

FACULTAD DE CIENCIAS DE LA ECONOMÍA Y DE LA EMPRESA
MÁSTER UNIVERSITARIO EN AUDITORÍA Y CONTABILIDAD SUPERIOR



TRABAJO FIN DE MÁSTER

UNCHAIN THE BLOCK.

Análisis del impacto de la tecnología blockchain en la auditoría

Autor: Rafael Alonso García

Tutor: Belén Toro Marín

Curso académico 2025/2026

Título:

UNCHAIN THE BLOCK. Análisis del impacto de la tecnología blockchain en la auditoría.

Autor:

Rafael Alonso García

Tutora:

Belén Toro Marín

Resumen:

El presente trabajo tiene por objeto evaluar el impacto de la tecnología blockchain (DLT) en la contabilidad y la auditoría en el contexto español, justificado por la confluencia de la innovación tecnológica y un marco regulatorio europeo inédito.

La investigación parte de la necesidad de superar los problemas recurrentes de la contabilidad tradicional, como los tiempos de cierre prolongados y el elevado coste de las conciliaciones.

La tecnología DLT introduce la contabilidad de triple partida, un registro compartido e inmutable que funciona como un recibo firmado y sellado por las partes y la red. Esta arquitectura promete una trazabilidad de extremo a extremo y facilita la evidencia continua.

La investigación se enmarca en un contexto normativo europeo activo, que incluye el Reglamento de Mercados de Criptoactivos (MiCA), el Régimen Piloto de DLT para infraestructuras de mercado tokenizadas, y normativas de resiliencia operativa digital (DORA y NIS 2). A nivel contable español, el Instituto de Contabilidad y Auditoría de Cuentas (ICAC) ha establecido que los criptoactivos deben clasificarse y valorarse por su función económica, generalmente como inmovilizado intangible, existencias o instrumentos financieros, según el Plan General de Contabilidad (PGC).

El objetivo general es evaluar si la implantación de registros contables on-chain se asocia a una menor proporción de opiniones modificadas o Cuestiones Clave de Auditoría (CCA) sobre conciliaciones. Para ello, la metodología combina una revisión bibliográfica y normativa con un estudio empírico basado en el análisis estadístico de informes de auditoría y cuentas anuales de entidades españolas de los ejercicios 2021 a 2024.

Abstract:

The purpose of this paper is to assess the impact of blockchain technology (DLT) on accounting and auditing within the Spanish context, justified by the convergence of technological innovation and an unprecedented European regulatory framework.

The research stems from the need to overcome recurrent issues in traditional accounting, such as lengthy closing processes and the high cost of reconciliations. DLT technology introduces triple-entry accounting — a shared, immutable ledger that acts as a receipt signed and sealed by both the parties and the network. This architecture promises end-to-end traceability and enables continuous assurance.

The study is framed within an active European regulatory environment, which includes the Markets in Crypto-Assets Regulation (MiCA), the DLT Pilot Regime for tokenised market infrastructures, and digital operational resilience regulations (DORA and NIS 2). At the Spanish accounting level, the Institute of Accounting and Auditing (ICAC) has established that crypto-assets must be classified and measured according to their economic function — generally as intangible assets, inventories, or financial instruments — in accordance with the Spanish General Accounting Plan (PGC).

The overall objective is to evaluate whether the implementation of on-chain accounting records is associated with a lower proportion of modified audit opinions or Key Audit Matters (KAMs) relating to reconciliations. To this end, the methodology combines a review of the literature and regulatory framework with an empirical study based on the statistical analysis of audit reports and annual accounts of Spanish entities for the financial years 2021 to 2024.

Palabras clave:

Blockchain, contabilidad de triple partida, auditoría financiera, criptoactivos, Distributed Ledger Technology (DLT), smart contracts, Cuestiones Clave de Auditoría (CCA).

Listado de acrónimos:

AECA: Asociación Española de Contabilidad y Administración de Empresas
BIS: Bank for International Settlements
BOICAC: Boletín Oficial del Instituto de Contabilidad y Auditoría de Cuentas
CCA: Cuestiones Clave de Auditoría
CCN: Centro Criptológico Nacional
CNMV: Comisión Nacional del Mercado de Valores
COSO: Committee of Sponsoring Organizations of the Treadway Commission
CPMI: Committee on Payments and Market Infrastructures
CSRD: Corporate Sustainability Reporting Directive
DLT: Distributed Ledger Technology (Tecnología de Registro Distribuido)
DORA: Digital Operational Resilience Act
ERP: Enterprise Resource Planning
ESG: Environmental, Social and Governance
ESRS: European Sustainability Reporting Standards
GDPR: General Data Protection Regulation
GdO: Garantías de Origen
HSM: Hardware Security Module
IASB: International Accounting Standards Board
ICAC: Instituto de Contabilidad y Auditoría de Cuentas
ICAEW: Institute of Chartered Accountants in England and Wales
IFRS: International Financial Reporting Standards
KAM: Key Audit Matter (Cuestión Clave de Auditoría, equivalente a CCA)
MiCA: Markets in Crypto-Assets Regulation
NIA-ES: Normas Internacionales de Auditoría adaptadas para España
NIGC-ES: Norma Internacional de Gestión de la Calidad (España)
NIST: National Institute of Standards and Technology
NRV: Norma de Registro y Valoración (del Plan General de Contabilidad)
PGC: Plan General de Contabilidad
PoA: Proof of Authority
PoS: Proof of Stake
PoW: Proof of Work

PpT: Pruebas de Trazabilidad

PYME: Pequeña y Mediana Empresa

RI: Riesgo Inherente

SLA: Service Level Agreement

TI: Tecnologías de la Información

TRD: Tecnología de Registro Distribuido

UE: Unión Europea

WWF: World Wide Fund for Nature

Índice

1.	Introducción.....	10
1.1.	Contexto y motivación.....	10
1.2.	Relevancia académica y profesional	12
1.3.	Estructura del trabajo	13
2.	Objetivo.....	14
2.1.	Objetivo general.....	14
2.2.	Preguntas de investigación.....	14
2.3.	Hipótesis contrastables.....	15
2.4.	Alcance del estudio	15
2.5.	Criterios de validación y contribución.....	16
3.	Marco teórico.	16
3.1.	Definición y fundamentos de blockchain.....	16
3.1.1	De la tablilla a la triple entrada.....	16
3.1.2	¿Qué es una blockchain?	17
3.1.3	Resumen cronológico de la tecnología (2008-2025).....	18
3.1.4	¿Por qué importa a la contabilidad? – La triple entrada y su relación con las teorías contables.....	18
3.2.	Algoritmos de consenso.....	19
3.2.1	¿Para qué sirve el consenso?	19
3.2.2	Principales familias de consenso	20
3.2.3	Del PoW al PoS (Ethereum).....	21
3.3.	Desafíos técnicos y operativos.....	23
3.3.1	Escalabilidad y almacenamiento.....	23
3.3.2	Interoperabilidad y puentes (bridges)	24
3.3.3	Errores lógicos en smart contracts:.....	25
3.3.4	Custodia de claves y gobierno de acceso.....	26

3.3.5	Riesgos emergentes para la blockchain	26
3.4.	Aplicaciones empresariales (triple partida, supply chain, etc.).....	27
3.4.1	La contabilidad de triple partida	27
3.4.2	Trazabilidad y cadena de suministro	28
3.4.3	Tokenización de activos y finanzas corporativas	28
3.4.4	Sector público: el ejemplo estonio.....	29
4.	Marco normativo.....	31
4.1.	Unión Europea.....	31
4.1.1	Reglamento (UE) 1114/2023 – Mercados de Criptoactivos (MiCA).....	33
4.1.2	Reglamento (UE) 858/2022 – Régimen Piloto de infraestructuras de mercado basadas en TRD.	34
4.1.3	Resiliencia digital	37
4.1.4	Calidad y portabilidad de la información	39
4.2.	España.....	42
4.2.1	Plan General de Contabilidad (PGC) y criterios ICAC.....	45
4.2.2	Ley 6/2023 y normativa CNMV-Banco de España.....	46
4.2.3	Información sobre sostenibilidad.....	47
5.	Metodología.....	48
5.1.	Diseño de la investigación.....	48
5.2.	Población y muestra.....	49
5.3.	Instrumentos y técnicas de análisis.....	51
5.4.	Limitaciones del estudio.....	53
6.	Resultados y análisis.....	53
6.1.	Impacto en la contabilidad financiera.....	55
6.2.	Impacto en la auditoría.....	56
6.3.	Matriz de riesgos blockchain vs pruebas NIA-ES	57
7.	Discusión.....	66
7.1.	Comparación con la literatura previa.....	66

7.2.	Implicaciones prácticas para despachos y empresas.....	67
8.	Conclusiones y líneas futuras de investigación.....	68
9.	Bibliografía.....	72
10.	Anexos.....	79

Índice de tablas

Tabla 1:	Hipótesis de investigación	15
Tabla 2:	Cronología de la teoría contable	16
Tabla 3:	Hitos recientes en tecnología blockchain.....	18
Tabla 4:	Principales familias de consenso.....	20
Tabla 5:	Datos medioambientales pre y post “Merge”	21
Tabla 6:	Buenas prácticas en custodia de claves.....	26
Tabla 7:	Ejemplo de asientos de triple partida	27
Tabla 8:	Casos de uso de KSI-Blockchain en Estonia	30
Tabla 9:	Calendario de aplicación de MiCA.....	33
Tabla 10:	Infraestructuras habilitadas en Régimen Piloto	35
Tabla 11:	Implicaciones de la aplicación de DORA al trabajo del auditor.....	37
Tabla 12:	Resultados de las pruebas estadísticas	54
Tabla 13:	Resultados de las pruebas robustez.....	54
Tabla 14:	Matriz de riesgos blockchain – Riesgo 1	58
Tabla 15:	Matriz de riesgos blockchain – Riesgo 2	59
Tabla 16:	Matriz de riesgos blockchain – Riesgo 3	60
Tabla 17:	Matriz de riesgos blockchain – Riesgo 4	61
Tabla 18:	Matriz de riesgos blockchain – Riesgo 5	61
Tabla 19:	Matriz de riesgos blockchain – Riesgo 6	62
Tabla 20:	Matriz de riesgos blockchain – Riesgo 7	63
Tabla 21:	Matriz de riesgos blockchain – Riesgo 8	64
Tabla 22:	Matriz de riesgos blockchain – Riesgo 9	64
Tabla 23:	Matriz de riesgos blockchain – Riesgo 10	65

Índice de Anexos

Anexo 1 – Hoja “Catalogo_variables”	79
Anexo 2 – Hoja “Diccionario_codigos”	81
Anexo 3 – Matriz_CCA	82

1. Introducción

1.1. Contexto y motivación

La digitalización de la información financiera constituye una prioridad estratégica para la Unión Europea desde la puesta en marcha del Digital Finance Package (Comisión Europea, 2020). En este marco, la Estrategia de Finanzas Digitales prevé crear una infraestructura de datos de la UE que mejore la transparencia y la sostenibilidad de los mercados de capitales (Comisión Europea, 2020, p. 15). La contabilidad tradicional -apoyada en el dogma de la doble partida formulado por Pacioli en 1494- se ha beneficiado durante décadas de los sistemas integrados de gestión (ERP), pero aún presenta tres problemas recurrentes: (1) tiempos de cierre prolongados, (2) coste elevado de conciliaciones intercompañía y (3) dependencia de controles internos de TI, cuyos fallos incrementan el riesgo de incorrección material (Dai & Vasarhelyi, 2017).

En paralelo, la tecnología blockchain ha pasado, en apenas quince años, de ser la capa transaccional de Bitcoin (Nakamoto, 2008) a convertirse en una plataforma versátil para tokenizar activos, automatizar cumplimientos contractuales y, más recientemente, registrar apuntes contables de manera inmutable y distribuida. La idea de la triple partida -descrita por Grigg (2005) y revisada por Cai (2021)- incorpora un tercer libro mayor compartido (la cadena de bloques) que actúa simultáneamente como recibo inmutable, sistema de sellado de tiempo y mecanismo de consenso entre las partes (Grigg, 2005). Esta arquitectura promete trazabilidad end-to-end, reducción de costes de auditoría y generación de evidencia continua (auditoría continua), alineándose con la búsqueda del regulador europeo de datos confiables “born-digital” (ESMA, 2023).

El interés no es meramente teórico: la compartición de un registro único reduce procesos de conciliación y fricciones en liquidación (BIS-CPMI, 2017; ECB, 2017); en España, proyectos como Alastria 3.0 (red permissionada basada en Besu/IBFT 2.0), la emisión del primer bono tokenizado de Banco Santander (septiembre 2019) y la iniciativa Iberdrola–Energy Web para certificados de energía renovable demuestran tracción empresarial. Estos pilotos generan los primeros estados financieros auditados en los que blockchain podría tener afectación en el balance y la cuenta de resultados, planteando interrogantes a contables y auditores.

Junto a la vertiente tecnológica emerge, además, un marco regulatorio inédito. El Reglamento (UE) 2023/1114 sobre mercados de criptoactivos (MiCA), el Régimen Piloto

DLT (Reglamento 2022/858) y el Reglamento DORA sobre resiliencia operativa digital (Reglamento 2022/2554) comenzaron a aplicarse de forma escalonada entre junio 2023 y enero 2025. España ha trasladado parte de estas normas mediante la Ley 6/2023, de los Mercados de Valores y de los Servicios de Inversión, que habilita registros DLT para valores y encomienda a la CNMV y al Banco de España la supervisión de nodos y custodios.

Paralelamente, el Instituto de Contabilidad y Auditoría de Cuentas (ICAC) ya ha ofrecido un primer criterio específico sobre criptoactivos: la Consulta 4 del BOICAC 120 (diciembre 2019), titulada “Sobre el tratamiento contable de la emisión de criptomoneda”, concluye que las monedas virtuales creadas por la propia empresa se registran como “existencias” (NRV 10.^a) cuando se emiten con la finalidad de ser vendidas -valoradas inicialmente por su coste de emisión y, posteriormente, por el menor entre coste y valor neto realizable-, mientras que aquellas no destinadas a la venta se califican como inmovilizado intangible (NRV 5.^a). Este posicionamiento oficial refuerza la necesidad de analizar cómo la adopción de blockchain impacta en la preparación de estados financieros y en los procedimientos de auditoría en España.

En síntesis, confluyen tres vectores -innovación tecnológica, presión normativa y demanda de transparencia- que justifican una investigación sobre cómo la blockchain puede transformar la función contable y la labor del auditor en España.

1.2.Relevancia académica y profesional

Desde una perspectiva académica, la investigación sobre blockchain y contabilidad ha crecido de forma notable, pero los estudios empíricos centrados en el encaje de la DLT en el PGC y las NIA-ES siguen siendo escasos. El último informe de la Fundación Cotec (2021), basado en encuestas a 152 empresas españolas, indica que el 69 % de las organizaciones que ya utilizan blockchain son micro y pequeñas empresas, pero sólo un pequeño porcentaje lo aplica a procesos relacionados con la contabilidad o la conciliación financiera. Esta brecha de aplicación contable refuerza la relevancia de investigar cómo la adopción de registros distribuidos puede afectar a la calidad de la información financiera y al riesgo de auditoría en el contexto español. El presente trabajo pretende cubrir precisamente ese vacío, aportando:

1. Encaje específico en el PGC: ¿cómo se clasifican y valoran los tokens de utilidad o de seguridad dentro de las Normas de Registro y Valoración?
2. Adecuación de las NIA-ES: ¿son suficientes los procedimientos sustantivos previstos para evidencias externas si estas residen en blockchain pública o permitida?
3. Impacto cuantificable en el riesgo de auditoría: ¿se reduce realmente la probabilidad de opinión modificada o la aparición de Cuestiones Clave de Auditoría (CCA) sobre conciliación cuando el registro subyacente es distribuido?

La presente investigación aspira a cerrar esta brecha, aportando evidencia estadística y análisis normativo anclado en el contexto español.

Para los preparadores de estados financieros, la adopción de DLT implica cambios en los procesos de consolidación, inventarios y tesorería, además de implantar controles específicos sobre custodia de claves criptográficas y adecuada segregación de funciones (KPMG, 2018). Los auditores, por su parte, se enfrentan a nuevos riesgos: fallos de smart contracts, dependencia de oráculos, ataques del 51 % en redes PoW o slashing en PoS. Las guías internacionales comienzan a ofrecer respuestas (ICAEW, 2024), pero la adaptación a las NIA-ES exige trabajos que ejemplifiquen pruebas de control y sustantivas apropiadas al entorno español.

Desde la óptica social, la transparencia distribuida puede elevar la confianza de inversores y acreedores, contribuir al cumplimiento de la normativa sobre sostenibilidad (ESG) al facilitar la trazabilidad de la huella de carbono (p. ej. CSRD-ESRS E1) y reforzar la lucha contra el fraude y el greenwashing. No obstante, subsisten desafíos éticos -privacidad de datos

personales bajo GDPR- y medioambientales -consumo energético de ciertos algoritmos de consenso- que deben valorarse con rigor (Chai et al., 2023).

1.3. Estructura del trabajo

El objetivo de esta Introducción es, por tanto, demostrar la oportunidad y necesidad de estudiar la convergencia entre blockchain, PGC y NIA-ES; posicionar la investigación dentro del debate académico actual; y aclarar la relevancia práctica para empresas y auditores.

El resto del trabajo se organiza así: el capítulo 2 formula el objetivo general, las preguntas de investigación y las hipótesis; el capítulo 3 profundiza en los fundamentos técnicos de la blockchain y en la contabilidad de triple partida; el capítulo 4 disecciona el marco normativo europeo y español; el capítulo 5 describe la metodología empírica -revisión bibliográfica sistemática y estudio transversal con ANOVA/ χ^2 sobre informes de auditoría 2022-2024-; el capítulo 6 presenta los resultados en términos de impacto contable y de auditoría; los capítulos 7 y 8 discuten los hallazgos, extraen conclusiones y proponen líneas futuras y, finalmente, se recoge la bibliografía en el capítulo 9.

2. Objetivo.

2.1. Objetivo general

Evaluar, en el contexto español, si la implantación de registros contables on-chain se asocia a una menor proporción de opiniones modificadas o Cuestiones Clave de la Auditoría (CCA) sobre conciliaciones, a una reducción significativa del riesgo de incorrección material percibido por los profesionales, y a diferencias de impacto en función del tamaño (PYME vs. gran empresa).

2.2. Preguntas de investigación

P-1. ¿En qué grado las entidades que implantan registros contables on-chain presentan menos opiniones modificadas o Cuestiones Clave de la Auditoría (CCA) sobre conciliaciones que las que utilizan únicamente ERP tradicionales?

P-2. ¿Cómo varía la evaluación del riesgo inherente y del riesgo de control (NIA-ES 315 R, 2024) por parte de los auditores cuando la evidencia proviene de un libro mayor distribuido?

P-3. ¿Existen diferencias sectoriales o de tamaño (PYME vs. gran empresa) tanto en los beneficios percibidos como en la reducción del riesgo percibido y en las barreras de implantación de la tecnología blockchain?

2.3. Hipótesis contrastables

Tabla 1: Hipótesis de investigación

Código	Hipótesis estadística (a contrastar a $\alpha = 0,05$)	Métrica prevista
H1	Empresas con blockchain muestran una proporción menor de opiniones modificadas o CCA sobre conciliación que las de ERP tradicional.	Opinión del auditor (0 = sin salvedades / 1 = modificada) \rightarrow test χ^2
H2	La valoración media del riesgo de incorrección material en el ciclo de ingresos es significativamente menor para los auditores que revisan entidades on-chain.	ANOVA de un factor
H3	El efecto de la blockchain sobre el riesgo percibido es mayor en PYMES que en grandes compañías.	ANOVA 2×2 Factor A = Blockchain (sí/no) Factor B = Tamaño (PYME / Gran empresa)

Fuente: Elaboración propia

2.4. Alcance del estudio

El análisis se circunscribe a:

- Horizonte temporal: ejercicios 2022-2024 cuyas cuentas anuales e informes de auditoría ya estén depositados en el Registro Mercantil a la fecha de corte de la investigación (oct-2025).
- Ámbito normativo: entidades españolas sometidas a auditoría obligatoria conforme a la Ley 22/2015, que aplican el PGC (RD 1514/2007) o el PGC-Pyme y cuyas auditorías se realizan según las NIA-ES vigentes.
- Objeto tecnológico: implantaciones de contabilidad de triple partida basadas en blockchain (permissioned o permissionless) con registros que generan evidencia apta para auditoría financiera.
- Fuentes de datos: Cuentas Anuales, individuales y/o consolidadas, e informes de auditoría 2022 – 2024 disponibles en el registro mercantil.

Quedan fuera del alcance: auditorías voluntarias, proyectos piloto sin impacto contable real, criptoactivos custodiados por terceros sin integración en el libro mayor de la entidad y aspectos puramente fiscales o de blanqueo de capital.

