

ORDEN MUNDIAL DIGITAL Y SEGURIDAD HUMANA: CBDC, BLOCKCHAIN Y TOKENIZACIÓN FINANCIERA EN LA RECONFIGURACIÓN DEL SISTEMA GLOBAL

Digital World Order and Human Security: CBDC, Blockchain, and Financial Tokenization in the Reconfiguration of the Global System

Recibido: 01 / 06 / 2026 | Revisado: 05 / 07 / 2026 | Aprobado: 11 / 09 / 2026

DOI : <https://doi.org/10.59794/rscd.2026.v12i12.178>



Rocío Cristy Santana González

República Dominicana

Correo: omphsantana@gmail.com

Orcid: <https://orcid.org/0009-0001-8321-7816>.

La autora es Contralmirante en situación de retiro de la Armada de República Dominicana, donde ocupó funciones de alto nivel en los ámbitos de educación militar, entrenamiento operativo, relaciones internacionales y gestión estratégica en defensa y seguridad. Es ingeniera en sistemas y cuenta con formación de posgrado en seguridad y defensa, así como especializaciones en geopolítica, derechos humanos y derecho internacional humanitario. Actualmente se desempeña como directora ejecutiva de Defensall Institute, institución dedicada a la formación y desarrollo de capacidades en defensa, seguridad y liderazgo estratégico, y cursa estudios doctorales en Seguridad Nacional y Humana. En su carrera institucional ha ejercido responsabilidades como la Dirección General del Comando Naval de Educación y Entrenamiento, la Dirección de Asuntos Internacionales y la

Jefatura de Relaciones Públicas, además de coordinar proyectos estratégicos vinculados a la transformación digital educativa en cooperación con organismos internacionales. Ha dirigido iniciativas editoriales y académicas, entre ellas revistas especializadas en defensa y seguridad, así como programas de difusión orientados al fortalecimiento de la cultura de defensa. Posee amplia experiencia en docencia, investigación y desarrollo curricular, y forma parte del Comité Científico de la Universidad Nacional para la Defensa, así como de la Carrera Nacional de Investigadores. Sus áreas de competencia incluyen liderazgo estratégico, ciberseguridad, gestión de crisis y relaciones internacionales, complementadas con formación continua en inteligencia estratégica, gestión de proyectos y educación superior. CEO, Defensall Institute, S.R.L. Código CNI: CNI-1197.



RESUMEN

El orden mundial del siglo XXI atraviesa una transformación tecnológica que incide en la comunicación, la defensa, la inteligencia artificial, la ciberseguridad y el núcleo del sistema financiero global. Este artículo analiza la incidencia diferenciada de las monedas digitales de bancos centrales (CBDC), blockchain y la tokenización financiera en la evolución del sistema global y sus implicaciones para la seguridad humana. La investigación adopta un enfoque cualitativo, documental-bibliográfico y analítico, mediante una revisión narrativa no sistemática de literatura académica, informes institucionales, documentos regulatorios y publicaciones estratégicas recientes. Los resultados del análisis muestran que la naturaleza digital del dinero y de los activos financieros puede favorecer la eficiencia, la interoperabilidad, la inclusión, la modernización de pagos y el acceso ampliado a mercados; sin embargo, también genera riesgos de control social financiero, pérdida de privacidad, brecha digital, incidentes de ciberseguridad, concentración de poder tecnológico-financiero y dependencia de infraestructuras críticas. Se concluye que las CBDC son formas digitales de dinero público, blockchain es una infraestructura de registro distribuido y la tokenización es un proceso de representación digital de activos o derechos; aunque son fenómenos distintos, convergen en la construcción del orden financiero digital. Su legitimidad dependerá de marcos jurídicos, institucionales y técnicos capaces de proteger la dignidad, el ejercicio de los derechos, la confianza pública y las dimensiones económica, personal y política de la seguridad humana.

Palabras clave: Seguridad humana; orden mundial digital; CBDC; blockchain; tokenización financiera; ciberseguridad; soberanía monetaria.

ABSTRACT

The world order of the twenty-first century is going through a technological transformation that affects communication, defense, artificial intelligence, cybersecurity, and the core of the global financial system. This article analyzes the differentiated impact of central bank digital currencies (CBDCs), blockchain, and financial tokenization on the evolution of the global system and its implications for human security. The research adopts a qualitative, documentary-bibliographic, and analytical approach, through a non-systematic narrative review of academic literature, institutional reports, regulatory documents, and recent strategic publications. The results of the analysis show that the digital nature of money and financial assets can favor efficiency, interoperability, inclusion, modernization of payments, and expanded access to markets; however, it also generates risks of financial social control, loss of privacy, digital divide, cybersecurity incidents, concentration of technological-financial power, and dependence on critical infrastructures. It is concluded that CBDCs are digital forms of public money, blockchain is a distributed ledger infrastructure, and tokenization is a process of digital representation of assets or rights; Although they are different phenomena, they converge in the construction of the digital financial order. Their legitimacy will depend on legal, institutional and technical frameworks capable of protecting dignity, the exercise of rights, public trust and the economic, personal and political dimensions of human security.

Keywords: Human security, digital world order, CBDC, blockchain, financial tokenization, cybersecurity, monetary sovereignty.



INTRODUCCIÓN

El orden mundial del siglo XXI se encuentra inmerso en una transformación tecnológica que modifica, entre otros ámbitos, las formas de producción, comunicación, defensa, comercio, vigilancia, cooperación internacional y organización financiera. Este proceso no es exclusivamente técnico ni se limita a empresas: alcanza a personas, instituciones y Estados, y atraviesa la soberanía, la gobernanza global, la seguridad nacional, la protección de datos, la inclusión social y la vida cotidiana. En lo que se refiere al sistema financiero, el dinero, los pagos, los activos y los mercados de capitales evolucionan mediante instrumentos e infraestructuras como las CBDC, blockchain y la tokenización financiera.

La seguridad humana ofrece el marco central de este análisis. Desde el enfoque introducido por el Programa de las Naciones Unidas para el Desarrollo, la seguridad no se limita a la defensa territorial o militar del Estado, sino que comprende la protección de la vida, la dignidad, el bienestar y la libertad de las personas frente al miedo, la necesidad y la vulnerabilidad (Programa de las Naciones Unidas para el Desarrollo [PNUD], 1994). En este artículo, el concepto se delimita operativamente a las dimensiones económica, personal y política de la seguridad humana: continuidad del acceso al dinero y a servicios esenciales; protección frente a fraude, exclusión y pérdida patrimonial; privacidad y protección de datos; y capacidad de ejercer derechos sin vigilancia desproporcionada. La ciberseguridad es una condición técnica transversal para proteger esas dimensiones, pero no es sinónimo de seguridad humana (PNUD, 2022).

