ISSN 2529-9824

Artículo de Investigación

Privacidad financiera en las CBDC: estándares, diseños y adopción comparada

Financial privacy in CBDCs: standards, designs, and comparative adoption

Pablo García González: Universidad Católica Santa Teresa de Jesús de Ávila, España y Deutsche Bank AG, España.
pablo.garcia-gonzalez@db.com
Sergio Luis Náñez Alonso[1]: Universidad Católica Santa Teresa de Jesús de Ávila, España.
sergio.nanez@ucavila.es

Fecha de Recepción: 03/03/2026

Fecha de Aceptación: 05/04/2026

Fecha de Publicación: 10/04/2026

Cómo citar el artículo

García González, P. y Náñez Alonso, S. L. (2026). Privacidad financiera en las CBDC: estándares, diseños y adopción comparada [Financial privacy in CBDCs: standards, designs, and comparative adoption]. *European Public & Social Innovation Review*, 11, 01-22. https://doi.org/10.31637/epsir-2026-2823

Resumen

Introducción: La investigación examina cómo las monedas digitales de banco central (CBDCs), reconfiguran la privacidad financiera al reemplazar transacciones anónimas en efectivo por registros digitales trazables. **Metodología:** El trabajo se configura como un estudio cualitativo descriptivo, de base documental y comparativa, sustentado en el análisis de fuentes públicas, regulatorias, académicas y técnicas. Metodológicamente, combina análisis documental y estudio comparado de casos (UE, China, Nigeria, Jamaica, Suecia y Bahamas), junto con el examen de proyectos multi-CBDC (Jura y Dunbar). **Resultados:** Los resultados muestran que los marcos más robustos integran "privacidad por diseño", minimización de datos y separación identidad-transacción; con pagos offline de alta privacidad (UE). China aplica "*anonimato controlable*" mediante umbrales KYC; Bahamas adopta niveles por límites; Jamaica exige KYC universal con trazabilidad total; Nigeria opera

[1] **Autor Correspondiente: Sergio Luis Náñez Alonso.** Universidad Católica Santa Teresa de Jesús de Ávila (España).

en red permisionada con acceso amplio del banco central, lo que se asocia a baja adopción. Los pilotos transfronterizos validan la viabilidad técnica, pero evidencian que la gobernanza y el intercambio mínimo de datos son el cuello de botella. **Discusión:** La discusión subraya que las elecciones de arquitectura traducen prioridades de política y condicionan la confianza: offline, umbrales y auditorías independientes mejoran la aceptabilidad. **Conclusiones:** Se concluye que solo una CBDC con garantías verificables y experiencias "similares al dinero efectivo" alcanzarán una adopción sostenida; sin ellas, prevalece la percepción de vigilancia y el uso es marginal.

Palabras clave: CBDC; privacidad financiera; euro digital; anonimato; pagos offline; protección de datos; adopción; gobernanza de datos.

Abstract
Introduction: This research examines how central bank digital currencies (CBDCs) reshape financial privacy by replacing anonymous cash transactions with traceable digital records. **Methodology:** This article is designed as a descriptive qualitative study, based on documentary and comparative analysis, and supported by public, regulatory, academic, and technical sources. Methodologically, it combines documentary analysis with a comparative case study (EU, China, Nigeria, Jamaica, Sweden, and the Bahamas), together with the examination of multi-CBDC projects (Jura and Dunbar). **Results:** The results show that the most robust frameworks integrate "privacy by design," data minimization, and identity-transaction separation, with highly private offline payments (EU). China applies "controllable anonymity" through KYC thresholds; the Bahamas adopts levels by limits; Jamaica requires universal KYC with full traceability; Nigeria operates on a permissioned network with broad central bank access, which is associated with low adoption. Cross-border pilots validate technical feasibility but show that governance and minimal data sharing are the bottlenecks. **Discussions:** The discussion highlights that architectural choices reflect policy priorities and condition trust: offline, thresholds, and independent audits improve acceptability. **Conclusions:** Only a CBDC with verifiable guarantees and "cash-like" experiences will achieve sustained adoption; without them, the perception of surveillance prevails and usage is marginal.

Keywords: CBDC; financial privacy; digital euro; anonymity; offline payments; data protection; adoption; data governance.

1. Introducción

Las monedas digitales de banco central representan una de las transformaciones más significativas del sistema monetario internacional desde el abandono del patrón oro (Raskin y Yermack, 2018; Fantacci y Gobbi, 2021; Bordo, 2022). En un contexto global caracterizado por la aceleración de la digitalización económica y el creciente cuestionamiento de los mecanismos tradicionales de pago, numerosos países y entidades supranacionales están explorando actualmente el desarrollo de sus propias monedas digitales (Náñez Alonso *et al*., 2020; Ozili y Alonso, 2024).

Esta revolución monetaria no constituye meramente una innovación tecnológica, sino que plantea interrogantes fundamentales sobre la arquitectura del sistema financiero, los derechos ciudadanos y la naturaleza misma del dinero en la era digital (Ozili, 2022; Wang y Gao, 2023). En dicho trabajo abordaremos la importancia de la privacidad financiera en la implementación de CBDC, dado que estos medios de pago introducen desafíos sin precedentes para la protección de dicha privacidad.

A diferencia del efectivo tradicional, que permite transacciones completamente anónimas, las monedas digitales generan inevitablemente registros detallados de cada transacción, creando oportunidades extraordinarias tanto para la eficiencia económica como para la vigilancia gubernamental (Kshetri y Loukoianova, 2022; Tronnier *et al*., 2022; Jabbar *et al*., 2023; Santaolalla Montoya, 2024; Tronnier y Qiu, 2024). Es por tanto necesario realizar un análisis comprehensivo que examina tanto los marcos teóricos como las implementaciones prácticas de protecciones de privacidad en CBDC.

La investigación se estructura para proporcionar una comprensión integral de cómo diferentes jurisdicciones han interpretado y aplicado consideraciones de privacidad en el diseño de sus monedas digitales, identificando patrones comunes, mejores prácticas y lecciones aprendidas que pueden favorecer desarrollos futuros. Por último, añadir que la introducción de una Moneda Digital de Banco Central tiene el potencial de transformar profundamente tanto el acceso a los servicios financieros como las herramientas disponibles para combatir el fraude y el lavado de dinero, al tiempo que plantea un delicado equilibrio entre seguridad y privacidad (Ozili, 2022; Tronnier *et al*., 2022; Tronnier y Qiu, 2024).

El objetivo de esta investigación ha sido analizar las consideraciones de privacidad en el diseño e implementación de las monedas digitales de los bancos centrales desde una perspectiva jurídica, técnica y comparativa internacional, con el fin de identificar marcos regulatorios efectivos y mejores prácticas que puedan aportar equilibrio entre la innovación financiera y la protección de la privacidad financiera.

Desde el punto de vista metodológico, este artículo se configura como un estudio cualitativo descriptivo, de base documental y comparativa. Examina fuentes públicas, regulatorias, académicas y técnicas para analizar, desde una perspectiva jurídica, técnica y comparada; las soluciones de privacidad adoptadas en distintas experiencias de CBDC.

El artículo se encuentra estructurado como sigue: Una Introducción que enmarca el auge de las CBDC, formula el objetivo y motiva el foco en privacidad financiera. Luego, un Marco Teórico delimita conceptos, modelos de distribución y fundamentos regulatorios de privacidad y protección de datos. La sección de Materiales y Metodología define el trabajo como un estudio cualitativo descriptivo, de base documental y comparativa, combina análisis documental con estudio de casos (UE, China, Nigeria, Jamaica, Suecia, Bahamas) y pilotos transfronterizos (Jura, Dunbar), y organiza la comparación mediante matrices.

Los Resultados se articulan en tres ejes—marcos regulatorios, soluciones técnicas (pseudo-anonimización, KYC por niveles, pagos offline) y niveles de adopción. La Discusión integra los hallazgos, extrae lecciones comparadas (liderazgo de la UE en privacidad por diseño; "anonimato controlable" en China…), y explicita limitaciones y futuras líneas de investigación. Finalmente, las Conclusiones subrayan que la adopción sostenible exige garantías verificables y experiencias similares al dinero en efectivo.

