será fácilmente detectable porque ante la mínima alteración en la información del bloque, hace cambiar el código hash y, por tanto, se evidenciaría el cambio que se ha introducido en el contenido del bloque. Además, cada bloque de la cadena contiene, adicionalmente, el hash del bloque que le precede cronológicamente, permitiendo el enlace entre bloques y, por tanto, la conformación de la cadena. No sólo no se puede manipular el bloque, sino que tampoco se puede hacer con la cadena en su conjunto. De ahí que se le atribuya esa característica fundamental que permite afirmar que la información es inmutable e inalterable.

- Por último, no se puede olvidar que blockchain es un registro distribuido, por lo que la cadena que se ejemplifica mantendrá copias en cada nodo de la red y, lógicamente, son idénticas.

Figura 07: Componentes de una cadena de bloques



Fuente: Extraída de la Demo de Blockchain de Anders Brownworth

Sobre este mecanismo y tales componentes, se construyen diferentes modelos de blockchain que se diferencian en función de la combinación de un conjunto de aspectos, como son: el tipo de red, pues pueden ser redes públicas, redes permisionadas y redes híbridas, así como el tipo de consenso que se requiere para validar el bloque (Dai & Vasarhelyi, 2017; Cachin & Vukolić, 2017). A su vez, los desarrollos actuales operan sobre plataformas que han ido surgiendo de forma desordenada y esporádicas que exigen que en este momento puedan ser interoperativas con el fin que todas las aplicaciones puedan ser compatibles (Cai, 2021). No es menos importante recabar en el dilema en que se encuentra la configuración de blockchain en ocasiones, reside en tener que saber conciliar características destacadas de la tecnología, como es la transparencia o la inmutabilidad en el registro de los datos, con otros intereses empresariales y la necesidad de respetar la privacidad. La búsqueda del equilibrio entre la transparencia y la privacidad se ha intentado encontrar en el diseño de diferentes tipologías de redes, pero también en los tipos de consenso y, por supuesto, en los protocolos criptográficos, con el fin de garantizar que blockchain sea una tecnología segura y confiable para los usuarios. Es por este motivo por el que este trabajo se siente obligado a entrar en tales aspectos.

3. Tipos de Redes

La clasificación de las redes blockchain responden, fundamentalmente, al grado de privacidad y las restricciones al acceso que se hayan establecido. Concretamente, se diferencia entre redes

abiertas o públicas, privadas o permisionadas e híbridas, que también toman el nombre de federadas o de consorcio (Butterin, 2015; O'Leary, 2017).

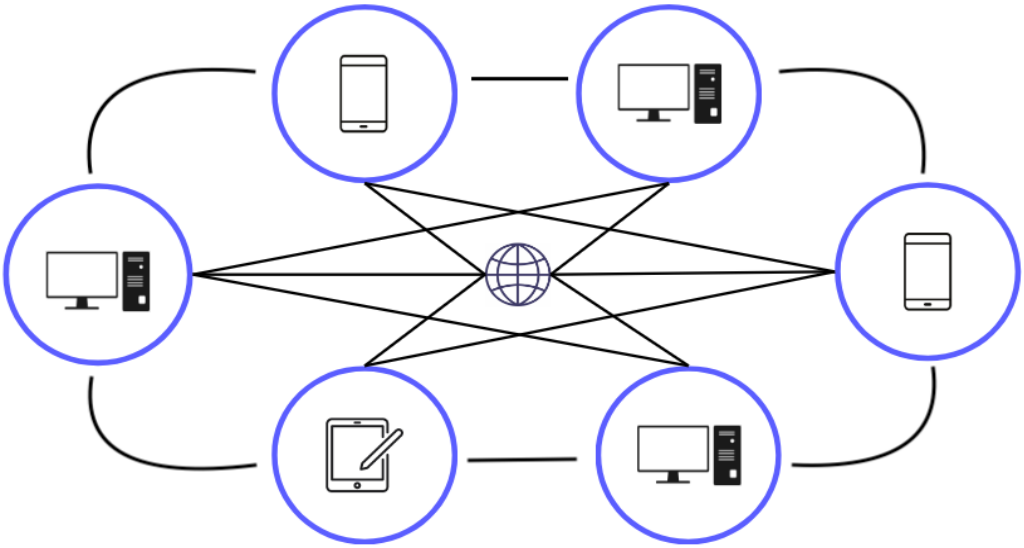
En el momento en que la tecnología blockchain comenzó a ser utilizada, las redes eran eminentemente públicas, ya que se pretendía conseguir hacer posible las transacciones de criptomonedas sin intermediación (Nakamoto, 2008) entre cualquier usuario que estuviera interesado. Con este objetivo, de hecho, nacieron redes públicas como Bitcoin o Ethereum que pretendían que las transacciones con criptomonedas estuvieran al alcance de todos. Sin embargo, progresivamente, otros intereses económicos, políticos y corporativos entraron en juego e impulsaron la aparición de nuevos tipos de cadenas de bloques que incluían condiciones a la hora de comenzar a formar parte de estas. Los gobiernos, las empresas y otros agentes de la vida económica y social comenzaron a utilizar la tecnología blockchain para aplicar sus propios proyectos, diseñando cadenas de bloques permisionadas, a las que solo tendrían acceso los usuarios seleccionados. Atendiendo a este marco, podemos profundizar en los tres tipos fundamentales de redes blockchain, las características y, especialmente, las utilidades de cada una de ellas.

3.1 Blockchain pública

Las redes blockchain públicas son aquellas que están abiertas a cualquier usuario y, por tanto, aquellas en las que cualquier persona tiene capacidad para introducir cambios y consultar la información registrada. Al ser de código abierto, cualquiera puede convertirse en miembro y generar un nodo, leer la información registrada, hacer transacciones y participar en el consenso requerido para introducir nuevos bloques (Appelbaum & Smith, 2018).

Un rasgo fundamental de las redes de esta naturaleza se encuentra en que al existir innumerables ordenadores o nodos conectados, la información se almacenada en todos ellos, consiguiendo una gran seguridad al tener que ser igual en todos. Además, muchas de ellas mantienen el principio del anonimato por el que se puede conocer la dirección de email del usuario pero no así su identidad completa. De hecho, ello es una de las principales características de Bitcoin, donde las transacciones se realizan con pseudónimos y las direcciones de Bitcoin no están asociadas directamente con la identidad real del usuario.

Figura 08: Red abierta



Fuente: Elaboración propia

En suma, esta tipología de red representa la máxima descentralización, pues el registro y la validación se realiza de manera distribuida entre los miembros de la red sin que exista ninguna autoridad central que pueda controlar o modificar el registro; y completa transparencia, pues cualquier persona podría acceder a la cadena y consultar el historial completo de registros. Como consecuencia de estas características, se abren nuevas posibilidades en la economía digital y, más allá de Bitcoin y Ethereum, principales plataformas blockchain públicas, una configuración de esta tipología tendría una gran utilidad en el ámbito del sector público y, en concreto, en materias que afecten a la aplicación de los presupuestos generales del Estado y de las cuentas públicas en general, haciendo posible una transparencia total de la información, con el valor añadido que es segura y verificable.

Sin embargo, las redes públicas y abiertas, a pesar de proporcionar completa transparencia, no tienen en cuenta otros intereses especialmente relevantes para empresas, ya que es posible que estas no quieran revelar información relativa a estrategias o transacciones que muestren datos que no desean desvelar. Es por ello, que muchos proyectos se han dirigido al diseño de redes permisionadas y, adicionalmente, al estudio de nuevos tipos de consenso y de técnicas que aseguren la privacidad y la confidencialidad de información delicada.

3.2 Blockchain privada

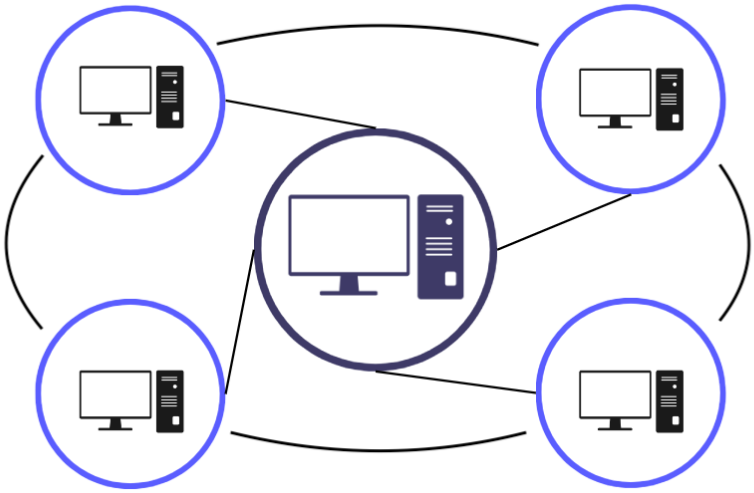
Una red blockchain privada, a diferencia de las anteriores, cuenta con restricciones para el acceso a la vez que puede asignar diferentes roles a los integrantes de la red. Así, en las cadenas de bloques permisionadas se necesita reunir una serie de condiciones para ser miembro de ellas. Se caracterizan porque cuentan con un nodo central que controla el acceso a las mismas de manera que solo las personas autorizadas y, en cierta forma seleccionadas, podrán participar en la blockchain.

Igualmente, se podrían establecer roles de forma que habría diferentes estatus entre los integrantes. Ello implicaría que solo los participantes seleccionados podrían consultar la información registrada, registrar información, participar en el consenso para añadir un nuevo bloque o en la aprobación de nuevos miembros de la red. El rango de restricciones o privilegios puede variar en gran medida hasta el punto de existir redes que otorgan el privilegio de anulación de registros a un nodo central aún a riesgo de debilitar la credibilidad de la cadena de bloques y poner en cuestión su propia naturaleza (Liu et al, 2019)

Las redes permisionadas responden a los intereses de gobiernos y empresas, que desean que cierta información no se encuentre a disposición de cualquier persona en la red, haciendo compatible las características de la blockchain con la eficacia de los proyectos que pretenden desarrollar. Sin embargo, como consecuencia de que hay un nodo central que tiene privilegios para controlar en mayor o menor medida la red—estamos ante una red parcialmente descentralizada—, la credibilidad en la información registrada podría verse afectada. La veracidad de las transacciones y demás registros depende, por tanto, del prestigio y la confianza que genere la empresa o institución que actúe como agente central y del sistema de consenso que se establezca (Kosmarski, 2020).

En definitiva, estamos ante cadenas de bloques que priorizan la privacidad que una red pública no puede garantizar, menoscabando algunos rasgos característicos de la tecnología. El control que se ejerce sobre la selección de los miembros que tienen acceso a la información, lleva a que ya no se puede afirmar con la misma firmeza que la red es completamente descentralizada e inmutable, ni que la información es completamente transparente ya que, como se ha dicho, existe un agente central que controla la red. En algunos casos puede tener la facultad de anular registros y en otros puede que se establezca que solo unos determinados miembros de la red cuenten con una copia de la cadena o que participen en el consenso.

Figura 09: Red permisionada



Fuente: Elaboración propia

Ejemplos de cadenas de bloques privadas son R3 Corda e Hyperledger Fabrik de IBM, propias de plataformas de aplicaciones empresariales y financieras. En concreto, Hyperledger Fabric se centra en construir redes privadas con mayor control sobre los permisos y la participación de los nodos y Corda se ha empleado mucho al permitir la transferencia segura de activos y datos entre las partes de un acuerdo comercial.

3.3 Blockchain Híbridas, de consorcio y federadas

Las redes híbridas reúnen características de las dos tipologías anteriores. Lo más habitual es que, por un lado, al igual que lo que sucede en las redes públicas, no hay ninguna exigencia concreta para participar en las mismas (no hay restricciones al acceso). Sin embargo, a diferencia de lo que sucede en esas redes abiertas, en la validación solo pueden intervenir una parte de los miembros de la red.

De esta manera, se consigue combinar el mantenimiento de cierta privacidad y seguridad, al poder establecer diferentes roles entre los miembros de la red, y la transparencia —aunque puede que no sea total—. Un ejemplo es Dragonchain, una plataforma híbrida desarrollada por Disney, si bien pasó a código abierto posteriormente, en la que las transacciones se llevan a cabo en una cadena pública que está interconectada con cadenas privadas secundarias, que

permiten a las empresas tener un mayor control sobre su información, a la vez que la cadena pública garantiza la inmutabilidad y la transparencia.

En ocasiones se matiza y se denomina de forma partcular este tipo de redes atendiendo a algunos aspectos de su funcionamiento. Así, se habla de blockchain de consorcio cuando varias organizaciones se unen para compartir datos y realizar transacciones de manera más eficiente y segura. Y se denomina blockchain federada cuando se establece un grupo de nodos validadores que son elegidos por el conjunto de organizaciones o participantes de la red.

3.4 Redes tokenizadas o no tokenizadas

Desde otra perspectiva, las redes también se pueden clasificar según utilicen tokens o no. Un token es una unidad digital que representa un activo o valor específico o una cuota del activo que se ha dividido en unidades más pequeñas o una utilidad. Los tokens pueden ser definidos igualmente como pruebas de derechos digitales (Xu et al., 2019).

De acuerdo con este criterio de clasificación, las cadenas de bloques tokenizadas utilizan tokens y realizan un proceso de consenso a través de la minería para crear una criptomoneda para sus operaciones o registros. Bitcoin y Ethereum son ejemplos de este tipo. En cambio, las cadenas de bloques sin token son cadenas de bloques que no tienen una unidad para la transferencia de valor y se utilizan para compartir información entre los miembros de una red (Bashir, 2018).

4. Tipos de consenso

En blockchain, existen diferentes mecanismos de consenso por los que los nodos de la red llegan a un acuerdo para validar transacciones y registrar información en el libro mayor distribuido de la cadena de bloques. Los protocolos de consenso en blockchain utilizan técnicas criptográficas para lograr el objetivo de garantizar la integridad y la seguridad de la red. En definitiva, son un conjunto de reglas y procedimientos que rigen el acuerdo entre los nodos, utilizando técnicas criptográficas como el cifrado de clave pública, las funciones hash, la firma digital y los algoritmos de prueba para garantizar la seguridad y la integridad de la red. Estos `pueden ser de diferente tipo y están en constante evolución, siendo los más conocidos y usados los siguientes:

- Prueba de trabajo o Proof-of-Work (PoW) es el mecanismo de consenso más conocido porque es utilizado por Bitcoin. En PoW, los nodos compiten entre sí para resolver un

problema matemático complejo, de tal forma que el primer nodo que lo resuelve tiene el derecho a agregar un bloque a la cadena y recibir una recompensa. Estos usuarios se denominan mineros y realizan un trabajo computacional intensivo para resolver el acertijo, con lo que este proceso consume mucha energía y es lento, pero es muy seguro (Conti et al., 2018).

- Prueba de participación o Proof-of-Stake (PoS) elige de forma aleatoria al nodo validador, pero ha de cumplir un conjunto de requisitos que están en función del compromiso que haya demostrado tener con la red. Este compromiso se mide atendiendo al número de participaciones, el tiempo de permanencia o la cantidad de monedas que posean. Cuanto mayor valor tengan esas variables, mayor probabilidad tendrá de ser elegido. Con ello, PoS es más eficiente energéticamente, así como más escalable que PoW (King et al., 2012).
- Prueba de autoridad o Proof-of-Authority (PoA): un grupo de nodos autorizados es el encargado de validar las transacciones y agregar bloques a la cadena. Los nodos son seleccionados por la red y son conocidos por todos los participantes. No pueden registrar más de un bloque seguido con el fin de evitar manipulaciones. PoA es muy rápido y consume poca energía, pero es más centralizado que los anteriores y, de ahí que sea más utilizado en blockchains privadas (Wang et al., 2022)
- Prueba de participación delegada o Delegated Proof of Stake (DPoS): en este algoritmo de consenso, los participantes de la red votan a los denominados nodos testigos o delegados para validar las transacciones y agregar bloques en su nombre. Estos nodos son elegidos por votación y reciben recompensas por su trabajo, incentivados para actuar de manera honesta, ya que si no actúan bien o de forma fraudulenta son expulsados de la comunidad (Salimitari et al., 2019).
- Prueba de participación alquilada o Leased Proof of Stake (LPoS) es una versión mejorada de Prueba de Participación que permite que los usuarios presten sus tokens a los validadores. A cambio, estos comparten una parte de sus ganancias con los arrendadores. Es utilizado en la plataforma Waves (Salimitari et al., 2019).
- Prueba de capacidad o Proof of Capacity (PoC): es un algoritmo de mecanismo de consenso que permite a los dispositivos de minería en la red utilizar el espacio disponible en el disco duro para decidir los derechos de minería y validar transacciones. No requiere tanto poder computacional como en el algoritmo de prueba de trabajo o el algoritmo de prueba de participación (Porta, 2019).