Dentro de esta transformación, las monedas digitales de bancos centrales, conocidas como CBDC por sus siglas en inglés, han adquirido creciente importancia. Una CBDC es una obligación digital directa del banco central, denomi-

nada en la unidad monetaria oficial y convertible a la par con otras formas de dinero del mismo Estado. Se diferencia de las criptomonedas o criptoactivos privados, que no constituyen pasivos de una autoridad monetaria y cuyo valor puede fluctuar según el mercado. También se distingue del dinero bancario convencional: no es dinero físico escaneado o convertido, sino una forma de dinero público que nace digital. Su diseño puede incidir en pagos, inclusión financiera, estabilidad monetaria e interoperabilidad transfronteriza, pero también plantea interrogantes sobre privacidad, control social financiero, protección de datos, resiliencia tecnológica y garantías para el ejercicio de derechos.

El Fondo Monetario Internacional ha desarrollado un manual virtual sobre CBDC orientado a responsables de política pública, bancos centrales y ministerios de finanzas. Este hecho evidencia que el dinero digital emitido por bancos centrales dejó de ser una hipótesis marginal y se convirtió en un asunto de gobernanza monetaria global (International Monetary Fund [IMF], s. f.). De manera complementaria, el Banco de Pagos Internacionales reportó que el 91 % de 93 bancos centrales encuestados exploraba CBDC minoristas, mayoristas o ambas modalidades, lo que confirma la consolidación de una agenda internacional sobre dinero público de naturaleza digital (Illes et al., 2025).

La transformación no se limita a las CBDC. Blockchain y otras tecnologías de registro distribuido han introducido formas compartidas de registrar, transferir, verificar y programar información y valor. Blockchain no es una moneda ni un activo por sí misma: es una arquitectura de datos en la que los registros se agrupan y enlazan criptográficamente, lo que dificulta su alteración sin dejar evidencia. Aunque se popularizó en el ecosistema de criptoactivos, se utiliza en pagos, mercados de capitales, custodia



digital, trazabilidad y tokenización. La literatura académica la reconoce como infraestructura habilitadora, pero advierte que sus beneficios dependen del diseño de gobernanza, la escalabilidad, la interoperabilidad y la seguridad (Treleaven et al., 2017; Schär, 2021).

La tokenización financiera constituye otro componente del orden mundial digital. Consiste en representar un activo, instrumento o derecho mediante un token registrado en una infraestructura digital. Puede facilitar transferencia, fraccionamiento, programación y negociación de bonos, acciones, fondos cotizados en bolsa (ETF, por sus siglas en inglés), bienes raíces, depósitos e instrumentos de deuda. La tokenización no equivale al activo subyacente en todos los casos: el contenido jurídico del token depende de si incorpora propiedad, crédito, participación, usufructo u otro derecho. Actores como BlackRock la vinculan con cambios en negociación, liquidación y acceso a inversiones (Fink, 2025), pero las fuentes corporativas deben contrastarse con literatura académica y regulatoria (Cong & He, 2019; International Organization of Securities Commissions [IOSCO], 2025).

Desde la seguridad humana, la cuestión no reside únicamente en la eficiencia, sino en cómo estas tecnologías impactan la vida, la privacidad, el acceso, la autonomía y la seguridad de las personas. Entre sus beneficios figuran pagos más rápidos y menos costosos, liquidación programable, mayor competencia, mejor acceso a instrumentos financieros y continuidad de servicios. Entre los riesgos se encuentran el control social financiero, la pérdida de privacidad, el fraude, la exclusión asociada con la brecha digital, la dependencia de infraestructuras críticas —sistemas de pago, telecomunicaciones, energía, nube, identidad digital y centros de datos cuya interrupción afecta funciones esenciales—, y una superficie de ataque más amplia para ransomware, denegación de servicio, robo de credenciales y explotación de contratos inteligentes. Estos riesgos están documentados en el sector

financiero global y no constituyen posibilidades meramente hipotéticas (IMF, 2024).

Santana González (2021) advirtió, desde el contexto dominicano, que el carácter intangible, transfronterizo y dinámico del ciberespacio ofrece oportunidades económicas y expone desfases entre la evolución tecnológica y los ritmos de actualización normativa. Este antecedente permite analizar la relación entre ciberseguridad, economía digital y protección institucional. El presente artículo amplía ese punto de partida mediante evidencia global sobre dinero público digital, activos tokenizados, riesgos cibernéticos sistémicos y gobernanza financiera.

El problema central consiste en que el sistema financiero global evoluciona hacia una arquitectura más digital, programable y tokenizada, mientras sus consecuencias jurídicas, técnicas y sociales no siempre se integran bajo un marco de seguridad humana. Las CBDC, blockchain y la tokenización suelen estudiarse por separado desde perspectivas monetarias, informáticas, jurídicas o de mercado. Se requiere analizarlas conjuntamente para determinar cómo la privacidad, la inclusión, el control social financiero, la ciberseguridad, la soberanía monetaria, la dependencia tecnológica, la concentración de poder y la resiliencia institucional inciden en las dimensiones económica, personal y política de la seguridad humana.

En este marco, la pregunta que orienta el artículo es: ¿de qué manera las CBDC, blockchain y la tokenización financiera inciden en la evolución del orden mundial digital y qué medidas de gobernanza permiten proteger las dimensiones económica, personal y política de la seguridad humana? El objetivo general consiste en analizar, mediante una revisión bibliográfica narrativa con enfoque analítico-prospectivo, la incidencia diferenciada y convergente de esas tecnologías e instrumentos, identificar beneficios y riesgos, y proponer criterios para una gobernanza financiera digital centrada en las personas.



Metodológicamente, el artículo adopta un enfoque cualitativo, documental-bibliográfico y analítico, mediante una revisión narrativa no sistemática. Se consultaron artículos académicos, informes institucionales, documentos regulatorios y publicaciones estratégicas. La selección priorizó trabajos publicados entre 2021 y 2026, incorporando fuentes anteriores cuando son fundacionales para seguridad humana, blockchain, dinero digital o gobernanza financiera. Las fuentes se organizaron en cuatro categorías de análisis: naturaleza jurídica y tecnológica; beneficios operativos; riesgos para las personas y el sistema; y respuestas regulatorias y de política pública.

