ÑEQUE. Revista de Investigación en Ciencias Administrativas Sociales
Volumen 9 / N° 24 / mayo-agosto 2026
https://doi.org/10.33996/revistaneque.v9i24.225

Artículo de revisión

Soberanía monetaria, privacidad y eficiencia financiera en la era de las monedas digitales de banco central: revisión bibliográfica

Monetary sovereignty, privacy, and financial efficiency in the era of central bank digital currencies: An integrative literature review

Simón Bolívar Parrales-Escalante[a] **Paco Egdon Granoble Chancay**[b]

Tatiana Mercedes Troya Reyes[c] **Luis Armando Vinces Menéndez**[d]

Alexis Javier Villegas Rivera[e]

[a]Universidad de Guayaquil. Guayaquil, Ecuador. Correo: simon.parralese@ug.edu.ec Ocid: https://orcid.org/0000-0002-1372-533X

[b]Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador. Correo: paco.granoble@unesum.edu.ec Orcid: https://orcid.org/0000-0001-6690-4916

[c]Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador. Correo: troya-tatiana9652@unesum.edu.ec Orcid: https://orcid.org/0009-0000-1697-6188

[d]Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador. Correo: vinces-luis1654@unesum.edu.ec Orcid: https://orcid.org/0009-0008-0052-1443

[e]Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador. Correo: villegas-alexis3711@unesum.edu.ec Orcid: https://orcid.org/0009-0001-2050-8691

Cómo citar: Parrales-Escalante, S. B., Granoble Chancay, P. E., Troya Reyes, T. M., Vinces Menéndez, L. A., & Villegas Rivera, A. J. (2026). Soberanía monetaria, privacidad y eficiencia financiera en la era de las monedas

Resumen

La digitalización de los pagos ha desplazado la discusión sobre la soberanía monetaria desde la emisión formal de moneda hacia el diseño institucional, tecnológico y regulatorio de las infraestructuras financieras. Este artículo analiza la relación entre soberanía monetaria, privacidad y eficiencia financiera en el contexto de las monedas digitales de banco central (CBDC), las stablecoins y los pagos transfronterizos. Se desarrolló una revisión bibliográfica integrativa, basada en las referencias del manuscrito original y en una actualización de diez fuentes académicas con identificador DOI, verificadas en Crossref y en páginas editoriales. El análisis se organizó mediante cuatro dimensiones: control público de la unidad de cuenta, protección de datos y trazabilidad, intermediación y estabilidad financiera, e interoperabilidad de pagos. Los resultados muestran que una CBDC no fortalece automáticamente la soberanía monetaria; su contribución depende de que preserve la confianza en la moneda nacional, limite la sustitución monetaria, asegure una gobernanza de datos proporcional y evite desintermediar de forma abrupta al sistema bancario. La privacidad no equivale a anonimato absoluto: requiere mecanismos escalonados, minimización de datos, separación funcional de información e intervención bajo garantías jurídicas. La eficiencia financiera, por su parte, debe evaluarse más allá de la velocidad de liquidación, incorporando costos de cumplimiento, resiliencia operacional, competencia, inclusión y estabilidad. Se concluye que la compatibilidad entre soberanía, privacidad y eficiencia constituye un problema de diseño público. Para las economías emergentes, una arquitectura de CBDC intermediada, interoperable y regulada puede ampliar la capacidad estatal sin convertir los pagos en un dispositivo de vigilancia ni agravar riesgos de fuga de depósitos.

Palabras clave: CBDC; Eficiencia financiera; Moneda digital de banco central; Privacidad financiera; Soberanía monetaria; Stablecoins

Abstract

The digitalization of payments has shifted the discussion on monetary sovereignty from the formal issuance of currency to the institutional, technological, and regulatory design of financial infrastructures. This article analyzes the relationship among monetary sovereignty, privacy, and financial efficiency in the context of central bank digital currencies (CBDCs), stablecoins, and cross-border payments. An integrative literature review was conducted, based on the references of the original manuscript and an update of ten academic sources with DOI identifiers, verified in

digitales de banco central: revisión bibliográfica. *Revista Ñeque.Vol.9*(24).1-1.15 https://doi.org/10.33996/revistaneque.v9i24.225

Crossref and editorial pages. The analysis was organized into four dimensions: public control of the unit of account, data protection and traceability, intermediation and financial stability, and payment interoperability. The results indicate that a CBDC does not automatically strengthen monetary sovereignty; its contribution depends on preserving confidence in the national currency, limiting currency substitution, ensuring proportional data governance, and avoiding abrupt disintermediation of the banking system. Privacy is not equivalent to absolute anonymity: it requires tiered mechanisms, data minimization, functional separation of information, and intervention under legal guarantees. Financial efficiency, for its part, must be evaluated beyond settlement speed, incorporating compliance costs, operational resilience, competition, inclusion, and stability. It is concluded that the compatibility among sovereignty, privacy, and efficiency constitutes a public design problem. For emerging economies, an intermediated, interoperable, and regulated CBDC architecture can expand state capacity without transforming payments into a surveillance tool or exacerbating deposit flight risks.

Keywords: CBDC; Financial efficiency; Central bank digital currency; Financial privacy; Monetary sovereignty; Stablecoins

Introducción

En primer lugar, la transformación digital ha reconfigurado las condiciones bajo las cuales se emite, circula, usa y supervisa el dinero. Durante buena parte del siglo XX, el debate monetario se concentró en la facultad estatal de definir la unidad de cuenta, emitir signos monetarios y conducir la política monetaria. Sin embargo, el avance de plataformas digitales, criptoactivos, stablecoins, mecanismos de pago instantáneo y redes transfronterizas ha trasladado una parte relevante de esa discusión hacia la arquitectura de los sistemas de pago. La cuestión ya no es únicamente quién emite dinero, sino también quién controla los datos que producen los pagos, qué reglas rigen la interoperabilidad, qué instituciones soportan la liquidación y cómo se distribuyen los riesgos entre banco central, intermediarios y usuarios.