- Prueba de tiempo transcurrido o Proof of Elapsed Time (PoET): es propuesto por Intel con el fin de tener un consumo de energía menor, planteando un proceso más eficiente que PoW por el que se elige de forma aleatoria al validador. Al ejecutar un código confiable dentro de un entorno seguro, el algoritmo PoET también mejora la transparencia al garantizar que los resultados sean verificables por participantes externos (Cachin & Vukolić, 2017).
- Prueba de importancia o Proof of Importance (PoI): consiste en un mecanismo que asigna una puntuación a la importancia de cada nodo en la red. Se utilizó por primera vez por NEM. Los nodos deben invertir una cantidad de monedas antes de ser elegibles para llevar a cabo la minería de bloques en proporción a la puntuación que indica su contribución a la red. A diferencia de Prueba de Participación (PoS), la puntuación no solo depende del monto total invertido por un nodo, sino también de muchas otras variables como los grupos de actividad, la reputación y las transacciones realizadas a través de cualquier dirección dada (Xiao et al., 2021).
- Prueba de actividad o Proof of Activity (PoA): es un consenso que combina PoW y PoS. Los mineros resuelven una ecuación matemática y una vez que se extrae el nuevo bloque, el sistema pasa a funcionar como Proof of Stake (PoS), disminuyendo a prácticamente a cero las posibilidades de un ataque del 51% (Zheng et al., 2018).
- Prueba de quemado o Proof of Burn (PoB), es un mecanismo por el que los usuarios queman o destruyen monedas para demostrar que tienen interés legítimo en la red, enviando las criptomonedas a una dirección de quemado o "burn address" que es inaccesible y no se puede recuperar. Esta acción se registra en blockchain y el usuario recibe una recompensa proporcional al valor de las criptomonedas que quemó (Menon et al., 2022).

Hay otro bloque de métodos basados en el consenso bizantino, que requieren una subdivisión o, al menos, unas líneas dedicadas a su fundamento. En los métodos de consenso bizantino se afronta el problema de coordinación en sistemas distribuidos donde algunos nodos pueden fallar o ser maliciosos. El problema es garantizar que los nodos restantes puedan llegar a un acuerdo sobre una decisión común, incluso si algunos nodos intentan sabotear el proceso. Se basan en el conocido problema de los generales bizantinos, creado para ilustrar el dilema de lograr un consenso entre los generales (usuarios) que tienen un objetivo común cuando entre ellos pueden existir traidores. Esto es, se contempla la posibilidad que entre ellos pueda existir uno o varios con intereses opuestos a la mayoría y que intenten hacer fracasar el proceso.

Además, da por supuesto que la comunicación entre los generales es limitada y no siempre segura. El planteamiento del problema simula un escenario de guerra, en donde los generales están acampados y sitiando una ciudad. Tienen que observar los movimientos del enemigo y comunicar sus observaciones para consensuar el plan de ataque entre ellos. Pero esta comunicación se realiza a través de mensajeros y no se descarta que algunos generales sean traidores, siendo factible que algunos mensajes contengan información errónea y mal intencionada. El algoritmo que solucione el problema debe asegurar que todos los generales leales adopten el mismo plan de ataque y que los traidores no logren engañar y hacer que el plan adoptado sea erróneo (Lamport et al., 1995). Para tal fin, existen distintos algoritmos, siendo los más utilizados los siguientes.

- Tolerancia práctica de fallas bizantinas o Practical Byzantine Fault Tolerance (PBFT), se utiliza especialmente en blockchains permisionadas, donde un conjunto limitado de nodos son responsables de validar y confirmar transacciones. El proceso de consenso en el algoritmo PBFT se divide en varias rondas. En cada ronda, un nodo se selecciona como líder y propone un bloque de transacciones. Los demás nodos validan el bloque y votan sobre su aceptación. Si la mayoría de los nodos votan a favor del bloque, se agrega a la cadena de bloques. Si no, se descarta el bloque y se inicia una nueva ronda. Se requiere que al menos dos tercios de los nodos sean honestos y estén en línea para garantizar la integridad de la base de datos. Además, el algoritmo PBFT utiliza un sistema de firma digital para garantizar que los mensajes provengan de nodos auténticos y no hayan sido falsificados o modificados de manera malintencionada (Swan, 2018; Xu et al., 2021).
- Tolerancia delegada de fallas bizantinas o Delegated Byzantine Fault Tolerance (dBFT), se aplica en blockchains públicas como NEO y ONTology, así como en blockchains permisionadas como Hyperledger Fabric. En este algoritmo, un conjunto limitado de nodos (validadores) son elegidos para validar y confirmar transacciones en la red. La principal diferencia con PBFT es que en dBFT, los nodos son elegidos mediante un proceso de votación o delegación (Comben, 2019).
- Protocolo de consenso estelar o Stellar Consensus Protocol (SCP), es una variante de PBFT que se denomina tolerancia de falla bizantina federada (FBFT) que consta de dos pasos, protocolo de nominación y protocolo de votación, que en ese orden se procesan con el fin de aceptar o rechazar los valores (Salimitari et al., 2019).

5. Plataformas blockchain

Una plataforma blockchain es un software que puede estar respaldada por una entidad que la mantiene y desarrolla, que sirve de marco y vehículo para la creación y gestión de aplicaciones y servicios basados en la tecnología blockchain. Por tanto, estas plataformas contienen registros descentralizados donde la información permanece inalterable, segura y transparente. Las plataformas blockchain se encuentran en constante evolución, existiendo una gran variedad que han ido adaptándose a las necesidades específicas que han ido surgiendo.

Bitcoin, además de la primera criptomoneda que surgió, es la primera plataforma blockchain en crearse (Nakamoto, 2009) y una de las más conocidas. Utiliza una blockchain pública y completamente descentralizada para registrar todas las transacciones que se realizan con criptomonedas Bitcoin. Esta plataforma se ha convertido en un medio de intercambio digital global y en una forma de inversión alternativa a pesar del intenso debate que genera en este aspecto y la altísima volatilidad que conlleva. Entre sus características, destaca el anonimato de las transacciones, ya que las direcciones de Bitcoin no están directamente asociadas con la identidad real del usuario; el sistema de incentivos que supone utilizar la minería como modo de validación (se premia con criptomonedas); y el hecho de que Bitcoin sea una criptomoneda digital escasa (existe un límite en la emisión de Bitcoin). Sin embargo, dejando a un lado la revolución que supuso al ser pionera en utilizar la cadena de bloques, no tiene especiales implicaciones como soporte en el ámbito contable y auditor porque no permite la inserción de smart contracts.

Ethereum es, junto a Bitcoin, la plataforma más influyente y destacada. Fue creada por Vitalik Buterin (2015) y el tiempo ha demostrado que es algo más que una criptomoneda y un instrumento para registrar las transacciones realizadas con ella. La moneda nativa se denomina ether (ETH) que, si bien se usa para pagar transacciones, no todas las aplicaciones construidas en ethereum requieren el uso de criptomonedas. Ethereum permite a los desarrolladores crear nuevos tipos de tokens basados en ETH que alimentan dApps mediante el uso de contratos inteligentes, pero no es necesario que todas las aplicaciones construidas en Ethereum tengan una criptomoneda. Es por ello que es considerado uno de los principales instrumentos para desarrollar el fenómeno de la tokenización, pues facilita la creación de tokens como representaciones digitales de un activo (bien físico, derechos en general, de propiedad, acciones, criptomonedas…) dentro de la red. Esta plataforma y, concretamente, la posibilidad de ejecutar contratos inteligentes tendría un gran impacto en la contabilidad al permitir la

automatización de procesos, garantizar cumplimiento automático de acuerdos, proporcionar un registro inmutable y facilitar la auditoría en tiempo real, como se explicará posteriormente.

Al margen de las dos principales plataformas, han surgido muchas otras para hacer frente a nuevas necesidades. Por un lado, se pueden encontrar redes centradas en la privacidad y la confidencialidad como Corda que persiguen la transferencia segura de activos y datos entre las partes involucradas en un acuerdo comercial. Por otro lado, existen plataformas que tratan de conseguir la interoperabilidad entre diferentes blockchains y acabar con el problema de la fragmentación y la falta de comunicación entre ellas, como Cosmos o Polkadot. En el ámbito de la Administración pública, existen redes y proyectos encaminados a aumentar la transparencia y la eficiencia del área. Por ejemplo, Estonia utiliza la tecnología blockchain para almacenar y proteger los registros médicos de los ciudadanos, mantener un registro seguro de los datos relativos a ciudadanía y residencia, y, a través del programa E-Residency, permite que cualquier persona pueda convertirse en residente digital de Estonia y, gracias a ello, acceder a servicios gubernamentales en línea, firmar documentos digitales, así como establecer y gestionar negocios en Estonia.

En el área contable, se recurre con mucha frecuencia a IOTA e Hyperledger Fabric. Hyperledger Fabric es utilizado fundamentalmente para fines empresariales ya que, además de admitir los smart contracts como Ethereum, permite construir redes privadas o permisionadas con mayor o menor control sobre los permisos y la participación de los nodos. IOTA, por su parte, implementa un modelo de contabilidad de triple entrada conocido como “Tangle” que facilita las transacciones y comunicaciones entre los dispositivos conectados a la red.

En definitiva, existe una gran variedad de plataformas con características y enfoques diferenciados, que cuentan con sus propias fortalezas y debilidades y que son idóneas para unos casos determinados y no otros. Como ya se ha dicho, existen plataformas diseñadas específicamente para campos de acción específicos como es el ámbito empresarial o la administración pública. Por ello, es importante seleccionar la plataforma adecuada teniendo en cuenta las características y limitaciones de cada una de ellas, aunque es importante resaltar que la tendencia para el futuro es la interoperabilidad y, probablemente ello conlleve una convergencia entre ellas.

IV. Aplicación a la contabilidad y auditoría

Son muchas las contribuciones de las tecnologías emergentes que impulsan un cambio en los diseños de negocio y, consiguientemente, en los mecanismos de registro y elaboración de la información, control, auditoría y análisis de los estados contables. Entre todas ellas hay que destacar la inteligencia artificial y blockchain por sus aplicaciones disruptivas. Blockchain ha demostrado su capacidad de generar confianza y el resto de los rasgos característicos que se han expuesto en los apartados anteriores. Y la inteligencia artificial, por su parte, evidencia su potencial para automatizar procesos, analizar problemáticas, aprender y tomar decisiones.

La combinación de ambas tecnologías da lugar a desarrollos con implicaciones de largo alcance en el ámbito de la contabilidad y las finanzas, en primer lugar, porque contribuye a superar la crisis de confianza existente en la actualidad que se ha acentuado tras los escándalos financieros que se han sucedido desde principios de siglo. Entre otros, cabe referenciar la desaparición de Arthur Andersen, una de las firmas de contabilidad y auditoría más grandes del mundo, debido a su implicación en el escándalo de Enron en 2001. Arthur Andersen fue acusada de encubrir irregularidades contables y destruir documentos relacionados con la auditoría de Enron. Estas acciones erosionaron la confianza del público y dañaron seriamente la reputación de la firma. Como resultado, las acusaciones llevaron a demandas y sanciones legales, que finalmente llevó a la empresa a perder muchos clientes y a su posterior quiebra en 2002. La quiebra de Lehman Brothers, una de las instituciones financieras más grandes, la crisis financiera de 2008, así como diversos escándalos financieros, han ido socavando progresivamente la confianza en la información contable (Betta, 2016).

Ante tal crisis de confianza, muchas asociaciones profesionales de contabilidad y auditoría han reconocido el impacto y el potencial de blockchain para dar mayor consistencia a los informes contables, mayor eficacia y transparencia, así como combatir la percepción y los mecanismos de corrupción. International Federation of Accountants (IFAC) ha publicado informes y guías relacionadas con blockchain y su aplicación en la contabilidad y la auditoría. Han destacado los beneficios de la tecnología blockchain en términos de transparencia, seguridad y eficiencia en los procesos financieros. American Institute of Certified Public Accountants (AICPA) ha reconocido el papel de blockchain en la transformación de la profesión contable. Han promovido la educación y el conocimiento sobre blockchain y han desarrollado recursos para ayudar a los profesionales contables a comprender y adoptar la tecnología. Institute of Chartered Accountants in England and Wales (ICAEW) también ha publicado informes y

artículos que exploran el impacto de blockchain en la profesión contable y la necesidad de comprender su funcionamiento y las implicaciones que ofrece la tecnología. Chartered Professional Accountants of Canada (CPA Canada) ha estudiado los desafíos y las oportunidades relacionados con blockchain en la profesión contable, promovido la formación en estas materias y alentado la adopción de la tecnología en la práctica contable (AICPA, 2021; ICAEW, 2018; CAANZ, 2020). La Asociación Española de Contabilidad y Administración de Empresas (AECA) dedica varios documentos con igual propósito y, así seguiría una larga lista de pronunciamientos de organizaciones competentes a nivel nacional e internacional que emiten declaraciones o informes que tratan estas tecnologías y sus implicaciones.

A estas iniciativas de las organizaciones profesionales sólo hay que añadir las actuaciones de las cuatro grandes empresas de auditoría --Deloitte, PwC, Ernst & Young (EY) y KPMG) – para comprobar la dimensión que está tomando la aplicación de estas tecnologías emergentes en contabilidad y auditoría. Los cuatro grandes han creado grupos de trabajo y aplicaciones de distinta índole para sus clientes y para su propio uso. Han desarrollado programas de auditoría que utilizan blockchain e inteligencia artificial que permiten a los auditores validar la integridad y la autenticidad de la información contable y ayuda tanto a identificar como a mitigar los riesgos de fraude y errores. Estas herramientas proporcionan una mayor transparencia y eficiencia en las auditorías. En síntesis, los programas desarrollados contienen las funciones de validación, análisis de datos en tiempo real, detección de patrones y anomalías, monitoreo, automatización de procesos, comprobaciones de cumplimiento y generación de informes. Permiten acceder a los datos registrados en blockchain en tiempo real y tienen una estructura modular en forma de suite donde se integran otras herramientas (Coyne & McMickle, 2017; Dai & Vasarhelyi, 2017; Kokina et al., 2017; Ferri et al., 2020; Schmitz & Leoni, 2019; KPMG, 2018; Deloitte, 2020; EY, 2020; PwC, 2020). Así pues:

- Ernst & Young ha desarrollado el programa de auditoría EY Blockchain Analyzer que integra otras herramientas como EY Canvas y EY DnA de análisis de datos que utilizan tecnología de aprendizaje automático para ayudar a los auditores a identificar patrones y anomalías en grandes conjuntos de datos. EY Helix es una plataforma de auditoría digital para trabajar de manera más eficiente y efectiva utilizando recursos de automatización y análisis avanzados de datos. Para la automatización de procesos repetitivos utiliza EY Synapse y para la auditoría de datos en la nube emplea EY Atlas.

- KPMG Chain Fusion es el programa de auditoría de KPMG que integra distintos módulos entre los que destacan KPMG Clara de análisis de datos, KPMG Ideation Challenge que es una plataforma colaborativa con empleados y clientes, KPMG Digital Labor por la que se automatizan procesos robóticos para tareas repetitivas y KPMG Risk Intelligence Platform para el análisis de riesgos.