El desarrollo se organiza en seis apartados. El primero aborda el orden mundial digital y la seguridad humana como marco de análisis. El segundo examina las CBDC y la soberanía monetaria digital. El tercero explica blockchain como infraestructura financiera programable. El cuarto analiza la tokenización financiera, los ETF y los valores digitales. El quinto estudia los principales riesgos para la seguridad humana. El sexto plantea escenarios prospectivos del orden financiero digital, considerando la tensión entre eficiencia, control, inclusión, privacidad, ciberseguridad y protección de derechos.

DESARROLLO

ORDEN MUNDIAL DIGITAL Y SEGURIDAD HUMANA

El orden mundial digital puede entenderse como una etapa de evolución del sistema internacional en la que poder, soberanía, seguridad y gobernanza están cada vez más condicionados por infraestructuras tecnológicas, datos, plataformas, sistemas de pago, dinero digital, redes financieras y capacidades de ciberseguridad. No es solo modernización instrumental, sino una reorganización de los mecanismos mediante los cuales Estados, empresas, organismos internacionales y personas producen, transfieren, almacenan y protegen información, activos y derechos de contenido económico. El Banco de Pagos Internacionales sostiene que la tokenización del dinero y los activos puede habilitar libros mayores unificados que combinen dinero de banco central, depósitos tokenizados y activos financieros en plataformas programables (Bank for International Settlements [BIS], 2023).

La dimensión financiera de este orden mundial digital resulta especialmente relevante porque el dinero es una institución central de la vida económica, política y social. Cuando los pa-

gos, los activos, los mercados de capitales y las reservas monetarias se trasladan progresivamente hacia infraestructuras digitales, también se modifican las condiciones de acceso, control, vigilancia, interoperabilidad, resiliencia y confianza. En esa dirección, el BIS sostuvo en 2025 que un libro mayor tokenizado que incorpore dinero de banco central, depósitos comerciales y bonos gubernamentales podrá sentar bases para un sistema monetario y financiero tokenizado de nueva generación (Bank for International Settlements, 2025).

La seguridad humana permite evaluar esta transformación desde una perspectiva centrada en las personas. El PNUD desplazó el énfasis exclusivo en territorios y armas hacia la protección frente al miedo, la necesidad y la vulnerabilidad (PNUD, 1994). Aplicado al entorno financiero digital, este artículo examina inseguridad económica —pérdida o indisponibilidad de fondos—, inseguridad personal —fraude, suplantación y exposición de datos— e inseguridad política —vigilancia desproporcionada o restricciones automatizadas al ejercicio de derechos—. Un sistema puede ser técnicamente eficiente y, a la vez, producir inseguridad si



interrumpe el acceso a alimentos, salud, transporte, energía o comunicaciones, o si debilita privacidad, inclusión y soberanía individual.

En la actualidad, la seguridad humana enfrenta amenazas que incluyen ciberataques, desigualdades, vigilancia y nuevas vulnerabilidades sociales. El PNUD advierte que las tecnologías digitales pueden ampliar libertades y, al mismo tiempo, generar consecuencias no deseadas (PNUD, 2022). Por ello, el dinero digital y las plataformas financieras deben evaluarse por sus efectos sobre derechos humanos y fundamentales como la intimidad, la protección de datos, la igualdad, la propiedad, el debido proceso y el acceso no discriminatorio a servicios esenciales.

El problema no es la naturaleza digital en sí misma, sino cómo se diseña, regula, gobierna y supervisa la infraestructura. Un sistema financiero digital puede reducir costos, ampliar inclusión, ofrecer seguimiento transaccional más detallado y facilitar pagos transfronterizos. A la vez, incrementa la dependencia funcional de electricidad, telecomunicaciones, centros de datos, servicios de nube, identidades digitales y redes de liquidación: la falla de un componente puede propagarse a pagos, crédito y servicios esenciales. También amplía superficies de ataque, intensifica el control social financiero y profundiza la brecha digital y generacional de quienes carecen de conectividad, dispositivos, accesibilidad o alfabetización digital. El Consejo de Estabilidad Financiera identifica vulnerabilidades de liquidez, apalancamiento, interconexión y fragilidad operativa, aunque advierte que la adopción aún es insuficiente para cuantificar de forma robusta su efecto agregado (Financial Stability Board [FSB], 2024).

La seguridad humana en el orden mundial digital exige una lectura jurídica y técnica integral. En República Dominicana, la Constitución reconoce la intimidad y la autodeterminación informativa, mientras la Ley núm. 172-13 regula el tratamiento de datos personales y reconoce

derechos de acceso, rectificación, cancelación y oposición. Ese marco debe proyectarse sobre cualquier futura infraestructura de dinero digital, junto con las normas financieras, de prevención del lavado de activos, protección al consumidor y ciberdelincuencia. La pregunta relevante no es solo quién controla los datos, sino bajo qué base jurídica, finalidad, proporcionalidad, seguridad, supervisión independiente y mecanismos de reclamación. IOSCO confirma que la tokenización exige protección del inversionista e integridad del mercado (IOSCO, 2025).

Esta mirada vincula seguridad nacional y seguridad humana sin confundirlas. La seguridad nacional procura continuidad y resiliencia de infraestructuras financieras críticas; la seguridad humana examina el impacto de una interrupción sobre las personas. Ataques de ransomware, denegación distribuida de servicio, compromiso de proveedores, suplantación, fraude de credenciales o explotación de vulnerabilidades en contratos inteligentes pueden impedir pagos, bloquear salarios, afectar remesas y ahorro, y erosionar la confianza institucional. Por ello, la protección de sistemas de pago, bases de datos, billeteras, identidades y redes de liquidación es un asunto estratégico del Estado y, simultáneamente, una condición para la vida cotidiana.

El antecedente de Santana González (2021) se utiliza como referencia contextual nacional, no como evidencia principal de actualidad. Su aporte permite identificar el desfase entre evolución tecnológica y respuesta normativa; las fuentes internacionales y académicas posteriores sustentan el análisis contemporáneo de amenazas, vulnerabilidades, impactos macrofinancieros y medidas de gobernanza.

El orden mundial digital reúne oportunidades, riesgos, amenazas y vulnerabilidades. La meta regulatoria no puede ser eliminar todo riesgo —objetivo imposible—, sino reducir su probabilidad e impacto, fortalecer resiliencia y



asegurar reparación. Un sistema legítimo deberá combinar inclusión, eficiencia e interoperabilidad con seguridad de la información, privacidad, debido proceso, supervisión y rendición de cuentas. La seguridad humana no crea por sí sola legitimidad jurídica; funciona como criterio sustantivo para evaluar si las decisiones públicas protegen a las personas y, junto con legalidad, participación, transparencia y control institucional, contribuye a la legitimidad social del orden financiero digital.