Las Monedas Digitales de Banco Central constituyen una manifestación del dinero fiduciario en formato electrónico, emitido y garantizado directamente por el banco central correspondiente (Carvalho Silva y Mira da Silva, 2025). Una CBDC representa, al igual que el formato físico, una obligación directa de la autoridad monetaria y mantiene paridad uno a uno con el dinero en efectivo (Yousaf y Goodell, 2023), asegurando su aceptación como medio de pago legal en todas las transacciones dentro de la jurisdicción (European Data Protection Supervisor, 2023; Bank of England, 2023).

Esta naturaleza centralizada otorga a las CBDC una estabilidad que las distingue de las criptomonedas privadas y de los sistemas de dinero electrónico emitidos por entidades comerciales, al tiempo que incorpora mecanismos de trazabilidad y prevención de la falsificación al asignar identificadores únicos a cada unidad digital (Ozili, 2022; Yousaf y Goodell, 2023; Bank of England, 2023; Atlantic Council, 2026). En contraste con las criptomonedas, cuya emisión y control recaen en redes descentralizadas y carecen de respaldo institucional, las CBDC ofrecen un valor estable respaldado por los bancos centrales de los estados y están reguladas por el marco legal de cada país, jurisdicción o área monetaria (Wang y Gao, 2023).

Mientras que las mencionadas criptomonedas fluctúan en función de la oferta y la demanda del mercado, una CBDC mantiene un valor fijo y está destinada tanto a transacciones cotidianas (Bijlsma *et al*., 2023) como a operaciones financieras internacionales, según se trate de versiones minoristas o mayoristas del activo digital (Themistocleous *et al*., 2023). Asimismo, a diferencia del dinero electrónico privado, que representa una obligación de entidades comerciales con acceso restringido a sus clientes; las CBDC extienden su disponibilidad al conjunto de la población, independizando el acceso del historial crediticio o bancario del usuario (Náñez Alonso *et al*., 2020; International Monetary Fund, 2024; Bank of Jamaica, 2025).

Los bancos centrales han explorado tres diseños diferentes fundamentales para distribuir sus monedas digitales. El modelo directo concede al banco central la responsabilidad de gestionar todas las cuentas de los usuarios y el cumplimiento de las labores de identificación y servicio al cliente, lo cual representa un cambio radical en su operativa tradicional (Laboure *et al*., 2021; European Data Protection Supervisor, 2023; Guo *et al*., 2024).

El modelo indirecto, en cambio, delega estas funciones en intermediarios financieros que mantienen la relación con el usuario, mientras el banco central conserva cuentas mayoristas. Esta alternativa alivia la carga operativa del emisor sin renunciar a su control sobre la oferta de dinero digital (Laboure *et al*., 2021; European Data Protection Supervisor, 2023; Guo *et al*., 2024).

Finalmente, el modelo híbrido combina ambos enfoques: el banco central emite directamente la CBDC y conserva el registro completo de transacciones, mientras los intermediarios gestionan la interfaz con el cliente, asegurando así tanto eficiencia operativa como resistencia del sistema (Bank for International Settlements [BIS], 2021; Guo *et al*., 2024).

Una cuestión fundamental (la privacidad), supone tener que hablar de la dimensión financiera de esta, la cual implica la protección de los datos personales y transaccionales de los usuarios frente a accesos no autorizados, garantizando la confidencialidad de la identidad y el detalle de cada operación; así como el control que los ciudadanos ejercen sobre su información (Tronnier *et al*., 2022; Bank of Canada, 2025).

En el sistema bancario tradicional, la privacidad resulta limitada y fragmentada: los bancos comerciales poseen datos de transacciones, pero están sujetos a marcos regulatorios que regulan el acceso y la divulgación, mientras que el efectivo ofrece el anonimato más absoluto al no dejar rastro digital.

Esta transición a un sistema digital con CBDC conlleva el riesgo de crear una línea de vigilancia gubernamental, capaz de monitorizar en tiempo real cada movimiento financiero, lo que genera preocupación sobre la erosión de las libertades individuales y el posible uso arbitrario de esa información (International Monetary Fund, 2024; Tronnier y Qiu, 2024).

En aras de mitigar estos riesgos, se han propuesto tecnologías avanzadas como las pruebas de conocimiento cero, que permiten demostrar la validez de una transacción sin revelar los datos subyacentes, y técnicas de pseudo-anonimización, cifrado homomórfico o compromiso de Pedersen, que preservan la confidencialidad mediante la transformación de identificadores directos en seudónimos.

Asimismo, el concepto de anonimato selectivo, utilizado en el yuan digital chino (Tronnier y Qiu, 2024), concede discreción para transacciones de bajo importe permitiendo su ejecución sin identificación, mientras que las operaciones de mayor cuantía requieren la revelación de la identidad para cumplir con las normas AML/CFT (Pocher y Veneris, 2021).

Los marcos regulatorios internacionales existentes exigen que las CBDC integren la privacidad desde su diseño (Beja y Correia Barradas, 2023). Por un lado, el Reglamento General de Protección de Datos en Europa impone principios de minimización, limitación de propósito y derechos de los usuarios (Napieralska y Kępczyński, 2024); mientras que el Banco de Pagos Internacionales ha establecido criterios para garantizar anonimato en pagos menores, identificación en transacciones significativas y monitoreo agregado para prevenir delitos financieros (Bank of Canada, 2025).

Este enfoque de "privacidad por diseño" resulta esencial para preservar la confianza ciudadana (Pocher y Veneris, 2021; Kshetri y Loukoianova, 2022; Bijlsma *et al*., 2023), ya que las encuestas demuestran que las preocupaciones sobre la privacidad constituyen el principal obstáculo para la adopción de CBDC, siendo señaladas por el 41% de los comentarios durante la consulta del BCE y por el 25% de la población española.

La estrecha relación entre privacidad y confianza se sustenta en la reputación de los bancos centrales como entidades independientes y neutrales, capaces de gestionar de forma honesta y ética los datos financieros de los ciudadanos, basada en la transparencia en el acceso y uso de la información, la claridad de las normas y la participación pública en el diseño regulatorio refuerzan la percepción de legitimidad del sistema (Kaur, 2024; Napieralska y Kępczyński, 2024).

Sin un equilibrio cuidadoso entre la supervisión necesaria para prevenir actividades ilícitas y la salvaguarda de los derechos individuales, las CBDC difícilmente lograrán el respaldo social indispensable para su éxito como instrumento de política monetaria digital.

Como contribución, este trabajo aborda las CBDC desde una perspectiva integrada, frente a una literatura que suele tratar por separado sus dimensiones jurídicas, técnicas y de adopción. El artículo combina análisis regulatorio, soluciones tecnológicas y evidencia comparada de implantación y uso.

Su aportación es, en primer lugar, comparativa, al reunir en un mismo marco analítico CBDC operativas (Bahamas, Jamaica y Nigeria), pilotos avanzados (China, Unión Europea y Suecia) y proyectos transfronterizos multi-CBDC (Jura y Dunbar), lo que permite contrastar modelos de gobernanza de datos, trazabilidad, pagos offline y acceso a la información.

En segundo lugar, su aportación es conceptual, al proponer un marco de análisis basado en cuatro variables: minimización y segregación de datos, visibilidad institucional del emisor, funcionalidades equivalentes al efectivo y adopción observada.

Por último, su aportación es analítica: la privacidad no se entiende como un elemento subordinado al cumplimiento AML/CFT, sino como una variable de diseño institucional que condiciona la legitimidad, la confianza social y la adopción sostenible de una CBDC.

2. Metodología

La presente investigación se configura como un estudio cualitativo descriptivo, de carácter no experimental y de base documental, que combina análisis documental y estudio comparado de casos, siguiendo estudios previos como los de (Náñez Alonso *et al*., 2020; Tronnier *et al*., 2023; Shafranova *et al*., 2024). Su finalidad es examinar, desde una perspectiva jurídica, técnica y comparativa internacional, cómo distintas jurisdicciones y proyectos de CBDC han incorporado mecanismos de privacidad financiera en su diseño e implementación.

El estudio se apoya en fuentes públicas y en documentación oficial, regulatoria, académica y técnica. El análisis se centra en la comparación sistemática de marcos regulatorios, soluciones técnicas, niveles de adopción y lecciones aprendidas en los casos seleccionados. Actualmente, según diversas fuentes como Kiff (2026); CBDC Tracker (2026) y Atlantic Council (2026) 137 países, jurisdicciones y uniones monetarias; están estudiando la posibilidad de crear una moneda digital del banco central (CBDC). Ahora bien, solamente Bahamas, Jamaica y Nigeria presentan una CBDC plenamente operativa actualmente. Es por ello, que estos países son seleccionados para el estudio.