2.5. Criterios de validación y contribución.

- Relevancia práctica: Los resultados mostrarán, con datos objetivos de informes de auditoría de los ejercicios 2022-24, si la triple entrada reduce la proporción de opiniones modificadas/CCA sobre conciliaciones y tiene afectación en la valoración del riesgo de incorrección material.
- Contribución académica: Aporta evidencia cuantitativa en España que vincula blockchain y calidad de auditoría, combinando ANOVA/ χ^2 con análisis sector-tamaño. Completa la literatura, mayoritariamente descriptiva (Dai & Vasarhelyi 2017; Grigg 2005), con un contraste estadístico replicable.

3. Marco teórico.

3.1. Definición y fundamentos de blockchain.

3.1.1 De la tablilla a la triple entrada.

Desde la tablilla mesopotámica (partida simple) y la obra de Pacioli (partida doble) el objeto ha sido siempre dotar de integridad al libro mayor. Grigg (2005) formaliza la contabilidad de triple entrada: un tercer asiento, distribuido y firmado digitalmente, actúa como recibo irrevocable compartido entre las partes. Esta capa común constituye la base para la evidencia contable y la auditoría continua (Dai & Vasarhelyi, 2017).

Tabla 2: Cronología de la teoría contable

Hito	Soporte físico / lógico	Aporte clave a la seguridad de la información
Mesopotamia (c. 3 500 a. C.)	Tablillas de arcilla con marcas cuneiformes	Primeros registros permanentes de deudas de grano y ganado (Burns et al., 2003).
Partida doble (Pacioli, 1494)	Papel – Diario y Mayor	Simetría “débito-crédito” → facilita detección de errores internos.
ERP (década 1970-)	Ordenador central → nube	Automatiza asientos, pero sigue basándose en la doble entrada.
Partida triple (Grigg, 2005)	Blockchain distribuida	Añade un recibo firmado y compartido por ambas partes y por la red.

Fuente: Elaboración propia a partir de Burns et al. (2003) y Grigg (2005)

3.1.2 ¿Qué es una blockchain?

La cadena de bloques es una base de datos distribuida, enlazada criptográficamente y resistente a la manipulación gracias al uso de funciones hash y firmas asimétricas (Antonopoulos, 2014). Cada bloque incluye cabecera (hash del bloque previo, raíz de Merkle y sello temporal) y cuerpo (transacciones). La variación de un solo bit invalida la cadena, garantizando inmutabilidad y tamper-evidence (Nakamoto, 2008).

Se distinguen tres modelos de red:

- Pública (Bitcoin, Ethereum): acceso sin permisos; seguridad basada en incentivos económicos.
- Privada (Hyperledger Fabric, Corda): nodos identificados; mayor rendimiento y confidencialidad.
- Permissionada (Alastria): híbrido que equilibra transparencia y control, idóneo para sectores regulados.

En resumen, podemos definir e identificar la blockchain con tres conceptos:

1. Libro contable compartido

Imagine un Excel que no está en el portátil de nadie, sino copiado exacto en decenas -o miles- de ordenadores repartidos por el mundo.

2. Sellado automático de cada página

Cada bloque de apuntes lleva un “sello digital” (un hash) que depende del bloque anterior. Si alguien intenta borrar o cambiar una línea, el sello ya no coincide y todos los nodos informan de la discordancia.

3. Acuerdo descentralizado

Antes de añadir una página nueva, los nodos votan siguiendo reglas matemáticas (llamadas algoritmos de consenso). Así se decide qué versión del libro es la verdadera sin autoridad central (Antonopoulos, 2014).

En la práctica, esto significa que ningún usuario puede alterar un asiento pasado sin que todos los demás lo noten, lo que acerca el sistema a la clásica aspiración contable de imagen fiel.

3.1.3 Resumen cronológico de la tecnología (2008-2025)

Tabla 3: Hitos recientes en tecnología blockchain

Año	Acontecimiento	Relevancia para la profesión contable
2008	Publicación del <i>white paper</i> de Bitcoin (Nakamoto)	Prueba de que un libro público puede funcionar sin entidad central.
2015	Lanzamiento de Ethereum	Introduce los <i>smart contracts</i> , programas que registran asientos sin intervención humana.
2019	Bono digital de Banco Santander	Primer valor español emitido y liquidado íntegramente en blockchain.
2022	Merge de Ethereum (PoW → PoS)	Reduce consumo energético $\approx 99\%$; alineándose con objetivos ESG.
2023-2024	Emisión piloto de dinero tokenizado Fnlity-Santander-UBS	Permite asientos contables de tesorería (NRV 9) en cadena de bloques con dinero “de banco central”.
2025	Hoja de ruta Alastria 3.0 alineada con MiCA y DORA	Ejemplo nacional de red permissionada compatible con normativa UE.

Fuente: *Elaboración propia*

3.1.4 ¿Por qué importa a la contabilidad? – La triple entrada y su relación con las teorías contables

Como paso natural a la seguridad de la información que se busca con los principios contables, Grigg (2005) introduce el concepto de “contabilidad de triple entrada”. En este sistema, se agrega un tercer libro diario que es custodiado y alojado en una blockchain.

- **Libro A (vendedor)** registra un ingreso.
- **Libro B (comprador)** registra un gasto.
- **Libro C (blockchain)** guarda el “recibo” firmado por ambos y sellado con tiempo.

Ese “tercer asiento” ayuda a reducir las conciliaciones y circularizaciones por parte del equipo de contable y auditores externos. Si el auditor ve que Libro C contiene la misma huella digital que los libros A y B, sabe que la operación es auténtica y que nadie la ha cambiado después (Grigg, 2005). Y, a diferencia de los correos o PDF usuales, el recibo es inmutable y accesible en cualquier momento.

Enlazando con las teorías clásicas de empresas, de acuerdo a la teoría de la responsabilidad de los administradores enunciada por Milton Friedman (1970), se debe cuestionar si la dirección de una entidad está mostrando la imagen fiel de esta o, por el contrario, la información mostrada está sesgada o manipulada, incumpliendo este principio esencial de la norma contable. En estos casos, la adopción de soluciones basadas en blockchain reforzaría la confianza de la información mostrada en los estados financieros, al dificultar de manera significativa la manipulación de cifras y datos ex post (IASB, 2018; Yermack, 2017).

Tomando como referencia los postulados, tanto la teoría de la agencia (Jensen & Meckling, 1976) como de la información asimétrica (Spence, 1978), la cuestión se centra en cómo reducir la brecha existente entre la información que poseen los gestores de las empresas (agentes) y la recibida por los inversores, propietarios y otras partes interesadas (principales). La propuesta de Catalini & Gans (2016) es que un libro público o permissionado, que sea siempre accesible a auditores externos, podría reducir significativamente los costes de verificación y las asimetrías de información.

Por otro lado, atendiendo a la teoría coste – beneficio (COSO, 2013), se deben desarrollar y aplicar controles razonables y proporcionados, que aseguren un adecuado nivel de mitigación del riesgo al que se refieren sin incurrir en costes innecesarios (proporcionalidad de la respuesta al riesgo). La adopción de soluciones contables basadas en blockchain podrían reducir las conciliaciones y las circularizaciones, con el consiguiente ahorro de costes operativos. Es en esta dirección en la que, el BIS-CPMI (2017) por una parte y Dai & Vasarhelyi (2017) por otra, apuntan y se alinean con los principios que subyacen en la NIA-ES 315 R (2024).

Como conclusión preliminar, podemos afirmar que la blockchain refuerza el papel tradicional de la contabilidad como garante de confianza, pero lo hace redistribuyendo la autoridad entre múltiples nodos y automatizando gran parte de la verificación.

3.2. Algoritmos de consenso.

3.2.1 ¿Para qué sirve el consenso?

En una blockchain no hay un “libro maestro” guardado en un único servidor. Cada nodo tiene su copia y, antes de añadir una página nueva, todos deben ponerse de acuerdo sobre cuál es la correcta.

Ese acuerdo se llama consenso y evita que dos personas gasten el mismo activo dos veces (double-spend) o que aparezcan versiones contradictorias del libro.

Esto se puede explicar con una sencilla metáfora: imagine que un grupo de 10 contables revisa todas las transacciones que realiza una entidad. Para que una transacción sea válida, y pueda anotarse en el diario, al menos 7 deben confirmarla. El algoritmo decide quién puede proponer una transacción y cuántas confirmaciones son necesarias para aprobarla.

3.2.2 Principales familias de consenso

Tabla 4: Principales familias de consenso

Algoritmo (sigla)	Cómo se decide quién escribe la “página”	Ventajas para la empresa	Limitaciones / riesgos
Proof-of-Work (PoW) Ej.: Bitcoin	El nodo que resuelve primero un acertijo matemático complejo (<i>hashcash</i>).	Seguridad muy alta – cambiar un bloque requeriría el 51 % de la potencia mundial de cálculo.	Gran consumo eléctrico; transacciones lentas (~10 min).
Proof-of-Stake (PoS) Ej.: Ethereum desde 2022	Se elige al azar entre quienes tienen “fichas” bloqueadas como garantía (<i>staking</i>).	99 % menos energía que PoW; transacciones más rápidas (~15 s) (Beekhuizen, 2021; Digiconomist)	Concentración de poder en las “ballenas”; penalización (<i>slashing</i>) si el nodo falla.
Delegated PoS (DPoS) Ej.: EOS/TRON	Los usuarios votan a 20-30 “delegados” que validan en su nombre.	Rendimiento muy alto (miles TPS); tarifas bajas.	Menor descentralización; riesgos políticos (delegados cartelizados).
Bizantino Fault Tolerance (BFT) Ej.: PBFT, Tendermint / IBFT (Alastria)	Pequeño grupo (≤ 50) intercambia mensajes firmados hasta llegar a los $\frac{2}{3}$ de los votos.	Latencia muy baja (< 5 s); idóneo para redes de empresas y bancos.	Requiere lista fija de nodos confiables y gobierno formal.

Fuente: Elaboración propia basada en Nakamoto (2008), Buterin (2014) y documentación técnica de Alastria.

En los proyectos españoles prevalece el esquema IBFT en red permissionada, compatible con el GDPR y con los requerimientos que establece DORA (Reglamento 2022/2554).

Dentro de estos proyectos, cabría destacar los siguientes casos:

- Finanzas - Bono digital de Banco Santander.

El banco ha utilizado Ethereum, que desde el Merge (15-sep-2022) opera con Proof-of-Stake (PoS). La elección de esta red responde a su liquidez global y a la disponibilidad de estándares ERC ampliamente soportados por wallets y custodios institucionales.

- Pymes - Red Alastria.

Las implantaciones empresariales en España se apoyan en la red Alastria, permissionada. Históricamente, la Red-T ha corrido sobre GoQuorum con IBFT 1.0 (familia BFT), alcanzando bloques < 5 s y facilitando cumplimiento RGPD gracias a la identidad soberana. (En la hoja de ruta 3.0 también se emplea Hyperledger Besu / IBFT 2.0 en la Red-B).

- Energía - Iberdrola + Energy Web.

Los casos de Garantías de Origen y PPAs se registran en Energy Web Chain, que utiliza Proof-of-Authority (PoA), una variante BFT con validadores autorizados por la fundación. La motivación es doble: gobernanza controlada y trazabilidad renovable apta para auditoría.

- Investigación - EUROchain (Eurosistema/BCE).

El Eurosistema ha desarrollado EUROchain, una red de pruebas basada en Corda (permissionada) con consenso a través del servicio Notary (implementaciones Raft/BFT). Los ensayos exploran pagos con preservación de privacidad, mediante mecanismos como los “anonymity vouchers”, que permiten mantener el anonimato en transacciones de bajo importe y, al mismo tiempo, conservar trazabilidad y auditoría selectiva para fines de cumplimiento en materia de prevención del blanqueo de capitales y de la financiación del terrorismo (PBC/FT). Se trata de prototipos de investigación -no despliegues productivos- orientados a estudiar requisitos técnicos de un eventual euro digital en entornos controlados.

3.2.3 Del PoW al PoS (Ethereum)

La siguiente tabla resume el salto energético tras el “Merge” de Ethereum el 15 de septiembre de 2022. Muestra el impacto energético de pasar de un algoritmo de consenso que premia la potencia de cálculo (PoW) a otro que selecciona validadores según las monedas depositadas en staking (PoS).

Tabla 5: Datos medioambientales pre y post “Merge”

Indicador	Antes del Merge (PoW)	Después (PoS – 15 sep 2022)
Consumo anual estimado	78 TWh (similar a Chile)	0,01 TWh (≈ pequeña ciudad)
Emisiones CO ₂ (t/año)	34 Mt	0,04 Mt

Fuente: Elaboración propia a partir de datos de Digiconomist (2022)

El paso de PoW a PoS en Ethereum tiene efectos directos en la presentación sobre información climática bajo ESRS E1 (CSRD) y en la lectura de “otra información” que realiza el auditor (NIA-ES 720, 2024), al reducir > 99 % el consumo estimado (Digiconomist, 2022) y, por tanto, la huella atribuible a registros on-chain.

Su relevancia radica en tres aspectos:

1. Impacto medioambiental de las emisiones (ESRS E1-9)

- Para la mayoría de las empresas, usar una red pública de blockchain genera emisiones indirectas (Emisiones de Alcance 3 en la cadena de valor).
- Tras el Merge, la huella de carbono se reduce > 99 %, lo que facilita cumplir el estándar ESRS E1 (Climate Change) publicado junto a la Directiva CSRD.

2. Taxonomía Verde UE (Reg. 852/2020)

- Las actividades TIC deben demostrar que “contribuyen sustancialmente” a la mitigación (art. 10) y “no causan daño significativo” a otros objetivos.

3. Divulgación SFDR.

- Los gestores de fondos que invierten en empresas blockchain deben reportar la intensidad de emisiones (t CO₂e/€ m) de sus participadas.

Esto tiene su impacto tanto en la Nota 15 “Información sobre medioambiente” (modelo normal de las cuentas anuales, según PGC), como en el informe de gestión e información sobre sostenibilidad (EINF/CSRD – ESRS). En esta nota debe describirse la política medioambiental de la entidad, así como las métricas relevantes asociadas. A efectos de justificar la materialidad, puede incorporarse un comparativo cuantitativo del consumo/huella vinculada al cambio de algoritmo (PoW → PoS) en la red utilizada. Un campo “antes/después” permite sostener por qué la gerencia considera que la huella derivada del uso de blockchain es no significativa en el ejercicio.

En el informe de gestión integrado con la información de sostenibilidad deben divulgarse los indicadores ESRS aplicables (en particular, ESRS E1 – Cambio climático) y los planes de descarbonización. En este contexto, el cambio de algoritmo de consenso puede documentarse como acción de mitigación, cuantificando la reducción lograda (> 99 % en consumo/emisiones al pasar de PoW a PoS, según la fuente técnica que utilices). Esta evidencia se incluye en el apartado de políticas, metas y métricas climáticas exigido por la CSRD–ESRS.

Respecto a su posible afectación al informe de auditoría, conforme a la NIA-ES 720 R (2024), el auditor debe leer la “otra información” (incluida la de sostenibilidad cuando acompaña a los estados financieros) y comprobar su coherencia con lo auditado. Si los datos climáticos asociados al uso de blockchain han sido especialmente significativos en la auditoría del periodo, el asunto podría presentarse como Cuestión Clave de la Auditoría (CCA) de acuerdo con la NIA-ES 701 (2024). En la práctica, el auditor contrastará el cálculo de emisiones/consumo declarado por la entidad con la fuente técnica empleada y describirá, en su caso, los procedimientos aplicados.

Estas respuestas de auditoría no eliminan riesgos residuales de escalabilidad, interoperabilidad, GDPR o errores lógicos, que se analizan a continuación desde la óptica del control interno y la obtención de evidencia suficiente y adecuada (NIA-ES 330, 2024 y NIA-ES 500, 2024).

3.3.Desafíos técnicos y operativos.

3.3.1 Escalabilidad y almacenamiento

Las redes públicas, como Ethereum, de acuerdo con Beekhuizen (2021), crecen muy deprisa. Un nodo “completo” guarda ya más de 1 TB; siendo difícil para las pymes españolas poder dedicar servidores tan costosos.

Para que cualquier empresa o auditor pueda revisar la información sin necesitar servidores de gran capacidad, los desarrolladores han propuesto una mejora (conocida como EIP-4444) que permite borrar de los ordenadores los detalles de las transacciones más antiguas una vez que han quedado definitivamente validadas.

Solo se conserva un “resumen” criptográfico que sigue garantizando la integridad de la cadena. Esta limpieza periódica forma parte del proyecto “Stateless Ethereum”, cuyo objetivo es lograr una red más ligera y fácil de verificar (Gheorghita, 2024).

Desde el punto de vista de la información financiera y sobre sostenibilidad, si la empresa decide llevar sus apuntes a una red pública, deberá evaluar el coste de infraestructura frente al ahorro en conciliaciones y podría tener que revelar esta circunstancia según su impacto (Memoria, Informe de Gestión o Informe sobre Sostenibilidad)

3.3.2 Interoperabilidad y puentes (bridges)

Las cadenas de bloques funcionan como “islas de datos”; cuando una empresa necesita mover un activo de la red A a la red B utiliza un puente (bridge). Los datos de la blockchain A quedan “inmovilizados”, emitiéndose uno equivalente en la blockchain B.

Cuando los datos o activos son transferidos de una red a otra se presenta una vulnerabilidad, al abrir “una pasarela” entre cadenas donde se concentran gran cantidad de datos de alto valor. De acuerdo al “*2025 Crypto Crime Report*”, publicado por Chainalysis (2025), hasta el año 2023 más del 60% de los ataques a blockchain se concentraron en bridges.

Es a partir de 2024 (Chainalysis, 2025) que este porcentaje se comienza a reducir hasta el 40%, gracias a una mejora en los protocolos de seguridad, auditorías de smart contracts y cooperación entre plataformas y autoridades.

Actualmente, los métodos de ataque han pasado a centrarse, entre otros, en la explotación de errores en smart contracts

Por otro lado, este mismo informe apunta a que los puentes son utilizados como herramientas para el blanqueo de capitales.

Desde el punto de vista de la auditoría, atendiendo a la NIA-ES 315 R (2024), el auditor debe considerar si la entidad utiliza puentes en su operativa habitual; evaluar la fiabilidad de la evidencia de la titularidad y la capacidad de recuperabilidad de los activos en caso de ciberataque o fallo en el protocolo del bridge; la dependencia de terceros (exchange, custodios...); y la existencia de informes de auditoría de los sistemas de TI.

En cuanto al cumplimiento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBCFT), y su desarrollo reglamentario mediante el Real Decreto 304/2014, así como para las obligaciones que el auditor debe considerar en su trabajo conforme a las NIA-ES 250 (2024) y NIA-ES 240 (2024), el aumento del uso de puentes como soporte de operaciones con el objeto blanquear fondos o fines ilícitos, hace necesario evaluar la adecuación del cumplimiento normativo en esta materia por parte de la entidad auditada y considerar los posibles efectos financieros y legales derivados de sanciones. El auditor deberá documentar adecuadamente su comprensión y respuesta ante estos riesgos.

3.3.3 Errores lógicos en smart contracts:

Según Dominik Muhs (2023), de *Smart Contract Security Field Guide*, ocho de cada diez fallos se deben a “despistes” en la lógica de los programas, no a fallos criptográficos. Además de la auditoría de código clásica, surgen dos retos nuevos:

- **Oráculos:** servicios que introducen datos externos (precio, clima). Si el oráculo falla, la transacción será incorrecta, aunque el contrato sea perfecto.
- **Código generado por IA:** herramientas como GPT-Coder aceleran el desarrollo, pero pueden introducir vulnerabilidades invisibles al ojo humano (ENISA, 2022).

Para evitar estos errores, los expertos recomiendan introducir una serie de controles:

- Segregación de funciones: quien aprueba el oráculo no puede firmar transacciones.
- Pruebas de “re-ejecución” del contrato en entorno aislado.
- Validación automática con herramientas slither o mythril y revisiones formales (formal verification) cuando los importes sean significativos.

Atendiendo al informe “2025 Crypto Crime Report” de Chainalysis (2024), los ciberataques a smart contracts representan más del 40% de los registrados entre los años 2023 y 2024. Estos ataques aprovechan las vulnerabilidades en la lógica de los programas que los desarrolladores no y sus protocolos de detección de errores no han podido detectar.

Es por esto por lo que, desde el punto de vista de la auditoría, los smart contracts representan un riesgo emergente significativo de acuerdo a la NIA-ES 315 R (2024).

Para dar respuesta a estos riesgos, el auditor deberá obtener evidencia del fondo económico de los smart contracts, evaluar el control que la entidad tiene sobre el programa y su código o depende de terceros, y si la entidad mantiene auditorías externas de código.