CBDC Y SOBERANÍA MONETARIA DIGITAL

Las monedas digitales de bancos centrales representan uno de los desarrollos más relevantes en la discusión sobre dinero, soberanía

y tecnología. Una CBDC es dinero público digital y puede mejorar la relación funcional entre banco central, intermediarios, usuarios y pagos. Su valor nominal se expresa en la moneda oficial y, cuando el diseño garantiza la unicidad del dinero, se intercambia a la par con efectivo y depósitos denominados en esa unidad. El manual del FMI sirve como guía para responsables de política pública, bancos centrales y ministerios de finanzas que evalúan su emisión (IMF, s. f.).

El interés global por las CBDC ha crecido de forma sostenida. El BIS reportó que, en una encuesta de 2024, el 91 % de 93 bancos centrales exploraba CBDC minoristas, mayoristas o ambas (Illes et al., 2025).

Figura 1

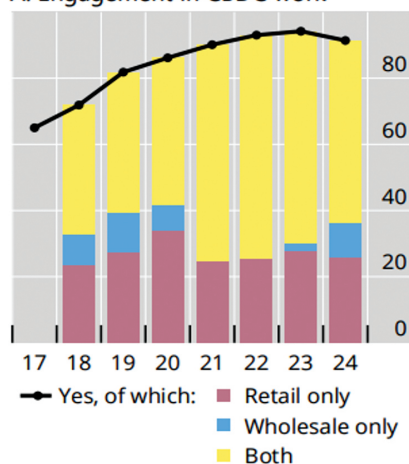
Exploración de monedas digitales de bancos centrales (CBDC), encuesta BIS 2024

Central bank involvement in CBDC work

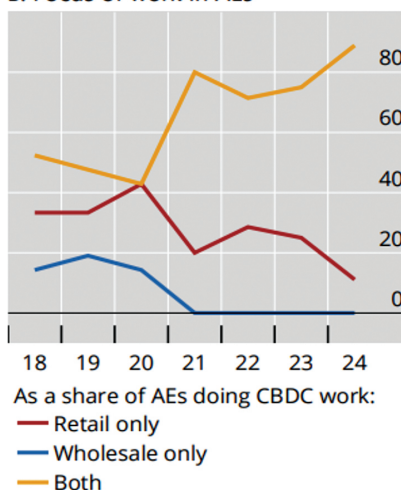
As a percentage of respondents

Graph 2

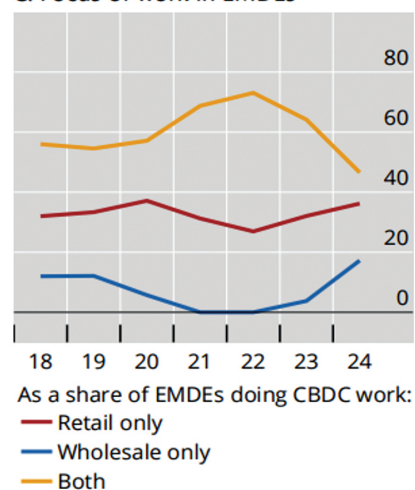
A. Engagement in CBDC work¹



B. Focus of work in AEs²



C. Focus of work in EMDEs²



¹ As a share of all respondents. ² As a share of all respondents doing CBDC work within the country group.

Sources: BIS surveys on CBDCs and crypto, 2017–24; authors' calculations.

Nota. Adaptado de Illes et al. (2025). El informe reporta que el 91 % de 93 bancos centrales encuestados exploraba una CBDC minorista, mayorista o ambas.



Este dato muestra que el dinero digital de banco central ya forma parte de una agenda monetaria internacional, aunque con distintos niveles de avance, motivaciones y diseños según cada jurisdicción.

Desde la perspectiva de la soberanía monetaria, las CBDC pueden interpretarse como una respuesta institucional a la expansión de pagos digitales privados, criptoactivos, stablecoins, plataformas globales y sistemas financieros transfronterizos. En un entorno donde el dinero circula crecientemente por canales digitales, los bancos centrales enfrentan el desafío de preservar la confianza pública, garantizar estabilidad, mantener la eficacia de la política monetaria y asegurar que el dinero soberano conserve relevancia dentro de la economía digital. El FMI ha abordado estos temas desde dimensiones macro financieras, legales, regulatorias, de integridad financiera y de estabilidad, lo que evidencia que las CBDC son un asunto de política pública y no solo de innovación tecnológica (IMF, 2025).

Sin embargo, la soberanía monetaria digital no debe reducirse al control estatal sobre la emisión de dinero. También implica capacidad institucional para proteger datos, asegurar interoperabilidad, prevenir exclusión, garantizar continuidad operativa y sostener la confianza ciudadana. Una CBDC técnicamente avanzada podría enfrentar resistencia social si la población percibe que comprometa su privacidad, facilita vigilancia excesiva o aumenta la dependencia de infraestructuras vulnerables. Por ello, la legitimidad de una moneda digital estatal dependerá tanto de su diseño tecnológico como de sus garantías jurídicas, éticas y sociales.

Las CBDC mayoristas, orientadas a instituciones financieras y pagos interbancarios, tienen otro tipo de relevancia estratégica. Su potencial se vincula con liquidación más rápida, reducción de riesgos operativos, pagos transfronterizos más eficientes e integración con depósitos tokenizados o activos financieros digitales. Aunque

sus efectos sobre la ciudadanía son menos directos que en una CBDC minorista, pueden incidir en la estabilidad del sistema financiero, los costos de transacción, la resiliencia de pagos internacionales y la arquitectura monetaria global. El BIS ha planteado que la integración de dinero de banco central, depósitos tokenizados y activos financieros en infraestructuras programables podría permitir aprovechar de forma más amplia los beneficios de la tokenización (BIS, 2023).

En este punto, la discusión sobre CBDC se vincula con el orden mundial digital. Si distintos países desarrollan monedas digitales con estándares incompatibles, podrían profundizarse la fragmentación financiera, las tensiones geoeconómicas y la competencia por influencia monetaria. Si, por el contrario, se desarrollan marcos interoperables, seguros y respetuosos de derechos, las CBDC podrían contribuir a una infraestructura financiera más eficiente y confiable. La diferencia entre ambos escenarios dependerá de decisiones institucionales, marcos regulatorios, cooperación internacional y diseño tecnológico.