- PwC Halo es el programa que utiliza PwC en donde integra, entre otras herramientas, Data analysis tools para procesar grandes volúmenes de información y detectar patrones y tendencias en los datos, Robotics process automation (RPA) para la automatización de tareas repetitivas y mejorar la eficiencia operativa, PwC's Global Investigative and Dispute Services (GIDS) para la resolución de conflictos y para identificar posibles irregularidades y fraudes en los datos empresariales, PwC's Cybersecurity and Privacy team, para garantizar la seguridad de los datos y protegerlos de amenazas cibernéticas.

- Deloitte ha desarrollado Deloitte Blockchain-Based Audit Tool, un programa de auditoría que concentra herramientas como Deloitte Risk Explorer para análisis de riesgos en tiempo real y priorizar las áreas en las auditorías, Deloitte AuditConnect para la colaboración en línea entre auditores y clientes con el fin de trabajar juntos en tiempo real y compartir documentos y comunicarse de manera eficiente, Deloitte Analytic Insights Module para el análisis de datos que utiliza tecnologías de big data, Deloitte Connect por la que proporciona información sobre el estado de la auditoría, incluyendo el calendario, las personas involucradas y los informes.

A su vez, las cuatro grandes han generado aplicaciones para sus clientes y han creado servicios que están íntimamente ligados a la veracidad y seguridad de las operaciones y de la información registrada. En este sentido, cabe citar la plataforma blockchain llamada "Smart Identity" creada por Deloitte para proporcionar soluciones de identidad digital y la autenticación de usuarios. Con propósito semejante, PwC ha desarrollado "Smart Credentials", una plataforma de identidad digital que utiliza blockchain para almacenar y verificar credenciales. Por su parte, KPMG ha creado la plataforma blockchain llamada "KPMG Origins" que se utiliza para rastrear la cadena de suministro de productos y mejorar la transparencia, desde la producción hasta la venta al cliente final. Y un último ejemplo, íntimamente relacionado con uno de los propósitos de este trabajo como se verá más adelante, es la solución de Ernst & Young denominada "EY Blockchain Analyzer and Zero Knowledge Proof" que combina la tecnología

blockchain con el concepto de "Zero Knowledge Proof" (Prueba de Conocimiento Cero) para permitir la validación de datos sin revelar información confidencial.

1. Contabilidad de Partida Triple (o Triple Entrada)

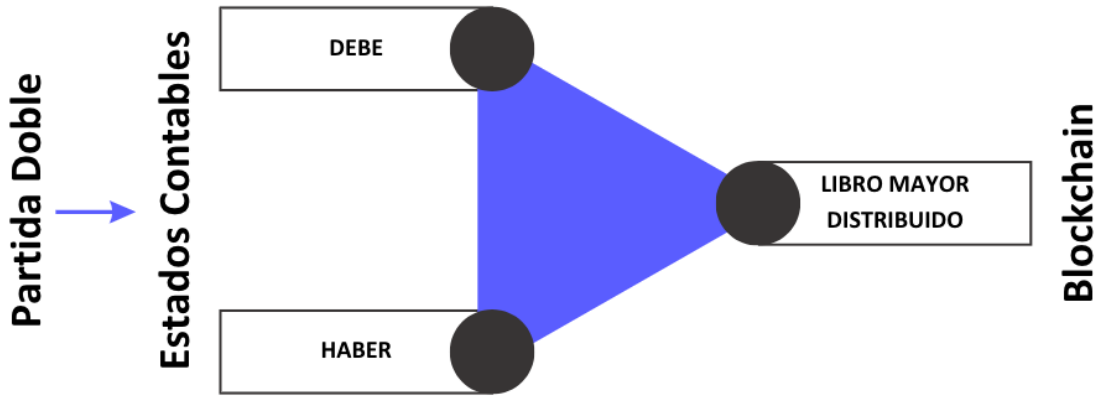
En la historia de la contabilidad se puede seguir el avance hacia un método que permita expresar la imagen fiel de la situación económico-financiera de una entidad de forma que proporcione un sistema de información para su análisis y toma de decisiones, previendo situaciones de riesgo y evitando el fraude. Así, la primitiva contabilidad de partida simple, muy inconsistente y propensa a cometer errores y fraude fue superada en el renacimiento por la contabilidad de partida doble. Dicho sistema de registro, el de partida doble, en el que se basa la contabilidad moderna y cuyo origen se encuentra en Luca Pacioli (1494), mejora en gran medida la confianza ya que, el principio de dualidad y el propio método exigen comprobaciones, facilitando de esta forma la evitación de errores y el control. Sin embargo, a pesar de que la contabilidad de partida doble mejora la información y reduce riesgos de fraude, no termina de evitarlos por la unilateralidad de los registros y la posibilidad que estos sean falseados. Ante ello, surge la necesidad de auditoría con el fin de que, a través de las opiniones de unos profesionales en la materia, se pueda considerar que la información recogida en las cuentas anuales de la empresa es ajustada a su realidad económico-financiera. No obstante, la auditoría en el momento actual cuenta con diversos problemas que hacen imposible acabar con la crisis de confianza existente. Entre ellos destacan dos: por un lado, el auditor basa su análisis en una muestra y no en la totalidad de los datos contables; por otro, hay un amplio espacio de tiempo desde el fin del periodo contable y la presentación de las cuentas anuales para que estas puedan ser auditadas. Por uno y otro motivo, en esos intervalos de tiempo, las cuentas puede ser objeto de manipulación o presentarse riesgos no previstos con suficiente antelación (Cai, 2019). De ahí, que de la mano de las tecnologías actuales se pueda impulsar el tránsito de la partida doble a la partida triple o de triple entrada, después de más de quinientos años y que esta nueva metodología marque la pauta de una nueva era en la historia de la contabilidad. Ello no va a significar una ruptura sino el aporte de un registro complementario para la información contable.

La primera referencia relevante de una contabilidad de triple entrada hay que encontrarla en Ijiri (1986) al proponer incorporar a los débitos y créditos tradicionales, una tercera entrada que registre en qué medida ese hecho contable contribuye a los objetivos y metas económicas

de la entidad. Sin embargo, el propósito actual de la contabilidad de triple entrada es diferente y se fundamenta en el planteamiento de Ian Grigg (2005), que si bien es anterior a la aparición de blockchain se realiza sobre la tecnología de bases de datos distribuidas y fundamenta su viabilidad.

La contabilidad de partida triple implicaría utilizar la tecnología blockchain para dotar al sistema contable de mayor eficiencia, transparencia, inmediatez y seguridad y, en definitiva, implicaría que la información recogida en las contabilidades propias de las empresas que interactúan entre sí —u otro tipo de agentes como instituciones o particulares—, estuviera a su vez, registrada en una cadena de bloques. Así, no estamos ante una tercera anotación con nuevas cuentas junto al debe y el haber como propuso Yuri Ijiri en 1986, sino ante un "respaldo" en la cadena de bloques con importantes implicaciones porque facilita el intercambio de libros contables inmutables (Dai & Vasarhelyi, M.A. 2017; Wanden-Berghe & Fernández Daza, 2018a; Wang & Kogan, 2018).

Figura 10: Contabilidad de partida triple

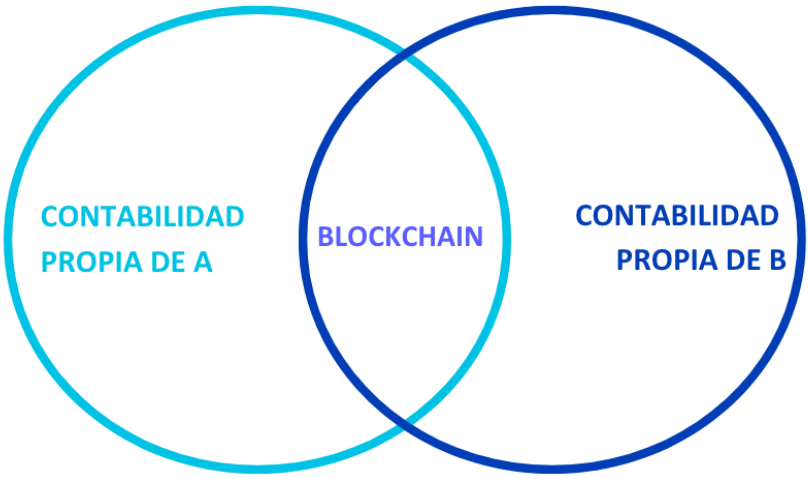


Fuente: Adaptado de Wanden-Berghe & Fernández Daza (2018a)

Por otra parte, blockchain es un registro distribuido que si se produce una transacción entre dos partes, estas insertan dicha información en un bloque que disfruta de todas las propiedades descritas anteriormente (seguridad, verificabilidad, inmutabilidad etc). Así, las partes, llevan sus propias contabilidades por partida doble, pero añaden e insertarían la información de la

transacción en una cadena de bloques que funciona como la tercera entrada. Este tercer registro valida la operación y dependiendo de la configuración de la red, quedará accesible de forma pública o solo podrán tener acceso a la información usuarios autorizados. El método implica que ninguna de las partes puede registrar algo diferente en sus propias contabilidades ni pueden cambiar o modificar la información registrada por la inmutabilidad de los registros en la cadena de bloques. Por otra parte, reguladores, autoridades tributarias, auditores, jueces, entidades certificadoras y otros usuarios implicados, podrían solicitar acceso a la red para proceder a sus funciones con fines tan diversos como la consulta, la fiscalización o la revisión.

Figura 11: Blockchain compartida



Fuente: Elaboración propia

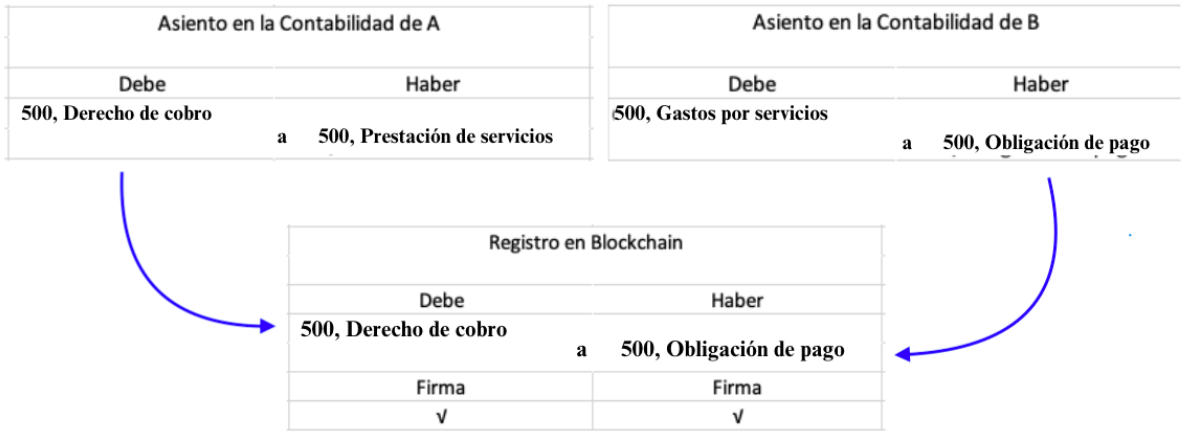
1.1 Operatividad de un sistema de contabilidad de partida triple

Para ilustrar cómo funcionaría un sistema de contabilidad de triple entrada utilizando blockchain en la práctica, supóngase que el agente A realiza una acción-petición que sería transmitida a todos los miembros de una red. Dicha acción-petición, sería validada por la red a través del algoritmo de consenso, creando un nuevo bloque que se enlazaría a la cadena y almacenando una copia idéntica en todos los nodos. Finalmente, el agente B recibiría la contraparte, como podría ser la recepción de fondos. Con este sistema, el registro en blockchain serviría de comprobante o recibo de la operación realizada, firmado digitalmente y consensuado por las partes que encontraría su respaldo en la confianza que proporciona la

tecnología. El atractivo de la idea reside en que las partes llevarían sus contabilidades de partida doble respectivas con sus consiguientes registros de debe y haber, respaldados y coincidentes con el registro en blockchain —que incluso podría estar conectado con los sistemas de contabilidad individuales a través de la programación y automatización del proceso— ya que en la transacción registrada, el debe anotado por una de las partes, es el haber registrado por la otra (Cai, 2019).

La Figura 12 presenta el caso de que la empresa A realiza una prestación de servicios a la empresa B por el importe de 500€. Por un lado, y al igual que sucede con el modelo utilizado actualmente de doble partida, tanto la empresa A como la empresa B registran en sus contabilidades la transacción correspondiente, figurando como ingreso para la primera y su consiguiente derecho de cobro, mientras que se anotaría como un gasto en la segunda con su correspondiente obligación de pago. En un sistema de triple entrada, a la vez que se realizan dichos registros, la empresa A anota un recibo en el tercer registro con su firma; la empresa B, al ver ese recibo, lo aprueba y lo firma igualmente. De esta manera, la transacción (consensuada) queda registrada en la cadena de bloques, lo que asegura la inmutabilidad y la reducción de errores y fraude, pues las empresas A y B no podrían registrar información diferente a la contenida en la cadena. Así, la tercera partida en blockchain serviría de respaldo documental y como soporte para validar la transacción automáticamente.

Figura 12: Soporte de las operaciones en blockchain



Fuente: Elaboración propia

Con este punto de partida, desde la comunidad informática como desde la contable se están desarrollando sistemas de contabilidad compartida que están respaldados por blockchain y que

sugieren soluciones que involucran la auditoría en tiempo real (Vijai et al., 2019; Dai & Vasarhelyi 2017; Alawadhi et al. 2015; Ibañez et al., 2022). Las implicaciones derivadas para la contabilidad son potencialmente importantes y radicales, especialmente cuando se aplica la criptografía avanzada (Rao 2020; Cai 2019; Gröblacher y Mizdraković 2019; Inghirami 2019) y se incluyen en la base de datos distribuida funcionalidades de inteligencia artificial.

2. Incorporación de la Inteligencia Artificial

Si blockchain nos proporciona el marco para hacer posible una contabilidad de partida triple donde las operaciones tienen un respaldo seguro, inmutable y verificable, la inteligencia artificial incorporada a la tecnología, incrementa exponencialmente las posibilidades que esta puede ofrecer, ya que proporciona oportunidades adicionales y mejora aún más la eficiencia y precisión de los procesos contables hasta aspectos que implican la gestión, el análisis y la revisión. Algunas de las aportaciones que realiza son las siguientes:

- Automatización de tareas: La IA puede automatizar tareas contables repetitivas y rutinarias, como la clasificación y la conciliación de transacciones. Al utilizar algoritmos de aprendizaje automático, la IA puede analizar patrones en los datos contables y realizar estas tareas de forma más rápida y precisa.

- Análisis de datos y detección de anomalías: La IA puede analizar grandes volúmenes de datos contables almacenados en la cadena de bloques, identificar patrones, tendencias y anomalías, así como detectar transacciones sospechosas o fraudulentas.

- Mejora de la precisión en la auditoría: La IA puede ser utilizada para realizar análisis avanzados en los datos contables y ayudar a los auditores a identificar áreas de riesgo, realizar pruebas de cumplimiento y evaluar la integridad de los datos contables.

- Generación automática de informes: La IA puede ser utilizada para generar informes financieros y contables de manera automática a partir de los datos almacenados en la cadena de bloques.