En esta situación, el auditor debe considerar la necesidad de recurrir a un experto en blockchain o ciberseguridad, conforme a la NIA-ES 620 (2024), para evaluar la fiabilidad técnica del entorno.

3.3.4 Custodia de claves y gobierno de acceso

El concepto “clave privada” blockchain hace alusión a la llave criptográfica utilizada para la autenticación y validación de los nodos en la red. Perder esta clave equivale a perder el activo. KPMG (2018) subraya la necesidad de un almacenamiento seguro, combinado con el mantenimiento y revisión del gobierno de estas. El gobierno de las claves de acceso debe identificar, entre otros, los riesgos por pérdida accidental de claves, la imposibilidad de modificarlas una vez compartidas y el almacenamiento o transmisión no cifrada de las mismas.

Para mitigar estos riesgos KPMG (2018) advierte que, desde el gobierno de accesos y permisos, deben configurarse controles sobre la gobernanza de las claves; mantener un registro y auditoría del uso de las claves; y hacer una adecuada gestión de algoritmos de hash y validación de su adecuación criptográfica.

En resumen, propone una serie de buenas prácticas que podrían resumirse en la siguiente tabla:

Tabla 6: Buenas prácticas en custodia de claves

Buenas prácticas	Equivalente contable / auditor
HSM o módulo hardware para firmar	Riesgo de IT (NIA-ES 315 R, 2024): verificar controles físicos sobre el dispositivo
Multi-firma (2-de-3)	Separar responsabilidades.
Renovación periódica de claves	Similar a cambiar contraseñas SOX, documentado en papel de trabajo

Fuente: Elaboración propia a partir de KPMG (2018)

3.3.5 Riesgos emergentes para la blockchain

Además de los riesgos actuales, en el ecosistema blockchain deben considerarse riesgos potenciales derivados de nuevas tecnologías o de casos de usos de las ya existentes. Entre los primeros, el más destacado es el desarrollo de la computación cuántica y la amenaza que supondría un ciberataque usando ordenadores basados en esta tecnología. El NIST (2023) establece esta posibilidad dentro de los próximos 10 años, considerando que un futuro ordenador cuántico podría romper la seguridad de las redes criptográficas actuales. Ante esta amenaza, organismos como el Centro Criptológico Nacional (CCN), proponen planes de mitigación a firmas post cuánticas (CCN, 2022).

En lo que refiere a amenazas provenientes de casos de uso de tecnologías actuales, cabe citar el “*prompt injection*” en smart contracts generados a través de inteligencia artificial (IA). En estos casos, el código generado por agentes basados en IA podría ejecutar órdenes no previstas. Esta situación requerirá de herramientas de análisis de prompts (*prompt linting*), revisión manual del código y control de versiones.

3.4. Aplicaciones empresariales (triple partida, supply chain, etc.)

3.4.1 La contabilidad de triple partida

Tabla 7: Ejemplo de asientos de triple partida

Paso	Asiento en el ERP (partida doble)	“Tercer asiento” en la blockchain
1. Venta: Empresa A vende mercancía a Empresa B por 10 000 € + 21%IVA	(1) 430 Clientes 12.100 a (2) 477 HP IVA repercutido 2 100 700 Ventas 10 000	Se emite un recibo digital: “ <i>DLT_recibo</i> ” - 12 100 € Firmado por A y B, con todos los datos de la operación y con sello de tiempo: <i>2025-06-21T11:42</i>
2. Cobro	572 Banco 12 100 A 430 Clientes 12 100	Se enlaza al recibo anterior un recibo de liquidación (“ <i>DLT_recibo_liquidado</i> ”) que cierra la deuda.

Fuente: Elaboración propia

La introducción de la contabilidad de triple partida (Grigg, 2005) proporciona evidencia continua para el auditor (Dai & Vasarhelyi, 2017), al introducir un tercer libro diario donde se recogen todas las operaciones. Es en este tercer libro, o Libro C, dónde se concilian las transacciones anotadas en los Libros A y B, haciendo evidente cualquier discrepancia cuando estos no están alineados.

Esta solución también aporta evidencia sobre cualquier cambio o manipulación, gracias a la información recogida en el hash de cada bloque.

A pesar de esto, la adopción de la triple partida no está exenta de limitaciones, como pueden ser los costes de integración con los sistemas ya existentes, la falta de homogeneidad en cuanto a criterios contables a nivel internacional o la dependencia de oráculos externos para datos referidos al mundo físico (*real world assets*).

Entre las soluciones de triple partida basadas en blockchain, cabría citar las propuestas de empresas como R3 y su solución, Corda, o los sistemas de pago desarrollados por Ripple

También existen proyectos piloto como los de Balanc3, Ledgerium o zkLedger, que actualmente aún no han pasado a producción.

3.4.2 Trazabilidad y cadena de suministro

Como proyecto pionero en España se debe citar la tokenización de Garantías de Origen (GdO) por parte de Iberdrola en su plataforma Energy Web Chain basada en PoA (*Proof of Authority*), donde se tokeniza cada MWh y el consumidor cancela el token al usar la energía. Esta solución busca solventar la problemática tradicional de las GdO en papel, que conllevan un riesgo de doble venta.

Desde el punto de vista de la información contable y financiera, las existencias de certificados (NRV 10) se "queman" automáticamente, y el auditor puede verificar este proceso de "*burn*". La red utilizada (Energy Web Chain) facilita una gobernanza controlada y una trazabilidad apta para auditoría.

Otro caso de uso pionero, proveniente de Estados Unidos, es el IBM Food Trust. Esta solución viene a dar respuesta a la problemática en la conciliación entre albaranes, certificados y controles sanitarios. Para ello, se establece un registro común para el productor, el transportista y el supermercado. Esto se traduce en una reducción en los ajustes de inventario, proporcionando evidencia externa siempre disponible (NIA-ES 505, 2024).

En esta línea de trazabilidad se enmarca la propuesta de Carrefour, OriginTrail (2023 – 2025). La cuestión a resolver es la dificultad en probar el origen de los productos. Por ejemplo, la procedencia de la leche fresca del lineal. Esto se soluciona asignando a cada lote un ID DLT y guardando su ruta en la red OriginTrail. Esta solución mejora la precisión de los inventarios (NRV 10, PGC) y reduce las devoluciones (NRV 14 y NRV 15) gracias a la mejora en la trazabilidad. En este caso, el auditor puede validar la ruta consultando los registros DLT.

3.4.3 Tokenización de activos y finanzas corporativas

La tecnología blockchain (DLT) ofrece soluciones concretas en el ámbito de la tokenización de activos y las finanzas corporativas al crear registros inmutables y compartidos

que reducen las fricciones de liquidación y garantizan la integridad y la titularidad de los instrumentos financieros.

Estas soluciones se enmarcan en un contexto regulatorio europeo activo, como el Reglamento de Mercados de Criptoactivos (MiCA) y el Régimen Piloto de DLT (Reglamento (UE) 2022/858), que buscan crear un entorno de pruebas para infraestructuras de mercado tokenizadas.

La tokenización de deuda se refiere a la emisión de bonos o instrumentos de deuda directamente sobre una cadena de bloques, utilizando smart contracts para gestionar automáticamente el pago de cupones. En España, el Banco Santander emitió el primer bono digital emitido y liquidado íntegramente en blockchain en septiembre de 2019. Desde el punto de vista contable, se aplica la Norma de Registro y Valoración (NRV) 9.^a (Instrumentos financieros). La valoración se realiza por su valor razonable, generalmente mediante el uso de un oráculo (como Bloomberg) para obtener el precio. El auditor, para obtener evidencia, deberá verificar el smart contract del cupón y el saldo en la wallet del depositario.

UBS, en colaboración con el Banco Santander, puso en marcha en 2024 el proyecto piloto Finality. Este proyecto aborda la liquidación inmediata de transacciones financieras utilizando representaciones digitales de dinero emitido por el banco central, en libras. Para su registro contable, el activo debería reclasificarse como efectivo “tokenizado” dentro del capítulo de Tesorería (NRV 9.^a), y debe ser revelado en la Memoria. Esta solución habilita la conciliación PvP (Pago contra Pago), lo que puede ser usado en auditoría para una prueba de re-ejecución de la liquidación en un nodo observador para validar la exactitud del proceso.

También en España, dentro del sandbox operado por la CMNV (2025) y de la mano de una socimi, se explora la opción de Capital Digital o *Equity Capital*. Esto se refiere a la representación de acciones o participaciones de capital social como tokens digitales. El tratamiento contable de esta operación se enmarca en la NRV 9.^a de instrumentos financieros. Para el auditor, elimina la necesidad de un registrador físico para la comprobación de la titularidad de los accionistas.

3.4.4 Sector público: el ejemplo estonio

Desde 2019, e-Health Estonia usa una mini-blockchain (KSI DLT) para recoger las modificaciones en los historiales clínicos: cada vez que un médico accede o modifica un dato, la operación se “firma” y se enlaza a la cadena gubernamental (Estonian Health Board, 2022).

En términos contables: el tráfico de operaciones de sanidad se documenta en tiempo real y el auditor nacional puede verificar la integridad con una simple comprobación de hashes. Aunque no es un asiento PGC, demuestra que la triple entrada se aplica también al sector público.

En Estonia el uso de KSI-Blockchain va mucho más allá de la sanidad: es un “tejido” que protege prácticamente todas las bases de datos críticas del Estado.

Tabla 8: Casos de uso de KSI-Blockchain en Estonia

Área de la administración	Registros o procesos protegidos con KSI	Ejemplo concreto
Justicia	Expedientes judiciales y firma de sentencias electrónicas	Todos los documentos de los tribunales se “hashean” y encadenan con KSI para garantizar que nadie pueda alterarlos después (northsearegion.eu)
Catastro y propiedad	Land Register (reg. de la propiedad)	Cada cambio de titularidad queda vinculado a una prueba KSI; el notario o el juez puede verificar en segundos la integridad del historial (e-estonia.com)
Registro mercantil	Business Register (alta de sociedades, cuentas depositadas)	Las inscripciones y depósitos se sellan diariamente para prevenir manipulaciones internas o externas (e-estonia.com)
Impuestos y aduanas	e-Tax / e-Customs	Los ficheros de declaraciones se firman con KSI antes de enviarse a la Agencia Tributaria; el contribuyente puede demostrar que “lo entregó tal día, tal hora” (e-estonia.com)
Presupuestos y finanzas públicas	Sistema de información financiera del Estado (HAAPS)	Los asientos contables de la Hacienda pública van acompañados de la huella KSI para auditoría continua (e-estonia.com)
Defensa y ciber-resiliencia	Copias “data-embassy” en Luxemburgo	Los backups cifrados se sellan con KSI para poder demostrar que los datos no fueron modificados en tránsito (sps.nyu.edu)
Telecom y cadena de suministro	Productos Guardtime para operadores y logística	Guardtime ha construido 12 líneas de negocio (telecom, supply-chain, incluso sector espacial) sobre la misma infraestructura KSI (investinestonia.com)

Fuente: Elaboración propia a partir de datos de e-Estonia (2025)

¿Por qué el Gobierno estonio lo extiende a tantas áreas?

- **Misma API para todos los ministerios:** El coste marginal de sumar un nuevo registro es muy bajo.

- **Prevención de fraude y de ataques internos:** Cada vez que un funcionario consulta o modifica un dato, el sistema genera una “huella” inmutable; si alguien cambia un expediente, el hash ya no coincide.
- **Auditoría continua:** El Tribunal de Cuentas puede contrastar, en tiempo real, que los libros mayores (financieros, judiciales, catastrales) no han sido alterados.
- **Cumplimiento regulatorio internacional:** La UE exige trazabilidad y ciber-resiliencia (NIS 2, DORA); el uso de KSI actúa como “póliza de seguro” tecnológica.

4. Marco normativo.

Las tecnologías de registro distribuido (TRD) representan una oportunidad para las empresas. Nos encontramos en un momento en el que la Unión Europea ha desplegado toda una batería regulatoria coherente para equilibrar innovación y protección: MiCA regula los criptoactivos y a sus proveedores; el Régimen Piloto TRD ensaya infraestructuras de mercado tokenizadas; DORA y NIS 2 elevan la resiliencia operativa; CSRD–ESRS homologan la divulgación de sostenibilidad; y el Data Act habilita la portabilidad y el acceso a datos industriales.

En paralelo, iniciativas públicas como EBSI y el futuro EUROPEUM-EDIC, en el marco comunitario, e ISBE – Infraestructura de Servicios Blockchain de España, en el caso nacional, refuerzan el despliegue de servicios transfronterizos basados en TRD. Este entramado condiciona cómo se clasifican, valoran y evidencian las operaciones registradas on-chain en las cuentas anuales, y qué pruebas debe diseñar el auditor para obtener evidencia suficiente y adecuada.

4.1.Unión Europea.

La Comisión Europea subraya que la competitividad de la UE en TRD depende de un marco jurídico único y predecible que evite la fragmentación normativa y garantice la protección de inversores y consumidores (Comisión Europea, 2024). Con esta premisa, la estrategia comunitaria aspira a posicionar a Europa como centro de plataformas y aplicaciones blockchain, al tiempo que alinea la innovación con los valores de la Unión: sostenibilidad, privacidad y ciberseguridad.

Este marco jurídico se sustenta sobre cinco pilares:

1. **Regulación de criptoactivos y proveedores (MiCA):** marco único para emisores de *tokens* y proveedores de servicios de criptoactivos (CASP, por sus siglas en inglés *Crypto-Assets Service Provider*), con obligaciones de gobierno, divulgación y salvaguardas (Reglamento (UE) 2023/1114).
2. **Mercados de capitales tokenizados (Régimen Piloto TRD):** entorno de pruebas con exenciones acotadas para los Sistemas Multilaterales de Negociación y Sistemas de Liquidación de Valores *on-chain* – *MTF*, *Multilateral Trading Facilities*, y *SS*, *Settlement System*, por sus siglas en inglés, respectivamente- (Reglamento (UE) 2022/858).
3. **Resiliencia digital:** DORA para todo el sector financiero (Reglamento (UE) 2022/2554) y NIS 2 para sectores esenciales e importantes (Directiva (UE) 2022/2555).
4. **Calidad y comparabilidad de la información:** CSRD y ESRS integran la sostenibilidad en el informe de gestión; la Directiva (UE) 2025/794 aplaza fases de aplicación para “resto de grandes” y pymes cotizadas; el Data Act asegura acceso y portabilidad de datos (Directiva (UE) 2022/2464; Reg. Del. (UE) 2023/2772; Reglamento (UE) 2023/2854).
5. **Políticas públicas y estandarización:** EBSI (servicios públicos con verificación de credenciales), EUROPEUM-EDIC (consorcio EDIC con personalidad jurídica para gestionar y evolucionar EBSI, al amparo del Reg. (UE) 2022/2484) y el European Blockchain Sandbox; todo ello acompañado por la participación europea en ISO TC 307, CEN/CENELEC JTC 19 y ETSI ISG PDL.

Para contables y auditores, el resultado práctico es doble: por un lado está la clasificación y valoración más homogéneas de activos y pasivos *on-chain* (encaje PGC/NIIF), y por el otro las pruebas de auditoría pueden combinar la lectura del mayor con verificaciones “*on-chain*” (NIA-ES 500, 2024 y NIA-ES 505, 2024), evaluando además controles de TI y resiliencia (NIA-ES 315 R, 2024; conexión con DORA/NIS 2).

La propia Comisión (2024) asegura que la UE quiere ser líder en tecnología blockchain y TRD, convirtiéndose en un importante innovador en blockchain y un hogar para plataformas, aplicaciones y empresas significativas.

A continuación, se examinan las principales normas europeas agrupadas por su ámbito de impacto. Para cada una se sintetizan objeto, cronograma de aplicación y efectos sobre la calidad de la información financiera y la auditoría.

4.1.1 Reglamento (UE) 1114/2023 – Mercados de Criptoactivos (MiCA)

El art.3 del Reglamento (UE) 1114/2023, MiCA, establece por primera vez un marco armonizado para criptoactivos no cubiertos por la normativa financiera previa, diferenciando entre: *tokens* referenciados a activos (ART), *tokens* de dinero electrónico (EMT), criptoactivos “genéricos”, y los proveedores de servicios de criptoactivos (CASP). La clasificación se rige por el principio fondo sobre forma: la naturaleza económica del token prima sobre su etiqueta comercial (Parlamento Europeo y Consejo, 2023).

Tabla 9: Calendario de aplicación de MiCA

Bloque	Aplicación	Supervisor
ART & EMT -incluida la autorización y los requisitos reforzados de reserva y gobierno-	30-jun-24	ABE / BCE
Criptoactivos genéricos + CASP	30-dic-24	ESMA + supervisores nacionales
“Travel rule” (Reg. 1113/2023)	30-dic-24	ESMA / ABE
Régimen transitorio para CASP	hasta 1-jul-2026	art. 143.3

Fuente: Reglamento (UE) 1114/2023

Bajo el prisma de la información financiera a revelar, los criptoactivos en balance deben encajar en las NRV 5.^a, 9.^a o 10.^a (intangible, instrumentos financieros o existencias), según su función económica -criterio ya anticipado por la Consulta 4/BOICAC 120 para criptomonedas emitidas por la propia empresa. MiCA no redefine categorías contables, pero reduce la incertidumbre sobre el instrumento subyacente y la disponibilidad de datos (gobierno, reservas, whitepaper, divulgación de riesgos).

En la memoria se deberá informar sobre los libros blancos (whitepapers) y, en ART/EMT, la información sobre reservas y mecanismos de estabilización, aportan datos verificables para la Memoria (PGC) y, en su caso, para el informe de gestión.

Para el auditor, se podrían identificar riesgos de incorrección material (NIA-ES 315 R, 2024) por valoración (volatilidad/mercado activo), custodia y segregación de criptoactivos, integridad del registro on-chain (existencia/completitud), dependencia de terceros (custodios, exchanges, oráculos) y gobierno TI.

Para la obtención de evidencia suficiente y adecuada (NIA-ES 500, 2024 y NIA-ES 505, 2024), cabría optar por una combinación de confirmaciones externas (custodios/terceros), verificación en nodo (hash, bloque, timestamp) y conciliaciones “triple partida” cuando existan recibos compartidos.

Gobierno y resiliencia: MiCA impone exigencias organizativas y de gestión de riesgos que dialogan con DORA; las deficiencias relevantes en controles generales de TI pueden elevar el riesgo significativo (y derivar en CCA si requirieron especial atención; NIA-ES 701, 2024).

Las fechas de junio y diciembre 2024 convierten MiCA en un gatillo regulatorio inmediato: mejora la trazabilidad y transparencia de la información financiera, que obliga a auditores y contables españoles a incorporar técnicas de verificación “on-chain” y control TI integrado antes del cierre 2025.

Una vez definido el marco para los criptoactivos mediante MiCA, el Reglamento (UE) 858/2022 permite poner a prueba infraestructuras de mercado basadas en TRD, completando así la cadena de valor financiera tokenizada.

4.1.2 Reglamento (UE) 858/2022 – Régimen Piloto de infraestructuras de mercado basadas en TRD.

El régimen piloto crea un marco regulatorio temporizado y con exenciones selectivas para probar infraestructuras de mercado que usen tecnología de registro distribuido (TRD) en la emisión, negociación y liquidación de instrumentos financieros tokenizados.

El objetivo es probar en condiciones reales cómo la TRD puede reducir fricciones (conciliaciones, tiempos de liquidación) sin comprometer la protección del inversor ni la estabilidad financiera (Reglamento (UE) 2022/858).

Su artículo 1 delimita las materias cubiertas: autorización, exención, supervisión y cooperación entre entidades TRD, autoridades nacionales y ESMA.

El artículo 2 define en tres “bloques” la tipología de las infraestructuras de TRD habilitadas de acuerdo al Régimen Piloto.

Tabla 10: Infraestructuras habilitadas en Régimen Piloto

Tipo	Equivalente tradicional	Función
SMN basado en TRD	MTF (MiFID II)	Negociación multilateral
SL basado en TRD	SSS (CSDR)	Liquidación / custodia
SNL basado en TRD	Fusión MTF-SSS	Negociación + liquidación en una sola entidad

Fuente: Reglamento (UE) 2022/858

Admite acciones, bonos y participaciones de IIC bajo ciertos umbrales y restricciones (no cubre derivados complejos). La autoridad nacional puede eximir temporalmente de obligaciones de MiFID II/CSDR cuando la propia TRD cubre el riesgo (p. ej., registro y final de liquidación on-chain), pero el solicitante debe aportar un plan de riesgos, políticas de gobernanza y continuidad y un mecanismo de protección del cliente (p. ej., procedimientos ante fallos del smart contract). ESMA coordina y evalúa el piloto.