Desde la seguridad humana, el diseño de una CBDC debería considerar al menos cinco principios. Primero, privacidad proporcional y protección de datos personales. Segundo, inclusión efectiva para poblaciones sin acceso pleno a servicios financieros o digitales. Tercero, resiliencia tecnológica frente a fallas, desastres o ciberataques. Cuarto, transparencia institucional sobre usos, límites y gobernanza de la información. Quinto, mecanismos de supervisión democrática que impidan usos abusivos o discriminatorios del sistema monetario digital. Estos principios no derivan de una preferencia normativa aislada, sino de la conexión entre seguridad humana, gobernanza digital y protección de derechos planteada por el PNUD en sus informes sobre amenazas contemporáneas (PNUD, 2022).

En síntesis, las CBDC constituyen una de las expresiones más visibles de la soberanía monetaria en el orden mundial digital. Su potencial no debe



ser negado: puede modernizar pagos, fortalecer la presencia del dinero público en la economía digital y ampliar servicios financieros. No obstante, su legitimidad dependerá de su capacidad para equilibrar eficiencia con derechos, trazabilidad con privacidad, innovación con inclusión y soberanía estatal con seguridad humana.

BLOCKCHAIN E INFRAESTRUCTURA FINANCIERA PROGRAMABLE

Blockchain puede entenderse como una tecnología de registro distribuido que permite almacenar, verificar y transferir información o valor mediante una red de participantes que comparten reglas de validación. Aunque su uso oficial se asoció principalmente con Bitcoin y los criptoactivos, su aplicación se ha extendido hacia ámbitos institucionales como pagos, liquidación, custodia, trazabilidad, contratos inteligentes, activos tokenizados y sistemas de mercado. En el contexto financiero, su relevancia no se limita a la descentralización, sino a la posibilidad de crear infraestructuras digitales programables donde el registro, la transferencia y la liquidación puedan integrarse de manera más automatizada.

La infraestructura financiera tradicional se apoya en intermediarios, registros separados, procesos de compensación y liquidación, custodios, cámaras de compensación y marcos regulatorios nacionales. Blockchain y otras tecnologías de registro distribuido proponen una arquitectura distinta: activos, dinero, reglas de ejecución y condiciones de cumplimiento pueden representarse digitalmente dentro de una plataforma o en sistemas interoperables. El BIS ha planteado que un libro mayor unificado podría reunir dinero de banco central, depósitos tokenizados y activos financieros en una infraestructura programable, con reglas, estándares y gobernanza compartida (BIS, 2023).

La noción de infraestructura financiera programable implica que ciertos procesos financieros

pueden ejecutarse automáticamente cuando se cumplen condiciones previamente establecidas. Los contratos inteligentes permiten programar transferencias, pagos, liquidaciones, cumplimiento normativo o restricciones de uso de activos digitales. En teoría, esto puede reducir fricciones operativas, mejorar trazabilidad, disminuir tiempos de liquidación y facilitar nuevas formas de supervisión. Sin embargo, también introduce riesgos vinculados con errores de código, dependencia tecnológica, concentración de proveedores, fallas de interoperabilidad y dificultad para resolver disputas cuando una operación programada produce efectos no deseados.

Desde una perspectiva de seguridad humana, la programabilidad financiera debe analizarse con cautela. La trazabilidad puede fortalecer la prevención de fraude, lavado de activos y financiamiento ilícito, pero también puede ampliar capacidades de vigilancia sobre ciudadanos y usuarios. La automatización puede reducir costos y aumentar eficiencia, pero también puede excluir a personas que no comprendan o no puedan acceder a sistemas digitales. La transparencia puede fortalecer confianza institucional, pero una transparencia mal diseñada puede comprometer datos sensibles. Por tanto, el problema central no es solo técnico, sino ético, jurídico y político.

El FMI sostiene que la tokenización representa un cambio estructural en la arquitectura financiera, no una simple mejora marginal de eficiencia. Según su análisis, los libros mayores compartidos, los activos financieros programables y la gestión de riesgos mediante contratos inteligentes pueden modificar la naturaleza de la liquidación, la liquidez y el riesgo sistémico (Adrián, 2026). Esta afirmación es importante porque confirma que blockchain y la tokenización ya no debe tratarse como fenómenos periféricos del ecosistema cripto, sino como componentes potenciales de la infraestructura financiera regulada.



La posibilidad de liquidación casi inmediata o atómica es uno de los argumentos más repetidos a favor de estas infraestructuras. En una operación financiera tradicional, la negociación y la liquidación pueden ocurrir en momentos distintos, lo que genera riesgos de contraparte, costes de intermediación y periodos en los que el capital queda inmovilizado. En sistemas tokenizados, la transferencia del activo y del pago podría ejecutarse simultáneamente, siempre que existan condiciones técnicas, jurídicas y regulatorias adecuadas. Sin embargo, la rapidez no garantiza por sí misma seguridad humana; también se requieren mecanismos de reversión, protección del usuario, solución de controversias, auditorías y responsabilidad institucional.

La ciberseguridad es otro componente decisivo. A medida que pagos, activos, identidades y registros se integran en plataformas digitales, aumenta la dependencia de infraestructuras críticas. Un ataque contra sistemas de pagos, billeteras digitales, custodios, puentes de interoperabilidad o plataformas de valores tokenizados puede afectar no solo a instituciones financieras, sino también a ciudadanos, empresas y servicios esenciales. Por eso, la seguridad de blockchain no debe reducirse a la criptografía del registro; debe incluir gobernanza, controles de acceso, auditoría de contratos inteligentes, protección de claves, continuidad operativa y capacidad de respuestas ante incidentes.

También debe considerarse la tensión entre descentralización y regulación. Las redes públicas abiertas prometen transparencia y resistencia a la censura, pero presentan desafíos para cumplimiento normativo, identificación de responsables, protección de inversionistas

y prevención de delitos financieros. Las redes permissionadas, por su parte, permiten mayor control institucional, pero pueden reproducir concentración de poder y dependencia de operadores autorizados. El diseño adoptado tendrá implicaciones distintas para privacidad, autonomía, acceso, supervisión y confianza.

En consecuencia, blockchain debe ser tratada en el artículo como infraestructura habilitadora, no como una solución automática. Su valor dependerá de la forma en que se articule con dinero de banco central, bancos comerciales, reguladores, custodios, emisores, inversionistas, usuarios y marcos jurídicos. Para la seguridad humana, la pregunta central no es si blockchain es innovadora, sino si su implementación protege derechos, reduce vulnerabilidades, mejora acceso, fortalece resiliencia y evita nuevas formas de exclusión o vigilancia abusiva.