Junto a ellos, se han incluido en el estudio China, la Unión Europea y Suecia. China ha lanzado ya varios ensayos de uso a gran escala en al menos 115 ciudades entre 2018 y 2022 (Huang, 2025). La U.E. por su parte pretende poner en marcha el euro digital en 2029. El Banco Central Europeo (BCE) espera aprobar el reglamento necesario en 2026, iniciar pruebas piloto en 2027 y lanzar la moneda posteriormente (European Central Bank, 2025). Ambos han sido seleccionados para el estudio por tener en marcha pruebas piloto; así como por abarcar jurisdicciones con 1410 y 450 millones de habitantes respectivamente. Suecia es incluida en el estudio dado que el país ha sido el gran experimento mundial del dinero sin efectivo (Julin, 2022).

Con solo una de cada diez compras en metálico y donde solo una pequeña minoría de ciudadanos (alrededor del 7-13%) de la población utiliza billetes y monedas habitualmente. Esto sitúa a Suecia como un caso principal de estudio, al estar a la vanguardia de una economía sin efectivo (*cashless*). A ello se suma también, que su CBDC (la e-Krona) se encuentra en fase avanzada de su piloto, teniendo como uno de sus pilares la "privacidad" (Zafar, 2026).

Finalmente, los proyectos Jura y Dunbar se incluyen porque permiten analizar una dimensión que no aflora con la misma intensidad en las CBDC nacionales: la privacidad y la gobernanza de datos en pagos transfronterizos entre jurisdicciones. Su interés comparado radica en que demuestran la viabilidad técnica de la interoperabilidad multi-CBDC (Inozemtsev y Nektov, 2022), pero también evidencian que la compartición mínima de datos, los controles de acceso y la coordinación regulatoria constituyen el principal cuello de botella para escalar estos sistemas (Kaur, 2024).

Tras ello, los casos fueron sometidos a comparación sistemática con el fin de identificar similitudes y diferencias en tres aspectos clave:

1. Enfoques regulatorios de privacidad y protección de datos.

2. Soluciones técnicas adoptadas (niveles de anonimato, capacidades offline, separación de datos de identidad y transaccionales).

3. Niveles de adopción alcanzados.

4. Lecciones aprendidas.

Para ello se emplean matrices comparativas. Este diseño metodológico nos ha permitido organizar y contrastar de forma rigurosa la evidencia disponible sobre privacidad en CBDC en diferentes jurisdicciones y proyectos.

Y todo ello, manteniendo el foco en la relación entre decisiones de diseño (jurídicas y técnicas) y sus implicaciones para la protección efectiva de la privacidad. Desde un plano analítico, la comparación no persigue únicamente describir diferencias entre jurisdicciones, sino identificar patrones relacionales entre cuatro variables:

1. Grado de minimización y segregación de datos.

2. Nivel de visibilidad institucional del emisor.

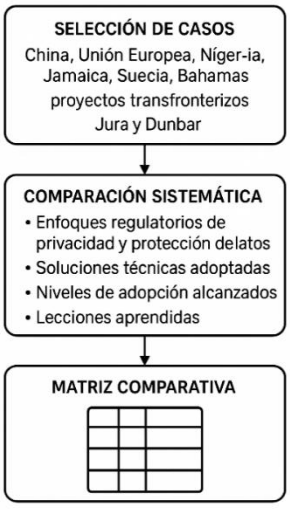
3. Existencia de funcionalidades equivalentes al efectivo, especialmente pagos offline.

4. Aceptabilidad o adopción observada.

A partir de estas variables, el estudio examina si los diseños que limitan de forma más verificable la correlación entre identidad y transacción muestran una mayor compatibilidad con la confianza social y con un uso más sostenido de la CBDC.

Figura 1.

Metodología empleada



Fuente: Elaboración propia.

3. Resultados

Todos los resultados obtenidos, se encuentran sintetizados en las tablas 1 y 2.

Tabla 1.

CBDCs en funcionamiento

Categoría	Bahamas (Sand Dollar)	Jamaica (JAM-DEX)	Nigeria (eNaira)
Enfoques regulatorios, privacidad y protección datos	Esquema por niveles (Tier 1 sin KYC formal; Tier 2 con KYC). Cumplimiento AML/CFT.	KYC obligatorio para todos; trazabilidad completa gobernada por el banco central.	Cumplimiento NDPR; acceso amplio del banco central a datos de cuentas/transacciones.
Soluciones técnicas	DLT permisionada, cifrado y MFA; límites por nivel.	No blockchain (eCurrency); gobernanza centralizada; trazabilidad total.	Hyperledger Fabric (permisionada); modelo basado en cuentas; integración BVN/NIN/TIN.
Niveles de adopción	Monederos >120k; circulación <0,5% del efectivo; uso discreto.	~centenares de miles de monederos; valores en circulación modestos; incentivos para uso.	Muy baja: <1% de población activa; gran inactividad de monederos.
Lecciones aprendidas	Inclusión distinta de uso: falta aceptación comercial e educación.	Cumplimiento sencillo, pero sin anonimato funcional, requiere incentivos.	Visibilidad del emisor desincentiva adopción; clave minimizar datos y limitar accesos.

Fuente: Elaboración propia.

Tabla 2.

Pilotos de CBDCs

Categoría	China (e-CNY)	Unión Europea (euro digital)	Suecia (e-krona)	Jura/Dunbar (multi-CBDC mayorista)
Enfoques regulatorios, privacidad y protección datos	"Anonimato controlable" con KYC por umbrales; amplias excepciones de seguridad nacional.	Privacidad por diseño (minimización, pseudonimización, segregación identidad/transacción); alta privacidad offline.	Reconoce que todo pago electrónico deja rastro; ajustes legales para confidencialidad financiera.	Enfoque interjurisdiccional: mínima compartición de datos, control de acceso y alineamiento AML/CFT.
Soluciones técnicas	KYC escalonado, pagos offline (NFC); funciones programables probadas en pilotos.	Arquitectura dos niveles; pagos offline con límites; estudio de "vouchers de privacidad".	Pilotos DLT; pruebas de offline; modelos de gobernanza con distinto grado de control público-privado.	DLT multi-CBDC; liquidación casi en tiempo real; interoperabilidad entre bancos centrales.
Niveles de adopción	Pilotos extensos (>200M+ monederos reportados en pruebas); sin emisión nacional plena.	Fase preparatoria (sin usuarios finales).	Piloto (sin emisión general).	Pruebas de concepto (sin producción).
Lecciones aprendidas	El modelo por umbrales es viable, pero exige salvaguardas contra correlación identidad-transacción.	La aceptación social exige alta privacidad (offline) y límites/gobernanza de datos claros.	Tecnología viable; éxito dependerá de marco legal y roles público-privados.	La gobernanza de datos y la privacidad compartida son el cuello de botella para escalar.

Fuente: Elaboración propia.

1.1. Enfoques regulatorios de privacidad y protección de datos

El análisis comparado muestra que los marcos más robustos para una CBDC integran privacidad por diseño, minimización de datos y limitación de propósito desde la concepción del sistema. En la Unión Europea (UE), el diseño del euro digital incorpora pseudo-anonimización fuerte para que el Eurosistema no pueda vincular identidades y pagos en operaciones online, y preserva espacios de "alta privacidad" para pagos offline, concebidos para replicar rasgos del efectivo (European Central Bank, 2019, 2024).

La consulta pública del BCE situó la privacidad como la preocupación prioritaria de la ciudadanía (43% de respuestas), lo que impulsó la exploración de umbrales y "vouchers" de privacidad para pagos de bajo riesgo (CNIL, 2023). En este marco, la UE perfila el estándar regulatorio más exigente entre las jurisdicciones analizadas: junto a la privacidad por diseño, el debate regula límites de tenencia —en el rango de 3.000–4.000 euros— para equilibrar privacidad con estabilidad financiera y desintermediación (European Parliament, 2023; Bruegel, 2025).