El reglamento del Régimen Piloto establece una serie de requisitos de gobernanza y control:

- Plan de negocio y normas TRD detallados ex-ante (art. 6).
- Sistemas de IT y ciberseguridad “específicos y sólidos” orientados a continuidad, integridad y fiabilidad de los contratos inteligentes (considerando 41).
- Custodia y segregación de activos on-chain, prohibición de uso propio salvo mandato expreso (considerando 42).
- Estrategia de salida y reversión a infraestructuras tradicionales (considerando 43).
- Informes anuales de ESMA y posibilidad de revocación inmediata ante fallos operativos o riesgos sistémicos (arts. 13-15 y ital 49-50)

Atendiendo a los requerimientos del PGC, para el emisor, la tokenización no cambia la naturaleza del instrumento: NRV 9.^a (instrumentos financieros) en PGC. La medición seguirá siendo coste o valor razonable, según el caso, y la Memoria debe describir la infraestructura utilizada, el proceso de liquidación y los riesgos operativos asociados (nota de instrumentos financieros y, si es significativo, nota de riesgos). Para el inversor tenedor, la contabilización del título no difiere por estar en TRD; sí puede mejorar la evidencia de existencia y titularidad.

Desde el punto de vista del revisor de la información financiera, de acuerdo a las NIA-ES, cabría aplicar las siguientes pruebas e indagaciones:

- NIA-ES 315 R (2024): mapa de procesos on/off-chain, gobierno de la plataforma (permissionada o pública), custodia (propia/tercero), y riesgos de integridad del registro.
- NIA-ES 500 (2024) y NIA-ES 505 (2024): pruebas sustantivas combinando confirmaciones externas (depositario, custodio, registrar) con verificación “on-chain” (hash, bloque, timestamp, liquidación).
- NIA-ES 402 (2024): si la infraestructura (o custodio) es un tercero de servicios, evaluar su entorno de control (certificaciones, SLAs...).
- NIA-ES 701 (2024): si el uso de TRD fue especialmente significativo (p. ej., liquidación T+0 sin cámara central), podría describirse como CCA, explicando el enfoque de auditoría.

El régimen piloto traslada a la práctica la tokenización de instrumentos financieros y obliga a contables y auditores a dominar:

- Análisis de smart contracts y pruebas de integridad de nodos.
- Valoración de activos TRD y revelaciones específicas (IFRS 7).
- Evaluación de salvaguardas IT y segregación según DORA & CSDR.

Tras delimitar la emisión y custodia de criptoactivos (MiCA) y la tokenización de mercados (Régimen Piloto), el binomio DORA + NIS 2 completa la cobertura regulatoria al exigir resiliencia operativa digital tanto al sector financiero como al resto de sectores críticos de la economía, garantizando así que la evidencia contable soportada por infraestructuras blockchain se mantenga disponible, íntegra y verificable incluso ante ciberincidentes de gran escala.

4.1.3 Resiliencia digital

a) Reglamento (UE) 2022/2554 – DORA (Resiliencia operativa digital)

DORA establece un marco único y directamente aplicable para que las entidades financieras (bancos, gestoras, sociedades de valores, etc.) gestionen el riesgo TIC de extremo a extremo: gobernanza, inventario de activos TIC, gestión de incidentes, resiliencia operativa (incluidas pruebas avanzadas como TLPT en entidades significativas), y gestión del riesgo de terceros (proveedores TIC críticos sujetos a supervisión europea). Es aplicable desde enero de 2025 y enlaza con lo expuesto en el punto 3.2.5, sobre riesgos clave en soluciones on-chain (nodos, HSM, oráculos, bridges).

Los requisitos clave recogidos en DORA son: la necesidad de un marco de gestión de riesgo TIC documentado y revisado anualmente (art. 6); notificación inicial, intermedia y final de incidentes graves a la autoridad competente vía plantilla común (art. 19); pruebas avanzadas de resiliencia (TLPT) para entidades significativas; y supervisión de proveedores TIC críticos (registro y derecho de auditoría).

En cuanto a la información financiera, DORA mejora de la fiabilidad de los sistemas que generan evidencia. Si la empresa usa TRD en procesos contables/financieros, los nodos, wallets, HSM y oráculos deben figurar en el inventario TIC, con controles y continuidad acordes a DORA/NIS2.

Para los auditores se presentan una serie de implicaciones, que podrían resumirse en la siguiente tabla:

Tabla 11: Implicaciones de la aplicación de DORA al trabajo del auditor

Ámbito	Riesgo / obligación	Respuesta del auditor
Controles generales TI	Marco DORA obligatorio	Evaluar diseño y eficacia; riesgo significativo si falta segregación de accesos.
Incidentes	Ventana de 24 h para notificación inicial	Comprobar cumplimiento; revisar acciones correctivas y ajustes contables por hechos posteriores.
Dependencia de terceros	Supervisión de cloud & core-banking	Test de cláusulas DORA en contratos y derechos de acceso para IT-audit.

Pruebas TLPT	Resultados confidenciales	Verificar corrección de acciones de remediación, posible impacto en provisiones.
--------------	---------------------------	--

Fuente: Reglamento (UE) 2022/2554 (DORA)

Aunque DORA actúa como *lex specialis* para las entidades financieras, la Directiva NIS 2 (en España, Ley SRI 2) mantiene su vigencia como norma de referencia horizontal. El artículo 2.3 de DORA aclara que, cuando una organización esté sujeta simultáneamente a ambos marcos, el cumplimiento de DORA se considera equivalente a las obligaciones de gestión de riesgos e incidentes de NIS 2. No obstante, DORA establece en su artículo 50 la obligación de las autoridades financieras de cooperar activamente con los CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática, por sus siglas en inglés *Computer Security Incident Response Team*) nacionales, lo que se traduce en una doble capa de reporte y coordinación.

Para los grupos empresariales con filiales no financieras, esto implica diseñar un sistema integrado donde las entidades reguladas por DORA lideren las mejores prácticas de resiliencia, mientras las compañías cubiertas solo por NIS 2 adoptan controles alineados, garantizando evidencias homogéneas para la consolidación contable y la auditoría.

b) Directiva (UE) 2022/2555 – NIS 2 (Ciberseguridad esencial)

La NIS 2 deroga la NIS 1 y fija un nivel mínimo común de ciberseguridad para entidades de sectores “esenciales” e “importantes” (energía, transporte, salud, etc.), ampliando la cobertura sectorial y armonizando las obligaciones de gestión de riesgo y notificación de incidentes.

Los requisitos clave que establece la NIS 2 son:

- Medidas de gestión de riesgos (art. 21): políticas de seguridad y análisis; gestión de incidentes; continuidad de las actividades; seguridad en la cadena de suministro; prácticas de ciberhigiene y formación en ciberseguridad; políticas y procedimientos de uso de criptografía; seguridad de los recursos humanos; y uso de soluciones de autenticación.
- Notificación de incidentes significativos a CSIRT nacionales (plazos 24 h / 72 h).

- Certificación por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) para TIC críticas (art. 21 bis).

Para entidades financieras, DORA actúa como *lex specialis*; sin embargo, DORA exige cooperación y flujo de información con los CSIRT y autoridades NIS 2.

En cuanto a la información a revelar en los estados financieros, para grupos con filiales fuera del perímetro DORA (p. ej. logística, energía interna), NIS 2 impone controles que aseguran integridad de datos operativos usados en consolidación.

El coste de cumplimiento (certificaciones, seguros ciber) debe revelarse en los estados financieros y, si es material, provisionarse.

Para el equipo auditor, partiendo de las NIA-ES 315 R (2024) y NIA-ES 330 (2024): aunque DORA/NIS2 no formen parte del marco de información financiera, su documentación alimenta la evaluación de controles generales de TI (ITGC) y ayuda a diseñar pruebas sobre integridad y disponibilidad de la evidencia on-chain.

En lo que respecta a la NIA-ES 705 (2024), si se detectan deficiencias significativas (p. ej., sin segregación de funciones en firmas multifactoriales), podrían elevar el riesgo significativo y, en casos extremos, derivar en salvedad por alcance.

Tras asegurar la resiliencia en IT, que está vertebrada por DORA y NIS 2, el marco europeo hace foco en la calidad, comparabilidad y portabilidad de la información. El reglamento CSRD (Directiva de Informes de Sostenibilidad Corporativa, por sus siglas en inglés *Corporate Sustainability Reporting Directive*), junto con los ESRS (Estándares Europeos de Información sobre Sostenibilidad, por sus siglas en inglés *European Sustainability Reporting Standards*) consolidan la transparencia sobre ESG (Medio ambiente, Social y Gobernanza, por sus siglas en inglés *Environmental, Social, and Governance*) en los estados financieros. Por otro lado, el reglamento Data Act establece reglas para el acceso y uso de datos industriales. Estas normas redefinen los sistemas fuente que nutren la contabilidad y, por extensión, el alcance de la auditoría

4.1.4 Calidad y portabilidad de la información

a) Directiva (UE) 2022/2464 – CSRD

La CSRD sustituye la NFRD (Directiva de Información No Financiera por sus siglas en inglés, *Non-Financial Reporting Directive*) y extiende la obligación de reporting de

sostenibilidad (ESRS) a: grandes empresas UE/tercer país, grupos y pymes cotizadas no micro.

Esta norma se integra en la Directiva 2013/34 (arts. 19 bis y 29 bis), incluyendo el informe de sostenibilidad dentro del informe de gestión, y añadiendo la verificación limitada obligatoria a partir de 2028 (art.26 bis).

La Directiva (UE) 2025/794 aplaza la entrada en vigor para algunos grupos:

- a) Entidades de Interés Público de más de 500 empleados: ejercicios 2024 (informes 2025)
- b) Resto grandes empresas: desde 2027
- c) PYMEs cotizadas: desde 2028
- d) Grupos terceros con volumen de negocios de más de 150 M€ en la Unión Europea: desde 2028

Normas ESRS

El Reglamento Delegado (UE) 2023/2772 es la “pieza operativa” de la CSRD: transforma el mandato genérico de transparencia ESG en un catálogo normativo de datos verificables.

A partir de los ejercicios iniciados el 1-enero-2024, las entidades obligadas deberán preparar su información de sostenibilidad siguiendo las Normas Europeas de Información sobre Sostenibilidad (ESRS), que fijan principios, métricas e indicadores comparables para toda la Unión. Este bloque inicial -doce normas en total- incorpora los conceptos de doble materialidad, cadena de valor y diligencia debida, y sienta las bases para que contables y auditores integren los datos ESG en el cierre financiero con la misma disciplina que la información financiera tradicional.

En lo referente al informe de sostenibilidad (art. 19 bis y 29 bis de la Directiva (UE) 2022/2464), se debe informar:

- ESRS E1 (clima): si la entidad utiliza redes públicas o privadas con consumo energético apreciable, debe estimar y revelar la huella (normalmente Alcance 3). El paso PoW→PoS en Ethereum reduce >99 % el consumo estimado, lo que facilita justificar materialidad y mitigación (véase 3.2.3).
- ESRS G1 (gobernanza) / SST (seguridad de la información): descripciones de controles y políticas sobre sistemas digitales relevantes para la preparación de la información (incluida TRD).

Por otro lado, se debería analizarse si se deben reclasificar los gastos de transición climática y las provisiones medioambientales, con el objetivo de conciliar la información financiera con los requerimientos sobre sostenibilidad.

En este sentido, el trabajo del auditor deberá basarse en lo recogido en las NIA-ES 315 R y NIA-ES 330 (2024), documentando los controles integrados IT-ESG, para obtener evidencia suficiente y adecuada, y riesgo de “*green-washing*” si los procesos de recopilación ESG no son robustos.

En lo que respecta a las NIA-ES 500, NIA-ES 530, NIA-ES 540 Y NIA-ES 620 (2024) se propone ampliar el alcance de las pruebas sobre la cadena de valor (datos scope 3, proveedores), con implicaciones sobre el muestreo. Por otro lado, la validación de procesos de estimación (por ejemplo, cálculo de emisiones alcance 3) que podrían requerir el uso de expertos del auditor.

Finalmente, atendiendo a la NIA-ES 720-R (2024), el auditor debe leer esta “otra información” y evaluar su coherencia con los EEEF; si el asunto fue significativo en la auditoría, puede describirse como CCA (NIA-ES 701, 2024)

La Directiva (UE) 2022/2464 establece en su art.26-bis que mientras no se haya establecido una norma de verificación, los estados miembros podrán aplicar otros procedimientos de verificación recogidos en la normativa nacional. Situación que podría requerir el diseño de procedimientos específicos en base a las Normas Europeas de Información de la Sostenibilidad, NEIS (E ‘Medioambiente’, S ‘Social’, G ‘Gobernanza’).

b) Reglamento (UE) 2023/2854 (“Data Act”)

Establece normas armonizadas para el acceso justo, la portabilidad y el uso de los datos generados por productos conectados y servicios asociados. Su lógica es doble: (i) impulsar la innovación habilitando nuevos modelos de negocio basados en datos industriales y (ii) eliminar los “cuellos de botella” contractuales y técnicos que hoy encarecen el intercambio y el cambio de proveedor *cloud*. Requisitos esenciales para el funcionamiento de los *smart contracts* usados para compartir datos (art.30 del Reglamento 2023/2854), al garantizar el control de acceso, la protección frente a reactivaciones no deseadas, el registro de operaciones, establecer un mecanismo de terminación segura y resistencia a errores.

En el contexto de la CSRD y las ESRS, el Data Act suministra la canalización legal y técnica que garantiza que los datos operativos (IoT, cadena de suministro, energía, etc.) fluyan

en formatos interoperables hasta los sistemas contables y los informes de sostenibilidad, reforzando la trazabilidad y la verificabilidad que contables y auditores necesitan para emitir una opinión con fundamento.

Esto tiene su implicación en la información a revelar en las cuentas anuales. Si la entidad emplea smart contracts para intercambiar datos (p. ej., entre filiales o con proveedores), esos contratos deben cumplir con el art. 30; y los riesgos operativos (interrupción, pérdida o exposición indebida de datos) se describirán en la Memoria.

También se debe revisar y explicar en la Memoria la política de capitalización de intangibles: licencias de datos, derechos de explotación y activos generados internamente.

El auditor debe evaluar el diseño de los controles de los smart contracts (terminación/cambio), el riesgo del tercero si el servicio es externalizado, y/o recurrir a expertos cuando haga falta para revisar el código o la configuración. Se deben implementar pruebas sobre portabilidad *cloud* y salida (“*switching*”) dentro del entorno de TI (NIA-ES 315 R, NIA-ES 402 y NIA-ES 620, 2024).

De acuerdo a la NIA-ES 330 (2024), se debe testar la integridad y el origen de los datasets empleados para las métricas ESRS (trazabilidad, locks cloud).

La revisión contractual de cláusulas FRAND (Justo, Razonable y No Discriminatorio, por sus siglas en inglés *Fair, Reasonable, And Non-Discriminatory*) y provisiones por litigios derivados de uso indebido de datos, debe encuadrarse dentro de los requerimientos de la NIA-ES 540 (2024).

El tándem CSRD-ESRS fija qué métricas deben revelarse y verificarse; el Data Act garantiza cómo se obtienen y comparten los datos subyacentes. Su implementación coordinada eleva la calidad de la información financiera y de sostenibilidad y redefine el alcance del auditor.

Todos estos reglamentos europeos se desarrollan en España mediante la Ley 6/2023 y las circulares CNMV/BdE que se analizan en 4.2.

4.2.España

En España, la normativa contable y de auditoría recae en el Instituto de Contabilidad y Auditoría de Cuentas (ICAC). Según su página de competencias, la Subdirección General de Normalización y Técnica Contable (SGNTC):

- «prepara proyectos legislativos y reglamentarios en materia contable»,

- «analiza y aprueba resoluciones que complementan el Plan General de Contabilidad», y
- «resuelve consultas vinculantes sobre la correcta interpretación de la normativa contable»

La SGNTC también emite informes sobre nuevas normas que afectan a la materia contable y coopera con el EFRAG y el IASB.

En el ámbito de la auditoría, la Subdirección General de Normas Técnicas de Auditoría se ocupa de elaborar y aprobar las Normas Técnicas y de Gestión de Calidad que adaptan al entorno español las NIAs y, desde 2023, las NIGC-ES. Estas recogen la exigencia de que los auditores:

- integren los controles de tecnología de la información (nodos, oráculos, claves) en la evaluación del riesgo (NIA-ES 315 R, 2024), y
- mantengan un sistema de gestión de calidad capaz de obtener evidencia continua cuando la empresa utiliza registros DLT (NIGC 1-ES).

Con estas competencias, el ICAC norma, interpreta y supervisa la contabilidad y la auditoría españolas. La adopción de blockchain deberá, por tanto, alinearse:

- con sus consultas BOICAC (única referencia específica: Consulta 4/BOICAC 120, dic-2019), y
- con las NIGC-ES y NIAs revisadas, que exigen incorporar los controles de TI -nodos, oráculos, claves- a la evaluación de riesgos (NIA-ES 315 R, 2024) y al sistema interno de calidad (NIGC 1-ES).

En paralelo, la Ley 11/2018 sobre información no financiera convive con el calendario de CSRD-ESRS, de modo que, durante el escalado de aplicación, algunas entidades continuarán reportando bajo 11/2018 mientras otras ya lo harán conforme a ESRS. Para el auditor financiero, esto se traduce en evidencia combinada (confirmaciones + verificación on-chain), revisión de controles TI (NIA-ES 315 R, 2024) y lectura de la otra información (NIA-ES 720, 2024) cuando se divulgue sostenibilidad.

Desde 2018, España ha impulsado la experimentación supervisada con tecnologías financieras a través de un sandbox (Ley 7/2020). Sobre ese terreno, la Ley 6/2023, de los Mercados de Valores y de los Servicios de Inversión, ha “aterrizado” los desarrollos europeos en materia de criptoactivos e infraestructuras de mercado basadas en TRD, definiendo un marco operativo con implicaciones directas para empresas y auditores.

El registro y la supervisión de criptoactivos se articulan conforme a MiCA. La CNMV es la autoridad competente para los proveedores de servicios de criptoactivos (CASP) y para determinados emisores -en especial, cuando se trate de *tokens* referenciados a activos (ART)-, mientras que el Banco de España asume competencias prudenciales cuando el instrumento es dinero electrónico (*E-Money Token* - EMT). La Circular 1/2024 de la CNMV (publicada en el BOE el 15-ene-2025) concreta el procedimiento de registro, las salvaguardas sobre activos de clientes y el régimen transitorio previsto por MiCA (art. 143.3), que permite a los CASP ya operativos seguir prestando servicios hasta 18 meses desde el 30-dic-2024 (esto es, hasta el 30-jun-2026), condicionado al cumplimiento de requisitos mínimos y a su regularización dentro del plazo. Para las compañías usuarias, este marco implica mayor trazabilidad regulatoria (libros blancos, gobierno, reservas) y, para el auditor, mejores fuentes de evidencia combinando confirmaciones externas de custodios con verificación independiente “on-chain” (NIA-ES 500 y NIA-ES 505, 2024), así como la evaluación de controles TI relevantes (NIA-ES 315 R, 2024).

En segundo término, la resiliencia operativa y el ciber-riesgo ganan protagonismo. El Reglamento DORA (UE 2022/2554), aplicable desde enero de 2025, exige a las entidades financieras una gestión integral del riesgo TIC (gobernanza, inventario de activos, gestión de incidentes, pruebas de resiliencia y control de terceros críticos). En paralelo, la Directiva NIS 2 (UE 2022/2555) extiende obligaciones de ciberseguridad a sectores “esenciales” e “importantes”. Cuando una compañía incorpora nodos, wallets/HSM, oráculos o bridges a procesos contables o de liquidación, esos activos deben figurar en su mapa de riesgos TIC y someterse a controles y continuidad acordes a DORA/NIS 2. Para el auditor, la documentación generada por estos marcos alimenta la identificación y valoración del riesgo (NIA-ES 315 R, 2024) y sustenta el diseño de pruebas sobre integridad y disponibilidad de la evidencia on-chain. Deficiencias significativas en los Controles Generales de TI – ITGC, por sus siglas en inglés *Information Technology General Controls* - pueden elevar el riesgo significativo y, en casos extremos, derivar en salvedades por limitación al alcance (NIA-ES 705, 2024).

Por último, en criterios contables y auditoría financiera, el PGC (RD 1514/2007) y el PGC-Pyme (RD 1515/2007) no contienen aún una norma específica para criptoactivos. El ICAC ha resuelto cuestiones mediante consultas BOICAC, destacando la Consulta 4/BOICAC 120 (dic-2019), y la práctica se apoya en la analogía con las NRV 5.^a (intangibles),

9.^a (instrumentos financieros) y 10.^a (existencias), según la naturaleza económica y la finalidad. En la Memoria conviene describir la política contable aplicada, la metodología de valor razonable (si procede) y los riesgos (volatilidad, custodia de claves, dependencia de terceros). El auditor, por su parte, deberá combinar procedimientos sustantivos (confirmaciones, verificación on-chain, conciliaciones de “triple partida” cuando existan recibos compartidos) con la evaluación de controles (NIA-ES 315 R, NIA-ES 402, NIA-ES 500, NIA-ES 505 y NIA-ES 701, 2024).