En este contexto, la soberanía monetaria conserva una dimensión jurídica y política, pero adquiere una dimensión infraestructural decisiva. Cruz et al. (2021) la vinculan con la unidad de cuenta, la emisión pública, el cumplimiento de obligaciones con la moneda nacional y la menor dependencia de pasivos externos. Estos criterios deben complementarse con el control de interfaces de pago y datos transaccionales. Paredes (2019) interpreta la moneda como un vínculo social de confianza y obligaciones, mientras que Valdés (2022) relaciona la soberanía con la condición política de ciudadanía. Así, la pérdida de control puede producirse cuando los agentes dejan de usar la moneda nacional como referencia de pagos, ahorro y obligaciones.

Además, la complejidad se observa en economías dolarizadas, áreas monetarias supranacionales y países con circulación de facto de monedas externas. Bruchanski (2024) destaca que el dinero soberano articula capacidad institucional, confianza pública y regla jurídica, no solo billetes. Ecuador y El Salvador, dolarizados oficialmente, y la eurozona ilustran configuraciones distintas. Los instrumentos digitales vuelven más porosas esas fronteras porque las plataformas pueden organizar la aceptación de monedas fuera del marco regulatorio doméstico.

Asimismo, Martino (2024) advierte que el dinero privado digital desafía la soberanía aun sin sustituir de inmediato al dinero público. Las stablecoins pueden integrarse con redes de pago, comercio y activos tokenizados; por ello, la cuestión es qué reglas permiten

innovación sin erosionar la unidad de cuenta, fragmentar liquidez o transferir datos financieros estratégicos a actores privados.

Por otra parte, las CBDC son una respuesta posible: dinero digital emitido como pasivo del banco central. Monsalve (2025) contrapone su función de soberanía a la lógica de confianza privada de las stablecoins, pero la distinción es insuficiente. Las CBDC pueden ser minoristas o mayoristas, basadas en cuentas o tokens, directas, híbridas o intermediadas, con diversos límites y reglas. La evaluación debe atender al diseño, no a la etiqueta.

A su vez, la literatura reciente enfatiza que una CBDC implica compensaciones. Agur et al. (2022) muestran que las preferencias de los usuarios por anonimato y seguridad influyen en la demanda de medios de pago y que una CBDC puede modificar la variedad de instrumentos existente, la intermediación bancaria y la provisión de crédito. Keister y Sanches (2023) llegan a una conclusión complementaria: la moneda digital puede mejorar la eficiencia del intercambio, pero también desplazar depósitos bancarios, elevar costos de fondeo y reducir la inversión si compite directamente con la intermediación privada. Esto obliga a abandonar la idea de que la digitalización del dinero es, por sí misma, una reforma neutral. Cada decisión sobre acceso, remuneración, límites y privacidad produce efectos distributivos, prudenciales y políticos.

De manera complementaria, el segundo eje es la privacidad. A diferencia del efectivo, los pagos digitales pueden asociarse con identidad, ubicación y hábitos. Murphy et al. (2024) advierten riesgos de filtraciones, abusos y transferencias de información, y Dionisópoulos et al. (2024) identifican la falta de privacidad como costo de adopción. La respuesta no es anonimato ilimitado, sino privacidad proporcional, verificable y compatible con controles de integridad financiera.

En este sentido, Soana y de Arruda (2024) formulan este asunto como un nuevo equilibrio entre integridad financiera y trazabilidad. El efectivo ofrece una privacidad predeterminada que protege al individuo frente a intrusiones estatales y privadas, pero los sistemas digitales pueden centralizar los registros y expandir la capacidad de observación. Kaur (2024), a partir de una revisión sistemática de la literatura, identifica preocupaciones recurrentes sobre la recolección extensa de datos, la retención de información por bancos centrales y la complejidad operacional de los modelos intermediados. Ahnert et al. (2025) resaltan, además, que la privacidad es un factor competitivo en la economía digital, debido a que la información de pagos puede reforzar posiciones de mercado de plataformas y condicionar el acceso a servicios de crédito o comercio.

Finalmente, el tercer eje es la eficiencia financiera, que comprende asignación de recursos, continuidad, competencia, accesibilidad, cumplimiento, prevención de fraude y estabilidad, además de velocidad y costo. Medina (2023) recuerda que las stablecoins se usan sobre todo en criptoactivos, pese a su potencial para pagos reales. Mena et al. (2024) subrayan que su estabilidad depende de respaldo, solvencia, redención y controles tecnológicos; rapidez no elimina riesgos de contraparte, ciberseguridad u opacidad.

En primer lugar, la relación entre soberanía, privacidad y eficiencia es crítica en pagos transfronterizos. Chu y Rathbun (2025) sostienen que los modelos de interoperabilidad condicionan la gestión de flujos de capital y la autonomía regulatoria. Aunque las plataformas comunes reducen fricciones, deben preservar reglas jurisdiccionales. Pérez

Cárdenas (2025) coincide en la necesidad de pagos que combinen seguridad de datos, confianza y eficiencia.

En este contexto, el objetivo del estudio es analizar cómo se articulan soberanía monetaria, privacidad financiera y eficiencia en la literatura sobre CBDC, stablecoins y pagos digitales. El artículo integra las citas originales con evidencia académica reciente bajo una estructura IMRDC. Su argumento central es que una CBDC solo puede reforzar capacidades públicas si se gobierna con proporcionalidad, competencia, resiliencia, protección de datos e interoperabilidad regulada. No recomienda su adopción inmediata en un país específico; ofrece criterios para evaluar ventajas y riesgos.