Además, el régimen de transferencias internacionales de datos se apoya en instrumentos como las Binding Corporate Rules (BCR) para garantizar salvaguardas cuando haya flujos extraterritoriales de datos personales (European Commission, 2021). El Supervisor Europeo de Protección de Datos (EDPS) advierte de riesgos sistémicos de vigilancia si se posibilita la correlación identidad-transacción, y recomienda segregación de datos de identidad y registros transaccionales, controles de acceso estrictos y Evaluaciones de Impacto en Protección de Datos (DPIA) continuas durante todas las fases del proyecto (European Data Protection Supervisor, 2023).

Fuera de la UE, China combina obligaciones severas en la Personal Information Protection Law (PIPL) —especialmente en transferencias transfronterizas y tratamiento de datos sensibles— con un diseño de "anonimato controlable" en el e-CNY, que gradúa la identificación por umbrales en función del importe y el riesgo (People's Bank of China, 2022). En términos comparados, la protección efectiva frente a correlaciones amplias es más limitada que en la UE, en línea con prioridades de soberanía digital.

Por lo que respecta a Nigeria, el eNaira se diseñó sobre red permisionada (Hyperledger Fabric) con identificación obligatoria apoyada en BVN/NIN/TIN y cumplimiento declarado de la NDPR; el Banco Central enfatiza "profundas consideraciones" de privacidad y protección de datos en su Design Paper (Central Bank of Nigeria, 2021; eNaira, 2023). No obstante, el enfoque implica acceso directo del banco central a transacciones y saldos, lo que la literatura crítica vincula con capacidades de vigilancia superiores a los sistemas tradicionales (Vessio y Adekunbi, 2024).

En el caso de Jamaica, JAM-DEX prioriza trazabilidad total: exige identidad para todos los usuarios y transacciones, y opera con tecnología de eCurrency (no blockchain), orientada a gobernanza por el banco central y transparencia de transacciones (DaCosta, 2024). La documentación oficial indica que "tu identidad no se registra" en cada pago, pero el acceso al sistema requiere KYC previo, por lo que el modelo no contempla anonimato funcional (Bank of Jamaica, 2025).

El Riksbank sueco, por su parte, ha explorado la e-krona con DLT y reconoce la necesidad de nuevas precisiones legales para compatibilizar la confidencialidad financiera con la trazabilidad inherente de los pagos electrónicos ("todos los pagos electrónicos dejan rastros") (Sveriges Riksbank, 2023). En paralelo, se evalúan modelos de gobernanza con distintos grados de control público-privado, preservando el papel del banco central y explorando pagos offline con límites y mitigaciones de riesgo (Ledger Insights, 2023).

En el caso de Bahamas, el Sand Dollar adopta un esquema por niveles: mayor privacidad con límites pequeños (Tier 1 sin identificación formal) y límites más altos con KYC (Tier 2), equilibrando inclusión y cumplimiento AML/CFT (Digital Euro Association, 2023). El banco central opera la infraestructura (DLT), aplicando cifrado y controles reforzados; la experiencia práctica subraya la importancia de ciberseguridad, educación y participación de comercios para sostener el uso (AFI Global, 2025; Intereconomics, 2023).

Finalmente, los proyectos transfronterizos (Jura/Dunbar); Ambos demuestran la viabilidad de plataformas multi-CBDC mayoristas con liquidación en tiempo real y eliminación de intermediarios corresponsales, pero evidencian retos de gobernanza y privacidad entre jurisdicciones (BIS, 2021; The Payments Association, 2024). La coordinación exige reglas claras sobre acceso a datos, compartición mínima necesaria y controles de cumplimiento armonizados para evitar asimetrías regulatorias.

A escala internacional, los estándares AML/CFT del GAFI/FATF introducen una "tensión" estructural con el anonimato: exigen diligencia debida, trazabilidad y conservación de registros para operaciones de mayor riesgo. De ahí la convergencia regulatoria hacia esquemas por niveles: alta privacidad en pagos de bajo valor y requisitos crecientes de identificación a medida que aumenta el riesgo (European Central Bank, 2024).

En paralelo, organismos como el Fondo Monetario Internacional (FMI) recomiendan centrar la gobernanza en el uso de datos a lo largo de todo el ciclo de vida: definir casos de uso, identificar riesgos por cada caso e implementar tecnologías de mejora de privacidad junto a controles que aseguren necesidad y proporcionalidad; este planteamiento es coherente con las advertencias del EDPS sobre riesgo evolutivo y necesidad de supervisión continua (International Monetary Fund, 2024; European Data Protection Supervisor, 2023).

1.2. Soluciones Técnicas Adoptadas

Respecto de las posibles soluciones técnicas adoptadas, los casos analizados convergen en una arquitectura de dos niveles (banco central-PSPs) y en el uso de DLT/infraestructura permisionada cuando se requiere gobernanza granular y control de acceso. Las técnicas comunes para proteger la privacidad son: pseudo-anonimización y separación de datos de identidad vs. transacciones, umbrales y perfiles de KYC escalonados, y pagos offline con límites y mitigaciones contra el doble gasto (European Central Bank, 2024). En la Unión Europea (futuro euro digital), el diseño técnico incorpora privacidad "por capas":

1. Pseudo-anonimización fuerte para que el Eurosistema no pueda vincular pagos con identidades en operaciones online ((Tronnier *et al*., 2022; Cotugno *et al*., 2024).

2. Modo offline con "alta privacidad" donde la transacción se realiza dispositivo a dispositivo sin participación del sistema central, sujeto a límites de importe/duración y controles anti–doble gasto (Cotugno *et al*., 2024).

3. Exploración de "vouchers de privacidad" y umbrales para pagos de bajo riesgo (European Central Bank, 2019, Tronnier *et al*., 2022; Tronnier y Qiu, 2024; CNIL, 2023).

Estas soluciones se alinean con el reglamento europeo de protección de datos y sus principios: minimización, limitación de propósito; y con la separación técnica identidad y transacción como salvaguarda central.

En China, por su parte el e-CNY implementa "anonimato controlable" mediante KYC por niveles: desde monederos de Nivel 1 con alta privacidad y límites bajos (solo número de teléfono) hasta niveles superiores con verificación reforzada y mayor funcionalidad; además, pagos offline vía NFC (Tronnier y Qiu, 2024). Técnicamente, el sistema mantiene capacidad de acceso del banco central a saldos y datos requeridos para la apertura de cuentas y ha probado caducidad programable de fondos en pilotos, ilustrando la tensión entre privacidad y control soberano (Zhu y Zhou, 2025).

Por su parte, Nigeria con el e-Naira presenta una arquitectura permisionada sobre Hyperledger Fabric, con modelo basado en cuentas y nodos operados por el banco central y contrapartes de confianza (Chukwuere, 2021); diseñado para alto rendimiento, baja latencia y confidencialidad (Central Bank of Nigeria, 2021). Esto supone, integrar identidad con (para cumplir con KYC) y por otro lado, cumplimiento NDPR. Sin embargo, el acceso directo del banco central a transacciones y saldos crea capacidades de vigilancia superiores a sistemas tradicionales (eNaira, 2023; Vessio y Adekunbi, 2024).

Por lo que respecta a Jamaica, su CBDC el JAM-Dex presenta una solución no-blockchain (tecnología eCurrency), orientada a gobernanza central y trazabilidad completa: KYC obligatorio para todos los usuarios, sin anonimato funcional; el banco central respalda 1:1 y los PSP distribuyen (DaCosta, 2024; Bank of Jamaica, 2025). Aunque la documentación oficial afirma que "la identidad no se registra en cada transacción", el acceso al sistema exige identificación previa, haciendo toda la actividad visible para la autoridad monetaria (Indira *et al*., 2025).

Bahamas puso en marcha su CBDC, el Sand Dollar, con una arquitectura DLT operada por el banco central con autenticación multifactor y cifrado; esquema por niveles que equilibra inclusión y cumplimiento: Tier 1 (límites bajos, requisitos mínimos) y Tier 2 (límites mayores con KYC y vinculación a cuenta), además de políticas de ciberseguridad y evaluaciones periódicas (Digital Euro Association, 2023; AFI Global, 2025). Suecia por su parte, al testar la e-krona, ha realizado pilotos DLT con tokens únicos (trazables) y experimentación con pagos offline bajo límites y mitigaciones.