En materia de sostenibilidad, durante el escalado de la CSRD y los ESRS (con las nuevas fechas fijadas por la Directiva (UE) 2025/794), seguirán conviviendo con la Ley 11/2018 para quienes aún no estén dentro del perímetro CSRD. Cuando el uso de TRD tenga impacto climático (p. ej., redes públicas de alto consumo o, a la inversa, la migración a PoS), la entidad deberá estimar y revelar las métricas pertinentes (normalmente Alcance 3 en ESRS E1). El auditor financiero no emitirá una opinión sobre el informe de sostenibilidad salvo encargo específico, pero debe leer y evaluar su coherencia con los estados financieros (NIA-ES 720, 2024) y, si la consideración de riesgos TRD fue especialmente significativa, puede comunicarla como CCA (NIA-ES 701, 2024).

4.2.1 Plan General de Contabilidad (PGC) y criterios ICAC

El PGC (RD 1514/2007) y el PGC-Pyme (RD 1515/2007) no contienen aún un tratamiento explícito de criptoactivos. En consecuencia, las entidades aplican el principio de analogía y las consultas del ICAC para clasificar y medir los saldos vinculados a DLT:

El principio rector es fondo sobre forma: la finalidad y la naturaleza económica del activo determinan su clasificación:

- Uso propio (p. ej., tenencia de criptoactivos para su empleo en la operativa de la entidad): NRV 5.^a (Inmovilizado intangible). Medición inicial al coste; no se amortiza si no hay vida útil definida; test de deterioro cuando existan indicios.
- Negociación o venta (p. ej., inventario en un intermediario): NRV 10.^a (Existencias). Medición al menor entre coste y valor neto realizable.
- Naturaleza financiera (p. ej., security tokens que otorgan derechos de crédito o de participación): NRV 9.^a (Instrumentos financieros). Medición posterior según corresponda (coste amortizado o valor razonable con cambios en PyG o patrimonio).

4.2.2 Ley 6/2023 y normativa CNMV-Banco de España.

La Ley 6/2023, de los Mercados de Valores y de los Servicios de Inversión, integra en el ordenamiento español los desarrollos europeos relativos a criptoactivos e infraestructuras de mercado basadas en TRD: MiCA para criptoactivos y el Régimen Piloto TRD para infraestructuras de mercado tokenizadas.

En referencia a MiCA (Reglamento (UE) 2023/1114), la CNMV actúa como autoridad competente para el registro y supervisión de los proveedores de servicios de criptoactivos (CASP) y de emisores, en su caso -en particular, de *tokens* referenciados a activos (ART)-, mientras que el Banco de España asume competencias prudenciales en relación con los *tokens* de dinero electrónico (EMT) y los sujetos bajo su perímetro. La Circular 1/2024 de la CNMV (publicada en el BOE el 15 de enero de 2025) desarrolla el procedimiento de alta, las salvaguardas sobre activos de clientes, las obligaciones de gobierno y reporting y el régimen transitorio previsto en el artículo 143.3 de MiCA, que permite a los CASP ya operativos continuar la prestación de servicios hasta 18 meses desde el 30 de diciembre de 2024 - esto es, hasta el 30 de junio de 2026 -, condicionado al cumplimiento de requisitos mínimos y a su regularización dentro del plazo.

Por lo que respecta a la tokenización de instrumentos financieros y a la utilización de TRD en negociación y/o liquidación, el Régimen Piloto TRD (Reglamento (UE) 2022/858) habilita, bajo exenciones controladas, la operativa de sistemas multilaterales de negociación, sistemas de liquidación y plataformas combinadas on-chain, con exigencias de planes de riesgos, gobernanza, protección del cliente y coordinación con la ESMA y las autoridades nacionales. El propósito es verificar en condiciones reales las potenciales ganancias de eficiencia -reducción de conciliaciones y tiempos de liquidación- sin comprometer la protección del inversor ni la estabilidad del sistema.

Todo esto redundará en mayor trazabilidad regulatoria (libros blancos, reservas, gobierno), salvaguardas en la custodia segregada de criptoactivos de clientes, y posibilidad de operar valores tokenizados en plataformas piloto.

En auditoría, su impacto se verá reflejado en las NIA-ES 500 Y NIA.ES 505 (2024) con la mejora en la calidad de las fuentes de evidencia (confirmaciones de custodios y verificación on-chain); en las NIA-ES 315 R (2024) para la evaluación de los controles TI (ITGC, segregación de funciones, gestión de incidencias); y en las NIA-ES 701 y NIA-ES 705 (2024), si el uso de TRD es relevante, se podría incluir como CCA; en caso de falta de

evidencia suficiente y adecuada, se debería estudiar la posibilidad de emitir una opinión modificada por una limitación.

Al amparo de DORA (UE 2022/2554) y NIS 2 (UE 2022/2555) las empresas generan documentación (inventario TIC, incidentes, pruebas de resiliencia) que alimenta la evidencia requerida por la NIA-ES 315 R (2024) cuando la entidad usa nodos, wallets/HSM, oráculos o bridges en procesos financieros.

4.2.3 Información sobre sostenibilidad.

En materia de sostenibilidad, en España conviven actualmente dos marcos normativos. La Ley 11/2018 sobre información no financiera y diversidad, es de aplicación a las entidades que todavía no están dentro del perímetro de la CSRD (Directiva 2022/2464), mientras que el calendario de esta última - ajustado por la Directiva (UE) 2025/794 - establece la aplicación progresiva de los ESRS (Reglamento Delegado 2023/2772). En la práctica, esto supone que hasta 2027-2028 coexistirán informes preparados bajo la Ley 11/2018 e informes alineados con los estándares europeos. El ICAC, conforme a su Plan Estratégico 2024-2026, asume un papel creciente en la supervisión de esta información, en coordinación con la EFRAG.

En la actualidad, la NIA-ES 720 - R (2024), expone la obligación del auditor a evaluar la coherencia de la información de sostenibilidad incluida en el informe de gestión con los estados financieros auditados. Además, si el impacto de la tecnología blockchain sobre indicadores ESG es relevante —por ejemplo, en relación con el consumo energético de las redes empleadas o con la trazabilidad de cadenas de suministro—, podría darse la relevancia suficiente para su inclusión como CCA (NIA-ES 701, 2024).

Esta interrelación refuerza la necesidad de que el auditor comprenda no solo los aspectos financieros, sino también las consecuencias medioambientales y sociales del uso de infraestructuras DLT.

5. Metodología.

La metodología adoptada se articula en torno a un diseño mixto que combina análisis documental, de carácter normativo y técnico, y por otro, un estudio empírico sobre informes de auditoría de cuentas anuales (CCAA) para contrastar hipótesis mediante χ^2 y ANOVA. Este enfoque permite contrastar las hipótesis planteadas con una base normativa sólida y evidencia empírica obtenida en el contexto español.

5.1. Diseño de la investigación.

El estudio consta de dos fases complementarias:

a) Revisión bibliográfica y normativa.

Se ha llevado a cabo un análisis sistemático de literatura académica (artículos en Scopus y Google Académico), informes profesionales (Deloitte, PwC, KPMG, Consensus, EFRAG, ESMA) y normativa aplicable en España y la Unión Europea (PGC, consultas BOICAC, NIA-ES, MiCA, DORA, CSRD/ESRS). El objetivo de esta fase es construir el marco teórico y normativo que fundamenta las hipótesis y delimitar las implicaciones para la información financiera y de auditoría de la adopción de blockchain.

b) Análisis estadístico de informes de auditoría y cuentas anuales.

Estos informes, elaborados conforme a la Ley 22/2015 de Auditoría de Cuentas y a las NIA-ES vigentes, y las cuentas anuales a las que estos se refieren, ofrecen indicadores verificables sobre la calidad de la información financiera y sobre la valoración del riesgo efectuada por los auditores. La elección del periodo temporal (2021 – 2023, y 2024 en su caso) se justifica porque coincide con el inicio de la aplicación de marcos normativos europeos relevantes —MiCA, DORA, CSRD/ESRS— y con la consolidación de proyectos empresariales de digitalización contable, lo que incrementa la probabilidad de identificar referencias al uso de tecnologías DLT.

La operabilidad de las hipótesis de investigación se articula en torno a tres relaciones: primero a la proporción de opiniones modificadas y su posible asociación con la adopción de soluciones blockchain, segundo a la comparación de medias en la valoración del riesgo inherente y de control cuando la evidencia procede de registros on-chain, y tercero a las diferencias sectoriales y por tamaño empresarial (PYME frente a gran empresa) en la percepción de beneficios y barreras de implantación. Para contrastar estas relaciones se

emplearán técnicas estadísticas complementarias: prueba χ^2 de independencia en el caso de variables categóricas (opiniones de auditoría) y ANOVA de un factor y factorial 2×2 en el caso de variables métricas (valoraciones de riesgo y diferencias de grupos).

Este diseño metodológico asegura la conexión entre el marco teórico desarrollado en los capítulos anteriores y la evidencia empírica derivada del análisis de informes de auditoría, garantizando la replicabilidad de los resultados y la coherencia con los objetivos generales y específicos de la investigación.

5.2. Población y muestra.

La población objeto de este estudio está constituida por los informes de auditoría de cuentas anuales de entidades españolas sometidas a auditoría obligatoria, conforme a lo dispuesto en la Ley 22/2015, de Auditoría de Cuentas. Se incluyen aquellas entidades que aplican el Plan General de Contabilidad (PGC, RD 1514/2007) o el PGC-Pymes (RD 1515/2007) y cuyas auditorías se han realizado bajo las Normas Internacionales de Auditoría adaptadas para España (NIA-ES).

El horizonte temporal de análisis comprende los ejercicios 2021–2023 (y 2024 en su caso), lo que asegura la disponibilidad de cuentas anuales ya depositadas en los Registros Mercantiles. Este periodo resulta especialmente adecuado, pues abarca la aplicación inicial de marcos normativos europeos de gran relevancia —MiCA, DORA y CSRD/ESRS—, así como la consolidación de proyectos empresariales de digitalización contable que potencialmente incorporan registros en blockchain.

La fuente primaria de datos será cuentas anuales e informes de auditoría depositados y accesibles públicamente, lo que garantiza su carácter verificable y libre de sesgos.

La muestra prevista estará integrada por un mínimo de 30 a 40 informes, distribuidos entre empresas que han evidenciado proyectos vinculados a tecnologías DLT/blockchain y un grupo de control formado por entidades que no han divulgado iniciativas de este tipo. Se incluirán tanto pymes como grandes empresas, lo que permitirá contrastar la hipótesis relativa a diferencias de tamaño. El criterio de inclusión será la disponibilidad pública del informe íntegro; se excluirán cuentas anuales abreviadas, auditorías voluntarias y entidades en liquidación.

Este diseño muestral ofrece una base empírica suficiente para aplicar análisis descriptivos y comparativos mediante pruebas χ^2 y ANOVA, aportando resultados exploratorios relevantes para el contexto español.

La muestra específica de este estudio la componen las CCAA e informes de auditoría de las siguientes entidades (y grupos) para los ejercicios 2021, 2022 y 2023 (y 2024 si estuviese ya disponible a la fecha de corte):

- Banco Santander
- Binance
- Bit2Me
- Cecabank
- CIE Automotive
- Correos
- Iberdrola
- Mercadona
- Telefónica
- BME Clearing
- FacePhi
- LleidaNET
- República Gráfica
- Soluciones 480
- Tendam Retail
- Irritec Ibérica
- Gestamp
- Repsol

La unidad de análisis es “cuentas anuales e informe de auditoría por ejercicio”.

Se incluyen CCAA individuales o consolidadas con informe de auditoría depositado, de las entidades del listado anterior. Han quedado excluidas entidades con auditorías voluntarias, cuentas anuales abreviadas sin informe completo, entidades en liquidación o pilotos sin impacto real en las CCAA.

5.3. Instrumentos y técnicas de análisis.

El análisis empírico se ha sustentado en un libro de extracción en formato hoja de cálculo, complementada con un catálogo de variables y un diccionario de codificación, que aseguran la trazabilidad desde las fuentes hacia las variables analíticas empleadas, y en un conjunto de técnicas estadísticas descriptivas e inferenciales alineadas con los objetivos del trabajo.

- Libro de extracción.

El libro cuenta con cuatro hojas: “Catalogo_variables”, “Diccionario_codigos”, “Hoja_extraccion” y “Matriz_CCA”.

El “Catalogo_variables” define para cada variable su tipo, valores, descripción operativa y fuente; el “Diccionario_codigos” consolida las reglas de codificación y valores permitidos; la “Hoja_extraccion” contiene los registros a nivel entidad–año con campos de identificación (Entidad, NIF, Ejercicio) y variables explicativas y dependientes; la “Matriz_CCA” recoge las citas de cuestiones clave de auditoría (CCA) por entidad–año, su categoría contable y una marca específica cuando el CCA incluye referencias a TI, conciliaciones y/o DLT.

Tanto la hoja “Catalogo_variables”, la hoja “Diccionario_codigos” y la hoja “Matriz_CCA” están disponibles en los anexos, como Anexo 1, Anexo 2 y Anexo 3, respectivamente.

En términos operativos, las variables clave empleadas han sido:

- a) indicadores de contexto (C1_Cotizada, C2_Big4, C3_Consolidacion, Sector, I2_Tamano),
- b) variables de adopción tecnológica (I1_Adopcion_onchain),
- c) resultados de auditoría (D1_Tipo_opinion, D1_Opinion_modificada).

A partir de la “Matriz_CCA” se han construido dos métricas de interés a nivel entidad–año: el recuento de CCA totales (cca_total) y el recuento de CCA relacionados con TI/conciliaciones/DLT (cca_ti_dlt). Estas variables permiten contrastar la relación entre adopción on-chain y el énfasis del auditor en controles de TI/DLT.

- Técnicas de análisis.

El estudio analítico ha combinado estadística descriptiva, contrastes no paramétricos de independencia y análisis de varianza (ANOVA) para comparar medias de conteos entre grupos, complementado con modelos de conteo como verificación de robustez.

- a. Estadística descriptiva.

Se han elaborado tablas de frecuencias absolutas y relativas para las variables binarias y categóricas (p. ej., I1_Adopcion_onchain, D1_Opinion_modificada, D2_Presencia_CCA_TI_DLT, C2_Big4, C1_Cotizada, I2_Tamano) y resúmenes de tendencia central y dispersión para los recuentos (cca_total, cca_ti_dlt). Estas tablas proporcionan una visión preliminar de la muestra y sirven para identificar posibles desequilibrios muestrales.

b. Chi-cuadrado de independencia (χ^2).

Se han aplicado contrastes χ^2 para evaluar la asociación entre:

1. adopción on-chain (I1_Adopcion_onchain) y opinión modificada (D1_Opinion_modificada),
2. adopción on-chain y presencia de CCA TI/DLT (D2_Presencia_CCA_TI_DLT),
3. pertenencia a Big Four (C2_Big4) y presencia de CCA TI/DLT,
4. cotización (C1_Cotizada) y opinión modificada.

Los resultados incluyen estadístico χ^2 , grados de libertad y valor p.

c. ANOVA de un factor.

Se ha empleado ANOVA para contrastar diferencias en los recuentos medios de CCA entre grupos, en particular:

1. cca_total frente a I1_Adopcion_onchain,
2. cca_ti_dlt frente a I1_Adopcion_onchain,
3. cca_total frente a C2_Big4,
4. cca_total frente a I2_Tamano.

d. Modelos de robustez.

Como análisis de robustez, se estimaron modelos multivariantes (Poisson y Quasi-Poisson) para cca_total y cca_ti_dlt, incorporando controles por pertenencia a Big4, cotización, tamaño, consolidación y sector. Las estimaciones se reportan como razones de tasas de incidencia (IRR) con intervalos de confianza al 95 %. Ante problemas de separación perfecta en cca_ti_dlt, se aplicó un ajuste Poisson regularizado (penalización L2), manteniendo la interpretación de IRR. Adicionalmente, se realizaron contrastes no paramétricos de Kruskal–Wallis para comprobar diferencias por grupos de tamaño, sector y consolidación. Los resultados confirman que, la

adopción on-chain no presenta efectos significativos sobre el número de CCA, mientras que tamaño y sector sí muestran asociación con el número de CCA.

- Supuestos y control de calidad.

Los contrastes χ^2 se han basado en la independencia de observaciones y frecuencias esperadas adecuadas. El ANOVA ha sido interpretado con cautela dado el carácter discreto de la variable dependiente; los modelos de conteo se han utilizado como verificación de robustez. La calidad de datos se ha controlado mediante revisión de valores conforme al “Diccionario_codigos” y conciliación de recuentos con la “Matriz_CCA”.

5.4.Limitaciones del estudio.

Las inferencias deben interpretarse en el contexto del tamaño muestral y la posible dispersión de ciertos datos analizados. Dado que los recuentos de CCA son sensibles a la complejidad y tamaño de las entidades, se recomienda considerar variables de control adicionales (Sector, consolidación, cotización) en análisis multivariantes. La codificación de “TI/Conciliaciones/DLT” se sustenta en criterios operativos explícitos y revisables, lo que permite revisar la metodología del proceso de clasificación.

6. Resultados y análisis.

Este apartado sintetiza los resultados empíricos obtenidos a partir de la base de datos construida y describe su interpretación desde la perspectiva contable y de auditoría. Se contrastan las relaciones entre adopción on-chain y distintos resultados de auditoría y se analiza el énfasis en cuestiones clave de auditoría (CCA), con especial atención a CCA de TI/conciliaciones/DLT.

Los resultados principales del estudio analítico y estadístico, así como los derivados de las pruebas de robustez posteriores pueden consultarse en las siguientes tablas.

Tabla 12: Resultados de las pruebas estadísticas

Contraste/Modelo	Estadístico	gl	n	p	Tamaño de efecto
Adopción DLT vs Opinión modificada (χ^2)	$\chi^2(1) = 0,174$	1	70	0,677	V de Cramér = 0,050
Adopción DLT vs CCA TI/DLT (χ^2)	$\chi^2(1) = 0,005$	1	70	0,943	V de Cramér = 0,009
Big4 vs CCA TI/DLT (χ^2)	$\chi^2(1) = 0,003$	1	70	0,959	V de Cramér = 0,006
Cotizada vs Opinión modificada (χ^2)	$\chi^2(1) = 2,097$	1	70	0,148	V de Cramér = 0,173
CCA totales ~ Adopción DLT (ANOVA)	$F(1, 68) = 1,4266$	1, 68	70	> 0,20	$\eta^2 = 0,173$
CCA TI/DLT ~ Adopción DLT (ANOVA)	$F(1, 68) = 2,191$	1, 68	70	0,143	$\eta^2 = 0,031$
CCA totales ~ Big4 (ANOVA)	$F(1, 68) = 1,630$	1, 68	70	0,206	$\eta^2 = 0,023$
CCA totales ~ Tamaño (ANOVA)	$F(1, 68) = 8,277$	1, 68	70	0,005	$\eta^2 = 0,109$

Nota. χ^2 = chi-cuadrado; gl = grados de libertad; η^2 = eta cuadrado. Valores p con coma decimal. Umbral de significación: 0,05

Tabla 13: Resultados de las pruebas robustez

Modelo	Variable	IRR	IC95%	p
Quasi-Poisson – CCA totales	Tamaño: PYME (vs base)	0,59	[0,46; 0,77]	< 0,001
Quasi-Poisson – CCA totales	Adopción on-chain (1 vs 0)	1,23	[1,00; 1,50]	0,051
Quasi-Poisson – CCA totales	Big4 (1 vs 0)	0,80	[0,60; 1,06]	0,120
Quasi-Poisson – CCA totales	Cotizada (1 vs 0)	1,37	[1,09; 1,73]	0,006
Quasi-Poisson – CCA totales	Consolidación (1 vs 0)	1,29	[0,76; 2,19]	0,355
Poisson (reg) – CCA TI/DLT	Tamaño: PYME (vs base)	1,59	[;]	
Poisson (reg) – CCA TI/DLT	Adopción on-chain (1 vs 0)	1,32	[;]	
Poisson (reg) – CCA TI/DLT	Big4 (1 vs 0)	1,63	[;]	
Poisson (reg) – CCA TI/DLT	Cotizada (1 vs 0)	0,90	[;]	
Poisson (reg) – CCA TI/DLT	Consolidación (1 vs 0)	0,52	[;]	

Nota. Se reportan IRR de Quasi-Poisson para CCA totales y Poisson regularizado para CCA TI/. Se incluyen controles por Big4, cotización, tamaño, consolidación y efectos por sector.