Método

Metodológicamente, se realizó una revisión bibliográfica integrativa, cualitativa y trazable. Arias (2023) entiende la investigación documental como búsqueda, recuperación, análisis e interpretación de datos secundarios; en consecuencia, este estudio no pretende ser una revisión sistemática ni un metaanálisis, sino una síntesis crítica de literatura heterogénea sobre dinero digital, privacidad y eficiencia. El corpus inicial fue el conjunto de dieciséis referencias del manuscrito original. Para conservarlas y elevar la solidez del texto se añadieron diez artículos con DOI, cuyos metadatos se verificaron en Crossref y, cuando fue posible, en páginas editoriales.

La búsqueda utilizó los términos “soberanía monetaria”, “CBDC”, “privacidad financiera”, “eficiencia de pagos”, “stablecoins”, “interoperabilidad” y “estabilidad financiera”, en español e inglés. Se conservaron los antecedentes localizados en Redalyc, Dialnet y Google Académico, y se priorizaron para la ampliación estudios de 2019-2026 directamente pertinentes, con identificación bibliográfica suficiente y DOI verificable. Se excluyeron duplicados y trabajos sin relación sustantiva con las dimensiones analíticas. Las fuentes originales no arbitradas se mantuvieron por integridad textual, pero se interpretaron con menor peso probatorio.

Para el análisis, las fuentes se codificaron en cuatro categorías: soberanía monetaria; privacidad y gobernanza de datos; eficiencia y arquitectura de pagos; y estabilidad e intermediación financiera. Se contrastaron convergencias y tensiones entre aportes conceptuales, jurídicos, tecnológicos y empíricos, y se elaboró una síntesis orientada a economías emergentes. La tabla 1 resume las dimensiones empleadas.

Tabla 1. *Dimensiones de análisis, preguntas orientadoras, indicadores examinados y fuentes representativas.*

Dimensión de análisis	Pregunta orientadora	Indicadores o elementos examinados	Fuentes representativas
Soberanía monetaria	¿La infraestructura de pagos preserva la unidad de cuenta y la capacidad de política pública?	Emisión pública, aceptación de moneda nacional, sustitución monetaria, gestión de flujos de capital	Cruz et al. (2021); Martino (2024); Chu y Rathbun (2025)

Dimensión de análisis	Pregunta orientadora	Indicadores o elementos examinados	Fuentes representativas
Privacidad e integridad	¿Los datos de pago se usan de manera proporcional y con garantías?	Minimización de datos, trazabilidad, controles AML/CFT, separación de funciones, ciberseguridad	Murphy et al. (2024); Kaur (2024); Soana y de Arruda (2024)
Eficiencia financiera	¿El sistema reduce fricciones sin trasladar riesgos excesivos a usuarios o intermediarios?	Tiempo de liquidación, costos, competencia, inclusión, resiliencia y cumplimiento	Agur et al. (2022); Ahnert et al. (2025); Pérez Cárdenas (2025)
Estabilidad e intermediación	¿El diseño evita desintermediación abrupta y riesgo de corridas?	Límites, remuneración, acceso, liquidez bancaria, monitoreo prudencial	Kumhof y Noone (2021); Keister y Monnet (2022); Luu et al. (2023)

Por último, la triangulación distinguió aportes conceptuales sobre dinero y soberanía, análisis de diseño y regulación de CBDC, y evidencia empírica o institucional sobre estabilidad, privacidad y pagos. Esta separación evita presentar coincidencias teóricas como pruebas causales y conserva trazabilidad entre afirmaciones y fuentes.

Resultados

La soberanía monetaria digital no se reduce al monopolio de emisión. La moneda es unidad de cuenta, medio de pago, reserva de valor e institución de confianza. Cruz et al. (2021) vinculan la soberanía con decidir la unidad de cuenta y recaudar en moneda nacional; Paredes (2019) la entiende como vínculo social de derechos, deberes y expectativas. Por ello, las monedas privadas pueden tener efectos políticos aun sin sustituir formalmente a la oficial.

Asimismo, el espacio monetario es más competitivo. Martino (2024) entiende el dinero privado digital como fuente simultánea de eficiencia y riesgo soberano. Las stablecoins pueden facilitar pagos, pero también desplazar de facto la denominación de precios, ahorros o contratos y debilitar información, transmisión monetaria y capacidad de respaldo del banco central.

A continuación, la diferencia entre soberanía formal y efectiva es decisiva. Un Estado puede emitir moneda, pero no lograr su adopción digital. Bruchanski (2024) destaca que el dinero soberano depende de legitimidad y confianza; una CBDC debe ofrecer una ventaja clara frente a aplicaciones privadas y disponibilidad en contingencias.

De manera complementaria, la dolarización oficial y la sustitución informal son contextos distintos. En el primer caso se limita emisión y política cambiaria, aunque subsisten responsabilidades de regulación, inclusión e infraestructura; en el segundo, el desafío es sostener la credibilidad de la unidad de cuenta. La digitalización puede reforzar el uso del dinero nacional o acelerar la sustitución por instrumentos externos.

Además, Chu y Rathbun (2025) muestran que la interoperabilidad transfronteriza no es puramente técnica: determina reglas de acceso, gestión de capital e intercambio de

información. Puede reducir costos, pero una integración sin controles puede dificultar decisiones macroprudenciales. Las economías emergentes requieren gobernanza, localización de datos y responsabilidades de supervisión explícitas.

En este sentido, las stablecoins movilizan valor fuera de la banca tradicional (Monsalve, 2025), pero sus efectos dependen de respaldo, redención y concentración del emisor. Mena et al. (2024) advierten que reservas opacas, insuficientes o ilíquidas deterioran la confianza; la estabilidad depende de activos, derechos de rescate y credibilidad regulatoria.

Por otra parte, Medina (2023) observa que las stablecoins se usan principalmente en criptoactivos, pese a su potencial para pagos reales. La rapidez de una red no asegura aceptación masiva, protección al consumidor, resolución de fraude ni conversión a dinero bancario. La eficiencia debe evaluarse en todo el ciclo transaccional, incluidos riesgos y cumplimiento.