Estas son solo una muestra de las formas en que se está utilizando la IA en este contexto. El alcance y la implementación puede variar según las necesidades y los objetivos de cada organización, máxime cuando los recursos de IA están en constante evolución y se pueden desarrollar aplicaciones a medida que la tecnología avanza, sin embargo su herramienta más

empleada para actuar en una red blockchain es el smart contract. (Minsky, 2007; Issa et al., 2016; Moşteanu et al., 2020; Sutton et al., 2016)

2.1 Smart Contracts

Un smart contract (Szabo, 1994, 1997) es un contrato programado para ser ejecutado automáticamente cuando se dan una serie de condiciones. Son códigos que se implementan en scripts y se almacenan en la cadena de bloques, conservando todas las características de la base de datos distribuida: inmutabilidad, inalterabilidad y seguridad. La condición para la ejecución de la orden puede ser simple, es decir, con una sola condición, o por el contrario, reunir un conjunto de requisitos como frecuentemente se establen en cualquier tipo de contrato. Al cumplirse las condiciones, el código se ejecutará con el mandato preestablecido en el código.

Son programaciones del tipo “if-then”, esto es, si se cumple una o varias condiciones, entonces ejecuta la acción. En consecuencia, contienen una estructura de control utilizada en muchos lenguajes de programación para tomar decisiones y ejecutar diferentes bloques de código en función de una condición. La estructura básica de un programa "if-then" es la siguiente:

```
if (condición) {
    // Código a ejecutar si la condición es verdadera
}
```

La "condición" es una expresión booleana que puede evaluar como verdadera o falsa. Si la condición es verdadera, se ejecutará el bloque de código que está dentro de las llaves {}. Si la condición es falsa, ese bloque de código se omite y se continúa con el resto del programa. Esta estructura es la más sencilla, pues a menudo se utiliza una variante denominada "if-then-else" (si-entonces-sino), que permite ejecutar diferentes bloques de código dependiendo del resultado de la condición. La estructura básica de un "if-then-else" es la siguiente:

```
if (condición) {
    // Código a ejecutar si la condición es verdadera
} else {
    // Código a ejecutar si la condición es falsa
}
```

En este caso, si la condición es verdadera, se ejecuta el bloque de código dentro del primer conjunto de llaves {}. Si la condición es falsa, se ejecuta el bloque de código dentro del segundo

conjunto de llaves {}. Por tanto, los programas "if-then" o "if-then-else" son fundamentales para la lógica y el flujo de control en la programación, ya que permiten tomar decisiones y realizar acciones diferentes en función de diferentes situaciones y condiciones.

Esta idea básica puede variar dependiendo de la plataforma blockchain en la que se desarrolle ya que el lenguaje de programación utilizado puede ser diferente. Uno de los lenguajes de programación más comunes para escribir smart contracts es Solidity[4], que se utiliza en la plataforma Ethereum. Un ejemplo de un smart contract en Solidity puede ayudar a comprender su funcionalidad y es el siguiente:

```
pragma solidity ^0.8.0;

contract MiContrato {
    // Variables de estado
    uint256 public miVariable;

    // Evento que se puede emitir
    event ValorActualizado(uint256 nuevoValor);

    // Constructor del contrato
    constructor() {
        miVariable = 0;
    }

    // Función para actualizar la variable
    function actualizarVariable(uint256 nuevoValor) public {
        miVariable = nuevoValor;
        emit ValorActualizado(nuevoValor);
    }
}
```

En este ejemplo, el smart contract tiene una variable de estado llamada miVariable, que se puede acceder de forma pública a través de la función public. También se define un evento llamado ValorActualizado, que se puede emitir cuando la variable se actualiza mediante la función actualizarVariable. El constructor del contrato se ejecuta una vez cuando el contrato se despliega en la red y se establece el valor inicial de miVariable en 0. La función actualizarVariable permite actualizar el valor de miVariable pasando un nuevo valor como

[4] Puede verse programación en https://soliditylang.org/

argumento. Después de actualizar la variable, se emite el evento ValorActualizado para notificar a los posibles observadores.

Este es un ejemplo de un smart contract básico para ilustrar su código, pero suelen ser mucho más complejos y pueden incluir una amplia gama de funcionalidades y lógica empresarial según los requisitos específicos del proyecto. Los smart contracts, por tanto, pueden facilitar innumerables funciones de comprobación como la adherencia de las empresas a diversas leyes y regulaciones (Pilkington, 2016; Wild, 2015) y potencian las posibles aplicaciones de la tecnología en ámbitos como la administración ciudadana, el voto, la sanidad, los seguros o los registros de la propiedad, entre otros, y lógicamente en el campo de la contabilidad y la administración en sentido amplio (Swan, 2015; Atzori, 2015).

En paralelo a los smart contracts, se están desarrollando ideas para implementar sensores en blockchain que aumenten las posibilidades de esta tecnología: detectar en tiempo real irregularidades, lo que tendría importantes implicaciones en la auditoría y el sistema tributario (Psaila, 2017); medir la polución u otras variables y, en general, acentuar la importancia de la contabilidad como instrumento de control y catapultar los recursos de información no financiera para lograr un desarrollo más justo y sostenible (Fernández Daza. & Wanden-Berghe, 2018).

Por tanto, los smart contracts abren la puerta a la automatización de procesos y, consiguientemente, a la mejora de tiempos y reducción de costes. Los avances de programación están permitiendo crear smart contracts complejos que se denominan DApps o aplicaciones descentralizadas y distribuidas en la red. (Lipton & Levi., 2018) De esta manera, la incorporación de smart contracts, que se ejecutan automáticamente si se dan una serie de condiciones, abren inmensas posibilidades para la contabilidad y la auditoría que aumentarían enormemente la eficiencia en distintos aspectos. En las transacciones, al eliminar la intervención humana e incluso no necesitar intermediación, pues la verificación y la expedición de órdenes podrían ser programadas. Simplemente, a través de smart contracts, las partes de la transacción predeterminarían las reglas del pago, por ejemplo, en un contrato digital autoejecutable. Por otra parte, posibilitan ajustarse de forma mucho más sencilla a regulaciones y cumplimientos, estableciendo la normativa a respetar en las condiciones del contrato inteligente. Conviene aclarar que los smart contracts no se limitan a órdenes relacionadas con las transacciones, ya que podrían emplearse para comprobaciones o sustitución de tareas repetitivas que se hacen manualmente o registrar asientos de la regularización contable, como

amortizaciones o deterioros que cabría programar al cumplirse una serie de circunstancias o condiciones, con el fin que se produjera el registro contable.

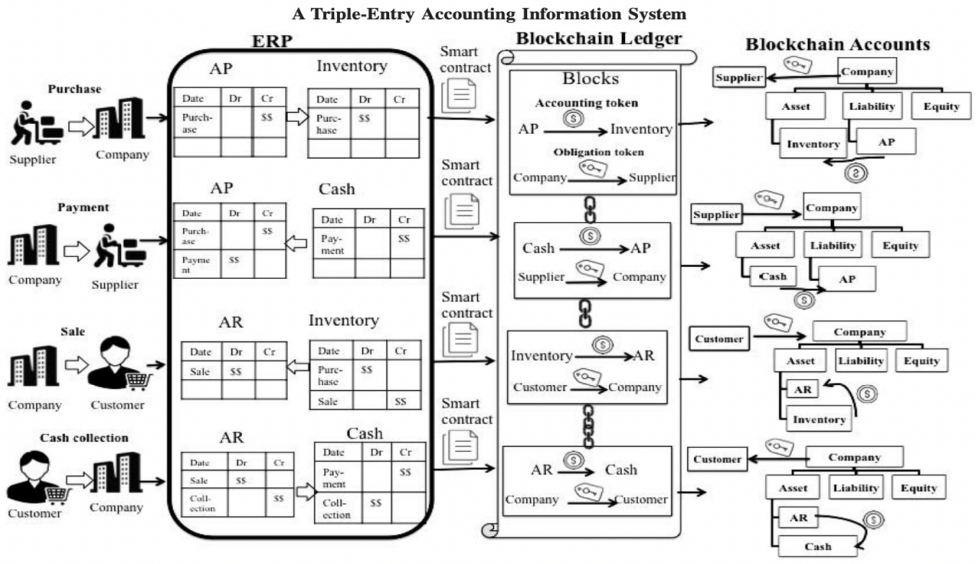
En cualquier caso, estos programas ejecutables implican reducir la intervención humana, la consiguiente reducción de costes y reducir las posibilidades de que exista un error humano, especialmente en tareas reiterativas. Por otro lado, la inteligencia artificial tiene muchas más expresiones y recursos que aún se encuentran en exploración.

3. Sistemas contables con aplicación de blockchain

La revisión bibliográfica realizada en el primer punto de este trabajo no muestra un sistema contable basado en blockchain que sea de consenso ni generalmente aceptado. No existe una arquitectura única y, dado el propósito de este trabajo, procede revisar los sistemas que se han diseñado con propósito, al fin y al cabo, de conseguir los objetivos de aumentar la eficiencia de las prácticas contable, auditoras y reducir la crisis de confianza.

El modelo de Dai y Vasarhelyi (2017), toma la iniciativa de Grigg (2005) para plantear una contabilidad de triple entrada que se construye sobre una cadena de bloques mantenida por un tercero de confianza. Se enfoca hacia el registro de transacciones y emite un recibo que las partes implicadas aceptan y firman digitalmente.

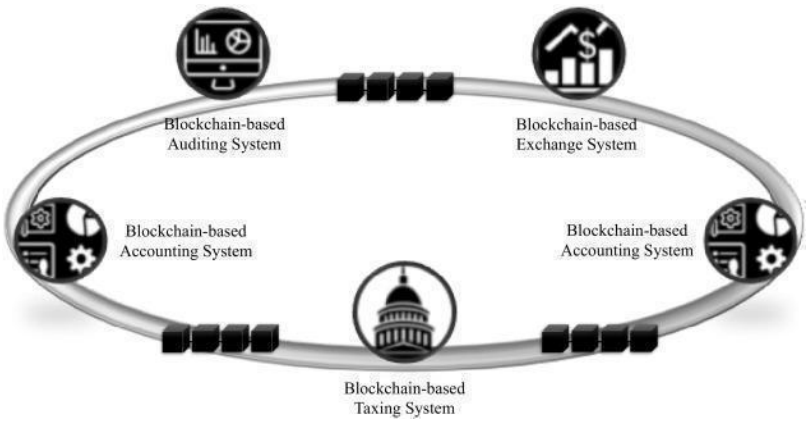
Figura 13: Un sistema de contabilidad de triple entrada



Fuente: Dai, J. and Vasarhelyi, M.A. (2017)

Con el mismo planteamiento inicial, Wang y Kogan (2018) desarrollan un prototipo para demostrar la funcionalidad de blockchain en contabilidad en tiempo real, monitoreo continuo y prevención del fraude. Aplican esquemas zk-SNARK (verificación sin conocimiento) y encriptación homomórfica que permite encadenar entre sí diferentes datos y garantizar la confidencialidad y la transparencia. Con ello, los datos almacenados en blockchain pueden validarse y agregarse sin revelar ningún detalle

Figura 14: Información compartida

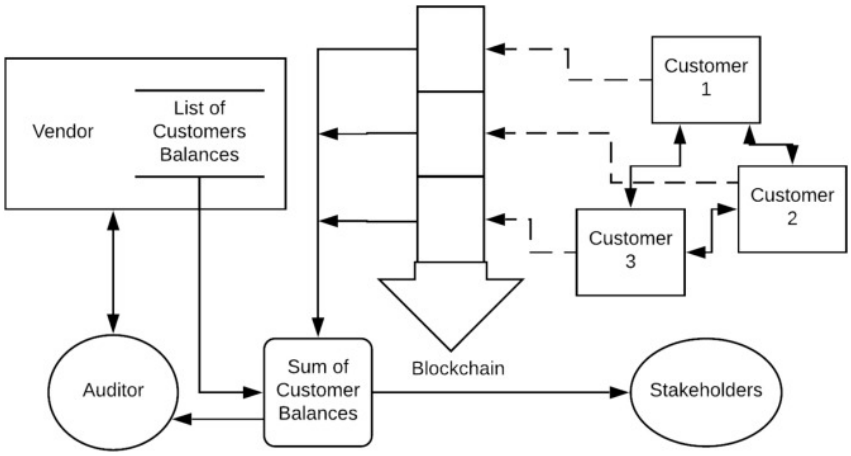


Fuente: Wang, y Kogan (2018)

Rozario y Thomas (2019) sugieren la creación de una segunda cadena de bloques propiedad de un auditor y conectada a la cadena de bloques del cliente den una red. De esta manera, los auditores podrían extraer datos del blockchain de las empresas y realizar procedimientos de auditoría inteligentes dentro de estas cadenas de bloques.

McCallig, Robb y Rohde (2019) diseñan un sistema de información contable garantizando la privacidad y a la vez con acceso público. En su propuesta aplican métodos de seguridad multiparte y utilizan criptografía de clave pública y análisis de red, para desarrollar una identidad digital. Con ello, la privacidad de la identidad real de las contrapartes de las transacciones se puede ocultar mientras se revela públicamente su ubicación en la red financiera. Sin embargo, está limitado a cuentas a cobrar exclusivamente. El sistema está limitado al proceso de auditoría de cuentas a cobrar, aunque es fácilmente traspasable a las cuentas a pagar, e implica la comunicación entre todos los clientes de la empresa, lo que conlleva una coordinación digital.

Figura 15: Sistema de información contable que garantiza la privacidad y de acceso público



Fuente: McCallig, Robb y Rohde (2019)

Fatz, Hake y Fettke (2019) irealizan un prototipo para verificaciones de cumplimiento y aplicación en tiempo real de impuestos relevantes, creando un sistema que emite certificados de llegada de mercancías y liquida el IVA en las transacciones entre dos empresas ubicadas en diferentes países de la UE.

Figura 16: Propuestas de Fatz y Fettle (2019)

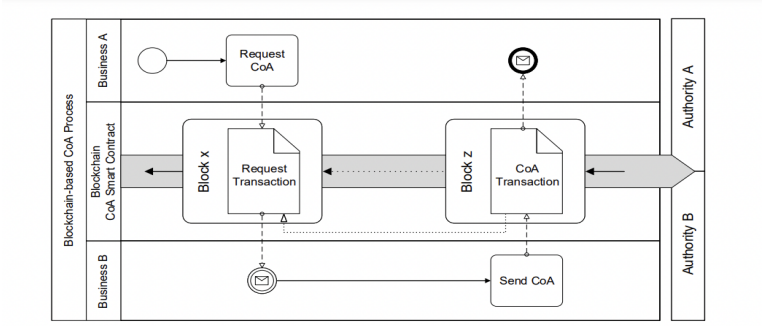


Figure 2. Blockchain-based CoA Process

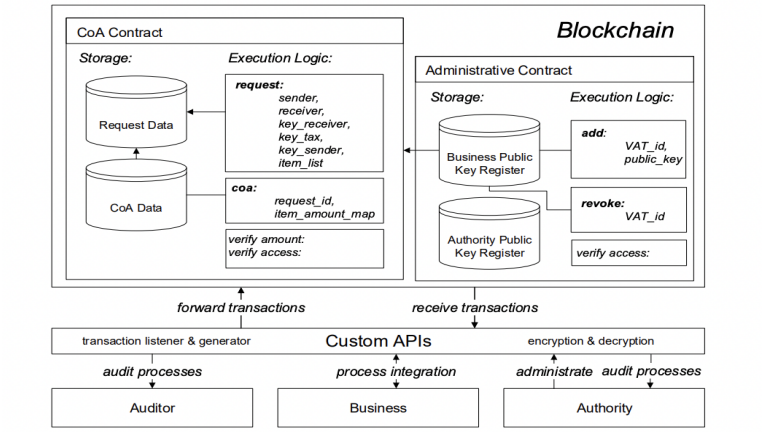


Figure 3. Blockchain CoA Architecture

Fuente: Fatz, Hake, y Fettke (2019)

En resumen, son diferentes planteamientos, pero con un conjunto de elementos comunes que se diferencian fundamentalmente en los desarrollos criptográficos y el alcance.

4. Operatividad en un sistema simple sin privacidad asegurada

En un sistema de contabilidad blockchain sin privacidad asegurada, la operatividad básica se mantiene a través de la transparencia y la confianza en el registro de las transacciones que son visibles para todos los participantes de la red. Esto significa que cualquier persona puede ver los detalles de las transacciones, incluidas las direcciones de envío y recepción, los montos involucrados y los registros de la línea de tiempo.