En su caso, el grado de control varía en tres modelos de gobernanza (de baja a muy alta estandarización de interfaces). Todo ello, buscando equilibrio entre innovación privada y control público (Sveriges Riksbank, 2023; Ledger Insights, 2023). El propio Riksbank reconoce que "todos los pagos electrónicos dejan rastro", por lo que la conciliación entre DLT (trazable) y confidencialidad financiera exige ajustes legales y de diseño (Sveriges Riksbank, 2023).

Finalmente, los proyectos transfronterizos Jura/Dunbar han probado plataformas multi-CBDC mayoristas sobre DLT con liquidación casi en tiempo real, disminución de intermediarios corresponsales y mejoras de liquidez (wCBDC de múltiples jurisdicciones). Las soluciones técnicas ponen el foco en interoperabilidad, gobernanza común, controles de acceso y compartición mínima de datos entre bancos centrales, a la vez que señalan retos de privacidad y cumplimiento entre marcos discrepantes (BIS, 2021; The Payments Association, 2024).

1.3. Niveles de Adopción Alcanzados

Respecto a los niveles de adopción alcanzados hay que decir que en el caso de Europa, China y Suecia aún se encuentran en fase piloto. En el caso de Europa con el futuro euro digital, el proyecto se encuentra en fase preparatoria (1 de nov. de 2023–oct. de 2025), sin emisión minorista ni métricas fiables de adopción todavía (Cotugno *et al*., 2024). El progreso reciente incluye el trabajo sobre el *Rulebook* y la recepción de unas 2.500 aportaciones de agentes de mercado y bancos centrales; la priorización de privacidad condiciona cualquier piloto futuro, pero aún no hay usuarios finales ni circulación (European Central Bank, 2024; CNIL, 2023).

En china, algo más avanzado su piloto; es el caso con mayor despliegue pues para inicios de 2022 se reportaron >261 millones de monederos y una expansión geográfica a >25 regiones (Bai *et al*., 2025), con usos que incluyen transporte, pagos públicos y salarios del sector público en ciudades piloto (People's Bank of China, 2022; BOFIT, 2023; Sanctionscanner, 2025). Suecia con el e-krona, continúa en fase piloto; no hay emisión general ni métricas de adopción minorista.

Las pruebas muestran factibilidad técnica (incluso pagos offline con límites) y compatibilidad con sistemas bancarios, pero el banco central subraya que "todos los pagos electrónicos dejan rastro", por lo que aún no hay despliegue al público (Sveriges Riksbank, 2023; Ledger Insights, 2023). Por su parte, los proyectos transfronterizos Jura y Dunbar, son aún pruebas de concepto mayoristas *multi-CBDC* sobre DLT. Hasta ahora solo hay resultados sobre su viabilidad técnica acreditada (liquidación casi en tiempo real, menos fricción y mejor acceso a liquidez); pero sin adopción productiva a escala. Persisten retos de gobernanza y privacidad entre marcos nacionales (BIS, 2021; The Payments Association, 2024).

En lo que respecta a Nigeria, Bahamas y Jamaica (ya con CBDCs operativas), el nivel de adopción es variable. Así, en Nigeria el eNaira, tras su lanzamiento (oct. 2021), la adopción es muy baja. En marzo de 2024, el eNaira representaba aproximadamente el 0,36% de la moneda en circulación; además, el 98,5% de las carteras nunca se usaron y solo el 1,5% transaccionaba semanalmente. En 2022 la adopción rondaba el 0,5% de la población, pese a incentivos y eliminación de requisitos bancarios para abrir monedero (Nairametrics, 2024; CBDC Tracker, 2024).

Por su parte, el JAM-DEX jamaicano, lanzado en 2022, presenta unos 260.000 monederos activos. Todo ello, sobre una población de 2,8 millones de habitantes; y cerca de JMD 257 millones en circulación a finales de 2023; sin embargo, la red depende aún de un único proveedor (NCB/Lynk) y ha requerido incentivos (transferencia inicial gratuita y *cashback*) para impulsar su uso (Ledger Insights, 2024; Jamaica Information Service, 2024). Finalmente, Bahamas con el Sand Dollar el cual fue emitido desde 2020, presenta adopción discreta: >120.000 monederos (población rondando los 400.000 habitantes), pero sólo 2,1 millones USD en circulación (<0,5% del efectivo en circulación).

La brecha entre aperturas de monedero y uso sostenido se atribuye a baja densidad de comercios e integración bancaria, y a carencias de educación financiera (Wenker, 2022; Bahamas Sand Dollar Update, 2024; CoinGeek, 2025). En términos comparados, estos resultados sugieren que la privacidad creíble funciona como una condición habilitante de la aceptación social de la CBDC, mientras que su ausencia o escasa verificabilidad reduce la propuesta de valor frente al efectivo y frente a los medios privados de pago. No obstante, la adopción observada indica también que las garantías de privacidad, por sí solas, no bastan: requieren integración comercial, facilidad de uso e incentivos institucionales para traducirse en uso efectivo.

1.4. Lecciones aprendidas

El Sand Dollar de Bahamas, valida el enfoque por niveles (Tier 1 mínimo KYC; Tier 2 con verificación plena) y una DLT permisionada con controles de seguridad (Wenker, 2022; Sisodia, 2024). Aun así, persisten brechas entre carteras abiertas y circulación efectiva (<0,5% del efectivo), en parte por baja densidad de comercios, escasa integración bancaria y educación financiera insuficiente (Digital Euro Association, 2023; Sisodia, 2024; AFI Global, 2025; Human Rights Foundation, 2024). Por tanto, la lección que se extrae es que, junto al diseño técnico, hacen falta estrategias de onboarding de comercios y alfabetización para consolidar el uso. Del caso nigeriano con la CBDC e-Naira, se obtiene información valiosa respecto a que el acceso directo del banco central a saldos y transacciones desalienta el uso.

El eNaira (recordemos Hyperledger Fabric, red permisionada), logró rendimiento alto (Ozili, 2022), pero su arquitectura centralizada en el emisor y la visibilidad amplia del regulador sobre saldos y operaciones alimentan percepciones de vigilancia; la adopción se mantiene muy baja (Central Bank of Nigeria, 2021; Ozili, 2022; Nairametrics, 2024; Ozili y Alonso, 2024; Vessio y Adekunbi, 2024). Por tanto, la lección que se extrae es que, el diseño debe minimizar datos y limitar accesos del banco central si se busca confianza y uso cotidiano.

Otra cuestión importante deriva de la experiencia de Jamaica. La trazabilidad total simplifica cumplimiento, pero reduce aceptabilidad. JAM-DEX exige KYC para todos y opera sin blockchain (Baker, 2024). Con trazabilidad integral "gobernada por el banco central, aunque la autoridad asegura que "no se registra tu identidad en cada transacción", el ingreso al sistema requiere identificación previa, habilitando visibilidad plena (Bank of Jamaica, 2025; DaCosta, 2024). Por tanto, la lección que se extrae es que, la ausencia de anonimato funcional limita el diferencial frente a medios privados y puede exigir incentivos continuos.

Del caso sueco, se extrae que "todos los pagos electrónicos dejan rastro" obliga a ajustes legales y de gobernanza (Ceylan, 2024). La e-krona funcionaría sobre DLT, pagos *offline* y prueba modelos de gobernanza (bajo-alto control estatal). El Riksbank admite la trazabilidad inherente y sugiere posibles reformas legales para conciliar confidencialidad financiera con DLT (Sveriges Riksbank, 2023; Ledger Insights, 2023).

Finalmente, del piloto Jura/Dunbar extraemos que la interoperabilidad *multi-CBDC* es factible, la gobernanza de datos es el cuello de botella. Los proyectos Jura y Dunbar prueban liquidación transfronteriza casi en tiempo real (Annathurai *et al*., 2024; Guo *et al*., 2024); pero chocan con asimetrías regulatorias en gobernanza, privacidad y cumplimiento (BIS, 2021; The Payments Association, 2024). Por tanto, la lección que se extrae es que, los *hubs multi-CBDC* requieren reglas comunes de mínima compartición de datos y controles de acceso interoperables.

4. Discusión

El examen comparado permite sostener que la variable decisiva no es la digitalización monetaria en sí misma, sino la forma en que cada arquitectura distribuye información, funciones y capacidad de observación entre banco central, intermediarios y autoridades de cumplimiento.