Como síntesis, la tabla 2 sintetiza los riesgos de las stablecoins preservados en el texto original y los relaciona con respuestas de política que se desprenden de la literatura reciente.

Tabla 2. *Riesgos y desafíos de las stablecoins: manifestaciones, implicaciones y respuestas de diseño o regulación.*

Riesgo o desafío	Manifestación en stablecoins	Implicación para soberanía, privacidad o eficiencia	Respuesta de diseño o regulación
Regulación y cumplimiento	Reglas fragmentadas o ausencia de supervisión homogénea	Incertidumbre jurídica, arbitraje regulatorio y menor protección del usuario	Requisitos de autorización, transparencia y coordinación transfronteriza
Riesgo de contraparte	Reservas insuficientes, ilíquidas u opacas; fallas de redención	Pérdida de confianza, ventas aceleradas y transmisión de tensión al sistema	Auditoría de reservas, activos elegibles y derechos claros de rescate
Riesgo tecnológico	Ataques, fallas de código, claves comprometidas o interrupciones	Pérdidas, indisponibilidad de pagos y exposición de datos	Ciberresiliencia, continuidad de negocio, pruebas y responsabilidad operativa
Riesgo de datos	Explotación comercial o uso indebido de información transaccional	Afectación de privacidad, discriminación y concentración de poder informacional	Minimización de datos, finalidad limitada y controles de acceso
Riesgo de sustitución monetaria	Predominio de unidades externas en pagos y ahorro digital	Menor eficacia de la política monetaria y fragmentación de liquidez	Interoperabilidad con dinero público, reglas de conversión y supervisión prudencial

Nota. Elaboración propia con base en Mena et al. (2024), Medina (2023), Martino (2024) y Soana y de Arruda (2024).

A partir de este hallazgo, la CBDC aparece, por tanto, como una alternativa para modernizar el dinero público y preservar un ancla de confianza en un mercado de pagos crecientemente digital. Legal et al. (2022) plantean que una moneda digital de banco

central puede apoyar la inclusión financiera, disminuir la dependencia del efectivo y fortalecer la eficiencia de los pagos, siempre que su introducción sea compatible con la estabilidad financiera y la política monetaria. No obstante, los resultados de la revisión no permiten afirmar que una CBDC deba sustituir al efectivo ni que deba adoptar un modelo universal. La elección entre una CBDC mayorista y una minorista, basada en tokens o en cuentas, directa o intermediada, incide de forma decisiva sobre riesgos y beneficios.

En segundo término, Agur et al. (2022) proponen que las preferencias heterogéneas de los usuarios respecto de anonimato y seguridad son centrales para el diseño. En su modelo, una CBDC semejante a los depósitos puede competir con el financiamiento bancario y contraer el crédito, mientras que una CBDC similar al efectivo puede desplazar a este último debido a efectos de red. El hallazgo tiene dos consecuencias. Primero, la privacidad debe tratarse como una característica funcional que afecta la demanda, no como un añadido posterior. Segundo, la tasa de remuneración, el acceso y la interoperabilidad pueden modificar la intensidad de la competencia entre medios de pago.

Asimismo, Andolfatto (2021) ofrece una visión menos determinista: una CBDC puede presionar a bancos con poder de mercado y ampliar financiamiento mediante mejores tasas e inclusión. El efecto depende de la estructura bancaria y del diseño: puede reducir rentas en sistemas concentrados, pero intensificar tensiones de liquidez en sistemas frágiles.

A continuación, Keister y Sanches (2023) muestran que una CBDC puede mejorar eficiencia, pero desplazar depósitos, encarecer fondeo y afectar inversión. No existe un diseño universal: competir con efectivo difiere de competir con depósitos. La política debe definir si busca inclusión, reducción de costos, competencia, resiliencia o menor sustitución monetaria.

En este sentido, Kumhof y Noone (2021) muestran que diferenciar CBDC y reservas, evitar convertibilidad automática desde depósitos y emitir contra activos elegibles puede mitigar corridas. Estos principios no prohíben dinero público digital; evitan que la arquitectura transforme una pérdida de confianza en fuga instantánea de depósitos.

De manera complementaria, Keister y Monnet (2022) identifican efectos ambiguos: la CBDC ofrece una alternativa segura que puede facilitar retiradas, pero reduce transformación de plazos y permite observar flujos agregados. Esa información puede mejorar supervisión macroprudencial, siempre que opere con límites legales, agregación y acceso restringido, sin vigilancia indiscriminada.

Por otra parte, Luu et al. (2023) encuentran asociaciones entre CBDC, mejores indicadores de estabilidad, menor apalancamiento y expansión del crédito, con efectos heterogéneos por tipo de CBDC y nivel de desarrollo. No es evidencia causal definitiva, pero muestra que capacidad institucional y contexto bancario condicionan los resultados.

En segundo lugar, la privacidad es el segundo núcleo. Murphy et al. (2024) advierten riesgos a lo largo de recolección, almacenamiento, uso, intercambio y eliminación de datos. Concentrar identificadores y registros aumenta exposición a filtraciones y vigilancia; descentralizar por completo puede dificultar protección e integridad. La cuestión es qué datos son necesarios, quién accede y bajo qué autorización.

Asimismo, Dionisópoulos et al. (2024) sostienen que el anonimato absoluto es difícil de conciliar con regulación, pero caben niveles de privacidad: umbrales para bajo valor, revelación judicialmente condicionada y separación entre identidad y transacciones. Agur et al. (2022) muestran que anonimato y seguridad percibidos inciden en la demanda y eficacia de una CBDC.

A continuación, Kaur (2024) identifica riesgos diferenciados: concentración de información en el modelo directo, retención e intercambio en el híbrido, y mayor exposición operacional en el intermediado. Ninguno elimina el problema; las responsabilidades deben distribuirse para usar datos con finalidad legítima, mínima intrusión y sin incentivos comerciales indebidos.