La validación está descentralizada por los nodos de la red en un sistema de contabilidad blockchain de estas características. Se verifica la autenticidad y la integridad de las transacciones mediante algoritmos criptográficos y en tal caso se agrega a un bloque y se incorpora a la cadena. En sistemas de contabilidad blockchain sin privacidad asegurada, es común utilizar algoritmos de consenso como Prueba de Trabajo (Proof of Work) o Prueba de Participación (Proof of Stake) como los más frecuentes. Estos algoritmos aseguran que los participantes validen las transacciones y contemplen el estado de la contabilidad de manera colectiva y completa. Una vez que una transacción se registra en la cadena de bloques, es muy difícil modificarla o eliminarla por la naturaleza de la tecnología. La inmutabilidad de la cadena de bloques asegura que las transacciones pasadas sean permanentes y no puedan ser alteradas sin el consenso de la red.

Aunque las direcciones de las transacciones son visibles, el anonimato de las partes involucradas puede ser parcial en un sistema sin privacidad asegurada. Si bien las identidades reales no están vinculadas a las direcciones, cabe asociar una dirección con una persona o entidad específica y, consiguientemente, podría rastrear y analizar las transacciones realizadas por esa dirección.

Con los smart contracts, la eficiencia de los registros y la operatoria en torno a ellos mejora en gran medida y crecen las opciones de control y gestión. Para mostrarlo, en el ejemplo que se ilustraba anteriormente sobre la prestación de un servicio, las empresas A y B habrían prefijado las condiciones del pago en un smart contract de forma que podrían haber acordado que la empresa B pagara los 500 € a la empresa A cuando esta preste efectivamente el servicio. Así,

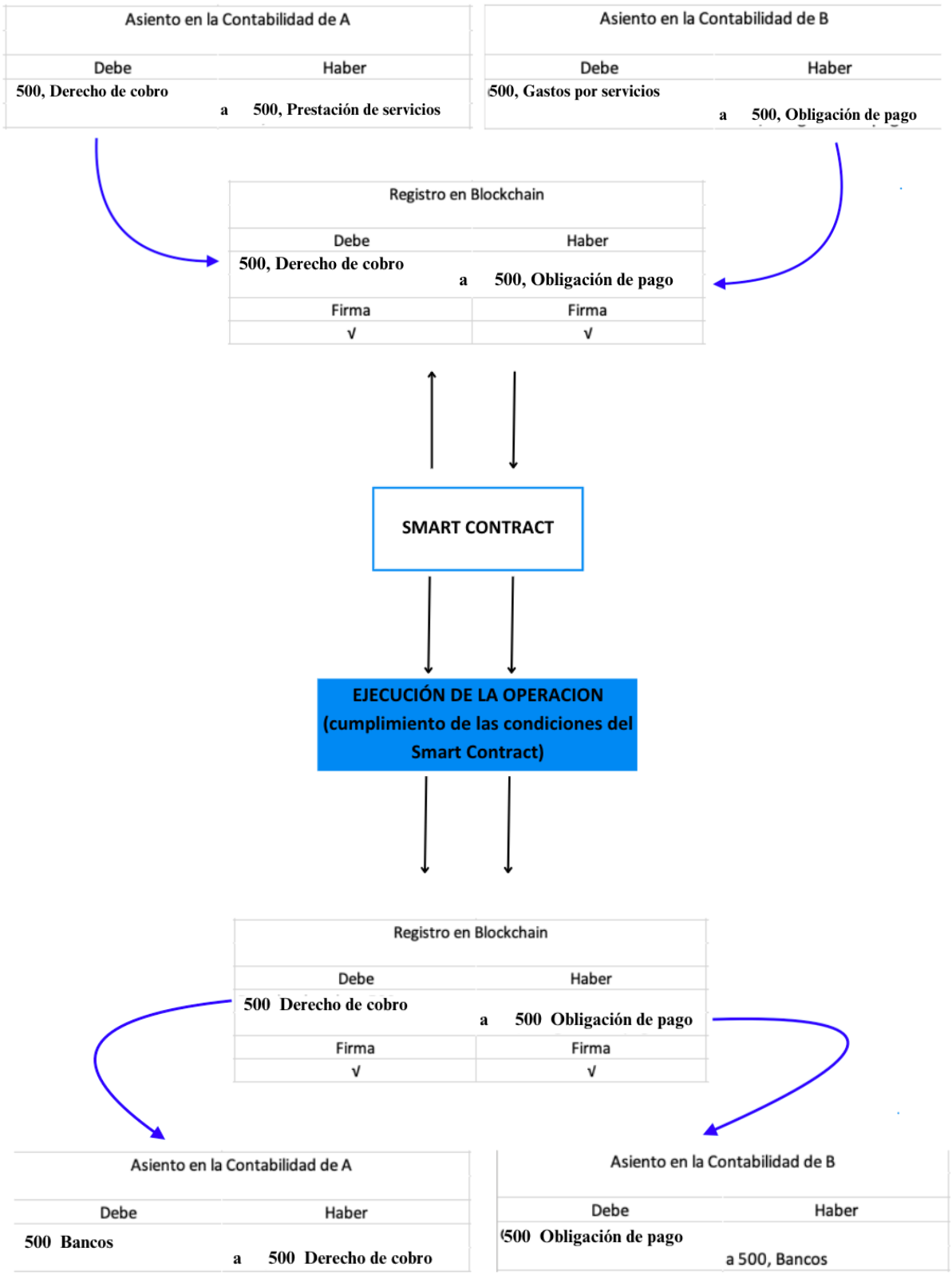
cuando B informe de que se ha producido la prestación del servicio, se ejecutará el pago en la manera y plazos previstos.

La operativa sería la siguiente: La empresa B, que debe pagar por la prestación de los servicios recibidos, emite una orden usando un software de contabilidad instalado en la nube que bien podría haberse ejecutado a través de otro smart contract. Dicha orden es enviada a blockchain con el correspondiente hash, detalles, plazos, condiciones de la transacción y es encriptada con la clave pública de la empresa A, a la que se notificará la solicitud de la transacción. Una vez se le notifique, la empresa A podrá verificar y aceptar la transacción. Con ello, la cadena de bloques se actualizaría como se explicó anteriormente. El cambio que implica el smart contract es que se autoejecutará una vez que el servicio se ha prestado y se firmará digitalmente el contrato de nuevo para que el registro se actualice y el programa informático realice la orden de pago.

Son múltiples los ejemplos que podrían plantearse, como el generar la orden de pago de manera prefijada en un smart contract que se diseñe de forma que una vez recibidos los productos o servicios se proceda a realizar el pago, asentar anotaciones contables ante cualquier circunstancia, emitir avisos o documentos al cumplirse una determina condición, ejecutar acciones etc. Y además, el vínculo que se crea entre la cadena de bloques compartida con los registros propios de las entidades implicadas hace que los errores y el fraude se reduzcan en gran medida y facilita la tarea auditora.

Este mecanismo es una realidad en algunas empresas o entidades públicas. Por ejemplo, la empresa Ledgerium ha creado una red blockchain llamada Luca, que tiene por objetivo permitir el registro de pagos de transacciones utilizando un sistema blockchain con triple entrada y smart contracts. Ledgerium tiene la limitación que se centra exclusivamente en cuentas a cobrar y cuentas a pagar, con lo que no llega al conjunto de un sistema contable y, adicionalmente, tiene el problema de la privacidad y de escalabilidad, pero aporta mucha seguridad en la gestión de derechos de cobro y obligaciones de pago, mayor agilidad en su tratamiento y reducción de costes (Khan & Salah, 2018; Cai, 2021).

Figura 17: Operatividad de smart contracts en un sistema de contabilidad de triple partida



Fuente: elaboración propia

En definitiva, al plantear un sistema de información contable sin asegurar la privacidad con las características descritas, se logran grandes logros como es la seguridad y la transparencia, con lo que podría adquirir mucha relevancia en la gestión de fondos públicos (Fernández Daza & Wanden-Berghe, 2022). La transparencia en la gestión de los fondos públicos es esencial para fortalecer la gobernabilidad, prevenir la corrupción, promover la participación ciudadana y mejorar la eficiencia en el uso de los recursos. Proporciona una base sólida para una gestión financiera responsable y una mayor confianza en las instituciones públicas. Sin embargo, es importante tener en cuenta que la falta de privacidad en un sistema de contabilidad blockchain puede presentar desafíos en términos de confidencialidad y protección de datos sensibles. De ahí que se hayan buscado soluciones y enfoques adicionales que pueden implementarse para mejorar la privacidad en sistemas de contabilidad blockchain, como el uso de criptografía avanzada o soluciones de capa de privacidad adicionales. Entre todas ellas, este trabajo opta por la solución criptográfica que representa el protocolo de conocimiento cero.

5. Sistema contable de privacidad asegurada

Muchos estudios sobre blockchain han tenido que debatirse en torno al equilibrio entre la privacidad y la transparencia. Ello se ha intentado encontrar en el diseño de las redes y de los tipos de consenso con el fin de garantizar que la tecnología sea segura y confiable para los usuarios. Y en ese sentido, un paso decisivo para alcanzar tal objetivo son los desarrollos basados en el protocolo de conocimiento cero.

El protocolo criptográfico de conocimiento cero, conocido por sus siglas en inglés ZKP (Zero Knowledge Proof) permite compartir y verificar información sin aportar datos sensibles. Este protocolo, en síntesis, diseña un procedimiento en el que un agente, denominado probador, afirma que algo es cierto, mientras que otro agente, el verificador, comprueba que efectivamente lo es, sin necesidad de conocer toda la información. Por tanto, es un sistema para demostrar el conocimiento de algo que ha sucedido sin que la prueba exija revelar todos los datos (Quisquater, et al., 1990)[5].

Hay diferentes protocolos de conocimiento cero que tienen en común demostrar que se conoce algo sin tener que decir exactamente qué es lo que se sabe. En el protocolo de conocimiento

[5] Quisquater et al. (1990) desarrollaron el ejemplo de la cueva de Alí Babá para explicar el funcionamiento del protocolo de conocimiento cero, siendo el trabajo de esa línea más citado y referenciado, incluso en la actualidad.

cero interactivo, el verificador y el demostrador interactúen entre sí varias veces antes de que el verificador pueda estar seguro de que el demostrador conoce la información requerida. El protocolo se fundamenta sobre la base de considerar que si el usuario realmente conoce la información, entonces debería ser capaz de responder ciertas preguntas o realizar ciertas operaciones con éxito, mientras que un impostor no sería capaz de hacerlo. En consecuencia, las pruebas de conocimiento cero interactivas tienen aplicaciones en diversas áreas, como la autenticación, la verificación de identidad, la protección de la privacidad y la seguridad en sistemas distribuidos.

En cambio, en el protocolo de conocimiento cero no interactivo (NIZK) el demostrador envía una sola prueba al verificador, sin que sea necesaria ninguna interacción adicional. En este tipo de protocolos, como la prueba de Schnorr, la parte que conoce el secreto interactúa con otra parte (el verificador) para demostrar que conoce el secreto sin revelarlo y sin necesidad de interactuar entre ellos. Algunos casos de sistemas basados en NIZK son las criptomonedas como Zcash y Monero, y las soluciones de autenticación de dos factores basadas en criptografía de clave pública como la Autenticación de Dos Factores Universal (U2F) (Shao, 2010).

Otro tipo de protocolo de conocimiento cero que aplica la teoría de grafos para demostrar el conocimiento de ciertas relaciones entre distintas partes de un grafo. El protocolo se basa en un desafío-respuesta entre las dos partes. En la primera fase, la parte que quiere demostrar que conoce la información (proponente) construye un grafo a partir de dicha información y lo envía a la otra parte (verificador). En la segunda fase, el verificador elige un nodo del grafo y envía una pregunta al proponente pidiéndole que proporcione la información relacionada con ese nodo. En la tercera fase, el proponente responde a la pregunta sin revelar información adicional sobre el grafo. El proceso se repite varias veces sobre diferentes nodos del grafo en cada iteración. Al final, si el proponente puede responder correctamente todas las preguntas del verificador, se considera que ha demostrado que conoce la información sin revelarla.

Por último, cabe apuntar el protocolo de conocimiento cero basado en criptografía de curva elíptica. Es un sistema de encriptación muy seguro que utiliza matemáticas complejas para cifrar y descifrar información. En este sistema, también se diferencia entre el emisor, el verificador y la prueba. Esta es el proceso que permite verificar la autenticidad de la información sin revelarla y para realizarla, el emisor y el verificador seleccionan una curva elíptica y un punto de partida en esa curva. El emisor luego realiza una serie de cálculos matemáticos utilizando la información que desea verificar y envía los resultados de estos

cálculos al verificador. El verificador utiliza estos resultados para determinar si la información es auténtica o no. Este protocolo es muy rápido y eficiente, lo que lo hace ideal para su uso en sistemas en línea y otros entornos de alta velocidad.

Narula, Vasquez y Virza (2018) diseñaron zkLedger definiéndolo como un sistema que utiliza la tecnología de contabilidad distribuida (DLT) y la privacidad del cero conocimiento (ZKP) para permitir transacciones confidenciales y seguras en un libro de contabilidad compartido. El propósito es que sea un sistema que pueda ser fácilmente auditado, sin que merme en ningún momento la privacidad.El sistema zkLedger se divide en tres componentes principales:

- La capa de consenso: Esta capa utiliza un algoritmo de consenso distribuido, como Proof of Stake (PoS) o Proof of Work (PoW), entre otros de los disponibles, para asegurar la integridad del libro mayor compartido y validar las transacciones.

- La capa de privacidad: Esta capa utiliza la criptografía de conocimiento cero para proteger la privacidad de las transacciones en el libro mayor compartido. Las transacciones se enmascaran mediante el uso de pruebas criptográficas de conocimiento cero, lo que significa que no es necesario que ninguna de las partes revele su información privada durante la transacción.

- La capa de aplicación: Esta capa se encarga de la lógica de la aplicación y los smart contrats, lo que permite que los usuarios interactúen con el libro mayor compartido y realicen transacciones en un entorno seguro y privado.

En resumen, zkLedger utiliza la criptografía de la prueba de conocimiento cero para ocultar la información privada de las transacciones mientras se mantiene la integridad y la seguridad del libro mayor compartido. Esto hace que zkLedger sea una opción atractiva para las aplicaciones de blockchain que requieren privacidad y seguridad mejoradas, como las finanzas descentralizadas (DeFi) y las soluciones de identidad digital.

En estos sistemas, la auditoría podría realizar la verificación de transacciones sin necesidad de revelar información confidencial y, por otro lado, son sistemas escalables y pueden manejar una gran cantidad de transacciones con lo que los convierten en una opción atractiva para aplicaciones financieras y contables en línea que requieren una auditoría de privacidad robusta.

El problema que puede presentar este sistema es el de la escalabilidad. Todavía no hay un sistema generalmente aceptado y disponible que utilicen la triple entrada con ambición a ser

utilizado mayoritariamente. Las pruebas realizadas son limitadas, pero se están desarrollando proyectos a gran escala. Un ejemplo es Pacio (2023) que está trabajando en una plataforma de contabilidad de triple entrada (TEA) con escalabilidad a las necesidades mundiales, integrada con un sistema de gestión (TARI) que se apoya en un sistema de estándares SSIM (Modelo de Información Semántica Estandarizada) para facilitar un uso comercial y financiero efectivo que armonice todos los datos empresariales al tiempo que conserva la compatibilidad con intentos anteriores como XBRL. Prevé opciones de transición de forma que si la empresa A que usa TEA compra a la empresa B que no usa TEA, la entrada TEA se registraría, pero solo estaría firmada por A. Cuando B adopta TEA, los registros pueden ser recogidos por B. Mientras tanto, el auditor o demás usuarios de B podrían encontrarlos para compararlos con los registros internos de B.