En términos analíticos, los casos estudiados se ordenan en un continuo que va desde modelos de privacidad reforzada, con separación estricta entre identidad y transacción y espacios de alta privacidad offline, como el de la Unión Europea, hasta modelos de trazabilidad integral o de alta visibilidad institucional del emisor, como los observados en Jamaica y Nigeria; entre ambos extremos se sitúan fórmulas intermedias de anonimato graduado y segmentación por riesgo, como China y Bahamas (Cotugno *et al*., 2024; Tronnier, Harborth y Hamm, 2022; Kaur, 2024; Tronnier y Qiu, 2024; Bai *et al*., 2025; DaCosta, 2024; Vessio y Adekunbi, 2024; Digital Euro Association, 2023).

Esta gradación permite afirmar que la aceptabilidad social de una CBDC no depende solo de su eficiencia técnica o de su cobertura normativa, sino del grado en que su diseño limita de manera verificable la posibilidad de correlacionar identidad y conducta transaccional. En este sentido, los esquemas AML/CFT tienden a reordenar la privacidad no como ausencia de control, sino como privacidad graduada e integrada en la propia arquitectura regulatoria, mediante umbrales, segmentación por riesgo y reglas de acceso a los datos "*regulation-by-design*" (Pocher & Veneris, 2021; Napieralska y Kępczyński, 2024; Fernández *et al*., 2025).

Las soluciones más pro-privacidad identificadas convergen en cuatro familias:

i) pseudo-anonimización con separación identidad-transacción (UE);

ii) umbrales con KYC por niveles (China, Bahamas);

iii) funcionalidades offline con límites y conciliación diferida (UE, Suecia, China); y

iv) DLT permisionada con controles de acceso y registro inmutable (Bahamas, Suecia) (Guo, Kreitem y Moser, 2024; Sisodia, 2024; Wenker, 2022).

En contraste, modelos de trazabilidad total como JAM-DEX maximizan el cumplimiento a costa del anonimato, y las arquitecturas con acceso directo del banco central —como eNaira— elevan el riesgo de vigilancia ex post, con impactos observables en la adopción (Baker, 2024; Chukwuere, 2021; Fernández *et al*., 2025). Desde esta comparación se desprende una relación central: las soluciones técnicas no son neutrales respecto de los derechos fundamentales.

Los pagos offline, la pseudo-anonimización fuerte y la separación funcional entre emisor e intermediarios no son meros atributos operativos, sino mecanismos que reducen la exposición del ciudadano a formas de vigilancia ex ante y ex post. En sentido inverso, cuando el diseño concentra en el emisor la información de identidad, saldos y transacciones, la CBDC pierde parte de su diferencial frente a medios privados ya bancarizados y aumenta el coste político de su implantación. Por ello, la verdadera solución no opone simplemente privacidad frente a cumplimiento, sino centralización informacional frente a confianza.

La evidencia de uso confirma estos patrones: China concentra el volumen piloto; Bahamas mantiene baja intensidad transaccional pese a la apertura de monederos; Nigeria registra uso marginal; Jamaica avanza en cuentas, pero requiere mayor aceptación comercial; mientras que Suecia y la UE continúan en piloto/preparación.

Los experimentos mayoristas transfronterizos (Jura/Dunbar) demuestran viabilidad técnica, pero el cuello de botella es la gobernanza de datos entre jurisdicciones (Themistocleous *et al*., 2023; Annathurai, Abdul Wahab y Jamil, 2024; Indira, Alamsyah y Yunita, 2025; Bai *et al*., 2025). Más allá de la ingeniería, la aceptación social depende de salvaguardas verificables: supervisión independiente con capacidad sancionadora, transparencia sobre accesos y evaluaciones de impacto continuas.

La privacidad por diseño y la experiencia offline "similares al dinero efectivo" incrementan la aceptabilidad, mientras que la concentración de capacidades de acceso reduce la propuesta de valor frente al efectivo y los medios privados (Bijlsma, van der Cruijsen, Jonker y Reijerink, 2023; Jabbar *et al*., 2023; Ozili y Alonso, 2024; Náñez Alonso *et al*., 2025). En suma, los diseños que distribuyen funciones entre intermediarios y limitan la visibilidad institucional mediante controles técnicos y de gobernanza muestran mayor compatibilidad con objetivos de inclusión y un potencial de uso más sostenido (Beja y Correia Barradas, 2023; Wenker, 2022).

La evidencia comparada no permite sostener una relación mecánica entre mayor privacidad y mayor uso, pero sí muestra una pauta consistente: allí donde las garantías de privacidad son débiles, inexistentes o poco creíbles, la CBDC necesita incentivos adicionales o mantiene un uso marginal; allí donde la privacidad se incorpora como rasgo constitutivo del diseño, la propuesta resulta más aceptable, aunque ello no baste por sí solo sin infraestructura comercial, integración en pagos cotidianos y claridad regulatoria.

Así, la privacidad aparece en los casos analizados como condición necesaria de legitimidad, aunque no suficiente por sí misma para asegurar adopción sostenida. Desde esta perspectiva, el artículo adopta un posicionamiento analítico claro: las CBDC más compatibles con una adopción sostenida no son aquellas que maximizan el control del emisor ni aquellas que prometen un anonimato absoluto, sino las que combinan privacidad graduada, límites estrictos de acceso a los datos, supervisión independiente y funcionalidades próximas al efectivo para pagos de bajo riesgo. En consecuencia, la privacidad no debe entenderse como una concesión residual subordinada al cumplimiento AML/CFT, sino como una variable de diseño institucional que condiciona la legitimidad, la proporcionalidad regulatoria y la utilidad social de la CBDC.

Como limitaciones de este estudio se pueden señalar dos. En primer lugar, la dependencia de fuentes heterogéneas (documentación regulatoria, técnica y divulgativa) que pueden no ser comparables entre jurisdicciones y que evolucionan con rapidez. En segundo lugar, la ausencia de evidencia primaria de comportamiento del usuario y del comercio (encuestas/experimentos), lo que limita inferencias causales sobre los determinantes de adopción. Como líneas futuras de investigación, se puede indicar el realizar un piloto controlado que mida el efecto de parámetros de privacidad (límites offline, granularidad de logs, ventanas de conciliación) sobre adopción y uso activo de consumidores y comercios.

5. Conclusiones

El análisis comparado de esta investigación muestra que el diseño técnico y la gobernanza de una CBDC determinan su equilibrio entre innovación y derechos fundamentales. La privacidad emerge como condición decisiva de aceptabilidad: los modelos que minimizan datos separan identidad y transacciones y habilitan pagos sin conexión con límites y mitigaciones generan mayor confianza social que aquellos que concentran visibilidad en la autoridad emisora o exigen identificación en todos los supuestos.

Las trayectorias nacionales confirman ese patrón. En entornos en producción, los esquemas por niveles (como en Bahamas) facilitan inclusión y cumplimiento, pero no aseguran por sí solos uso sostenido si faltan aceptación comercial, integración con pagos cotidianos e incentivos adecuados.

Donde la trazabilidad es total (Jamaica) o el emisor mantiene acceso amplio a saldos y operaciones (Nigeria), la percepción de vigilancia actúa como freno a la adopción. En pilotos, Suecia subraya la necesidad de ajustes legales para compatibilizar DLT con confidencialidad financiera; los ensayos transfronterizos (Jura/Dunbar) acreditan viabilidad técnica, pero la gobernanza de datos entre jurisdicciones es el "cuello de botella".

En conjunto, una CBDC con garantías verificables como:

1. límites claros de acceso a la información,

2. auditoría independiente y reglas de mínima compartición de datos,

3. que además ofrezca experiencias "similares al dinero en efectivo" en pagos de bajo riesgo

4. e integre a comercios y pagos a públicos; es la que tiene mayores probabilidades de adopción sostenible. Sin cumplir dichas características, incluso soluciones técnicamente sólidas corren el riesgo de ser percibidas como instrumentos de vigilancia, con baja intensidad de uso y beneficios limitados frente a los medios de pago existentes.