Por otra parte, Soana y de Arruda (2024) entienden privacidad y trazabilidad como una compensación de arquitectura. La proporcionalidad evita tanto disponibilidad total de datos como opacidad completa, y diferencia pagos cotidianos, alto valor, operaciones transfronterizas e investigaciones según diligencia, conservación y autorización de acceso.

En este sentido, la protección de datos también se vincula con competencia y eficiencia. Ahnert et al. (2025) analizan cómo el uso de información de pagos puede reforzar el poder de plataformas digitales y afectar decisiones de crédito, comercio y publicidad. Si un proveedor controla simultáneamente el medio de pago, los datos transaccionales y el acceso a mercados digitales, puede crear barreras de entrada difíciles de superar. Una CBDC o infraestructura pública interoperable podría reducir esas barreras si permite portabilidad, estándares abiertos y límites al uso secundario de los datos. Pero el beneficio no es automático: una arquitectura pública centralizada sin controles sólidos también podría concentrar poder informacional.

En esta materia, el aporte de Liu et al. (2023) debe interpretarse desde su ámbito técnico. Los autores desarrollan mecanismos de agregación resilientes a abandonos para aprendizaje automático que preserva privacidad. Aunque su estudio no analiza CBDC, demuestra que existen herramientas computacionales para generar conocimiento agregado sin exponer todos los datos individuales. En el diseño de dinero digital, técnicas de privacidad diferencial, pruebas criptográficas, agregación segura y separación de bases de datos pueden apoyar supervisión de riesgos y análisis estadístico. La adopción de estas tecnologías, sin embargo, no sustituye a la gobernanza jurídica: los controles técnicos son eficaces únicamente si existen reglas de finalidad, auditoría independiente, gestión de incidentes y responsabilidad institucional.

Asimismo, Larrea y Abad (2025) enfatizan que los modelos de aprendizaje automático aplicados a finanzas plantean tensiones entre innovación, capacidad analítica y privacidad. El punto es particularmente relevante para una CBDC porque la información de pagos puede alimentar modelos de detección de fraude, riesgos crediticios o perfiles de comportamiento. Si tales modelos se implementan sin transparencia, pueden reproducir sesgos, excluir usuarios o ampliar la vigilancia. La eficiencia algorítmica no debe evaluarse solo por precisión predictiva; debe incorporar explicabilidad, no discriminación, gobernanza de datos y mecanismos de reclamo.

De manera complementaria, Ortiz (2025) subraya que la preservación de datos personales es un elemento central de confianza en plataformas digitales. Este principio puede trasladarse al ámbito monetario: la adopción de una CBDC dependerá en buena

medida de que los usuarios perciban que sus transacciones no serán utilizadas para fines ajenos al pago o a la protección legítima del sistema. La privacidad, por consiguiente, cumple una función económica además de jurídica. Reduce la percepción de riesgo, protege la autonomía de los usuarios y evita que la infraestructura de pagos se convierta en una fuente de extracción de valor basada en información.

Por otro lado, la tercera dimensión de resultados se refiere a la eficiencia financiera y a la programabilidad. El manuscrito original menciona tres enfoques para incorporar programación en pagos: integrar la funcionalidad en el libro mayor, añadir un módulo complementario o externalizar funciones a proveedores de servicios. Dionisópoulos et al. (2024) advierten que la programabilidad puede elevar la complejidad y reducir el rendimiento si requiere datos adicionales y cálculos intensivos. A ello se suman cuestiones de gobernanza: ¿quién define las reglas programables?, ¿pueden imponerse restricciones de uso?, ¿qué ocurre ante un error de código?, ¿cómo se protege la neutralidad del dinero?

Respecto de la eficiencia financiera, una distinción es necesaria. La programabilidad de pagos, por ejemplo, automatizar liquidaciones condicionadas, no debe confundirse con la programabilidad del dinero como instrumento que limita unilateralmente dónde, cuándo o para qué puede gastarse. La primera puede reducir costos de conciliación y riesgos de cumplimiento contractual; la segunda puede afectar fungibilidad, libertad económica y confianza. La literatura revisada sugiere que las reglas deberían dirigirse a servicios de pago específicos y estar sometidas a consentimiento, reversibilidad y revisión jurídica, evitando convertir la unidad monetaria en un permiso condicionado por diseño.

En particular, la eficiencia tampoco es equivalente a centralización. Un sistema centralizado puede ofrecer alto rendimiento, pero crear un punto único de falla y un repositorio atractivo para atacantes. Un sistema distribuido puede mejorar resiliencia o trazabilidad en algunos casos, pero aumentar costos de validación y complejidad de coordinación. La decisión tecnológica debe responder a requisitos de volumen, latencia, continuidad operativa, recuperación ante desastres y protección de información, no a preferencias por una tecnología de moda. En esta línea, Legal et al. (2022) consideran que las implicancias de una CBDC para estabilidad y política monetaria deben evaluarse de modo integral, teniendo en cuenta objetivos públicos y restricciones operativas.

Por otra parte, Pérez Cárdenas (2025) vincula la eficiencia de pagos transfronterizos con identidad, privacidad y tecnologías de registro. Esta vinculación es pertinente porque las transferencias internacionales suelen enfrentar fricciones asociadas a múltiples intermediarios, verificaciones duplicadas, normas de cumplimiento y diferencias de horario. Las CBDC interoperables podrían reducir parte de esas fricciones, pero solo si los estándares de identidad y mensajería no obligan a una transferencia indiscriminada de datos entre jurisdicciones. El diseño debe permitir el intercambio de información estrictamente necesaria para el cumplimiento, al tiempo que protege datos personales y secretos comerciales.