Cuando alguno de los desarrollos pueda estar disponible, es obligado cooperar con muchos partícipes, desarrolladores de aplicaciones, proveedores de software de contabilidad y auditoría, institutos normalizadores, organismos de establecimiento de normas contables y de auditoría, organizaciones profesionales, reguladores, entidades certificadoras, autoridades fiscales, etc. Es decir, que aun cuando la tecnología alcance una solución viable esta estará acompañada de numerosas acciones en todos los órdenes afectados.

V. Impacto de Blockchain y la Inteligencia Artificial en contabilidad y auditoría

De todo lo dicho en los apartados anteriores podemos concluir que la aplicación de blockchain y de la tecnología artificial a la contabilidad y la auditoría es especialmente esperanzadora a la vista de los objetivos que puede llegar a cubrir. Con el objeto de profundizar en los mismos, se tratará de forma separada de los beneficios y riesgos que tendría su aplicación en la contabilidad y en la auditoría, si bien existe una clara relación entre prácticamente todos ellos.

1. Impacto de la Aplicación de Blockchain e IA en la Contabilidad

La incorporación de las nuevas tecnologías al mundo de la contabilidad tiene un potencial enorme al transformar y mejorar significativamente los procesos contables tradicionales. Blockchain y los smart contracts pueden cambiar los métodos de facturación, contratación, mantenimiento de registros y procesamiento de pagos para el comercio porque la tecnología es capaz de registrar, conciliar datos simultáneamente y ejecutar programas (CPA Canadá &

AICPA, 2017). El estudio de su impacto se puede centrar en diferentes subáreas fundamentales: registro contable, automatización de los procesos y cumplimiento de acuerdos, intervención de intermediarios, transparencia y confiabilidad y trazabilidad.

1.1 Automatización de los procesos y cumplimiento de acuerdos

La incorporación de blockchain y la inclusión de smart contracts, provocarían una mejora significativa en la eficiencia de la contabilidad, reduciendo la cantidad de tiempo y esfuerzo que los contables emplean en el registro repetitivo tradicional (KPMG, 2018). Ello, junto con una automatización de las operaciones contables y de los sistemas de control (Contabilidad Inteligente) llevaría a una transformación de la técnica contable (Desplebin et al, 2021).

Los smart contracts permiten que las condiciones, términos y plazos de un contrato se establezcan directamente en el código del contrato inteligente insertado en la red blockchain. Ello hace que se asegure que las partes cumplan con sus obligaciones (en caso de que se den las condiciones establecidas) y que sus contabilidades propias sean congruentes con el registro existente en la red que funcionaría como el tercero de los asientos en una contabilidad de triple partida. Además, ello facilita significativamente la labor de conciliación y, en definitiva, las tareas de auditoría (Swan, 2018).

Adicionalmente, los contratos inteligentes o autoejecutables podrían automatizar procesos contables como la emisión de facturas, el seguimiento de pagos y la conciliación de transacciones, reduciendo los errores y agilizando los procesos contables. La razón se encuentra en que la red (y los smart contracts incorporados en ella) estaría conectada con las contabilidades propias a través de un sistema de contabilidad de triple partida. Así, por ejemplo, tomando las facturas como muestra, mientras en un sistema tradicional estas son emitidas manualmente en formato físico o electrónico y existe un riesgo de pérdida y puede haber demoras en la entrega, en un sistema contable que incorpore las nuevas tecnologías, la emisión de las facturas estaría automatizada en función de si se dan las condiciones programadas en el smart contracts, se agilizan los procesos de emisión y entrega de facturas y, además, las facturas quedarían registradas en la cadena de forma inmutable. En referencia a los pagos, sucedería algo similar: se evolucionaría desde un proceso manual de verificación, autorización y ejecución de pagos dependiente de intermediarios a un sistema donde el pago se produciría automáticamente (o, en un escenario más realista, cuasi-automáticamente) y únicamente

dependería del cumplimiento de las condiciones del smart contract (Liu et al., 2019; Wanden-Berghe & Fernández Daza, 2018a).

1.2 Intervención de intermediarios

Blockchain es una tecnología que elimina en mayor o menor medida los intermediarios según estemos en una red centralizada o descentralizada y, por ello, reduce los tiempos y los costes que implican las operaciones. En este punto existen planteamientos antagónicos, siendo el más extremo el de prescindir de intermediarios financieros tradicionales, mientras que los enfoques más razonables se inclinan por una reestructuración de las labores de intermediación con el fin de reducir costes y tiempos. Ahora bien, es importante indicar que de expandirse la desintermediación en el sistema económico tendría implicaciones tan trascendentales que sobrepasan el objeto de los trabajos que estudian y diseñan la aplicación de las tecnologías emergentes en contabilidad y auditoría (Wanden-Berghe, 2018b).

1.3 Registro contable confiable

Junto a la automatización de procesos, la implicación con mayor significación de la incorporación de blockchain a la contabilidad es el cambio que supondría en el registro contable. Actualmente, existe un registro mutable (una de las principales razones de la crisis de confianza) y de partida doble. Sin embargo, con estas tecnologías, se conseguiría un tercer registro inmutable que da seguridad, sirve de soporte y hace posible una conciliación automática en tiempo real (Patil, 2017) en caso de que las contabilidades propias estuvieran conectadas a la red donde se registran las operaciones y se ejecutan diferentes contratos inteligentes. Esto es, en un sistema de partida triple, todas las partes de una transacción pueden consultar la información registrada en blockchain (Simoyana et al, 2017) dotadas de ciertas características que dificultan la posibilidad de que las cuentas se encuentren manipuladas (Schmitz & Leoni, 2019).

En concreto, con la llevanza de un sistema de partida triple a través de blockchain, las cuentas de una determinada compañía deberían corresponderse con el registro inmutable de la cadena de bloques como ya se ha explicado, lo que reduce las posibilidades de fraude. A su vez, aumenta la confiabilidad de que la información de las cuentas anuales de una empresa refleje fielmente su realidad (Maffei 2021, Wanden–Berghe et al, 2018b).

1.4 Transparencia

Blockchain es un libro mayor distribuido, inmutable y verificable por la red que funciona como un respaldo de las operaciones realizadas y dependiendo del tipo de red puede llegar a que cualquier miembro de la red tenga la facultad de consultar dicha información de manera inmediata y con la seguridad de que las operaciones allí registradas son verídicas, al contar con el respaldo de una red que cuenta con unas características y elementos criptográficos únicos que hacen que la información sea transparente y confiable (Dai, 2017).

La transparencia en las cuentas públicas es un anhelo demandado por los ciudadanos, que de forma natural y abierta se logra con la aplicación de estas tecnologías, dando una mayor visibilidad a la información sobre las actividades financieras de las instituciones públicas. Es una forma de fortalecer la confianza en las instituciones y prevenir comportamientos sospechosos que puedan socavar su uso. Ampliar y reforzar la transparencia en la actividad pública y garantizar el derecho de acceso a la información relacionada con esa actividad es un objetivo fundamental del gobierno abierto. Ello ayuda a establecer obligaciones de buen gobierno que deben cumplir quienes ejercen una responsabilidad pública, hacer el seguimiento de su cumplimiento, de forma que estas tecnologías sean un instrumento de transparencia y control (Wanden-Berghe & Fernández Daza, 2022).

1.5 Trazabilidad y control de inventarios

La tecnología blockchain permite la trazabilidad de los productos a lo largo de la cadena de suministro. Esto significa que se puede hacer un seguimiento en tiempo real de los productos, desde su origen hasta su destino final, y registrar y verificar todas las transacciones de manera accesible y transparente. El propósito de un sistema de trazabilidad es brindar a los consumidores garantías sobre la autenticidad y calidad del producto, asegurando que cumpla con las normas y regulaciones aplicables.

La trazabilidad también se puede realizar sobre los fondos o flujos económicos. Esto significa que cada vez que un fondo cambia de manos, la información se registra en blockchain y puede ser verificada por los usuarios de la red. Esto aumenta la transparencia y puede reducir el fraude.

1.6 Cuadro resumen de implicaciones positivas en el área contable

	Pre-Blockchain	**Post-Blockchain**
Registro contable	Sistema de partida doble, mutable y con una forma de llevanza manual y repetitiva	Sistema de partida triple apoyado en un registro inmutable y con una forma de llevanza informatizada y automatizada
Procesos contables del día a día de la empresa	Probabilidad de errores Cumplimiento de contratos no asegurado Necesidad de procedimientos de conciliación Dependencia de terceros intermediarios…	Los smart contracts, hacen que el cumplimiento de las obligaciones fijadas en ellos sea seguro (si se dan las condiciones) y automatización de los procesos
Intermediarios	Tiempos y costes para llevar a cabo operaciones	No hay costes de transacción y se agilizan las operaciones
Trazabilidad y control de inventarios	Necesidad de realizar inventarios	Seguimiento de activos desde su entrada hasta la salida y monitoreo de las cadenas de suministro
Nivel de control sobre los registros contables	Ausencia de control de terceros involucrados en los registros contables	Registros contables doblemente verificados a través de smart contracts y otras técnicas

Fuente: Adaptado de Maffei et al. (2021)

1.7 Riesgos y desafíos de su aplicación

Al margen de los beneficios comentados y que han sido abordados de forma sustancial en la literatura académica, se debe hacer una aproximación a los retos que plantea su aplicación y a las posibles amenazas que podría suponer una incorrecta adopción de la tecnología blockchain en el ámbito de la contabilidad. Entre ellas, cabe destacar la privacidad y confidencialidad, la escalabilidad, ciertos retos que se darían en el comienzo de su aplicación, desafíos de naturaleza económica y, por último, incluir algunas consideraciones sobre el debate existente acerca de si estas tecnologías hicieran innecesaria la intervención humana.

La escalabilidad es uno de los principales retos a los que se enfrenta blockchain. A pesar de la existencia de ideas disruptivas y de tecnologías capaces de llevarlas a cabo, es necesario que todos los integrantes de una determinada sociedad estén presentes en la red para el sistema sea completamente efectivo.

La privacidad y la confidencialidad han sido ampliamente tratadas en apartados anteriores, como una de las necesidades empresariales que ha provocado la evolución de las redes hacia la incorporación de configuraciones criptográficas que aseguren dicha confidencialidad y hacia la creación de redes más restringidas, en las que unos pocos nodos podrían tener un control excesivo sobre las mismas (Coyne y McMickle, 2017), salvo que se apliquen protocolos de conocimiento cero como se ha indicado en el punto anterior.

En cuanto a los retos que podría suponer su implantación, la complejidad de la tecnología blockchain requeriría un cuidadoso planteamiento inicial para asegurar el correcto funcionamiento del sistema a la vez que generaría la necesidad de que los contables estuvieran cualificados en su funcionamiento. Para ello tiene que haber un cambio en la formación e, incluso en los planes de estudio que les facultan para ejercer la profesión.

Igualmente, en el ámbito de los costes, a pesar de que en el medio-largo plazo, la implementación del sistema conllevaría una reducción de los mismos, serían necesarios considerables esfuerzos económicos para su adopción inicial e incluso en algunas fases sucesivas (Maffei et al, 2020).

Algunos autores han hablado de la posibilidad de hackear la red y alterar o incluso eliminar parte de los registros. En ese sentido, cabe decir que la eliminación sería prácticamente imposible pues para ello se debería hackear tantos nodos como copias haya de la cadena de bloques y ello dificulta inmensamente la labor de los piratas informáticos. En cuanto a la

alteración, únicamente podría hacerse mediante la inserción de un nuevo bloque y realizando un ataque del 51% de los nodos (Heilman et al, 2015; Marcus et al, 2018), cuestión que se puede evitar con algunos protocolos de consenso. A través de determinadas formas de validación, se podría llegar a disminuir a prácticamente a cero las posibilidades de un ataque del 51% (Zheng et al., 2018). En cambio, en algunas redes privadas con un nodo central sería posible alterar el contenido de los bloques por quienes tienen funciones de validación.

Por último, muchos autores han comentado sobre si la introducción de blockchain y smart contracts llevaría a la desaparición de la labor del contable al estar todo automatizado e informatizado (Baron, 2017; Karajovic et al., 2019). La respuesta a dicha cuestión es rotundamente que no se produciría tal situación ya que el sistema requeriría en todo caso el estar monitorizado por profesionales de la contabilidad. La tecnología en ningún caso podría sustituir la profesionalidad aportada por los contables a la hora de interpretar los datos y de introducir las órdenes que la tecnología necesitaría para funcionar. Como indica el Instituto de Contabilidad de Gales, la introducción de las nuevas tecnologías puede suponer una ampliación de su alcance y un impulso para centrarse en los detalles de las transacciones registradas y en las operaciones más complejas (ICAEW, 2018).

2. Impacto de la Aplicación de Blockchain e IA en la Auditoría

La auditoría es una actividad necesaria para verificar la exactitud de los estados financieros, el cumplimiento de leyes y regulaciones, detectar fraudes y errores que pueda haber en los libros contables. En su función reposa, en buena parte, mantener la confianza de las partes interesadas garantizando que la información contable es precisa. La labor auditora, por tanto, consiste en comprobar que la información contabilizada por una empresa se corresponde con la realidad y, para ello, cuenta con una gran variedad de técnicas como la revisión documental, la conciliación de cuentas, la solicitud de confirmaciones a clientes, proveedores o instituciones financieras, entre otras.

Dichas labores, se verían tremendamente beneficiadas gracias a la incorporación de las nuevas tecnologías, teniendo en cuenta que blockchain, precisamente, es una red que permite llevar un registro inmutable transparente y verificable (Weber, 2017) de las operaciones realizadas. La irrupción de blockchain en la auditoría supondría una gran revolución de la misma y, a efectos expositivos, se puede centrar fundamentalmente de dos consecuencias que puede provocar: la auditoría integral que se podría realizar de forma continua y el aumento de la eficiencia.

2.1 Auditoría integral y continua

En una red blockchain, además de las partes que intervienen en una operación, existen otros miembros que pueden acceder al registro y consultar el historial de operaciones encadenadas. Esta funcionalidad facilita significativamente la labor del auditor, máxime si la empresa objeto de auditoría lleva una contabilidad de triple partida como la que se ha explicado. En ese sentido, la eficiencia de la auditoría se vería incrementada si la empresa utilizara un sistema contable de triple partida apoyado en blockchain: sus registros se corresponderían a las operaciones anotadas en la red y los auditores podrían acceder a ellos y revisarlos con la certeza de que ningún nodo ha podido modificarlos (Maffei et al, 2021; Wanden-Berghe et al 2019).

El hecho de poder consultar toda la información en cualquier momento permite que se pueda decir que la auditoría continua e integral sea una realidad gracias a blockchain. Igualmente, los auditores ya no necesitarían basarse en una muestra para verificar las cuentas anuales y se conseguiría superar el problema que supone la posibilidad de manipular las cuentas en el amplio intervalo de tiempo entre la elaboración y su presentación (Cai, 2018).

En definitiva, cabe pensar en las posibilidades de mantener una auditoría integral y continua que incrementaría exponencialmente la confiabilidad del informe y la previsión de riesgos. No solo por ser el resultado de una comprobación integral y continua que no se ha circunscrito a muestras y plazos, sino también por estar apoyado en una tecnología que cuenta con características que nos permiten hablar de información real y segura. De esta manera, podría superarse la crisis de confianza en la auditoría producida como consecuencia de que sus técnicas no fueron capaces de detectar los escándalos financieros de principios de siglo (Martínez Laguna, L.; Rodríguez Martín, A.; Yubero Hermosa, P. 2006)

2.2 Eficiencia

La inclusión de smart contracts y otros recursos de inteligencia artificial pueden ser un impulso para transformar igualmente las técnicas auditoras. Procesos de revisión podrían automatizarse provocando que muchas tareas que actualmente exigen esfuerzos manuales pasen a ser relevados a procedimientos programados. Así, ante tal escenario, los profesionales podrían dedicar el tiempo conseguido con la automatización para atender aspectos de mayor complejidad y riesgo (Rozario, A, Vasarheyu, M.A, 2018).