TOKENIZACIÓN FINANCIERA, ETF Y VALORES DIGITALES

La tokenización financiera consiste en representar digitalmente un activo, derecho o instrumento financiero mediante un token registrado en una infraestructura digital, generalmente basada en tecnología de registro distribuido o en sistemas con características similares. El activo tokenizado puede corresponder a bonos, acciones, fondos, ETF, depósitos, bienes raíces, deuda privada, instrumentos de mercado monetario y otros derechos económicos. Su promesa principal es convertir activos tradicionalmente menos líquidos o más difíciles de fraccionar en unidades digitales transferibles, programables y potencialmente negociables con mayor eficiencia.



Tabla 1.
Tipos de activos tokenizados y naturaleza del derecho representado

Categoría	Ejemplos	Derecho representado	Riesgo principal
Deuda	Bonos, pagarés, deuda privada	Crédito y pago de capital/intereses	Incumplimiento y prioridad jurídica
Participación	Acciones, participaciones societarias	Propiedad, voto o dividendo según emisión	Diferencia entre token y registro societario
Fondos	ETF y fondos de inversión	Participación económica en una cartera	Custodia, liquidez y protección del inversionista
Depósitos y dinero	Depósitos tokenizados	Crédito frente a una entidad financiera	Riesgo de emisor e interoperabilidad
Activos reales	Bienes raíces y otros bienes	Propiedad, copropiedad, usufructo o crédito	Validez registral y jurisdicción

Nota. Elaboración propia del autor.

El Foro Económico Mundial sostiene que la tokenización puede ofrecer un nuevo modelo de propiedad digital que mejore transparencia, eficiencia y accesibilidad en los mercados financieros. Su informe de 2025 analiza casos de uso en emisión, financiamiento de valores y gestión de activos, pero también reconoce que la implementación exitosa depende de condiciones regulatorias, operativas, tecnológicas y de mercado (World Economic Forum [WEF], 2025). Por ello, la tokenización debe examinarse como una posibilidad en desarrollo, no como una realidad plenamente consolidada no homogénea.

Los beneficios potenciales de la tokenización suelen agruparse en cinco dimensiones. Primero, mayor eficiencia operativa, al reducir procesos manuales o intermediaciones redundantes. Segundo, liquidación más rápida, al integrar transferencia del activo y pago. Tercero, fraccionamiento de activos, lo que podría permitir acceso a inversiones antes reservadas a

grandes patrimonios. Cuarto, trazabilidad, al registrar movimientos y titularidad con mayor precisión. Quinto, programabilidad, al incorporar reglas de cumplimiento, restricciones de transferencia o pagos automáticos dentro del propio instrumento digital. No obstante, cada beneficio depende del diseño concreto del sistema, la calidad de la regulación y la confianza de los usuarios.

La infraestructura financiera programable permite que sistemas informáticos ejecuten automáticamente instrucciones cuando se cumplen condiciones previamente establecidas. Los llamados contratos inteligentes son programas informáticos desplegados en una red; no sustituyen por sí mismos al contrato jurídico ni resuelven cuestiones de consentimiento, jurisdicción o responsabilidad. En la práctica ya automatizan transferencias, liquidaciones y controles en mercados de activos digitales. Su uso puede reducir conciliaciones y tiempos, pero los errores de có-



digo pueden ejecutar operaciones irreversibles; la dependencia de oráculos puede introducir datos falsos; y la falta de interoperabilidad o reglas de gobernanza puede dificultar la solución de controversias (Cong & He, 2019; Schär, 2021).

La relación entre tokenización y ETF resulta especialmente relevante para este artículo, porque los ETF representan instrumentos ya integrados en los mercados financieros tradicionales y ampliamente utilizados por inversionistas institucionales y minoristas. A posibilidad de registrar particiones de ETF en infraestructuras distribuidas sugiere un puente entre finanzas tradicionales y activos digitales. En 2026, F/m Investments informó que su propuesta de tokenización de acciones del ETF TBIL buscaba representar la titularidad de una acción ordinaria del fondo en formato digital sobre un registro distribuido permissionado, sin convertir el ETF en una criptomoneda ni alterar su activo subyacente. Este tipo de iniciativas muestra cómo la tokenización intenta insertarse dentro de marcos regulatorios existentes, no necesariamente reemplazarlos (F/m Investments, 2026).

Desde la seguridad humana, la programabilidad exige cautela. La trazabilidad fortalece prevención de fraude y financiamiento ilícito, pero también amplía el seguimiento de activos y actividades de los usuarios. Las personas con analfabetismo digital, discapacidad, brecha generacional o conectividad limitada enfrentan mayores barreras. Además, el acceso excesivo o no autorizado a datos transaccionales puede revelar salud, religión, afiliación política, ubicación, hábitos de consumo y relaciones personales. La respuesta no es renunciar a la tecnología, sino imponer minimización de datos, separación de funciones, privacidad por diseño, auditorías independientes, mecanismos de impugnación y alternativas de acceso inclusivas.

IOSCO también ha advertido que la tokenización de activos financieros tiene implicaciones para la protección del inversionista y la integri-

dad de mercado. Entre los riesgos se encuentran la incertidumbre sobre la naturaleza jurídica del token, la dependencia de terceros emisores, los riesgos operativos, la ciberseguridad, la interoperabilidad, la custodia, las posibles conexiones con mercados de criptoactivos menos regulados (IOSCO, 2025). Esta advertencia es fundamental para mantener el equilibrio del artículo: la tokenización puede aportar eficiencia, pero también puede trasladar o amplificar riesgos si no existe gobernanza adecuada.

El FSB, por su parte, ha examinado las implicaciones de la tokenización para la estabilidad financiera. Su análisis reconoce que estos instrumentos podrían mejorar eficiencia y transparencia, pero también advierte que la tokenización puede generar vulnerabilidades relacionadas con liquidez, apalancamiento, interconexiones financieras, fragilidad operativa y transmisión de riesgos entre mercados tradicionales y digitales (FSB, 2024). En punto es clave para el enfoque de seguridad humana, porque los riesgos sistémicos no afectan únicamente a instituciones financieras; en crisis amplias, sus consecuencias pueden trasladarse a empleo, ahorro, crédito, pagos, servicios públicos y confianza social.

Desde la seguridad humana, la tokenización financiera debe analizarse en términos de acceso, protección y poder. El acceso puede ampliarse si los activos se fraccionan y se reducen barreras de entrada, pero también puede generar exposición de pequeños inversionistas a instrumentos complejos. La protección puede mejorar si existen trazabilidad, custodia segura y supervisión adecuada, pero puede debilitarse si los usuarios no comprenden la diferencia entre poseer un activo, un derecho económico, una representación sintética o una promesa contractual. El poder puede descentralizarse si aumenta la participación de nuevos actores, pero también puede concentrarse si grandes plataformas, custodios y gestores controlan la infraestructura.