6. Referencias

AFI Global. (2025, 17 de febrero). Central bank digital currency: Lessons from The Bahamas. https://acortar.link/rvHD7d

Annathurai, A., Abdul Wahab, N. y Jamil, N. S. (2024). A review on governance principles of cross-border Central Bank digital currency interoperability: A case study of Project Dunbar. *Journal of Governance and Integrity*, *7*(2), 813-819. https://doi.org/10.15282/jgi.7.2.2024.11509

Atlantic Council. (2026). *Central bank digital currency tracker*. Atlantic Council. https://www.atlanticcouncil.org/cbdctracker/

Bahamas Sand Dollar Update. (2024). Sand Dollar circulation and wallet metrics. https://n9.cl/k55ty

Bai, H., Cong, L. W., Luo, M. y Xie, P. (2025). Adoption of central bank digital currencies: Initial evidence from China. *Journal of Corporate Finance*, 91, 102735. https://doi.org/10.1016/j.jcorpfin.2025.102735

Baker, C. (2024). Examining the potential of the JAM-DEX® CBDC to improve financial inclusion in Jamaica. In *Advances in Finance, Accounting, and Economics* (pp. 170-193). IGI Global. https://doi.org/10.4018/979-8-3693-5588-6.ch012

Bank for International Settlements. (2021). CBDCs: An opportunity for the monetary system. BIS. https://www.bis.org/publ/arpdf/ar2021e3.pdf

Bank of Canada. (2025). *Privacy-Enhancing technologies for CBDC solutions*. Bank of Canada. https://www.bankofcanada.ca/2025/01/staff-discussion-paper-2025-1/

Bank of England. (2023). *The digital pound: a new form of money for households and businesses?* Bank of England. https://acortar.link/FAUOMZ

Bank of Jamaica. (2025, 16 de enero). CBDC FAQs. https://boj.org.jm/core-functions/currency/cbdc/cbdc-faqs/

Beja, A. y Correia Barradas, B. (2023). Central bank digital currency: a focus on anonymity. In *Information Technology and Law Series* (pp. 107-124). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-579-9_7

Bijlsma, M., van der Cruijsen, C., Jonker, N. y Reijerink, J. (2023). What triggers consumer adoption of Central Bank Digital Currency? *Journal of Financial Services Research*, *65*(1), 1–40. https://doi.org/10.1007/s10693-023-00420-8

BOFIT – Bank of Finland Institute for Emerging Economies. (2023). China's e-CNY pilots and use cases. https://www.bofit.fi/en/monitoring/weekly/2023/vw202328_1/

Bordo, M. D. (2022). Central bank digital currency in historical perspective: another crossroad in monetary history. *Capitalism: A Journal of History and Economics*, *3*(2), 421-442. https://doi.org/10.1353/cap.2022.0015

Bruegel. (2025, 1 de junio). On the digital euro holding limits. https://www.bruegel.org/analysis/digital-euro-holding-limits

Carvalho Silva, E. y Mira da Silva, M. (2025). Central bank digital currency: a multivocal literature review. *Journal of Internet and Digital Economics*. https://doi.org/10.1108/jide-03-2024-0013

CBDC Tracker. (2024). Nigeria eNaira usage statistics. https://www.atlanticcouncil.org/cbdctracker/

CBDC Tracker. (2026). *CBDC tracker*. Today's Central Bank Digital Currencies Status. https://cbdctracker.org/

Central Bank of Nigeria. (2021, octubre). Design paper for the eNaira [Documento técnico]. https://n9.cl/uaq2rt

Ceylan, F. (2024). A review of central bank digital currency: Current status and changing trends. *İzmir İktisat Dergisi*, *39*(2), 568-589. https://doi.org/10.24988/ije.1422562

Chukwuere, J. E. (2021). The eNaira - Opportunities and challenges. *Journal of Emerging Technologies*, *1*(1), 72-77. https://doi.org/10.57040/jet.v1i1.92

CNIL. (2023, 11 de diciembre). Digital euro: What is at stake for privacy and personal data protection? https://n9.cl/efqu4

CoinGeek. (2025). Bahamas Sand Dollar adoption and merchant onboarding. https://coingeek.com/bahamas-to-force-banks-to-support-its-cbdc/

Cotugno, M., Manta, F., Perdichizzi, S. y Stefanelli, V. (2024). Ready for a digital Euro? Insights from a research agenda. *Research in International Business and Finance*, 67, 102117. https://doi.org/10.1016/j.ribaf.2023.102117

DaCosta, V. (2024, 14 de enero). JAM-DEX: Jamaica's central bank digital currency. https://acortar.link/Q0ls6l

Digital Euro Association. (2023, 22 de junio). Lessons from the first implemented CBDC: The Sand Dollar. https://digital-euro-association.de/blog/lessons-from-the-sand-dollar

eNaira. (2023, 30 de junio). Design Paper. https://enaira.gov.ng/design-paper/

European Central Bank. (2019). Exploring anonymity in central bank digital currencies. (Occasional Paper Series).

European Central Bank. (2024). Digital euro and privacy. https://acortar.link/9XkXhU

European Central Bank. (2024, 2 de diciembre). Progress on the preparation phase of a digital euro. https://acortar.link/4TACr4

European Central Bank. (2025, October 30). *Progresos en el euro digital*. European Central Bank. https://www.ecb.europa.eu/euro/digital_euro/progress/html/index.es.html

European Commission. (2021, 31 de diciembre). Binding Corporate Rules (BCR). https://n9.cl/rfcc9

European Data Protection Supervisor. (2023, 29 de marzo). TechDispatch #1/2023 – Central bank digital currency (pp. 1–12). https://n9.cl/i3svs

European Parliament. (2023). A legal framework for the digital euro (PE 741.518). Economic Governance and EMU Scrutiny Unit. https://n9.cl/3iim4

Fantacci, L. y Gobbi, L. (2021). Stablecoins, central bank digital currencies and US dollar hegemony. *Accounting, Economics, and Law: A Convivium*, *14*(2), 173-200. https://doi.org/10.1515/ael-2020-0053

Fernández, M. Á. E., Bas, D. S. y Alonso, Y. S. L. N. (2025). Un análisis de las divisas virtuales centralizadas (CBDC) y de la propuesta del euro digital. *REVISTA PROCESOS DE MERCADO*, 283-300. https://doi.org/10.52195/pm.v22i1.1015

Guo, S., Kreitem, J. y Moser, T. (2024). Dlt options for cbdc1. *Journal of Central Banking Theory and Practice*, *13*(1), 57-88. https://doi.org/10.2478/jcbtp-2024-0004

Huang, J. (2025). *Impact assessment of digital currency pilot programs on regional financial stability: A difference-in-differences model analysis based on 15 pilot cities in china*. Elsevier BV. https://doi.org/10.2139/ssrn.5853935

Human Rights Foundation. (2024). CBDC Tracker: Bahamas Sand Dollar. https://cbdctracker.hrf.org/currency/the-bahamas

Indira, R., Alamsyah, A. y Yunita, I. (2025). Central bank digital currencies: A technical exploration of infrastructure, access, and crossborder models. *2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, 264-269. https://doi.org/10.1109/iaict65714.2025.11100853

Inozemtsev, M. I. y Nektov, A. V. (2022). Digital platforms for cross-border settlement of CBDC. In *The Platform Economy* (pp. 131-145). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3242-7_9

Intereconomics. (2023). The evolution of Sand Dollar. https://n9.cl/jmwl49

International Monetary Fund. (2024). Central Bank Digital Currency: Data use and privacy protection (Fintech Note 2024/004). https://n9.cl/37cb3

Jabbar, A., Geebren, A., Hussain, Z., Dani, S. y Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, *64*, 101826. https://doi.org/10.1016/j.ribaf.2022.101826

Jamaica Information Service. (2024). JAM-DEX adoption figures. https://n9.cl/gthfr

Julin, E. (2022). The Swedish e-krona: A means of guaranteeing the possibility of making payments for all. In *Central Banking, Monetary Policy and the Future of Money* (pp. 187-208). Edward Elgar Publishing. https://doi.org/10.4337/9781800376403.00014

Kiff, J. (2026, February 10). *Jurisdictions where retail CBDC is being explored*. Kiffmeister Chronicles. https://acortar.link/0gCVIQ

Kaur, G. (2024). Privacy implications of central bank digital currencies (CBDCs): A systematic review of literature. *EDPACS*, *69*(9), 87-123. https://doi.org/10.1080/07366981.2024.2376794

Kshetri, N. y Loukoianova, E. (2022). Data privacy considerations for central bank digital currencies in Asia–Pacific countries. *Computer*, *55*(3), 95-100. https://doi.org/10.1109/mc.2022.3141228