2.3 Cuadro resumen de las implicaciones en la auditoría

Característica	Pre-Blockchain	Post-Blockchain
Conciliación	Manual y periódica (comparando 2 sets de información)	Automática y en tiempo real
Conformidad	Manual y basada en una muestra	Automática basada en la información total. No hay posibilidad de informe sin opinión.
Análisis de datos	Manual y basada en una muestra	Continua y basada en toda la información

Fuente: Adaptado de Maffei et al (2021)

2.4 Retos y desafíos

La auditoría con blockchain también se enfrenta a retos y amenazas. En primer lugar, es indudable que la tecnología no podría acabar con la picardía y el fraude: aunque las transacciones se encuentren registradas y dotadas de inmutabilidad en la cadena de bloques, pueden ser objeto de prácticas ilegales y nada impide que haya acuerdos paralelos que hagan que la información registrada no sea completa (Cai, 2018). Así, los auditores deberían reenfocar en cierta medida sus análisis implementando procedimientos específicos de auditoría para detectar esas situaciones (Rosario et al, 2018).

En segundo lugar, al igual que sucede en la contabilidad, pese al debate existente sobre si la automatización de los procesos y técnicas de auditoría podría acabar sustituyendo la labor humana y profesional, en ningún caso la tecnología podría acabar sustituyendo al auditor. Sin duda que muchas tareas las mejora y el control intrínseco que proporciona el sistema facilita la auditoría pero no tiene el mismo grado de garantía que un profesional de la materia. Al igual que lo comentado al tratar este aspecto para los cantables, la auditoría pasaría a aumentar la muestra a la población total y permitiría incrementar el alcance.

En tercer lugar, la confidencialidad y la privacidad que muchas empresas podrían verse reticentes a transmitir al auditor por falta de confianza en él, podrían verse solucionadas gracias a protocolos de conocimiento cero, que autentican la validez de una afirmación (Bashir, 2018) a la vez que garantizan la privacidad, como ya se ha explicado.

3. Escenarios futuros: ¿Hacia un ecosistema de información compartida?

Las implicaciones anteriores en contabilidad y auditoría pueden variar en función del alcance de la aplicación de estas tecnologías en el sistema económico y social. Si inicialmente blockchain se aplicó para transacciones en criptomonedas y gradualmente se ha ido aplicando a medios de pago y, posteriormente se ha aprovechado la vertiente técnica de la cadena de bloques para seguir la trazabilidad de la cadena de suministros o de los fondos públicos, la tokenización de activos, la gestión de todo tipo de registros etc, no es descartable su extensión a todo el sistema.

Las opiniones sobre la trayectoria que va a tener en el futuro varían desde considerar un nivel de aplicación mínimo, en el que Blockchain fuera utilizado únicamente para llevar un registro de transacciones que sea fiable por su inmutabilidad y transparencia (Weber, 2017) hasta un nivel más ambicioso en el que empresas, entidades financieras e instituciones de regulación y control compartan información, formando un ecosistema (Liu et al., 2019). Lo cierto es que el nivel mínimo ya se ha superado al extender la aplicación de blockchain a muchas funciones económicas y sociales como expedientes jurídicos, historial médico, contratación pública, votaciones, entre otras muchas.

En los escenarios de menor alcance, las empresas y las entidades públicas recurren a redes, en mayor o menor medida restringidas, donde poder llevar a cabo transacciones seguras e inmutables. Las aplicaciones de contabilidad de triple entrada se harían por acuerdos individuales entre las partes como un recurso para facilitar el trabajo contable y auditor, así como mejorar la eficiencia del funcionamiento de estas áreas sin mayores implicaciones que las ya indicadas en el apartado anterior. Este es el estado actual y en esta línea se está avanzando por parte de las cuatro grandes empresas de auditoría y cada vez más iniciativas de instituciones financieras, grandes empresas y organismos de la administración pública.

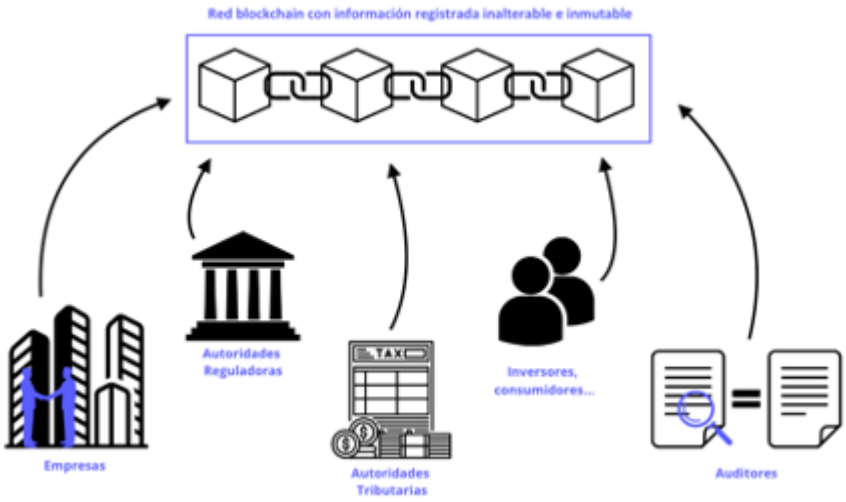
Conforme las infraestructuras y las diferentes redes blockchain se desplieguen, se vayan conectando plataformas y servicios, interoperen más entidades con soportes de contabilidad de triple entrada, se irá conformando una gran comunidad en la que intervienen empresas, inversores, auditores, autoridades tributarias y reguladoras, entre otros agentes, se podría estar ante un nuevo ecosistema. Se podría interactuar reduciendo muchos trámites administrativos, procedimientos de conciliación y control que actualmente alargan los procesos de elaboración y análisis de las cuentas anuales. Esta evolución sería más rápida si se hace una difusión de las oportunidades que ofrecen las tecnologías emergentes y, más aún si existiese voluntad por parte de la administración pública exigiendo legalmente o dando incentivos a la implantación de estos recursos.

En ese contexto, las implicaciones serían inmensas: la auditoría continua sería una realidad pues el auditor podría consultar el soporte, inmutable y verificable, de los documentos contables en cualquier momento, eliminando los procesos de conciliación (Simoyama et al., 2017); el funcionamiento de las cadenas de suministros quedaría revolucionado a través de los smart contracts (Law, 2017); sería posible la liquidación automática de múltiples declaraciones (Bible et al,, 2017) y el pago de impuestos se automatizaría cuando se produzca el hecho imponible (Schmitz y Leoni, 2019; Yu et al., 2018); la problemática que existe para constatar la valoración de determinados activos quedaría solucionada al quedar registrada en la red, e incluso podría estar sujeta a actualizaciones; las funciones de los diferentes registros (mercantil, de la propiedad, catastro…) agilizarían la consulta y verificación, reduciría muchos de los errores que se dan en los mismos; el control sobre el cumplimiento de diferentes regulaciones podría facilitarse a través de la incorporación de sensores o alarmas en la red, entre otras repercusiones de diversa naturaleza (Zhang, 2022). Sin embargo, todas ellas tienen en común que facilitan el acceso a información que necesita ser compartida para diferentes propósitos (controlar, invertir, conciliar cuentas, auditar…). Con estas redes, en definitiva, podría acabar conformándose un ecosistema en el que la información fuera consultada por aquellas personas o entidades en que existe un interés (voluntario o impuesto legalmente) para acceder al registro.

Como se ha indicado anteriormente, el estado actual ha avanzado hacia aplicaciones en muchos campos de actuación y sectores económicos y sociales, pero a día de hoy aún existe mucho desconocimiento sobre las posibilidades que ofrecen las nuevas tecnologías y cierta resistencia a involucrarse en estas redes. Para llegar a un ecosistema de información compartida real se requiere que, por un lado, se aporten los conocimientos relativos a estas tecnologías para, esencialmente, hacer conocer a la sociedad las oportunidades que ofrecen y la transparencia

que significaría para la gestión pública. Por otro lado, hace falta una regulación en los ámbitos mercantil y administrativo (especialmente, en el campo administrativo-tributario) que realmente ahonde en la cuestión y cree un marco legal para su desarrollo. En la actualidad, en la legislación mercantil española, Ley 34/2002 de 11 de julio sobre contratación electrónica, no incluye ninguna alusión a blockchain ni a los smart contracts.

Figura 19: Ecosistema de información compartida



Fuente: Elaboración propia

Es preciso que se realice una difusión de las tecnologías y sobre todo desde la vertiente técnica. La difusión pública que se ha realizado sobre blockchain que más ha impactado en la población en general es la relacionada con las criptomonedas y de alertas sobre el riesgo financiero que tienen asociadas, lo que en ningún caso ayuda a que agentes interesados lleguen a conocer la vertiente técnica de blockchain y su faceta como instrumento en áreas como la de la contabilidad, la auditoría y la administración pública en general. En resumen, contamos con unas tecnologías lo suficientemente avanzadas como para revolucionar el sistema, pero necesitaría voluntad política, formación y conciencia social para que llegue a producirse.

VI. Conclusiones

Blockchain y la inteligencia artificial ofrecen una gran oportunidad para revolucionar todos los ámbitos en donde intervenga un registro de información. A pesar de que la mayoría de la sociedad concibe blockchain como un medio a través del cual llevar a cabo transacciones con

criptomonedas, razón de su nacimiento, las posibilidades que ofrece son mucho más amplias. La denominada "vertiente técnica" de la tecnología puede ser aprovechada en distintas áreas, siendo adaptada a las necesidades de cada una de ellas y, en definitiva, provocar un cambio significativo en el modo de funcionamiento y en los mecanismos de control.

En contabilidad y auditoría estas tecnologías habilitan el sistema de triple partida, donde los registros de partida doble de cada entidad estarían soportados y conectados a una cadena de bloques que asegure que las operaciones y valoraciones contabilizadas sean exactas y precisas. A su vez, los procesos contables se agilizarían por la ejecución de programas automáticos, eliminando la necesidad de conciliaciones, comprobaciones manuales y generando muchos procesos de elaboración de la información, su control y análisis que puede conectarse con la gestión en sentido amplio. Igualmente, sería posible una auditoría íntegra y continua ya que los auditores, además de automatizar procesos a través de smart contracts, podrían acceder a la cadena de bloques en todo momento y comprobar que la información registrada en los libros de la empresa auditada se corresponde con el registro en blockchain.

La confianza que proporciona blockchain reposa en que permite crear registros inmutables, transparentes, enlazados mediante criptografía y fácilmente verificables. Los miembros de la red, entre los que se encontrarían los auditores, podrían acceder a la cadena en cualquier momento, consultar y revisar los registros con la certeza de que dicha información ha sido validada y consensuada por todas las partes intervinientes, entre las que podría encontrarse una autoridad supervisora.

Los beneficios que proporcionan blockchain y la inteligencia artificial gracias a la naturaleza y funcionalidad de los registros son evidentes. Sin embargo, una de las cuestiones más debatidas en blockchain es la confidencialidad o privacidad de los datos. Los registros en blockchain recogen información que, si se inserta en una red abierta y pública, cualquier persona puede acceder a ellas. Ello resultaría de gran utilidad en la administración de recursos públicos donde se busca la transparencia, por ser tan influyente en la confianza en las instituciones. Sin embargo, en un contexto empresarial puede revelar estrategias y datos sobre transacciones que muchas entidades no desean desvelar. De ahí que se diseñen redes permisionadas en ese tipo de entorno, donde solo las personas autorizadas (que podría incluir autoridades supervisoras, tributarias, auditores…) puedan acceder a los datos. También por la forma de proceder al consenso se ha buscado soluciones para acercarse a la situación de equilibrio entre transparencia y privacidad, apostando este trabajo por la incorporación del

protocolo de conocimiento cero a blockchain. Con él, sería posible demostrar que se conoce algo sin tener que decir exactamente qué es lo que se sabe. Así, se combinarían todos los rasgos de la red blockchain con la confidencialidad que se desea mantener, compatibilizando necesidades de privacidad con la conservación total de la confiabilidad.

Para el despliegue de estos sistemas de información contable, tanto los totalmente abiertos tan indicados para la gestión pública como los de ámbito privado para entidades privadas, es necesario que converjan contables, que aporten rigor y profesionalidad en la materia, con profesionales de la informática y la criptografía, que aporten los conocimientos técnicos para su programación. Y para ello, se requiere formación en ambos sentidos en el sentido que los profesionales del área contable y auditora sepan los recursos y herramientas con que pueden contar para el diseño de sus sistemas pese a que no conozcan las particularidades de su programación. Los planes de estudio para habilitar el ejercicio de la profesión deberían recoger la impartición de conocimientos tecnológicos y criptográficos. De lo contrario, continuará en pie una barrera para comprender el funcionamiento y oportunidades que ofrecen las tecnologías emergentes.

En el trabajo se han expuesto distintos escenarios sobre el futuro de la aplicación de blockchain, donde se contempla la posibilidad de una expansión hacia un nuevo ecosistema, aun no llegando a ser totalmente alcanzado. Para ello, se tienen que superar obstáculos de carácter técnico, como el problema de la escalabilidad y la interoperabilidad entre plataformas. También se requeriría un nuevo marco legal en distintos órdenes: mercantil, civil, fiscal, administrativo ... Y, así mismo, requiere un apoyo de difusión por parte de los responsables públicos. La aplicación de estas tecnologías se encuentra en un momento incipiente para su potencial, pero ciertamente avanza a un ritmo considerable. Prueba de ello es que actualmente existe una gran variedad de plataformas con diferentes fines que están demostrando la efectividad y los cambios significativos que provocan en las áreas en las que operan. Sin embargo, la idea sobre la formación de un ecosistema de información compartida en el que los diferentes agentes de una sociedad interactúen entre sí de forma ágil y segura parece más cerca de ser una utopía que una realidad. El que parezca difícil llegar a un nuevo ecosistema no invalida ni resta valor a los logros que ya se han visto viables y se están aplicando.

En definitiva, en el ámbito de la contabilidad y la auditoría, la disrupción de las tecnologías se han manifestado en la contabilidad de partida triple, ya que los registros inmutables y seguros de blockchain, combinado con los smart contracts y la criptografía avanzada, pueden

revolucionar los procesos manuales y repetitivos que actualmente se llevan a cabo, acabar con la crisis de confianza existente y haciendo que los sistemas de información contable y su auditoría sean más eficientes, efectivos y transparentes, así como una herramienta para luchar contra la corrupción y el fraude.

VII. Referencias Bibliográficas

Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with BlockAudit. Journal of Network and Computer Applications, 145.

AICPA (2021). Blockchain risk: considerations for professionals. Disponible en: https://www.aicpa-cima.com/resources/download/blockchain-risk- considerations-for-professionals [Consultado 20-02-2023]

Alawadhi, A., Ames, B., Maciel de Aquino, C. E., Arthúrsdóttir, M., Brennan, G., Brown-Liburd, H. L., Bumgarner, N., Byrnes, P., Criste, T. R., Ghosh, S., Gross, J. A., Gullkvist, B., Hardy, C., Jónsson, H. M., Lasslet, G., Medinets, A., Moon, D., Miyaki, E. H., Sigolo, N., Sigurjónsson, S., Stewart, T. R., Teeter, T., Vasarhelyi, M. A., and Warren, J. D. (2015). Audit Analytics and Continuous Audit: Looking Toward the Future. American Institute of Certified Public Accountants. New York, United States of America: AICPA.

Angelis, J., & Ribeiro da Silva, E. (2019). Blockchain adoption: A value driver perspective. Business Horizons, 62(3), 307-314.

Appelbaum, D., & Smith, S. (2018). Blockchain basics and hands-on guidance: Taking the next step toward implementation and adoption. The CPA Journal, 88(6), 28-37.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. Dismonible en: SSRN 2709713.