La tokenización también se relaciona con la soberanía y la geopolítica financiera. Si activos, pagos y mercados se desplazan hacia plataformas digitales globales, los Estados deberán asegurar que sus marcos legales, sistemas de supervisión y capacidades de ciberseguridad puedan responder a operaciones que cruzan fronteras y jurisdicciones. El FMI advierte que, en entornos tokenizados, las transacciones pueden ejecutarse en libros mayores compartidos que abarcan múltiples jurisdicciones, lo que desafía los mecanismos tradicionales de gestión de crisis y resolución financiera, históricamente diseñados sobre instituciones nacionales y marcos legales delimitados (Adrián, 2026).

En síntesis, la tokenización financiera, los ETF tokenizados y los valores digitales representan una frontera de convergencia entre finanzas tradicionales, tecnología blockchain, regulación de mercados y gobernanza global. Su valor potencial reside en la eficiencia, la accesibilidad, la trazabilidad y la innovación, sus riesgos se concentran en la protección del inversionista, la privacidad, la ciberseguridad, la interoperabilidad, la concentración de poder y la estabilidad sistémica. Por ello, el análisis de la tokenización no debe quedar limitado a la rentabilidad o a la eficiencia de mercado, sino que debe incorporarse al debate sobre seguridad humana en el orden mundial digital.

RIESGOS PARA LA SEGURIDAD HUMANA

La liquidación casi inmediata y la liquidación simultánea de las obligaciones vinculadas son argumentos recurrentes a favor de estas infraestructuras. En las operaciones tradicionales, negociación y liquidación pueden ocurrir en momentos distintos, lo que genera exposición de contraparte. La automatización puede reducir esa ventana, pero no elimina riesgos operativos, jurídicos ni cibernéticos; exige controles,

auditoría, continuidad operativa, atribución de responsabilidad y mecanismos de solución de controversias.

Uno de los primeros riesgos es la privacidad financiera. Las CBDC, blockchain y las plataformas tokenizadas pueden aumentar la trazabilidad de pagos y activos, lo cual puede contribuir a prevenir fraudes, lavado de activos y financiamiento ilícito. Sin embargo, si esa trazabilidad no se acompaña de límites legales, controles institucionales y protección de datos, podría ampliar la capacidad de vigilancia sobre ciudadanos, empresas y comunidades. Por ello, el debate no debe centrarse únicamente en la eficiencia de los registros digitales, sino también en quién accede a los datos, con qué propósito, bajo qué controles y con qué garantías para el usuario.

La ciberseguridad es un componente decisivo. La dependencia funcional de infraestructuras críticas aumenta cuando pagos, activos, identidades y registros operan sobre electricidad, telecomunicaciones, nube, centros de datos, sistemas de autenticación y redes de liquidación. Un ataque o incidente de seguridad de la información puede afectar disponibilidad, integridad, autenticidad o confidencialidad. La resiliencia requiere arquitectura redundante, copias verificadas, segmentación, autenticación robusta, monitoreo, respuesta a incidentes y opciones de operación fuera de línea cuando sean viables (IMF, 2024).

La alfabetización financiera digital será, por tanto, una condición de seguridad humana. No basta con que una persona tenga acceso formal a una aplicación o billetera si no comprende los riesgos de fraude, endeudamiento, exposición de datos, suplantación de identidad o pérdida de credenciales. La OCDE reportó que, en 2023, el 40% de adultos que compraron bienes y servicios en línea en 39 economías no alcanzó el puntaje mínimo de alfabetización financiera digital, lo cual confirma que la expansión de servicios



digitales puede crear vulnerabilidades cuando no va acompañada de educación y protección del usuario (Organisation for Economic Co-operation and Development [OECD], 2025).

El tercer riesgo es la ciberseguridad financiera. A medida que pagos, activos, contratos, identidades y valores se integran en infraestructuras digitales, aumenta la exposición de ataques contra sistemas de pago, billeteras, custodios, plataformas de inversión, contratos inteligentes y redes de liquidación. El FMI advierte que el sector financiero está altamente expuesto al riesgo cibernético y que un incidente severo podría generar riesgos macro financieros mediante pérdida de confianza, interrupción de servicios críticos y efectos de contagio hacia otras instituciones (IMF, 2024).

También debe considerarse la tensión global entre descentralización y regulación. Las redes públicas abiertas ofrecen verificabilidad y resistencia frente a la modificación unilateral de registros, pero plantean desafíos de identificación de responsables, privacidad, jurisdicción y cumplimiento normativo. Las redes autorizadas facilitan control y supervisión, aunque pueden concentrar poder. Por ello, no existe una arquitectura universalmente superior: la elección debe responder al riesgo, la finalidad y los derechos implicados.

El quinto riesgo es la fragmentación regulatoria. Las CBDC, los activos tokenizados y los valores digitales pueden circular a través de infraestructuras transfronterizas, pero los marcos legales siguen organizados principalmente por jurisdicciones nacionales. El FMI advierte que el éxito de la tokenización dependerá de confianza pública, marcos de política claros, activos seguros de liquidación, gobernanza robusta del código, certeza legal y coordinación internacional; sin esos anclajes, la tokenización podría amplificar inestabilidad por velocidad, concentración y fragmentación (Adrian, 2026).

En consecuencia, blockchain debe tratarse como infraestructura habilitadora, no como solución automática. Su utilidad dependerá de cómo se articule con dinero de banco central, entidades financieras privadas, reguladores, sistemas de identidad y marcos jurídicos. Desde la postura de la autora, su implementación solo es admisible cuando incorpora evaluación de impacto, seguridad y privacidad por diseño, gobernanza identificable, auditoría independiente, posibilidad de corrección y reparación, y canales no digitales para evitar exclusión.

Desde la seguridad humana, estos riesgos deben evaluarse en relación con la vida cotidiana. Una falla en pagos digitales puede impedir comprar alimentos, recibir salarios o acceder a servicios esenciales. Una brecha de datos puede exponer información sensible. Una CBDC mal diseñada puede generar temor de vigilancia. Una plataforma tokenizada vulnerable puede afectar ahorros e inversiones. Una infraestructura financiera concentrada puede reducir autonomía ciudadana. Por ello, la pregunta central no es si la tecnología funciona, sino si protege efectivamente a las personas.

ESCENARIOS PROSPECTIVOS DEL ORDEN FINANCIERO DIGITAL

El futuro del orden financiero digital no debe entenderse como una trayectoria única ni inevitable. Las CBDC, blockchain y la tokenización financiera pueden evolucionar de distintas maneras según el diseño institucional, la cooperación internacional, la regulación, la confianza pública, la ciberseguridad y la capacidad de los Estados para proteger derechos. Por ello, más que predecir un resultado definitivo, conviene plantear escenarios prospectivos que permitan anticipar oportunidades, riesgos y decisiones críticas.