Los resultados de este estudio no apoyan, en esta muestra, que la adopción on-chain por sí sola incremente las opiniones modificadas ni el peso relativo de CCA TI/DLT.

La materialidad operativa y el tamaño sí muestran relación con el número de CCA, coherente con un enfoque NIA-ES basado en riesgos.

La evaluación contable debe centrarse en la clasificación y valoración PGC de los activos y pasivos afectados, y en la revelación adecuada de riesgos tecnológicos y dependencias de terceros.

En sostenibilidad, la trazabilidad on-chain puede ser un habilitador de evidencia, con la contrapartida de nuevos riesgos de calidad de datos.

Al introducir controles por tamaño, auditada por Big4, cotización, consolidación y efectos sectoriales, la adopción on-chain no muestra un efecto estadísticamente significativo sobre el número de CCA ni sobre los CCA específicos TI/DLT. Los resultados son robustos atendiendo a análisis basados en Quasi-Poisson y Poisson regularizado, así como a contrastes no paramétricos, confirmando que la complejidad y el tamaño de la entidad constituyen los principales determinantes del énfasis de auditoría en esta muestra.

6.1. Impacto en la contabilidad financiera.

Se han examinado 70 observaciones entidad-año, no mostrando los contrastes χ^2 una asociación estadísticamente significativa entre la adopción on-chain (I1_Adopcion_onchain) y la existencia de opinión modificada (D1_Opinion_modificada) ni entre la adopción on-chain y la presencia de CCA TI/DLT (p-valores > 0,60). El ANOVA de un factor indica que el número total de CCA (cca_total) difiere de manera significativa por tamaño de la entidad (PYME vs GE; $F \approx 8,28$; $p \approx 0,005$), mientras que no se observan diferencias significativas por adopción on-chain o por pertenencia a Big4. En conjunto, la evidencia sugiere que, en esta muestra, la complejidad/escala organizativa explica mejor el número de CCA que la adopción on-chain por sí sola.

Bajo la perspectiva del Plan General de Contabilidad (PGC), el despliegue de soluciones DLT impacta en varios aspectos: reconocimiento, valoración, deterioro y presentación de activos y pasivos, así como en el registro de ingresos y conciliaciones de cuentas. En particular:

1. Criptoactivos propios no destinados a la venta inmediata suelen clasificarse como inmovilizado intangible si aportan beneficios económicos futuros y no otorgan derechos de cobro frente a terceros; la valoración típica es al coste menos deterioro, al no existir, por regla general, un derecho contractual de cobro que permita tratarlos como instrumento financiero (criterio alineado con prácticas internacionales).
2. Criptoactivos mantenidos para su venta ordinaria podrían encajar en existencias, aplicando coste y comprobación de deterioro.
3. Tokenización de activos financieros: cuando el token representa derechos contractuales de cobro o entrega de efectivo, procede aplicar normas de instrumentos financieros del PGC.

4. Conciliaciones y trazabilidad: la disponibilidad de registros inmutables on-chain facilita evidencia de integridad e integraciones auxiliares libro mayor–red; contablemente, refuerza conciliaciones bancarias/terceros y auxiliares, sin alterar por sí misma los criterios de reconocimiento.

La ausencia de asociación estadística entre adopción on-chain y modificaciones de la opinión no implica irrelevancia contable; indica que, en la muestra, los impactos se canalizan más por complejidad y controles internos que por la mera adopción tecnológica.

En términos contables, la prioridad recae en la correcta clasificación (intangible, existencias, instrumento financiero...), la valoración (coste, deterioro y, cuando proceda, valor razonable soportado por mercado activo) y la revelación en memoria sobre riesgos tecnológicos, custodia y dependencias de oráculos. Para la presentación, procede salvaguardar la consistencia con el Marco Conceptual del PGC y la imagen fiel.

6.2. Impacto en la auditoría

Los χ^2 no hallan asociación significativa entre adopción on-chain y CCA TI/DLT; el ANOVA muestra mayor volumen de CCA en entidades de mayor tamaño. Esto apunta a una respuesta del auditor proporcional a la escala del cliente, más que a la etiqueta “blockchain” per se. No obstante, se observa presencia de CCA específicamente clasificados como TI/Conciliaciones/DLT en un subconjunto relevante de casos, lo que refleja atención a riesgos tecnológicos.

- Lectura de los resultados bajo la óptica de las NIA-ES (enfoque basado en riesgos).
 - a) Identificación y valoración del riesgo: la NIA-ES 315 – R (2024) exige entender el sistema de TI, incluidos componentes on-chain, gobernanza de claves y oráculos.
 - b) Respuestas a los riesgos: la NIA-ES 330 (2024) requiere diseñar pruebas de controles y/o sustantivas que aborden integridad, existencia, derechos y valoración de transacciones on-chain.
 - c) Evidencia de auditoría: la NIA-ES 500 (2024) subraya suficiencia y adecuación; el hecho de que un dato esté on-chain no lo convierte automáticamente en evidencia fiable si intervienen oráculos o custodia de terceros (NIA-ES 402, 2024).
 - d) Estimaciones y valoración: cuando la medición implica juicios relevantes (por ejemplo, deterioro de intangibles cripto), es de aplicación la NIA-ES 540 (2024).

- e) Informes: la decisión sobre CCA y, en su caso, modificaciones de opinión se rige por las NIA-ES 700 (2025) y NIA-ES 705 (2024); los hallazgos tecnológicos pueden derivar en CCA relacionados con TI y conciliaciones, o en párrafos de énfasis si corresponde.
- f) Fraude y salvaguardas: la NIA-ES 240 (2024) es especialmente pertinente ante riesgos de apropiación de claves, transacciones no autorizadas o lavado de activos vinculado a criptoactivos; requiere procedimientos adicionales y escepticismo profesional.

En entornos con métricas ESRS, la trazabilidad on-chain puede aportar rastro de verificación para KPIs ambientales/sociales, pero introduce riesgos de calidad de datos de oráculos y continuidad operativa. En la verificación de información sobre sostenibilidad, la integridad de datos y el control interno sobre la información no financiera deben evaluarse de forma equivalente a la financiera.

6.3. Matriz de riesgos blockchain vs pruebas NIA-ES

A continuación se presenta una matriz de riesgos sobre blockchain, que incluye afirmaciones afectadas, impacto, probabilidad estimada (cualitativa), controles clave, y pruebas mapeadas a NIA-ES con naturaleza/extensión/oportunidad (N/E/O), población y evidencia esperada.

Las afirmaciones estimadas son:

- Existencia: verificación de operaciones y saldos on-chain.
- Derechos y obligaciones: titularidad de claves, contratos inteligentes y condiciones de cambio.
- Integridad: correlación de registros entre ERP y cadena.
- Exactitud: correcta cuantificación y registro contable de importes on-chain.
- Valoración: medición conforme a PGC (coste, deterioro; valor razonable si aplica).
- Presentación: clasificación y revelación adecuadas en estados financieros y memoria.

Tabla 14: Matriz de riesgos blockchain – Riesgo 1

Riesgo 1:	Pérdida/compromiso de claves privadas (apropiación de activos)	
Afirmaciones:	Existencia Derechos Obligaciones	
Impacto:	Alto	
Probabilidad:	Media	
Controles:	Custodia segregada HSM/multi-firma Políticas de rotación Conciliaciones diarias	
Pruebas NIA-ES:		
	NIA-ES 315/330	Walkthrough de circuito de custodia Test de diseño y operatividad de multi-firma
	NIA-ES 500	Obtención de evidencia externa independiente
Evidencia esperada:	Confirmaciones de terceros Logs de autorización Transacciones de prueba firmadas	
Criterios de validación:	Segregación efectiva de funciones Ausencia de anomalías en logs Conciliación sin diferencias	
Documentación:	Matrices RCM sobre riesgo en equipos TI Capturas de evidencias Guías de verificación criptográfica	

Tabla 15: Matriz de riesgos blockchain – Riesgo 2

Riesgo 2:	Oráculos y calidad de datos externos	
Afirmaciones:	Exactitud Integridad Valoración	
Impacto:	Medio-Alto	
Probabilidad:	Media	
Controles:	Proveedores recurrentes Validaciones cruzadas SLA (Service Level Agreement) Monitorización	
Pruebas NIA-ES:		
	NIA-ES 402	Entender y evaluar controles del servicio de oráculo Obtener carta del prestador del servicio
	NIA-ES 500/540:	Pruebas sustantivas de cuantías dependientes de los oráculos Sensibilidad y back-testing de datos
	Evidencia esperada:	Respuestas de proveedores Reconciliaciones con fuentes alternativas Resultados de back-testing
	Criterios de validación:	Diferencias dentro de la tolerancia establecida SLA cumplidos

Tabla 16: Matriz de riesgos blockchain – Riesgo 3

Riesgo 3: Conciliación ERP - Blockchain

Afirmaciones: Integridad | Corte de operaciones | Exactitud

Impacto: Medio -
Alto

Probabilidad: Media

Controles: Conciliaciones automáticas | Controles de interfaz | Hashes de
verificación

**Pruebas NIA-
ES:**

NIA-ES Prueba de control sobre interfaz

330

Replicación de conciliaciones sobre muestra

Trazabilidad hash - apunte

NIA-ES Muestreo de transacciones

500

Recálculo de importes

Comisiones

Tabla 17: Matriz de riesgos blockchain – Riesgo 4

Riesgo 4:	Clasificación contable inadecuada de criptoactivos	
Afirmaciones:	Presentación Valoración Derechos Obligaciones	
Impacto:	Alto	
Probabilidad:	Media-Alta	
Controles:	Políticas contables aprobadas Revisión técnica Segregación entre trading/uso propio	
Pruebas NIA-ES:		
	NIA-ES 540	Evaluación de juicios de la dirección Contraste con PGC aplicable
	NIA-ES 700/705	Implicaciones de presentación/revelación y necesidad de CCA o salvedades
	Evidencia esperada:	Política contable Papeles de clasificación Razonamientos de la dirección

Tabla 18: Matriz de riesgos blockchain – Riesgo 5

Riesgo 5:	Valoración y deterioro de intangibles cripto	
Afirmaciones:	Valoración Presentación	
Impacto:	Alto	
Probabilidad:	Media	
Controles:	Test de deterioro periódico Fuentes de precio documentadas Metodología aprobada	
Pruebas NIA-ES:		
	NIA-ES 540	Evaluación de modelos Procedimientos analíticos sustantivos

NIA-ES 500	Comprobación de precios de mercado observables Método de conversión
Evidencia esperada:	Series de precios Actas de aprobación Cálculos de deterioros
Criterios de validación:	Supuestos razonables Trazabilidad de las fuentes

Tabla 19: Matriz de riesgos blockchain – Riesgo 6

Riesgo 6: Dependencia de terceros (custodios / plataformas)

Afirmaciones: Existencia | Derechos | Integridad

Impacto: Medio-Alto

Probabilidad: Media

Controles: Evidencia de solvencia del tercero | Cláusulas de disponibilidad/seguridad | Reportes de control

Pruebas NIA-ES:

NIA-ES 402	Entender el servicio Obtener información sobre los controles del tercero Reconciliación de saldos
NIA-ES 500	Confirmaciones externas
Evidencia esperada:	Confirmaciones Informes de control Conciliaciones
Criterios de validación:	Confirmaciones sin diferencias

Controles del tercero efectivos

Tabla 20: Matriz de riesgos blockchain – Riesgo 7

Riesgo 7:	Smart contracts con lógica de negocio crítica
Afirmaciones:	Derechos y obligaciones Exactitud Integridad
Impacto:	Alto
Probabilidad:	Baja-Media
Controles:	Revisiones de código Controles de cambios Pruebas de integración
Pruebas NIA-ES:	
	NIA-ES 315/330
	Walkthrough de diseño
	Pruebas de cambios
	Replicación de casos de uso
	NIA-ES 500
	Evidencia técnica de pruebas superadas
	Expertos (NIA-ES 620)
	Evidencia esperada:
	Resultados de auditorías de código
	Actas de aprobación
	Criterios de validación:
	Ausencia de vulnerabilidades críticas
	Cobertura de pruebas suficiente

Tabla 21: Matriz de riesgos blockchain – Riesgo 8

Riesgo 8:	Cumplimiento y prevención de fraude	
Afirmaciones:	Existencia Derechos Presentación	
Impacto:	Alto	
Probabilidad:	Baja-Media	
Controles:	Know Your Customer (KYC)/Anti-Money Laundering (AML) Listas de sanciones Monitorización de direcciones	
Pruebas NIA-ES:		
	NIA-ES 240	Indagaciones ampliadas Pruebas dirigidas a riesgos de fraude
	NIA-ES 250	consideración de leyes y reglamentos aplicables
	Evidencia esperada:	Políticas AML Reportes Registro de alertas
	Criterios de validación:	Cumplimiento normativo Ausencia de alertas no justificadas

Tabla 22: Matriz de riesgos blockchain – Riesgo 9

Riesgo 9:	Continuidad operativa y ciberseguridad en nodos/infraestructura	
Afirmaciones:	Integridad Corte Exactitud	
Impacto:	Medio	
Probabilidad:	Media	
Controles:	Backups Redundancia Planes de continuidad y recuperación	
Pruebas NIA-ES:		
	NIA-ES 315/330	Evaluación de controles de TI Pruebas de continuidad

NIA-ES 570	Consideración de incertidumbres que afecten al principio de empresa en funcionamiento
Evidencia esperada:	Resultados de pruebas de recuperación, políticas y ejecuciones de backup.
Criterios de validación:	Tiempos y puntos de recuperación en umbrales aceptables Evidencias de test recientes

Tabla 23: Matriz de riesgos blockchain – Riesgo 10

Riesgo 10:	Trazabilidad de métricas de sostenibilidad soportadas on-chain
Afirmaciones:	Integridad Presentación
Impacto:	Medio
Probabilidad:	Baja-Media
Controles:	Gobernanza de datos Validación de fuentes Segregación de funciones no financieras

Verificación sobre información no financiera:

Enfoque análogo a NIA-ES 315/330/500 aplicado a KPIs ESRS (si procede)

Pruebas sobre cadena de custodia de datos y oráculos

Evidencia esperada:	Diccionario de datos ESG Rastros on-chain Reconciliación de sistemas fuente
Criterios de validación:	Consistencia con definiciones ESRS Evidencia de integridad

7. Discusión.

Esta sección integra los resultados obtenidos con el marco teórico y normativo, destacando su relevancia para la práctica profesional y apuntando las líneas de mejora metodológica y de investigación futura. En la muestra analizada, el volumen total de cuestiones clave de auditoría (CCA) se asocia significativamente con el tamaño de la entidad, mientras que la adopción on-chain no muestra relación estadísticamente significativa ni con la modificación de la opinión ni con la presencia de CCA TI/DLT.

A continuación se contextualizan estos hallazgos frente a la literatura y las implicaciones prácticas derivadas.

7.1.Comparación con la literatura previa.

Los resultados no evidencian una relación directa entre adopción on-chain y mayor probabilidad de opinión modificada o mayor presencia de CCA TI/DLT. Este patrón es coherente con una lectura basada en riesgos en la que el auditor se enfoca en aspectos que la materialidad y complejidad exigen, no por presentar la etiqueta tecnológica per se.

Se ha podido evidenciar una convergencia con la literatura que subraya que el impacto de nuevas TI en auditoría depende de su integración en procesos críticos y del control interno.

Los resultados también presentan discrepancias con los trabajos que anticipan efectos de la adopción de soluciones blockchain sobre el informe de auditoría; sugiriendo un efecto contingente a contexto, madurez de implementación y gobierno de datos.

La evidencia muestra diferencias significativas en el número de CCA por tamaño (PYME vs GE). Esto encaja con planteamientos que vinculan el volumen de CCA a la complejidad organizativa, diversidad operativa y exposición a riesgos. En términos de auditoría, el mayor tamaño suele implicar más procesos, entornos de TI más complejos y mayor dependencia de terceros, factores que tienden a incrementar el alcance de CCA, incluidos los de TI/conciliaciones.

La literatura técnica suele enfatizar que los impactos contables de blockchain se concentran en la clasificación y valoración de criptoactivos, la trazabilidad de transacciones y las conciliaciones. Los resultados alcanzados, al no encontrar efectos directos de la adopción on-chain sobre la opinión, respaldan la idea de que la calidad contable depende menos de la tecnología en sí y más de cómo se diseñan políticas contables y los controles.

7.2. Implicaciones prácticas para despachos y empresas.

- Para las firmas de auditoría.
 1. Planificación basada en riesgos (NIA-ES 315, 2024 y NIA-ES 330, 2024)

Priorizar la comprensión del ciclo de TI y de los puntos de integración on-chain - ERP. La adopción on-chain, por sí misma, no justifica más CCA; lo hará el riesgo inherente asociado a procesos soportados por blockchain.
 2. Evidencia suficiente y adecuada (NIA-ES 500; 2024 y NIA-ES 402, 2024)

Diseñar pruebas para: gobierno de claves (existencia/derechos), oráculos (exactitud y calidad de datos), conciliaciones (integridad y corte), dependencia de terceros (informes de control, confirmaciones) ...
 3. Estimaciones y juicios (NIA-ES 540, 2024)

Ante criptoactivos o intangibles relacionados, reforzar el examen sobre los criterios de registro, métodos de valoración, fuentes de precios y deterioro, y documentar sensibilidades.
 4. CCA y comunicación
Cuando proceda, estructurar CCA que describan con claridad el riesgo TI/DLT y la respuesta de auditoría.
 5. Capacidades y herramientas
Fortalecer competencias en: verificación criptográfica, análisis de logs on-chain, trazabilidad de hashes y revisión de smart contracts con apoyo de expertos (NIA-ES 620, 2024), cuando sea relevante.
- Para las empresas.
 1. Políticas contables y clasificación PGC
Precisar la naturaleza económica de los activos/contratos tokenizados y mantener papeles de soporte que sustenten la clasificación (intangible, existencias, instrumento financiero) y la valoración aplicada.
 2. Gobierno de TI y control interno
Implementar gobierno de claves (segregación, multifirma, HSM), conciliaciones automáticas y controles de interfaz ERP-cadena. Documentar roles y segregación de funciones.
 3. Gestión de terceros y oráculos

Formalizar acuerdos, SLA y reportes de control con custodios/proveedores;
introducir redundancia de fuentes y back-testing de datos críticos.

4. Preparación para auditoría

Consolidar un paquete de evidencias: extractos on-chain, pruebas de firma, trazas hash, conciliaciones, políticas contables y memorandos de valoración. Anticipar requerimientos de confirmaciones externas.

5. Sostenibilidad y datos trazables

Cuando existan KPIs de sostenibilidad con soporte on-chain, reforzar gobierno de datos, diccionarios, trazabilidad y controles de oráculos para facilitar aseguramiento.

8. Conclusiones y líneas futuras de investigación.

En el presente trabajo se ha analizado el impacto de la adopción de tecnologías blockchain en la contabilidad financiera y la auditoría en España, empleando una base de datos estructurada a nivel entidad-año y técnicas descriptivas e inferenciales. La evidencia empírica sugiere que el volumen total de cuestiones clave de auditoría (CCA) se asocia con el tamaño de la entidad, más que con la adopción on-chain. En la muestra no se aprecia relación estadísticamente significativa ni con modificaciones de la opinión ni con la presencia de CCA específicas de TI/conciliaciones/DLT.

Sobre esta base se presentan las conclusiones y las derivaciones prácticas y de investigación.

Primera. La adopción on-chain observada se orienta principalmente a plataformas o aplicaciones orientadas a criptoactivos, con especial presencia de criptomonedas y tokens de circulación normal. Esta orientación sugiere un foco operativo en tenencia, custodia y pagos, más que en casos de uso aplicados al ámbito de la gestión de la información financiera o contable. Cuando tales tenencias son relevantes, la problemática contable se concentra en clasificación y valoración conforme al PGC, así como en revelaciones sobre custodia, riesgos tecnológicos y dependencias de terceros. Por lo que, en estos casos, la prioridad se centra en una clasificación y valoración consistentes con el PGC de los activos y pasivos vinculados a blockchain, en la documentación del propósito de la tenencia y en la revelación de riesgos tecnológicos y de custodia.

Atendiendo al planteamiento inicial sobre el impacto en las CCA de la adopción de sistemas basados en blockchain frente a ERP tradicionales, no se puede concluir que exista una menor presencia de opiniones modificadas o CCA por falta de casos de uso en fase de producción.

Segunda. En términos de evaluación del riesgo inherente y el riesgo de control (NIA-ES 315R, 2024), la respuesta del auditor parece venir explicada, en mayor medida, por la materialidad y la complejidad de la entidad auditada, más que por la presencia de un libro mayor distribuido. De nuevo, esta conclusión aparece por falta de casos de uso en fase de producción.

Por otro lado, esto es coherente con el enfoque NIA-ES basado en riesgos: la tecnología habilita nuevas fuentes de evidencia, pero también introduce riesgos de gobiernos y dependencia de terceros.