Además, la inclusión financiera constituye otra dimensión de eficiencia. No basta con poner a disposición una aplicación digital si los usuarios carecen de conectividad, identificación funcional, alfabetización financiera o dispositivos adecuados. Las políticas de CBDC deberían incorporar opciones de bajo costo, asistencia, canales fuera de línea y compatibilidad con proveedores regulados. Una moneda digital que excluya a grupos rurales, personas mayores o trabajadores informales puede aumentar la eficiencia

promedio de quienes ya están integrados, pero deteriorar la eficiencia social del sistema. La cobertura debe entenderse como condición de legitimidad y no solo como indicador de adopción.

A continuación, los resultados sobre privacidad conducen a un hallazgo adicional: las salvaguardas no son un costo externo a la eficiencia. Un sistema que recolecta datos excesivos puede enfrentar mayores gastos de ciberseguridad, litigios, pérdidas reputacionales y resistencia de usuarios. Del mismo modo, un sistema con controles de identidad innecesariamente rígidos puede excluir a personas de bajos ingresos y dirigir transacciones hacia canales informales. El diseño proporcional reduce esos costos. La eficiencia sostenible surge de equilibrar prevención de riesgos, facilidad de uso y protección de derechos.

De manera complementaria, un cuarto resultado es la necesidad de diferenciar dinero público, dinero bancario y dinero privado digital. La formulación original de que las stablecoins deberían complementar, y no necesariamente competir con, el dinero público puede mantenerse si se entiende como objetivo de política y no como descripción de un resultado automático. Martino (2024) advierte que la regulación debe impedir que las innovaciones privadas erosionen la función de coordinación de la moneda pública. Al mismo tiempo, Andolfatto (2021) y Agur et al. (2022) muestran que la competencia bien diseñada puede disciplinar estructuras de mercado y ampliar las opciones de usuarios. El desafío consiste en establecer un perímetro regulatorio que promueva innovación compatible con seguridad, respaldo, transparencia y defensa de la unidad de cuenta.

Discusión

A partir de estos resultados, la discusión permite interpretar las implicaciones institucionales, regulatorias y de política pública del equilibrio entre soberanía monetaria, privacidad y eficiencia financiera. En lugar de asumir que las innovaciones digitales producen beneficios uniformes, el análisis exige considerar sus efectos sobre la unidad de cuenta, los datos de pago, la intermediación y la resiliencia del sistema.

De manera complementaria, la articulación entre estos instrumentos requiere tres principios. El primero es la interoperabilidad regulada: los usuarios deben poder convertir y mover valor entre sistemas bajo reglas transparentes, sin quedar cautivos de una plataforma. El segundo es equivalencia de riesgos: actividades que cumplen funciones de pago semejantes deben enfrentar exigencias comparables de reservas, gobernanza, protección al consumidor y ciberresiliencia. El tercero es neutralidad competitiva: ni el banco central ni un proveedor privado deberían usar la infraestructura de pagos para imponer ventas vinculadas, extraer datos sin base legítima o bloquear injustificadamente a competidores.

En este sentido, la revisión también revela que la soberanía monetaria se relaciona con la capacidad de respuesta ante crisis. En una economía con pagos digitalizados, la continuidad de la infraestructura es tan importante como la disponibilidad de efectivo. Un apagón, un ciberataque o una falla de telecomunicaciones pueden impedir transacciones básicas incluso si la moneda mantiene su valor legal. Por ello, una CBDC debe ser parte de una estrategia de resiliencia que contemple redundancia, protocolos de contingencia, capacidad de operación fuera de línea, participación de múltiples

proveedores y pruebas periódicas. La dependencia de un único operador tecnológico puede convertirse en vulnerabilidad soberana.

Asimismo, esta preocupación es coherente con la discusión de Murphy et al. (2024) sobre riesgos de fuga y abuso de datos. La ciberseguridad no puede limitarse a la protección de una aplicación móvil; debe cubrir gestión de identidades, claves criptográficas, interfaces de programación, proveedores externos, centros de datos y procesos de actualización. Una vulnerabilidad en cualquiera de esos componentes puede comprometer la confianza en la moneda. La resiliencia operativa debe, por tanto, ser un criterio de eficiencia y soberanía.

Por consiguiente, la evidencia revisada ofrece implicaciones diferenciadas para economías emergentes. Por una parte, estos países pueden obtener beneficios considerables de pagos más baratos, mayor inclusión, competencia y menor dependencia de infraestructuras extranjeras. Por otra, suelen enfrentar restricciones de conectividad, menor capacidad fiscal para absorber fallas, mayor exposición a sustitución monetaria y marcos de protección de datos en consolidación. Chu y Rathbun (2025) advierten que la configuración de redes transfronterizas afecta de manera especial a las economías que necesitan gestionar flujos de capital volátiles. La política de CBDC debe, por tanto, ser gradual, reversible y ajustada a capacidades institucionales reales.

En esta dirección, resulta conveniente pensar en pilotos con objetivos delimitados. Antes de emitir una CBDC de uso general, un banco central podría evaluar casos de uso mayorista, pagos gubernamentales, distribución de ayudas con salvaguardas, liquidación interbancaria o remesas específicas. Cada piloto debe incluir métricas no solo de transacciones procesadas, sino de impacto en inclusión, ciberseguridad, privacidad, costos para intermediarios, fallas operativas y percepción de confianza. La adopción debe justificarse con evidencia y no con la necesidad de seguir una tendencia internacional.

Como criterio integrador, la síntesis permite proponer un marco de evaluación. Una CBDC contribuye a la soberanía cuando refuerza el uso confiable de la unidad de cuenta nacional, preserva la capacidad de aplicar políticas monetarias y macroprudenciales, y evita una dependencia excesiva de infraestructuras externas. Contribuye a la privacidad cuando limita la recolección de datos, separa identificación de detalle transaccional, permite acceso escalonado y somete las excepciones a controles jurídicos. Contribuye a la eficiencia cuando reduce fricciones sin trasladar costos desproporcionados a usuarios, bancos o Estado; mantiene continuidad operativa; favorece competencia; y evita inestabilidad financiera.