Bartolacci, F., Caputo, A., & Soverchia, M. (2020). Sustainability and financial performance of small and medium sized enterprises: A bibliometric and systematic literature review. Business Strategy and the Environment, 29(3), 1297-1309.

Bashir, I. (2018). Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained (2nd ed.). Packt.

Bellucci, M., Cesa Bianchi, D., & Manetti, G. (2022). Blockchain in accounting practice and research: systematic literature review. Meditari Accountancy Research, 30(7), 121- 146

Betta, M. (2016). Three Case Studies: Australian HIH, American Enron, and Global Lehman Brothers. In: Ethicmentality - Ethics in Capitalist Economy, Business, and Society. Issues in Business Ethics, vol 45. Springer, Dordrecht. Disponible en: https://doi.org/10.1007/978-94-017-7590-8_5 [Consultado 15-03-2023]

Cachin, C., & Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild. IBM Research - Zurich, 24. Disponible en: doi:arXiv:1707.01873v2 [Consultado 25-02-2023]

Cai, C. W. (2019). Triple-entry Accounting with Blockchain: How far Have we Come? Accounting & Finance. Accounting and Finance Association of Australia and New Zealand.

Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come?. Accounting & Finance, 61(1), 71-93.

Cazazian, R. (2022). Smart Contracts in Blockchain-based Accounting Information Systems and Artificial Intelligence-enabled Auditing Techniques. Analysis and Metaphysics, (21), 58-73.

Comben, C. (14 de marzo de 2019). Coin Rivet. 11 de enero de 2020. Disponible en: https://coinrivet.com/es/delegated-byzantine-fault-tolerance-dbft-explained/

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 39.

Coyne, J., & McMickle, P. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(2), 101.

Dai, J. y Vasarhelyi, M.A. (2017), "Toward blockchain-based accounting and assurance", Journal of Information Systems, Vol. 31 No. 3, pp. 5-21.

Dai, J., Wang, Y., & Vasarhelyi, M. A. (2017). Blockchain: an emerging solution for fraud prevention. The CPA Journal, 87(6), 12-14.

Deloitte. (2020), "The blockchain galaxy, a comprehensive research on distributed ledger technologies", Disponible en: www2.deloitte.com/content/dam/Deloitte/it/Documents/financial-services/Deloitte_Blockchain_galaxy.pdf [Consultado 02-05-2023]

Desplebin, O., Lux, G., & Petit, N. (2021). To be or not to be: blockchain and the future of accounting and auditing. Accounting Perspectives, 20(4), 743-769.

Du, W., Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. The Journal of Strategic Information Systems, 28(1), 50-65.

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. International Journal, 72(4), 538-562.

European Investment Bank, Verbeek, A., Lundqvist, M.(2021). Artificial intelligence, blockchain and the future of Europe – How disruptive technologies create opportunities for a green and digital economy: main report, Publications Office of the European Union. Disponible en: https://data.europa.eu/doi/10.2867/126279 [Consultado 04-02-2023]

EY (2020). "Going public", EY Global Blockchain Summit 2020, Disponible en: https://assets.ey.com/content/dam/ey-sites/ey-com/en_au/pdfs/going-public-how-public-blockchains-will-create-exponential-growth.pdf [Consultado 10-02-2023]

Fatz, F., Hake, P. and Fettke, P. (2019), "Towards tax compliance by design: a decentralized validation of tax processes using blockchain technology", 2019 IEEE 21st Conference on Business Informatics (CBI), IEEE, pp. 559-568.

Fernández Daza, E. & Wanden-Berghe, J.L. (2022). Sector público: transformación digital y gobierno abierto. AECA: Revista de la Asociación Española de Contabilidad y Administración de Empresas, ISSN 1577-2403, Nº 140, 2022, pp. 11-15

Fernández Daza, E. & Wanden-Berghe ,J.L. (2018). La criptocontabilidad en Blockchain de la información financiera y no financiera de las empresas. En Blockchain: Aspectos tecnológicos, empresariales y legales ISBN 978-84-9197-432-1, pp. 295-317

Ferri, L., Spanò, R., Ginesti, G., & Theodosopoulos, G. (2021). Ascertaining auditors' intentions to use blockchain technology: Evidence from the Big 4 accountancy firms in Italy. Meditari Accountancy Research, 29(5), 1063-1087.

Gómez Carpena, M. (2018). Aplicación de la tecnología blockchain a soluciones de la Internet de las Cosas.

Gountia, D., 2019, Towards Scalability Trade-off and Security Issues in State-of-the-art Blockchain, ICST Transactions on Security And Safety 5(18), 157416. doi: 10.4108/eai.8- 4-2019.157416.

Gröblacher, M., and Mizdraković, V. (2019). Triple-entry Bookkeeping: History and Benefits of the Concept. Digitisation and Smart Financial Reporting, 58-61

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In 24th {USENIX} Security Symposium ({USENIX} Security 15) (pp. 129-144).

Ibañez, J. I., Bayer, C. N., Tasca, P., & Xu, J. (2020). REA, triple-entry accounting and blockchain: Converging paths to shared ledger systems. arXiv preprint arXiv:2005.07802.

ICAEW (2018). Blockchain and the future of accountancy. Disponible en: https://www.icaew.com/technical/technology/blockchain/blockchain-articles/blockchain-and-the-accounting-perspective (Accessed: 3 December 2019).

Ijiri, Y. (1986). A framework for triple-entry bookkeeping. Accounting Review, 745-759. International Data Corporation (2023)

Inghirami, I. E. 2019. Accounting Information Systems: the Scope of Blockchain Accounting. Conference paper. ITAIS and MCIS 2019: 13th Mediterranean Conference on Information Systems and 16th Conference of the Italian Chapter of AIS (Pavia). IRS. 2015. Publication 583 (01/2015), Starting a Business and Keeping Records. Internal Revenue Service.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1-20.

Iza, X. C., Sampedro, X. Z., Morales, M. M., & Cardoso, S. M. (2021). Análisis Comparativo de Métodos de Consenso sobre Plataformas Blockchain. Revista Tecnológica-ESPOL, 33(2), 25-42.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

King, s. y Nadal, S. (2012) "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", August.

Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. Journal of Emerging Technologies in Accounting, 14(2), 91-100.

Kosmarski, A. (2020). Blockchain adoption in academia: Promises and challenges. Journal of Open Innovation: Technology, Market, and Complexity, 6(4).

KPMG. (2018), "Blockchain and digital currencies challenge traditional accounting and reporting models", Disponible en: https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/10/defining-issues-18-13-blockchain.pdf [Consultado 20-02-2023]

Kuzior, A., & Sira, M. (2022). A bibliometric analysis of blockchain technology research using VOSviewer. Sustainability, 14(13), 8206.

Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In Concurrency: the works of leslie lamport (pp. 203-226).

Law, A. (2017). Smart contracts and their application in supply chain management (Doctoral dissertation, Massachusetts Institute of Technology).

Lipton, A. y Levi, S.(2018). «An Introduction to Smart Contracts and Their Potential and Inherent Limitations», The Harvard Law School Forum on Corporate Governance, 26 de mayo de 2018. Disponible en: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-theirpotential-and-inherent-limitations/ [Consultado 20-02-2023]

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. Current Issues in auditing, 13(2), A19-A29.

Lombardi, R & Secundo, G.(2020). Intellectual Capital and Digital Technologies in Academic Entrepreneurship: premises for a revolution?. In Intellectual Capital in the Digital Economy (pp. 106-122). Routledge.

Lombardi, R., & Secundo, G. (2021). The digital transformation of corporate reporting– a systematic literature review and avenues for future research. Meditari Accountancy Research, 29(5), 1179-1208.

Louis C. Guillou Jean-Jacques Quisquater y Thomas A. Berson. "How to Explain Zero-Knowledge Protocols to Your Children". En: Advances in Cryptology - CRYPTO '89 (1990). Proceedings 435: 628-631. Disponible en: http://pages.cs.wisc.edu/~mkowalcz/628.pdf. [Consultado 15-02-2023]

Maffei, M., Casciello, R., & Meucci, F. (2021). Blockchain technology: uninvestigated issues emerging from an integrated view within accounting and auditing practices. Journal of Organizational Change Management, 34(2), 462-476.

Marcus, Y., Heilman, E., & Goldberg, S. (2018). Low-resource eclipse attacks on ethereum's peer-to-peer network. Cryptology ePrint Archive.

MarketsandMarkets (2023). Blockchain Market Size, Share, Trends, Revenue Forecast & Opportunities. Disponible en: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology- market-90100890.html [Consultado 10-04-2023]

Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: undertaking a structured literature review in accounting. Accounting, Auditing & Accountability Journal.

McCallig, J., Robb, A. and Rohde, F. (2019), "Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain", International Journal of Accounting Information Systems, Vol. 33, pp. 47-58, Elsevier Inc.

Menon, A. A., Saranya, T., Sureshbabu, S., & Mahesh, A. S. (2022). A Comparatıve Analysis on Three Consensus Algorithms: Proof of Burn, Proof of Elapsed Time, Proof of Authority. In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021 (pp. 369-383). Springer Singapore.

Minsky, M. (2007). The emotion machine: Commonsense thinking, artificial intelligence, and the future of the human mind. Simon and Schuster.

Moşteanu, D., Roxana, N., Faccia, D., Cavaliere, L. P. L., & Bhatia, S. (2020). Digital technologies' implementation within financial and banking system during socio distancing restrictions–back to the future. International Journal of Advanced Research in Engineering and Technology, 11(6).

Narula, N., Vasquez, W. & Virza, M. (2018), zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, Presented at the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), Renton.

O'Leary, D.E. (2017), Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems, "Intelligent Systems in Accounting Finance & Management", 24(4), October, pp. 138-147

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hr objartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A.,Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P. and Moher, D. (2021), "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", The BMJ, Sage, London, Vol. 372, pp. 1-9

Patil, H. (2017). «CPA Trendlines: 22 ways blockchain will change the Accounting profession forever».

Peprah, W. K., Abas Jr, R. P., & Ampofo, A. Applicability of Blockchain Technology to The Normal Accounting Cycle.

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Xavier Olleros & M. Zhegu (Eds.), Handbook of research on digital transformations (pp. 225-253). Edward Elgar.

Porta, M. (2019). The Cryptonomist. Disponible en: https://en.cryptonomist.ch/2019/08/17/proof-of-capacity-poc-consensus-algorithm/ [Consultado 12-04-2023]

Psaila, G., & Bringas, P. G. (2017). Blockchain: retos y oportunidades, más allá de bitcoin. DYNA, 92(5), 517-521.

PwC. (2020), "Time for trust. The trillion-dollar reasons to rethink blockchain", Disponible en: https://image.uk.info.pwc.com/lib/fe3111707564047570 1c74/m/2/434c46d2-a889-4fed-a030-c52964c71a64.pdf [Consultado 17-04-2023]

Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, Thomas A. Berson. How to explain zero-knowledge protocols to your children. Advances in Cryptology—CRYPTO '89: Proceedings, vol. 435, pp. 628–631, 1990.

Rao, V. S.(2020). Blockchain Accounting in A Triple Entry System – Its Implications on the Firm. Our Heritage, 68 (1), 10499-10512.

Rozario, A.M. and Thomas, C. (2019), "Reengineering the audit with blockchain and smart contracts",Journal of Emerging Technologies in Accounting, Vol. 16 No. 1, pp. 21- 35.

Salimitari, M., & Chatterjee, M. (19 de Junio de 2019). A Survey on Consensus Protocols in Blockchain for IoT Networks. Disponible en: doi:15. arXiv:1809.05613v4 [Consultado 10-05-2023]

Salimitari, M., Joneidi, M., & Chatterjee, M. (2019, December). Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based iot networks. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. Australian Accounting Review, 29(2), 331-342.

Secinaro, S., Dal Mas, F., Brescia, V., & Calandra, D. (2021). Blockchain in the accounting, auditing and accountability fields: a bibliometric and coding analysis. Accounting, Auditing & Accountability Journal, 35(9), 168-203.

Shao, Z. (2010). "Fair exchange protocol of Schnorr signatures with semitrusted adjudicator". Computers & Electrical Engineering,

Sheldon, M. D. (2018). Using blockchain to aggregate and share misconduct issues across the accounting profession. Current Issues in Auditing, 12(2), A27-A35.

Simoyama, F. D. O., Grigg, I., Bueno, R. L. P., & Oliveira, L. C. D. (2017). Triple entry ledgers with blockchain for auditing. International Journal of Auditing Technology, 3(3), 163-183.

Sutton, S.G., Holt, M. and Arnold, V. (2016), "The reports of my death are greatly exaggerated - artificial intelligence research in accounting", International Journal of Accounting Information Systems, Vol. 22, pp. 60-73.

Swan, M. (2018). Blockchain for business: Next-generation enterprise artificial intelligence systems. In Advances in computers (Vol. 111, pp. 121-162). Elsevier.

Szabo, N. (1994). Smart Contracts. Disponible en: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [Consultado 07-03-2023]

Szabo, N. (1997). The idea of smart contracts. Nick Szabo's papers and concise tutorials, 6(1), 199.

Vijai, C., Elayaraja, M., Suriyalakshimi, S. M., and Joyce, D. (2019). The Blockchain Technology and Modern Ledgers Through Blockchain Accounting. Adalya Journal 8 (2), 545-557.

Wanden-Berghe, J. L., & Fernández Daza, E. (2020). Blockchain: instrumento de transparencia y control del sector público. Revista española de control externo, 22(64), 132-149.

Wanden-Berghe Lozano, J. L., Bednárová, M., & Fernández Daza, E. (2019). La tecnología blockchain y sus implicaciones en el ámbito empresarial. Asociación Española de Contabilidad y Administración de Empresas (AECA). Documento nº 15 de la Comisión de Contabilidad y nuevas tecnologías

Wanden-Berghe, J. L., & Fernández Daza, E. (2018a). La contabilidad de triple entrada y las implicaciones de Blockchain. In Blockchain: Aspectos tecnológicos, empresariales y legales (pp. 269-294). Aranzadi Thomson Reuters.

Wanden-Berghe, J. L., & Fernández Daza, E. (2018b). «Una propuesta de aplicación de la Contabilidad en Blockchain», XVIII Encuentro Internacional AECA, Lisboa. Disponible en: https://aeca.es/wp-content/uploads/2014/05/80g.pdf [Consultado 23-04-2023]

Wang, W., & Vasarhelyi, M. (2021). The Application of Continuous Audit and Monitoring Methodology: A Government Medication Procurement Case. Available at SSRN 4397672.

Wang, Y. and Kogan, A. (2018), "Designing confidentiality-preserving blockchain-based transaction processing systems", International Journal of Accounting Information Systems, Vol. 30, pp. 1-18.

Wang, Q., Li, R., Wang, Q., Chen, S., & Yang, X. (2022). Exploring unfairness on proof of authority: Order manipulation attacks and remedies. Ithaca: Cornell University Library,

arXiv.org. Disponible en: https://www.proquest.com/working-papers/exploring-unfairness-on-proof-authority-order/docview/2637207270/se-2 [Consultado 23-04-2023]

Wild, J. J., Shaw, K. W., and Chiappetta, B. 2011. Fundamental Accounting Principles. New York, United States of America: McGraw-Hill/Irwin.

Xiao, B., Jin, C., Li, Z., Zhu, B., Li, X., & Wang, D. (2021, December). Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization. In IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (pp. 510-513).

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.

Xu, X., Zhu, D., Yang, X., Wang, S., Qi, L., & Dou, W. (2021). Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.

Yu, T., Lin, Z., & Tang, Q. (2018). Blockchain: The introduction and its application in financial accounting. Journal of Corporate Accounting & Finance, 29(4),

Zhang, W., & Zhu, M. (2022). Environmental Accounting System Model Based on Artificial Intelligence Blockchain and Embedded Sensors. Computational Intelligence and Neuroscience, 2022.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352-375. Disponible en: doi: 10.1504/IJWGS.2018.10016848 [Consultado 08-05-2023]