Desde este prisma, la prioridad debería centrarse en asegurar que existe una clasificación y valoración consistentes con el PGC de los activos y pasivos vinculados a blockchain, en la documentación del propósito de la tenencia y en la revelación de riesgos tecnológicos y de custodia. Casos sobre los que se ha obtenido evidencia suficiente.

Tercera. En cuanto a las diferencias sectoriales o de tamaño (PYME vs gran empresa), planteadas en el capítulo 2, se evidencia un mayor énfasis innovador en el grupo PYME en lo que respecta a soluciones o plataformas enfocadas a criptoactivos. Lo que supone una palanca de crecimiento exponencial de estas entidades, como puede ser el caso de Bit2Me.

Por el contrario, al poner el foco del objeto social en plataformas o soluciones enfocadas a este tipo de activos, la entidad queda expuesta a las volatilidades de los mercados en que estos se negocian. Esta situación ha podido ser contrastada durante el análisis de las memorias de algunas entidades, con el consecuente efecto en el informe de auditoría, donde se pone en cuestión la aplicación del principio de empresa en funcionamiento (NIA-ES 570R, 2024)

Finalmente, se observa un interés creciente de las entidades en soluciones basadas en blockchain para registrar y controlar huella de carbono, así como otros aspectos relacionados con el impacto en materia de sostenibilidad, responsabilidad social y gobierno. Esta tendencia se alinea con la necesidad de trazabilidad e integridad de datos que exige el marco de reporte de sostenibilidad. La utilización de blockchain como soporte de datos sobre sostenibilidad, responsabilidad social y gobierno, puede reforzar la integridad y la trazabilidad, siempre que exista gobierno de datos, diccionario de métricas y controles sobre oráculos.

Sintetizando y dando respuesta a las preguntas e hipótesis planteadas en el capítulo 2 referente a los objetivos del estudio, podemos concluir:

P-1. ¿En qué grado las entidades que implantan registros contables on-chain presentan menos opiniones modificadas o Cuestiones Clave de la Auditoría (CCA) sobre conciliaciones que las que utilizan únicamente ERP tradicionales?

Los resultados estadísticos no muestran relación significativa entre la adopción on-chain y la presencia de opiniones modificadas o CCA. Se observa, en cambio, que el tamaño de la entidad se asocia con el número de CCA. En consecuencia, no se puede afirmar que la adopción on-chain reduzca, por sí misma, modificaciones de opinión o CCA vinculadas a conciliaciones.

P-2. ¿Cómo varía la evaluación del riesgo inherente y del riesgo de control (NIA-ES 315 R) por parte de los auditores cuando la evidencia proviene de un libro mayor distribuido?

La investigación no incorpora un indicador observable y contrastable de la valoración de riesgos por parte del auditor, por lo que no se ofrece contraste empírico específico. La discusión proporciona una lectura conceptual alineada con el enfoque NIA-ES basado en riesgos, según la cual la adopción on-chain, aisladamente considerada, no justifica cambios automáticos en la valoración de riesgos. La respuesta es, por tanto, parcial e indirecta.

P-3. ¿Existen diferencias sectoriales o de tamaño (PYME vs. gran empresa) tanto en los beneficios percibidos como en la reducción del riesgo percibido y en las barreras de implantación de la tecnología blockchain?

La evidencia empírica indica que el tamaño se asocia de forma significativa con el número de CCA. En consecuencia, se confirma la existencia de diferencias por tamaño, si bien no puede atribuirse el efecto a la adopción on-chain de manera independiente.

H1. Empresas con blockchain muestran una proporción menor de opiniones modificadas o CCA sobre conciliación que las de ERP tradicional.

Los resultados no evidencian diferencias significativas atribuibles a la adopción on-chain. En consecuencia, la hipótesis se rechaza con la muestra disponible.

H2. La valoración media del riesgo de incorrección material en el ciclo de ingresos es significativamente menor para los auditores que revisan entidades on-chain.

La investigación no incorpora una medida empírica de la valoración del riesgo inherente o de control que permita su contraste. La hipótesis no queda, por tanto, empíricamente contrastada y su tratamiento es parcial.

H3. El efecto de la blockchain sobre el riesgo percibido es mayor en PYMES que en grandes compañías.

Al no disponerse de un indicador observable de riesgo ni de un contraste de interacción entre adopción on-chain y tamaño, la hipótesis no se contrasta empíricamente. La evidencia disponible únicamente confirma la asociación del tamaño con el número de CCA, sin atribución específica al componente on-chain.

Por lo que tomando las conclusiones obtenidas como punto de partida, las futuras líneas de investigación podrían orientarse a reforzar los puntos en los que el estudio se ve necesitado y profundizar en la evidencia contrastada.

Entre otros, cabría analizar tanto la adopción como la madurez de las soluciones implantadas, cubriendo la criticidad de los procesos afectados, grados de automatización, dependencia de terceros, tipo de red (pública/permissionada), custodia...

El estudio también podría ampliarse a una muestra que abarque un mayor número periodos y entidades, así como casos sectoriales.

Desde el punto de vista contable, podría extenderse al análisis de casos de tokenización de activos reales, en cuanto a su reconocimiento, derechos y revelación.

Para la auditoría, se debe tener en cuenta que este enfoque aumenta la dependencia de terceros, tanto para la entidad como para el equipo auditor. Haciendo necesario reforzar la evidencia obtenida de terceros (NIA-ES 402, 2024 y NIA-ES 505, 2024) y estrechar colaboraciones con expertos (NIA-ES 620, 2024).

En cuanto a los riesgos, bajo el paraguas de la NIA-ES 315R (2024), es importante documentar los protocolos establecidos para el gobierno de claves y los modelos de custodia de estas. Se deben tener en cuenta las adopciones de tecnologías emergentes que impacten en la información a revelar por la entidad, así como en la evidencia y trazabilidad del dato.

Cabe destacar los hallazgos sobre el uso de soluciones blockchain aplicadas a cuestiones sobre sostenibilidad. Abriendo en este aspecto una línea de investigación nueva que analice el impacto sobre la calidad del dato y la relación costes versus beneficios, entre otros.

9. Bibliografía

- AECA. (2019). La tecnología blockchain y sus implicaciones en el ámbito empresarial (Documento n.º 15). Asociación Española de Contabilidad y Administración de Empresas.
- Alastria. (2021, 22 de septiembre). New general-management at Alastria: Roadmap “Alastria 3.0”. <https://alastria.io/en/new-general-management-at-alastria-2/>
- Alastria. (2023). Memoria de actividades 2022–2023. https://alastria.io/wp-content/uploads/2023/07/Memoria-Alastria-AAFF_19.07.23.pdf
- Antonopoulos, A. M. (2014). Mastering bitcoin: Unlocking digital crypto-currencies. O’Reilly Media.
- APTE & DISRUPTIVE. (2024). Informe de situación: Blockchain 2024. https://ptedisruptive.es/wp-content/uploads/2024/12/INFORME-DE-SITUACION_-BLOCKCHAIN_-2024.pdf
- Bank for International Settlements, Committee on Payments and Market Infrastructures (CPMI). (2017). Distributed ledger technology in payment, clearing and settlement: An analytical framework.
- Beekhuizen, C. (2021, 18 de mayo). Ethereum’s energy usage will soon decrease by ~99.95 %. Ethereum Foundation Blog. <https://blog.ethereum.org/2021/05/18/country-power-no-more>
- Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on blockchain technologies: When, which and how. IEEE Communications Surveys & Tutorials, 21(4), 3796–3838. <https://doi.org/10.1109/COMST.2019.2928178>
- Bit2Me Academy. (s. f.). Precio histórico del bitcoin. <https://academy.bit2me.com/precio-historico-del-bitcoin/#precio-bitcoin-2009-2010>
- Bit2Me Academy. (s. f.). ¿Qué es un hash? <https://academy.bit2me.com/que-es-hash/>
- Bit2Me Academy. (s. f.). ¿Qué es un árbol Merkle? <https://academy.bit2me.com/que-es-un-arbol-merkle/>
- Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform [White paper]. Ethereum Foundation. <https://ethereum.org/en/whitepaper>
- Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come? Accounting & Finance, 61(1), 71–93.

- Catalini, C., & Gans, J. S. (2016). Some simple economics of the blockchain (NBER Working Paper No. 22952). National Bureau of Economic Research.
- Centro Criptológico Nacional. (2022). CCN-TEC-009: Recomendaciones para una transición post-cuántica segura. <https://www.ccn.cni.es/eu/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file>
- Chai, T. Y., Haw, S. C., Jahangir, M., Hoe, K., Heng, L., & Vellaisamy, M. (2023). Advancing retail operations: A customizable iot-based smart inventory system. *International Journal of Membrane Science and Technology*, 10(3), 1885-1897.
- Chainalysis. (2025). Crypto Crime Report 2025. Chainalysis Inc. <https://www.chainalysis.com/reports/2025-crypto-crime-report/>
- CNMV. (2025, 15 de enero). Circular 1/2024 por la que se concreta el régimen transitorio y el procedimiento de registro de proveedores de servicios de criptoactivos (MiCA). Boletín Oficial del Estado.
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework.
- Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5–21. <https://doi.org/10.2308/isys-51804>
- De Beers Group. (2022, 26 de abril). De Beers Group introduces world's first blockchain-backed diamond source platform at scale. <https://www.debeersgroup.com/media/company-news/2022/de-beers-group-introduces-worlds-first-blockchain-backed-diamond-source-platform-at-scale>
- Digiconomist. (s. f.). Ethereum energy consumption index. <https://digiconomist.net/ethereum-energy-consumption>
- España. (2023). Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión.
- España. Jefatura del Estado. (2010). Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.
- España. Jefatura del Estado. (2015). Ley 22/2015, de 20 de julio, de Auditoría de Cuentas.
- España. Jefatura del Estado. (2018). Ley 11/2018, de 28 de diciembre, de información no financiera y diversidad.

- España. Ministerio de Asuntos Económicos y Transformación Digital. (2021). Real Decreto 2/2021, de 12 de enero, por el que se aprueba el Reglamento que desarrolla la Ley 22/2015, de Auditoría de Cuentas.
- España. Ministerio de Economía y Hacienda. (2007). Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad.
- España. Ministerio de Economía y Hacienda. (2007). Real Decreto 1515/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad de Pequeñas y Medianas Empresas.
- European Central Bank, & Bank of Japan. (2017). Project Stella: Payment systems — Liquidity saving mechanisms in a distributed ledger environment.
- European Commission. (2020, 24 de septiembre). Digital finance package — Digital finance strategy for the EU (COM(2020) 591 final). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2020:591:FIN>
- European Data Protection Board. (2021, 18 de junio). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
- European Securities and Markets Authority. (2023). ESMA data strategy 2023–2028: Setting the foundations for an EU data-driven supervision. <https://www.esma.europa.eu/document/esma-data-strategy-2023-2028>
- European Union Agency for Cybersecurity. (2022). Distributed ledger technology (DLT): Cybersecurity threat landscape. <https://www.enisa.europa.eu/publications/dlt-cybersecurity-threat-landscape>
- e-Estonia. (2025, 13 de febrero). KSI blockchain. <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>
- Friedman, M. (1970). The Social Responsibility of Business Is to Increase Its Profits. The New York Times Magazine. <https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html>
- Fundación Cotec para la Innovación. (2021). *Estudio sobre la innovación y el uso de blockchain en España*. <https://online.flippingbook.com/view/452041876/>
- Gheorghita, N. (2024, 15 de noviembre). EIP-4444 implementation plan: History expiry in Ethereum. HackMD. https://hackmd.io/@hBXHLw_9Qq2va4pRtI4bIA/ryzBaf7fJx

- Grigg, I. (2005). Triple-entry accounting. https://iang.org/papers/triple_entry.html
- Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111. <https://doi.org/10.1007/BF00196791>
- IBM. (s. f.). Hyperledger. <https://www.ibm.com/es-es/topics/hyperledger>
- ICAEW. (2024). Considerations for auditing cryptocurrencies. Institute of Chartered Accountants in England and Wales. <https://www.icaew.com/-/media/corporate/files/technical/technology/know-how/considerations-for-auditing-cryptocurrencies.ashx>
- Instituto de Contabilidad y Auditoría de Cuentas. Página principal. <https://www.icac.gob.es/>
- Instituto de Contabilidad y Auditoría de Cuentas. (2019). Consulta 4/BOICAC n.º 120 (diciembre 2019): Sobre el tratamiento contable de la emisión de criptomoneda.
- Instituto de Contabilidad y Auditoría de Cuentas. (2024). Norma Internacional de Gestión de la Calidad 1 (NIGC 1-ES): Gestión de la calidad en las firmas de auditoría que realizan auditorías de estados financieros.
- Instituto de Contabilidad y Auditoría de Cuentas. (2024). Norma Internacional de Gestión de la Calidad 2 (NIGC 2-ES): Revisiones de la calidad de los encargos.
- Instituto de Contabilidad y Auditoría de Cuentas. (2024). Normas Internacionales de Auditoría adaptadas para España (NIA-ES) 315 (Revisada), 330, 402, 500, 505, 540 (Revisada), 701, 705 y 720 (Revisada) — texto consolidado.
- Instituto de Contabilidad y Auditoría de Cuentas. (2025). Normas Internacionales de Auditoría adaptadas para España (NIA-ES) 260 (Revisada) y 700 (Revisada) — texto consolidado.
- International Accounting Standards Board. (2018). Marco conceptual para la información financiera (Versión 2018). IFRS Foundation.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- KPMG. (2018). Auditing blockchain solutions. KPMG International. https://assets.kpmg.com/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf

- Liu, M., Robin, A., Wu, K., & Xu, J. (2022). Blockchain's impact on accounting and auditing: A use case on supply chain traceability. *Journal of Emerging Technologies in Accounting*, 19(2), 105–119.
- 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.
- Mendling, J., Weber, I., van der Aalst, W. M. P., vom Brocke, J., Cabanillas, C., Daniel, F., ... Zhu, L. (2018). Blockchains for business process management—Challenges and opportunities. *ACM Transactions on Management Information Systems*, 9(1), Article 4. <https://doi.org/10.1145/3183367>
- Muhs, D. (n.d.). Smart Contract Security Field Guide. Retrieved from <https://scsfg.io/>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
- National Institute of Standards and Technology. (2023). Status report on the third round of the NIST post-quantum cryptography standardization process (NISTIR 8413 rev. 1). <https://doi.org/10.6028/NIST.IR.8413r1>
- Observatorio de la Industria 4.0 & Group-IPS. (2022). Evaluación sobre la utilización de blockchain en la industria. <https://observatorioindustria.org/wp-content/uploads/2022/04/Informe-Blockchain-Observatorio-de-la-Industria-4.0.pdf>
- Observatorio Nacional de Tecnología y Sociedad. (2022). Informe blockchain en la empresa española. Ministerio de Asuntos Económicos y Transformación Digital.
- OpenSC. (s. f.). OpenSC. <https://opensc.org>
- Parlamento Europeo y Consejo. (2022). Directiva (UE) 2022/2464, de 14 de diciembre de 2022, relativa a la presentación de información sobre sostenibilidad por parte de las empresas (CSRD). Diario Oficial de la Unión Europea.
- Parlamento Europeo y Consejo. (2022). Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad (NIS 2). Diario Oficial de la Unión Europea.
- Parlamento Europeo y Consejo. (2022). Reglamento (UE) 2022/2554, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2022). Reglamento (UE) 2022/858, de 30 de mayo de 2022, sobre un régimen piloto de infraestructuras del mercado basadas en TRD. Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2023). Reglamento (UE) 2023/1113, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos (travel rule). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2023). Reglamento (UE) 2023/1114, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2023). Reglamento (UE) 2023/2772, de 31 de julio de 2023, por el que se completan las normas europeas de información sobre sostenibilidad (ESRS). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2023). Reglamento (UE) 2023/2854, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización (Data Act). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2024). Reglamento (UE) 2024/1183, de 11 de abril de 2024, que modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al marco europeo de identidad digital (eIDAS 2). Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2025). Directiva (UE) 2025/794, de 14 de abril de 2025, por la que se modifican las Directivas (UE) 2022/2464 y (UE) 2024/1760 en lo que respecta a fechas de aplicación de obligaciones de sostenibilidad. Diario Oficial de la Unión Europea.

R3. (s. f.). Corda. <https://r3.com/corda/>

Ripple. (s. f.). Ripple. <https://ripple.com/>

Scapens, R. W., Burns, J. E., & Ezzamel, M. (2003). The challenge of management accounting change: Behavioural and cultural aspects of change management.

Spence, M. (1978). Job market signaling. In *Uncertainty in economics* (pp. 281-306). Academic Press.

Tan, B. S., & Low, K. Y. (2019). The future of triple entry accounting enabled by blockchain. *Australian Accounting Review*, 29(2), 446–459. <https://doi.org/10.1111/auar.12230>

WWF-Australia. (s. f.). WWF-Australia and OpenSC. <https://wwf.org.au/get-involved/panda-labs/wwf-australia-and-opensc/>

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31.

<https://doi.org/10.1093/rof/rfw074>

10. Anexos.

Anexo 1 – Hoja “Catalogo_variables”

Variable	Tipo	Valores	Descripción operativa	Fuente
Entidad	texto	Nombre legal	Denominación social tal como figura en las CCAA	Informe/CCAA
NIF	texto	—	Si está disponible	Registro Mercantil
Ejercicio	entero	2021–2024	Año de las CCAA	Informe
Auditor	texto	—	Firma de auditoría	Informe
C2_Big4	binari o	0;1	1 si auditor es Big4	Informe
Cotizada	binari o	0;1	1 si cotiza	Memoria/RI
C1_Cotizada	binari o	0;1	Variable espejo	—
Consolidación	binari o	0;1	1 si consolidado	Informe
C3_Consolidacion	binari o	0;1	Variable espejo	—
Sector	catego ría	Financiero/Energía/Manuf actura/Servicios/Otros	Sector principal	Memoria
I1_Adopcion_on chain	binari o	0;1	Evidencia DLT en procesos financieros/conciliación	Memoria/Informe
I2_Tamano	catego ría	PYME/GE	Tamaño de la entidad	Memoria
I3_Anio	entero	2021–2024	Año como variable	—

C4_Entorno_regulacion_critico	binario	0;1	DORA/sector crítico	Memoria
D1_Tipo_opinion	categoría	Sin salvedades/Con salvedades/Desfavorable/Denegada	Tipo de opinión	Informe
D1_Opinion_modificada	binario	0;1	1 si modificada	Informe
D2_Presencia_CCA_TI_DLT	binario	0;1	CCA sobre conciliaciones/TI/DLT	Informe (CCA)
Notas_PGC_relevantes	texto	NRV 5ª/9ª/10ª, etc.	Notas PGC afectadas	Memoria
Categoria_CCA	texto	Ingresos Valoración de activos/pasivos Deterioro de activos/pasivos Existencias/Producción Instrumentos financieros Impuestos Combinaciones de negocio TI/Conciliaciones/DLT Provisiones/Contingencias Operaciones intragrupo Empresa en funcionamiento Estimaciones	Tipo de CCA	Informe (CCA)

Anexo 2 – Hoja “Diccionario_codigos”

Campo	Valores_validos	Notas
C2_Big4	0,1	1=Big4
C1_Cotizada	0,1	1=cotiza
C3_Consolidacion	0,1	1=consolida
I1_Adopcion_onchain	0,1	1=evidencia DLT; 0=no verificado
I2_Tamano	PYME,GE	GE=gran empresa
Sector	Financiero, Energía, Manufactura, Servicios, Otros	Seleccione una
D1_Tipo_opinion	Sin salvedades, Con salvedades, Desfavorable, Denegada	Según informe
D1_Opinion_modificada	0,1	1=modificada
D2_Presencia_CCA_TI_DLT	0,1	CCA sobre conciliaciones/TI/DLT

Anexo 3 – Matriz_CCA

Entidad	Ejercicio	Texto_CCA_literal	Categoria_CCA	Incluye_TI_DL
Banco Santander, S.A.	2021	- Estimación del deterioro del valor de los activos financieros a coste amortizado - préstamos y anticipos a la clientela - por riesgo de crédito.	Instrumentos financieros	0
Banco Santander, S.A.	2021	- Evaluación del deterioro de los fondos de comercio.	Deterioro de activos/pasivos	0
Banco Santander, S.A.	2021	- Provisiones por litigios y contingencias.	Provisiones/Contingencias	0
Banco Santander, S.A.	2021	- Sistemas de información.	TI/Conciliaciones/DLT	1
Banco Santander, S.A.	2022	- Estimación del deterioro del valor de los activos financieros a coste amortizado - préstamos y anticipos a la clientela - por riesgo de crédito.	Instrumentos financieros	0

Banco Santander, S.A.	2022	- Evaluación del deterioro de los fondos de comercio.	Deterioro de activos/pasivos	0
Banco Santander, S.A.	2022	- Provisiones por litigios y contingencias.	Provisiones/Contingencias	0
Banco Santander, S.A.	2022	- Sistemas de información.	TI/Conciliaciones/DLT	1
Banco Santander, S.A.	2023	- Estimación del deterioro del valor de los activos financieros a coste amortizado - préstamos y anticipos a la clientela - por riesgo de crédito.	Instrumentos financieros	0
Banco Santander, S.A.	2023	- Evaluación del deterioro de los fondos de comercio.	Deterioro de activos/pasivos	0
Banco Santander, S.A.	2023	- Provisiones por litigios y contingencias.	Provisiones/Contingencias	0
Banco Santander, S.A.	2023	- Sistemas de información.	TI/Conciliaciones/DLT	1
Banco Santander, S.A.	2024	- Estimación del deterioro del valor de los activos	Instrumentos financieros	0

		financieros a coste amortizado - préstamos y anticipos a la clientela - por riesgo de crédito.		
Banco Santander, S.A.	2024	- Evaluación del deterioro de los fondos de comercio.	Deterioro de activos/pasivos	0
Banco Santander, S.A.	2024	- Provisiones por litigios y contingencias.	Provisiones/Contingencias	0
Banco Santander, S.A.	2024	- Sistemas de información.	TI/Conciliaciones/DLT	1
Banco Bilbao Vizcaya Argentaria, S.A.	2021	- Deterioro del valor de préstamos y anticipos a la clientela.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2021	- Valoración de instrumentos financieros a valor razonable.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2021	- Riesgo asociados a la Tecnología de la información.	TI/Conciliaciones/DLT	1
Banco Bilbao Vizcaya Argentaria, S.A.	2022	- Estimación de las pérdidas por deterioro por riesgo de crédito	Instrumentos financieros	0

de la cartea de
préstamos y
anticipos a la
clientela a coste
amortizado.