Por otra parte, este marco también permite explicar por qué el trinomio no se cumple automáticamente. Una CBDC con trazabilidad absoluta puede facilitar supervisión, pero reducir confianza y aumentar riesgos de abuso. Una CBDC que imite de forma completa el anonimato del efectivo puede proteger privacidad, pero dificultar la gestión de actividades ilícitas. Una CBDC muy atractiva frente a depósitos puede aumentar competencia, pero generar riesgo de desintermediación. El objetivo de la regulación no es eliminar todas las tensiones, sino hacerlas explícitas, distribuirlas de manera legítima y crear mecanismos de corrección.

Finalmente, el debate sobre soberanía monetaria debe reconocer que la confianza no se decreta. La población adoptará dinero público digital si percibe utilidad, seguridad, privacidad razonable y continuidad. La moneda nacional mantendrá su función de

coordinación si el Estado ofrece reglas estables, infraestructura confiable y protección efectiva. Paredes (2019) y Bruchanski (2024) permiten entender que la soberanía es una relación institucional antes que un atributo puramente técnico. Por ello, la digitalización monetaria exige una gobernanza democrática que combine capacidad estatal, derechos individuales y vigilancia regulatoria de los actores privados.

Conclusiones

En síntesis, la revisión confirma que la soberanía monetaria, la privacidad y la eficiencia financiera forman un sistema de interdependencias. La soberanía no se limita a emitir una moneda; depende de que esa moneda conserve su función de unidad de cuenta, medio de pago y referente de confianza dentro de una infraestructura financiera cada vez más digital. Las CBDC pueden contribuir a esta finalidad al ofrecer acceso digital a dinero público, reducir dependencia de plataformas privadas y mejorar la capacidad de supervisión y resiliencia. Sin embargo, sus efectos no son automáticos ni uniformes. El resultado depende del modelo de acceso, la remuneración, los límites de tenencia, la gobernanza de datos, el papel de intermediarios y la interoperabilidad transfronteriza.

Asimismo, la privacidad debe incorporarse como requisito de diseño desde el inicio. El análisis muestra que anonimato y trazabilidad no son categorías excluyentes, sino extremos entre los cuales pueden construirse soluciones escalonadas. La minimización de datos, la separación funcional de información, la revelación condicionada por garantías jurídicas, la auditoría y el uso de técnicas de privacidad computacional son instrumentos que permiten proteger a los usuarios sin abandonar los objetivos de integridad financiera. Una infraestructura que trate todos los pagos como fuente de vigilancia pierde legitimidad y puede desincentivar su adopción.

De manera complementaria, la eficiencia financiera exige una evaluación más amplia que la reducción de tiempo o costo por transacción. Debe incluir estabilidad bancaria, resiliencia operativa, competencia, inclusión, protección al consumidor, costos de cumplimiento y continuidad ante contingencias. La literatura revisada demuestra que una CBDC puede mejorar ciertos resultados, pero también desplazar depósitos o amplificar tensiones si compite de manera inadecuada con la banca. Los principios de diseño orientados a límites, convertibilidad, remuneración y arquitectura intermediada son determinantes para administrar esos riesgos.

Para las economías emergentes, la recomendación analítica es avanzar con una aproximación gradual, basada en pilotos, evaluación pública y proporcionalidad regulatoria. La interoperabilidad con redes transfronterizas puede generar eficiencia, pero no debe sacrificar capacidad de gestión de flujos de capital, jurisdicción sobre datos ni autonomía regulatoria. La coexistencia entre CBDC, dinero bancario, efectivo y soluciones privadas debe organizarse mediante reglas de equivalencia de riesgos, transparencia de reservas, ciberresiliencia y defensa de la unidad de cuenta.

En síntesis, una CBDC no constituye una solución tecnológica aislada, sino una decisión de política monetaria, institucional y democrática. Su potencial para reforzar la soberanía dependerá de que preserve los derechos de las personas, sostenga la estabilidad del sistema y mejore realmente la calidad de los pagos. La agenda futura de investigación debería incorporar estudios empíricos en economías latinoamericanas, experimentos de adopción y confianza, análisis de costos de ciberseguridad, evaluación de mecanismos de

privacidad y comparaciones entre modelos de interoperabilidad. Tales avances permitirán sustituir afirmaciones genéricas sobre innovación por evidencia contextualizada y útil para la formulación de políticas públicas.

Acerca de

Contribución de los autores: Todos los autores contribuyeron a la conceptualización del estudio, desarrollo metodológico, análisis e interpretación de los datos, redacción del manuscrito y revisión crítica de su contenido intelectual. Todos aprobaron la versión final para su publicación.

Financiamiento: Los autores declaran que no recibieron financiamiento para esta investigación.

Conflicto de interés: Los autores declaran que no existe conflicto de intereses para la publicación del presente artículo científico.

Certificación ética: El protocolo del presente estudio fue sometido a revisión y aprobado por el Comité de Ética en Investigación de la Universidad, en cumplimiento de los principios éticos y normativas institucionales aplicables.

Historia del artículo: Artículo recibido 01 de mayo 2026 | Arbitrado 26 de junio 2026 | Publicado 20 de julio 2026.