Laboure, M., H. P. Müller, M., Heinz, G., Singh, S. y Köhling, S. (2021). Cryptocurrencies and CBDC: the route ahead. *Global Policy*, *12*(5), 663-676. https://doi.org/10.1111/1758-5899.13017

Ledger Insights. (2023, 13 de abril). Sweden's e-krona project explores freedom of payment providers. https://acortar.link/O9QMAQ

Ledger Insights. (2024). JAM-DEX adoption, wallets and incentives. https://www.ledgerinsights.com/jamaica-cbdc-incentivize-merchants-jam-dex/

Nairametrics. (2024, 20 de julio). eNaira makes up less than 1% of currency in circulation https://nairametrics.com/

Náñez Alonso, S. L., Echarte Fernández, M. Á., Sanz Bas, D. y Kaczmarek, J. (2020). Reasons fostering or discouraging the implementation of central bank-backed digital currency: a review. *Economies*, *8*(2), 41. https://doi.org/10.3390/economies8020041

Náñez Alonso, S. L., Ozili, P. K., Hernández, B. M. S. y Pacheco, L. M. (2025). Evaluating the acceptance of CBDCs: Experimental research with artificial intelligence (AI) generated synthetic response. *Quantitative Finance and Economics*, *9*(1), 242-273. https://doi.org/10.3934/qfe.2025008

Napieralska, A. y Kępczyński, P. (2024). Balancing transparency and privacy in central bank digital currencies (CBDCs). En *Advances in Finance, Accounting, and Economics* (pp. 208-223). IGI Global. https://doi.org/10.4018/979-8-3693-1882-9.ch013

Ozili, P. K. (2022). CBDC, Fintech and cryptocurrency for financial inclusion and financial stability. *Digital Policy, Regulation and Governance*, *25*(1), 40-57. https://doi.org/10.1108/dprg-04-2022-0033

Ozili, P. K. y Alonso, S. L. N. (2024). Central bank digital currency adoption challenges, solutions, and a sentiment analysis. *Journal of Central Banking Theory and Practice*, *13*(1), 133-165. https://doi.org/10.2478/jcbtp-2024-0007

People's Bank of China. (2022). Progress of research & development of E-CNY in China. http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/index.html

Pocher, N. y Veneris, A. (2021). Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–9. https://doi.org/10.1109/icbc51069.2021.9461090

Raskin, M. y Yermack, D. (2018). Digital currencies, decentralized ledgers and the future of central banking. In *Research Handbook on Central Banking*. Edward Elgar Publishing. https://doi.org/10.4337/9781784719227.00028

Sanctionscanner. (2025). Digital yuan adoption metrics. https://n9.cl/mr6xg

Santaolalla Montoya, C. (2024). Bitcoin vs CBDC. *CUADERNOS DE DERECHO TRANSNACIONAL*, *16*(1), 578-602. https://doi.org/10.20318/cdt.2024.8436

Shafranova, K., Navolska, N. y Koldovskyi, A. (2024). Navigating the digital frontier: A comparative examination of Central Bank Digital Currency (CBDC) and the Quantum Financial System (QFS). *SocioEconomic Challenges*, *8*(1), 90-111. https://doi.org/10.61093/sec.8(1).90-111.2024

Sisodia, H. (2024). Case study on the Sand Dollar CBDC of the Bahamas. In *Advances in Finance, Accounting, and Economics* (pp. 298-314). IGI Global. https://doi.org/10.4018/979-8-3693-1882-9.ch018

Sveriges Riksbank. (2023). E-krona pilot. https://n9.cl/b6rjw

The Payments Association. (2024, 16 de septiembre). How CBDCs can enhance cross-border inefficiencies. https://acortar.link/YWiOxp/

Themistocleous, M., Rupino da Cunha, P., Tabakis, E. y Papadaki, M. (2023). Towards cross-border CBDC interoperability: Insights from a multivocal literature review. *Journal of Enterprise Information Management*, *36*(5), 1296-1318. https://doi.org/10.1108/jeim-11-2022-0411

Tronnier, F. y Qiu, W. (2024). How do privacy concerns impact actual adoption of central bank digital currency? An investigation using the e-CNY in China. *Quantitative Finance and Economics*, *8*(1), 126-152. https://doi.org/10.3934/qfe.2024006

Tronnier, F., Harborth, D. y Biker, P. (2023). Applying the extended attitude formation theory to central bank digital currencies. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00638-3

Tronnier, F., Harborth, D. y Hamm, P. (2022). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, 53, 101158. https://doi.org/10.1016/j.elerap.2022.101158

Vessio, M. y Adekunbi, A. (2024). Central bank digital currencies (CBDCs): Exploring "technical privacy" through the lens of Nigeria's eNaira. Annual Banking Law Update 2024, Centre for Banking Law, University of Johannesburg. https://centaur.reading.ac.uk/118963/

Wang, H. y Gao, S. (2023). The future of the international financial system: The emergingCBDCnetwork and its impact on regulation. *Regulation & Governance*, *18*(1), 288-306. https://doi.org/10.1111/rego.12520

Wenker, K. (2022). Retail central bank digital currencies (CBDC), disintermediation and financial privacy: the case of the Bahamian Sand Dollar. *FinTech*, *1*(4), 345-361. https://doi.org/10.3390/fintech1040026

Yousaf, I. y Goodell, J. W. (2023). Linkages between CBDC and cryptocurrency uncertainties, and digital payment stocks. *Finance Research Letters*, 54, 103765. https://doi.org/10.1016/j.frl.2023.103765

Zafar, A. (2026). Privacy as institutional design: A legal-technological analysis of CBDC governance and compliance. *Computer Law & Security Review*, 60, 106258. https://doi.org/10.1016/j.clsr.2025.106258

Zhu, Z. y Zhou, X. (2025). How does digital RMB encourage enterprises' oversea investment behaviors? Evidence from the pilot project of e-CNY. *Finance Research Letters*, 108877. https://doi.org/10.1016/j.frl.2025.108877

CONTRIBUCIONES DE AUTORES/AS, FINANCIACIÓN Y AGRADECIMIENTOS

Contribuciones de los autores:

Conceptualización: Náñez Alonso, Sergio Luis; **Validación:** García González, Pablo; Náñez Alonso, Sergio Luis**; Análisis formal:** García González, Pablo; **Curación de datos:** García González, Pablo**; Redacción-Preparación del borrador original:** García González, Pablo; Náñez Alonso, Sergio Luis**; Redacción-Revisión y Edición:** Náñez Alonso, Sergio Luis**; Visualización:** Náñez Alonso, Sergio Luis**; Supervisión:** Náñez Alonso, Sergio Luis**.**
Todos los autores han leído y aceptado la versión publicada del manuscrito: García González, Pablo; Náñez Alonso, Sergio Luis.

Financiación: Esta investigación no recibió financiación externa.

Agradecimientos: Los autores quieren agradecer a la UCAV por su apoyo en la ejecución de esta investigación.

Conflicto de intereses: Los autores declaran que no existe ningún conflicto de interés.

AUTOR/ES:

Pablo García González
Universidad Católica Santa Teresa de Jesús de Ávila, España y Deutsche Bank AG, España.

Pablo García González es Graduado en Derecho por la Universidad Católica de Ávila (2025), es estudiante del Grado en Administración y Dirección de Empresas en dicha universidad. Actualmente ejerce de becario de banca comercial en Deutsche Bank AG.
pablo.garcia-gonzalez@db.com

Sergio Luis Náñez Alonso
Universidad Católica Santa Teresa de Jesús de Ávila, España.

Sergio Náñez Alonso es Doctor en Derecho y Economía por la Universidad CEU-San Pablo (2019), sobresaliente Cum Laude por unanimidad. Acreditado en las figuras de Profesor Contratado Doctor, Profesor de Universidad Privada y Profesor Ayudante Doctor por ANECA desde el 26 de marzo de 2021; y desde el 26 de Febrero de 2026, Profesor Titular de Universidad por ANECA. Posee un sexenio de investigación reconocido (periodo 2019-2024) por CNEAI-ANECA.
sergio.nanez@ucavila.es

Índice H: 20
Orcid ID: https://orcid.org/0000-0001-5353-2017
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57216823311
Google Scholar: https://scholar.google.es/citations?user=JgLRs5oAAAAJ&hl=es
ResearchGate: https://www.researchgate.net/profile/Sergio-Nanez-Alonso?ev=hdr_xprf