Banco Bilbao Vizcaya Argentaria, S.A.	2022	- Valoración de instrumentos financieros a valor razonable.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2022	- Aplicación de la NIC 29 "Información financiera en economías hiperinflacionaria s" a los negocios en Turquía y registro de la oferta pública de adquisición voluntaria dirigida a Türkiye Garanti Bankai A.S.	Combinaciones de negocio	0
Banco Bilbao Vizcaya Argentaria, S.A.	2022	- Riesgo asociados a las tecnologías de la información.	TI/Conciliaciones/DLT	1
Banco Bilbao Vizcaya Argentaria, S.A.	2023	- Estimación de las pérdidas por deterioro por riesgo de crédito de la cartea de	Instrumentos financieros	0

préstamos y
anticipos a la
clientela a coste
amortizado.

Banco Bilbao Vizcaya Argentaria, S.A.	2023	- Valoración de instrumentos financieros a valor razonable.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2023	- Riesgo asociados a las tecnologías de la información.	TI/Conciliaciones/DLT	1
Banco Bilbao Vizcaya Argentaria, S.A.	2024	- Estimación de las pérdidas por deterioro por riesgo de crédito de la carrea de préstamos y anticipos a la clientela a coste amortizado.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2024	- Valoración de instrumentos financieros a valor razonable.	Instrumentos financieros	0
Banco Bilbao Vizcaya Argentaria, S.A.	2024	- Riesgo asociados a las tecnologías de la información.	TI/Conciliaciones/DLT	1
Binance Spain, S.L.	2023	- Reconocimiento de ingresos provenientes de	Ingresos	1

las comisiones
 obtenidas como
 casa de cambio de
 activos digitales.

Binance Spain, S.L.	2023	- Reconocimiento y valoración de las deudas a corto plazo con los usuarios de la Sociedad y los otros activos líquidos correlacionados.	Instrumentos financieros	1
Binance Spain, S.L.	2024	- Reconocimiento de ingresos provenientes de las comisiones obtenidas como casa de cambio de activos digitales.	Ingresos	1
Binance Spain, S.L.	2024	- Reconocimiento y valoración de las deudas a corto plazo con los usuarios de la Sociedad y los otros activos líquidos correlacionados.	Instrumentos financieros	1
Bitcoinforme, S.L.	2021	- Reconocimiento de los ingresos del importe neto de la	Ingresos	1

cifra de negocios y
 los
 correspondientes
 gastos por
 aprovisionamiento
 en las operaciones
 ordinarias.

Bitcoinforme, S.L.	2022	- Reconocimiento de los ingresos del importe neto de la cifra de negocios y los correspondientes gastos por aprovisionamiento en las operaciones ordinarias.	Ingresos	1
Bitcoinforme, S.L.	2023	- Reconocimiento de los ingresos del importe neto de la cifra de negocios y los correspondientes gastos por aprovisionamiento en las operaciones ordinarias.	Ingresos	1
Cecabank, S.A.	2021	- Depositaria y custodia de valores de terceros.	Instrumentos financieros	0

Cecabank, S.A.	2021	- Valoración de instrumentos financieros.	Instrumentos financieros	0
Cecabank, S.A.	2021	- Aspectos asociados a los sistemas informáticos.	TI/Conciliaciones/DLT	1
Cecabank, S.A.	2022	- Depositaria y custodia de valores de terceros.	Instrumentos financieros	0
Cecabank, S.A.	2022	- Valoración de instrumentos financieros.	Instrumentos financieros	0
Cecabank, S.A.	2022	- Aspectos asociados a los sistemas informáticos.	TI/Conciliaciones/DLT	1
Cecabank, S.A.	2023	- Depositaria y custodia de valores de terceros.	Instrumentos financieros	0
Cecabank, S.A.	2023	- Valoración de instrumentos financieros.	Instrumentos financieros	0
Cecabank, S.A.	2023	- Aspectos asociados a los sistemas informáticos.	TI/Conciliaciones/DLT	1
Cecabank, S.A.	2024	- Depositaria y custodia de	Instrumentos financieros	0

valores de
terceros.

Cecabank, S.A.	2024	- Valoración de instrumentos financieros.	Instrumentos financieros	0
Cecabank, S.A.	2024	- Aspectos asociados a los sistemas informáticos.	TI/Conciliaciones/DLT	1
CIE Automotive, S.A.	2021	- Recuperación del fondo de comercio.	Valoración de activos/pasivos	0
CIE Automotive, S.A.	2021	- Recuperación de los activos por impuestos diferidos.	Impuestos	0
CIE Automotive, S.A.	2022	- Recuperación del fondo de comercio.	Valoración de activos/pasivos	0
CIE Automotive, S.A.	2022	- Recuperación de los activos por impuestos diferidos.	Impuestos	0
CIE Automotive, S.A.	2023	- Recuperabilidad del fondo de comercio.	Valoración de activos/pasivos	0
CIE Automotive, S.A.	2024	- Recuperabilidad del fondo de comercio.	Valoración de activos/pasivos	0
Sociedad Estatal Correos y	2021	- Reconocimiento de ingresos.	Ingresos	0

Telegrafos, S.A., S.M.E.				
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2021	- Evaluación de la existencia y valoración de provisiones y pasivos contingentes.	Provisiones/Contingencias	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2021	- Evaluación del deterioro de valor de los terrenos y construcciones de la Sociedad dominante.	Deterioro de activos/pasivos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2021	- Evaluación del riesgo de reconocimiento de las compensaciones de explotación de la Sociedad dominante.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2022	- Reconocimiento de ingresos.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2022	- Evaluación de la existencia y valoración de provisiones y	Provisiones/Contingencias	0

pasivos
contingentes.

Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2022	- Evaluación del deterioro de valor de los terrenos y construcciones de la Sociedad dominante.	Deterioro de activos/pasivos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2022	- Evaluación del riesgo de reconocimiento de las compensaciones de explotación de la Sociedad dominante.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2023	- Reconocimiento de ingresos.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2023	- Evaluación de la existencia y valoración de provisiones y pasivos contingentes.	Provisiones/Contingencias	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2023	- Evaluación del deterioro de valor de los terrenos y construcciones de	Deterioro de activos/pasivos	0

		la Sociedad dominante.		
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2023	- Evaluación del riesgo de reconocimiento de las compensaciones de explotación de la Sociedad dominante.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2024	- Reconocimiento de ingresos.	Ingresos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2024	- Evaluación de la existencia y valoración de provisiones y pasivos contingentes.	Provisiones/Contingencias	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2024	- Evaluación del deterioro de valor de los terrenos y construcciones de la Sociedad dominante.	Deterioro de activos/pasivos	0
Sociedad Estatal Correos y Telegrafos, S.A., S.M.E.	2024	- Evaluación del riesgo de reconocimiento de las compensaciones	Ingresos	0

de explotación de
la Sociedad
dominante.

Iberdrola, S.A.	2021	- Deterioro de activos no financieros	Deterioro de activos/pasivos	0
Iberdrola, S.A.	2021	- Provisiones para pensiones y obligaciones similares	Provisiones/Contingenc ias	0
Iberdrola, S.A.	2021	- Uso de estimaciones contables	Estimaciones	0
Iberdrola, S.A.	2022	- Deterioro de activos no financieros	Deterioro de activos/pasivos	0
Iberdrola, S.A.	2022	- Provisiones para pensiones y obligaciones similares	Provisiones/Contingenc ias	0
Iberdrola, S.A.	2022	- Uso de estimaciones contables	Estimaciones	0
Iberdrola, S.A.	2023	- Deterior de valor del fondo de comercio y activos intangibles de vida útil indefinida	Deterioro de activos/pasivos	0
Iberdrola, S.A.	2023	- Valoración de los activos afectos a los planes de pensiones	Valoración de activos/pasivos	0

Iberdrola, S.A.	2023	- Reconocimiento de ingresos: Energía suministrada pendiente de facturar	Ingresos	0
Iberdrola, S.A.	2024	- Deterioro de valor de los activos no corrientes no financieros	Deterioro de activos/pasivos	0
Iberdrola, S.A.	2024	- Reconocimiento de ingresos: Energía suministrada pendiente de facturar	Ingresos	0
Mercadona, S.A.	2021	- Reconocimiento de ingresos	Ingresos	0
Mercadona, S.A.	2021	- Gestión de las existencias en tienda	Valoración de activos/pasivos	0
Mercadona, S.A.	2022	- Reconocimiento de ingresos	Ingresos	0
Mercadona, S.A.	2022	- Gestión de las existencias en tienda	Valoración de activos/pasivos	0
Mercadona, S.A.	2023	- Reconocimiento de ingresos	Ingresos	0
Mercadona, S.A.	2023	- Gestión de las existencias en tienda	Valoración de activos/pasivos	0

Mercadona, S.A.	2024	- Reconocimiento de ingresos	Ingresos	0
Mercadona, S.A.	2024	- Gestión de las existencias en tienda	Valoración de activos/pasivos	0
Telefónica, S.A.	2021	- Valoración de los fondos de comercios.	Valoración de activos/pasivos	0
Telefónica, S.A.	2021	- Reconocimiento de ingresos (Ingresos reconocidos pendientes de facturar)	Ingresos	0
Telefónica, S.A.	2021	- Provisiones y pasivos contingentes por litigios fiscales y regulatorios en Telefónica Brasil	Provisiones/Contingencias	0
Telefónica, S.A.	2021	- Valoración de la inversión en VMED O2 UK ltd.	Valoración de activos/pasivos	0
Telefónica, S.A.	2022	- Valoración de los fondos de comercios.	Valoración de activos/pasivos	0
Telefónica, S.A.	2022	- Reconocimiento de ingresos (Ingresos reconocidos	Ingresos	0

		pendientes de facturar)		
Telefónica,S.A.	2022	- Provisiones y pasivos contingentes por litigios fiscales y regulatorios en Telefónica Brasil	Provisiones/Contingencias	0
Telefónica,S.A.	2022	- Valoración de la inversión en VMED O2 UK ltd.	Valoración de activos/pasivos	0
Telefónica,S.A.	2023	- Valoración de los fondos de comercios.	Valoración de activos/pasivos	0
Telefónica,S.A.	2023	- Reconocimiento de ingresos (Ingresos reconocidos pendientes de facturar)	Ingresos	0
Telefónica,S.A.	2023	- Provisiones y pasivos contingentes por litigios fiscales y regulatorios en Telefónica Brasil	Provisiones/Contingencias	0
Telefónica,S.A.	2023	- Valoración de la inversión en VMED O2 UK ltd.	Valoración de activos/pasivos	0

Telefónica,S.A.	2024	- Análisis del deterioro de las unidades generadoras de efectivo, incluyendo fondos de comercio.	Deterioro de activos/pasivos	0
Telefónica,S.A.	2024	- Reconocimiento de ingresos (Ingresos reconocidos pendientes de facturar)	Ingresos	0
Telefónica,S.A.	2024	- Litigios fiscales y regulatorios en Telefónica Brasil	Provisiones/Contingencias	0
Telefónica,S.A.	2024	- Valoración de la inversión en VMED O2 UK ltd.	Valoración de activos/pasivos	0
BME Clearing, S.A.	2021	- Reconocimiento de ingresos.	Ingresos	0
BME Clearing, S.A.	2022	- Reconocimiento de ingresos.	Ingresos	0
BME Clearing, S.A.	2023	- Reconocimiento de ingresos.	Ingresos	0
FacePhi Biometrica, S.A.	2021	- Deterioro del valor de los	Deterioro de activos/pasivos	0

		activos no corrientes		
FacePhi Biometrica, S.A.	2021	- Reconocimiento de ingresos	Ingresos	0
FacePhi Biometrica, S.A.	2022	- Deterioro del valor de los activos no corrientes	Deterioro de activos/pasivos	0
FacePhi Biometrica, S.A.	2022	- Reconocimiento de ingresos	Ingresos	0
FacePhi Biometrica, S.A.	2023	- Reconocimiento de ingresos procedentes de contratos con clientes.	Ingresos	0
FacePhi Biometrica, S.A.	2023	- Reconocimiento y valoración de los gastos de desarrollo de aplicaciones informáticas.	TI/Conciliaciones/DLT	1
FacePhi Biometrica, S.A.	2024	- Reconocimiento de ingresos procedentes de contratos con clientes.	Ingresos	0
FacePhi Biometrica, S.A.	2024	- Reconocimiento y valoración de los gastos de desarrollo	TI/Conciliaciones/DLT	1

LleidaNET	2021	- Valoración de los gastos de investigación activados	Valoración de activos/pasivos	0
LleidaNET	2021	- Valoración del fondo de comercio en consolidación	Valoración de activos/pasivos	0
LleidaNET	2022	- Valoración de los gastos de investigación activados	Valoración de activos/pasivos	0
LleidaNET	2022	- Valoración del fondo de comercio en consolidación	Valoración de activos/pasivos	0
LleidaNET	2023	- Valoración de los gastos de investigación activados	Valoración de activos/pasivos	0
LleidaNET	2023	- Valoración del fondo de comercio en consolidación	Valoración de activos/pasivos	0
LleidaNET	2023	- Aplicación del principio de empresa en funcionamiento	Empresa en funcionamiento	0
LleidaNET	2024	- Valoración de los gastos de investigación activados	Valoración de activos/pasivos	0
LleidaNET	2024	- Valoración del fondo de comercio en consolidación	Valoración de activos/pasivos	0

República Gráfica	2021	- Reconocimiento de ingresos	Ingresos	0
República Gráfica	2022	- Reconocimiento de ingresos	Ingresos	0
República Gráfica	2023	- Reconocimiento de ingresos	Ingresos	0
República Gráfica	2024	- Reconocimiento de ingresos	Ingresos	0
Soluciones 480, S.A.	2021	- Reconocimiento inicial de activos y pasivos en una combinación de negocios	Valoración de activos/pasivos	0
Soluciones 480, S.A.	2021	- Recuperabilidad del fondo de comercio de consolidación y otros activos intangibles	Valoración de activos/pasivos	0
Soluciones 480, S.A.	2021	- Reconocimiento de ingresos	Ingresos	0
Soluciones 480, S.A.	2022	- Reconocimiento inicial de activos y pasivos en una combinación de negocios	Valoración de activos/pasivos	0
Soluciones 480, S.A.	2022	- Recuperabilidad del fondo de comercio de consolidación y otros activos intangibles	Valoración de activos/pasivos	0

Soluciones 480, S.A.	2022	- Reconocimiento de ingresos	Ingresos	0
Soluciones 480, S.A.	2023	- Recuperabilidad del fondo de comercio de consolidación y otros activos intangibles	Valoración de activos/pasivos	0
Soluciones 480, S.A.	2023	- Reconocimiento de ingresos	Ingresos	0
Soluciones 480, S.A.	2024	- Recuperabilidad del fondo de comercio de consolidación y otros activos intangibles	Valoración de activos/pasivos	0
Soluciones 480, S.A.	2024	- Reconocimiento de ingresos	Ingresos	0
Tendam Retail, S.A.	2021	- Evaluación del test de deterioro de activos materiales, intangibles, fondo de comercio y derechos de uso.	Deterioro de activos/pasivos	0
Tendam Retail, S.A.	2021	- Recuperación de los créditos fiscales	Impuestos	0
Tendam Retail, S.A.	2022	- Evaluación del test deterioro de activos materiales, intangibles y	Deterioro de activos/pasivos	0

		fondo de comercio.		
Tendam Retail, S.A.	2023	- Evaluación del test de deterioro de activos materiales, intangibles, fondo de comercio y derechos de uso.	Deterioro de activos/pasivos	0
Irritec Iberica	2021	- Reconocimiento de ingresos por ventas de productos terminados y mercaderías	Ingresos	0
Irritec Iberica	2021	- Transacciones con partes vinculadas realizadas a precios de mercado	Operaciones intragrupo	0
Irritec Iberica	2022	- Reconocimiento de ingresos por ventas de productos terminados y mercaderías	Ingresos	0
Irritec Iberica	2023	- Reconocimiento del importe neto de la cifra de negocio	Ingresos	0

Gestamp Automoción, S.A.	2021	- Valoración de los activos intangibles e inmovilizado material	Valoración de activos/pasivos	0
Gestamp Automoción, S.A.	2021	- Recuperabilidad de los créditos fiscales	Impuestos	0
Gestamp Automoción, S.A.	2021	- Reconocimiento de ingresos	Ingresos	0
Gestamp Automoción, S.A.	2022	- Valoración de los activos intangibles e inmovilizado material	Valoración de activos/pasivos	0
Gestamp Automoción, S.A.	2022	- Recuperabilidad de los créditos fiscales	Impuestos	0
Gestamp Automoción, S.A.	2022	- Reconocimiento de ingresos	Ingresos	0
Gestamp Automoción, S.A.	2023	- Valoración de los activos intangibles e inmovilizado material	Valoración de activos/pasivos	0
Gestamp Automoción, S.A.	2023	- Recuperabilidad de los créditos fiscales	Impuestos	0

Gestamp Automoción, S.A.	2023	- Reconocimiento de ingresos	Ingresos	0
Gestamp Automoción, S.A.	2024	- Valoración de los activos intangibles e inmovilizado material	Valoración de activos/pasivos	0
Gestamp Automoción, S.A.	2024	- Recuperabilidad de los créditos fiscales	Impuestos	0
Gestamp Automoción, S.A.	2024	- Reconocimiento de ingresos	Ingresos	0
Repsol, S.A.	2021	- Evaluación de la recuperación del valor en libros de las inversiones en empresas del grupo, multigrupo y asociadas a largo plazo considerando los impactos de la transición energética y el cambio climático.	Valoración de activos/pasivos	0
Repsol, S.A.	2021	- Evaluación de la recuperación del valor en libros	Impuestos	0

		de los activos por impuesto diferido		
Repsol, S.A.	2022	- Evaluación de la recuperación del valor en libros de las inversiones en empresas del grupo, multigrupo y asociadas a largo plazo considerando los impactos de la transición energética y el cambio climático.	Valoración de activos/pasivos	0
Repsol, S.A.	2022	- Registro contable de la reorganización societaria del negocio de Exploración y Producción	Valoración de activos/pasivos	0
Repsol, S.A.	2022	- Evaluación de la recuperación del valor en libros de los activos por impuesto diferido por créditos fiscales	Impuestos	0

Repsol, S.A.	2023	- Evaluación de la recuperación del valor en libros de las inversiones en empresas del grupo, multigrupo y asociadas a largo plazo considerando los impactos de la transición energética y el cambio climático.	Valoración de activos/pasivos	0
Repsol, S.A.	2023	- Evaluación de la recuperación del valor en libros de los activos por impuesto diferido por créditos fiscales	Impuestos	0
Repsol, S.A.	2024	- Evaluación de la recuperación del valor en libros de las inversiones en empresas del grupo, multigrupo y asociadas a largo plazo considerando los impactos de la	Valoración de activos/pasivos	0

		transición energética y el cambio climático.		
Repsol, S.A.	2024	- Evaluación de la recuperación del valor en libros de los activos por impuesto diferido por créditos fiscales	Impuestos	0