Referencias

Agur, I., Ari, A., & Dell'Ariccia, G. (2022). Designing central bank digital currencies. *Journal of Monetary Economics*, 125, 62–79. https://doi.org/10.1016/j.jmoneco.2021.05.002

Ahnert, T., Hoffmann, P., & Monnet, C. (2025). Payments and privacy in the digital economy. *Journal of Financial Economics*, 169, 104050. https://doi.org/10.1016/j.jfineco.2025.104050

Andolfatto, D. (2021). Assessing the impact of central bank digital currency on private banks. *The Economic Journal*, 131(634), 525–540. https://doi.org/10.1093/ej/ueaa073

Arias, F. (2023). Investigación documental, investigación bibliométrica y revisiones sistemáticas. *REDHECS Revista Electrónica de Humanidades, Educación y Comunicación Social,* 22(31), 9–28. https://dialnet.unirioja.es/servlet/articulo?codigo=9489470

Bruchanski, M. (2024). Una aproximación teórica al dinero soberano. *Márgenes*, (10), 81–100. https://revistas.ungs.edu.ar/index.php/margenes/article/view/1201/1472

Chu, Y., & Rathbun, N. S. (2025). Monetary sovereignty and central bank digital currencies: Competing models for future cross-border payment platforms. *Global Policy, 16*(2), 329–340. https://doi.org/10.1111/1758-5899.13495

Cruz, E., Parejo, F., Rangel, J., & Garzón, E. (2021). La soberanía monetaria a debate: La historia del dinero y sus controvertidas implicaciones políticas. *Política y Sociedad,* 58(3). https://doi.org/10.5209/poso.65724

Dionisópoulos, L., Marra, M., & Urquhart, A. (2024). Central bank digital currencies: A critical review. *International Review of Financial Analysis*, 91, 103031. https://doi.org/10.1016/j.irfa.2023.103031

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

Keister, T., & Monnet, C. (2022). Central bank digital currency: Stability and information. *Journal of Economic Dynamics and Control*, 142, 104501. https://doi.org/10.1016/j.jedc.2022.104501

Keister, T., & Sanches, D. (2023). Should central banks issue digital currency? The Review of Economic Studies, 90(1), 404–431. https://doi.org/10.1093/restud/rdac017

Kumhof, M., & Noone, C. (2021). Central bank digital currencies—Design principles for financial stability. *Economic Analysis and Policy,* 71, 553–572. https://doi.org/10.1016/j.eap.2021.06.012

Larrea, J., & Abad, Y. C. (2025). Entre la innovación y la regulación: Evaluación sistemática de la privacidad de datos en el uso financiero del machine learning. *Revista Anual Virtual, 6*(13). https://doi.org/10.5281/zenodo.17945309

Legal, D., Blanco, C., & Ortiz, G. (2022). Moneda digital del banco central: Implicancias para la estabilidad financiera y la política monetaria en Paraguay. *Banco Central del Paraguay.* https://pabloacastillo.me/wp-content/uploads/2022/08/dt_nro27.pdf

Liu, Z., Guo, J., Lam, K., & Zhao, J. (2023). Efficient dropout-resilient aggregation for privacy-preserving machine learning. *IEEE Transactions on Information Forensics and Security,* 18, 1839–1854. https://doi.org/10.1109/TIFS.2022.3163592

Luu, H. N., Nguyen, C. P., & Nasir, M. A. (2023). Implications of central bank digital currency for financial stability: Evidence from the global banking sector. *Journal of International Financial Markets, Institutions and Money,* 89, 101864. https://doi.org/10.1016/j.intfin.2023.101864

Martino, E. D. (2024). Monetary sovereignty in the digital era: The law & macroeconomics of digital private money. *Computer Law & Security Review*, 52, 105909. https://doi.org/10.1016/j.clsr.2023.105909

Medina, J. (2023). *Stablecoins: Riesgos y desafíos jurídicos, un análisis de la regulación contenida en el Reglamento MiCA* [Trabajo de fin de máster, Universitat Pompeu Fabra]. Repositori UPF. https://repositori.upf.edu/handle/10230/57688

Mena, L., Martínez, G., & Estrada, H. (2024). El potencial de las stablecoins para fomentar la estabilidad monetaria. *RevisTAP,* 3(2). https://revistap.ejeutap.edu.co/index.php/utap/article/view/146

Monsalve, R. (2025, 19 de noviembre). CBDC, stablecoins y la guerra por el nuevo orden financiero digital. *Misión Verdad*. https://misionverdad.com/investigaciones/cbdc-stablecoins-y-la-guerra-por-el-nuevo-orden-financiero-digital

Murphy, K., Sun, T., Zhou, Y., Tsuda, N., Zhang, N., Budau, V., et al. (2024). *Central bank digital currency data use and privacy protection* (Fintech Note No. 2024/004).

Fondo Monetario Internacional. https://doi.org/10.5089/9798400286971.063.A001

Ortiz, L. (2025). *Equilibrio entre privacidad y eficiencia: Impacto de las normas de protección de datos en las plataformas de resolución electrónica de conflictos en Colombia* [Trabajo de grado, Universidad Externado de Colombia]. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/f6bdfa3f-185d-4932-8210-e28b50e58911/content

Paredes, G. (2019). Un análisis de la pérdida de soberanía monetaria desde la teoría de la regulación: Argentina y Ecuador. *Ciclos,* 30(52), 81–100. https://www.scielo.org.ar/pdf/ciclos/v30n52/1851-3735-ciclos-30-52-81.pdf

Pérez Cárdenas, D. (2025). *Privacidad, identidad y eficiencia: Mejorando pagos transfronterizos con Hyperledger Besu y tecnologías blockchai*n [Trabajo de grado, Universidad de los Andes]. Repositorio Institucional Universidad de los Andes. https://repositorio.uniandes.edu.co/entities/publication/4196eb7f-134f-415c-9ee4-59d124871951

Soana, G., & de Arruda, T. (2024). Central bank digital currencies and financial integrity: Finding a new trade-off between privacy and traceability within a changing financial architecture. *Journal of Banking Regulation*, 25(4), 467–486. https://doi.org/10.1057/s41261-024-00241-2

Valdés, D. (2022). *La persona, el ciudadano y la soberanía. Centro de Convivencia*. https://centroconvivencia.org/la-persona-el-ciudadano-y-la-soberania/