IOSCO advierte que la tokenización de activos financieros tiene implicaciones para la protección



del inversionista y la integridad del mercado. Los riesgos incluyen incertidumbre sobre la naturaleza jurídica del token, dependencia de terceros emisores, fallas operativas, ciberseguridad, interoperabilidad, custodia y conexiones con mercados de criptoactivos menos regulados (IOSCO, 2025). Una gobernanza adecuada no elimina esos riesgos, pero puede reducirlos, distribuir responsabilidades, mejorar su detección y establecer mecanismos de respuesta y reparación.

Este escenario híbrido podría aportar beneficios para la seguridad humana si mejora la continuidad de los pagos, reduce costos, amplía inclusión financiera y mantiene garantías de privacidad, protección del usuario y supervisión democrática. Sin embargo, también exigirá capacidades estatales más sólidas en ciberseguridad, protección de datos, regulación financiera, educación ciudadana y coordinación internacional. La eficiencia técnica no será suficiente si los usuarios no confían en el sistema o si grupos vulnerables quedan fuera de la infraestructura digital.

Un segundo escenario es el de una concentración financiero-tecnológica. En este caso, grandes gestores de activos, bancos globales, proveedores de nube, plataformas de pagos, custodios digitales y empresas tecnológicas podrían controlar partes sustanciales de la infraestructura financiera tokenizada. La promesa sería eficiencia, escala y acceso ampliado; el riesgo sería dependencia tecnológica, asimetría de información, concentración de datos, poder de mercado y menor capacidad de los Estados para supervisar sistemas transnacionales complejos.

Este escenario debe preocupar a la seguridad humana porque la concentración de infraestructura puede afectar autonomía, privacidad y acceso. Si unas pocas entidades controlan la custodia, distribución, identidad digital, datos transaccionales o acceso a instrumentos financieros, los usuarios pueden quedar expuestos a decisiones opacas, fallas sistémicas o condiciones de ser-

vicio difíciles de cuestionar. En este contexto, la protección del ciudadano dependería no solo de innovación, sino de regulación efectiva, competencia, transparencia y rendición de cuentas.

La expansión de infraestructuras financieras digitales ofrece eficiencia, inclusión y modernización, pero también introduce vulnerabilidades relacionadas con ciberataques, control social financiero, desigualdad y exclusión. Estas consecuencias son pertinentes, aunque determinadas formas de tokenización todavía no estén plenamente consolidadas, porque ya existen implementaciones, pilotos y mercados en operación. El análisis se concentra en los efectos observados y en los riesgos razonablemente previsibles, no en presentar toda innovación como madura o inevitable (PNUD, 2022; IOSCO, 2025).

El primer riesgo es la privacidad financiera y el control social financiero. Las CBDC, blockchain y las plataformas tokenizadas permiten mayor trazabilidad, útil para prevenir fraude, lavado de activos y financiamiento ilícito. Pero el emisor público también debe estar sujeto a límites. En un Estado de derecho, legalidad, finalidad, necesidad, proporcionalidad, minimización de datos, autorización judicial cuando corresponda, supervisión independiente y recursos efectivos limitan el poder estatal. En República Dominicana, la Constitución y la Ley núm. 172-13 ofrecen una base general de protección de datos, pero una eventual CBDC exigiría normas específicas sobre acceso, conservación, intercambio, decisiones automatizadas y responsabilidad. Experiencias como Project Tourbillon del BIS muestran que es técnicamente posible explorar privacidad semejante al efectivo, aunque persisten compensaciones entre anonimato, seguridad y cumplimiento (BIS, 2023).

Un cuarto escenario, deseable desde el enfoque de este artículo, es el de una gobernanza humanista del dinero digital. Este escenario no rechaza la innovación financiera, pero la subordina a criterios de seguridad humana; privacidad,



inclusión, resiliencia, transparencia, protección de datos, alfabetización financiera, interoperabilidad segura y supervisión democrática. En esta visión, las CBDC, blockchain y la tokenización solo serán legítimas si fortalecen la protección de las personas y no únicamente la eficiencia de los mercados.

La alfabetización financiera digital es una condición de seguridad humana. En 2023, el 40 % de los adultos que compraron bienes o servicios en línea en 39 economías no alcanzó el puntaje mínimo de alfabetización financiera digital (Organisation for Economic Co-operation and Development [OECD], 2025). La autora propone que cualquier despliegue público incluya evaluación previa de brecha digital, formación accesible, simuladores de fraude, asistencia presencial, canales de reclamación, límites de responsabilidad del usuario y métricas periódicas de inclusión, desagregadas por edad, discapacidad, territorio y nivel socioeconómico.

El tercer riesgo es la ciberseguridad financiera. La integración de pagos, activos, contratos, identidades y valores en plataformas digitales incrementa

el número de componentes y dependencias susceptibles de ataque. Ransomware, denegación de servicio, compromiso de la cadena de suministro, robo de credenciales, manipulación de datos y explotación de contratos inteligentes pueden interrumpir pagos minoristas, salarios, remesas, cajeros, liquidación interbancaria y acceso a billeteras. El FMI advierte que un incidente severo puede producir pérdida de confianza y contagio: problemas de liquidez, retiros o interrupciones que se propagan desde una entidad conectada hacia otras y hacia la economía real (IMF, 2024).

En síntesis, el orden financiero digital hacia los próximos años estará marcado por una tensión entre eficiencia y protección. La eficiencia buscará pagos instantáneos, liquidación rápida, mercados continuos y activos programables. La protección exigirá privacidad, inclusión, ciberseguridad, regulación, resiliencia y confianza pública. Desde la seguridad humana, el criterio decisivo será si la nueva infraestructura financiera mejora la vida de las personas o si, por el contrario, crea nuevas formas de vulnerabilidad, dependencia y control.

CONCLUSIONES

El orden mundial digital constituye una dimensión emergente de la evolución global del siglo XXI. Sus efectos alcanzan el núcleo financiero: dinero, pagos, activos, mercados de capitales e infraestructuras de liquidación. El análisis muestra que las CBDC, blockchain y tokenización son categorías distintas, pero convergentes: dinero público digital, infraestructura de registro y proceso de representación de activos o derechos. Esta distinción evita tratarlas como activos equivalentes y permite evaluar sus consecuencias específicas.

Las CBDC pueden fortalecer el dinero público en la economía digital, modernizar pagos y favorecer inclusión. Sus resultados dependerán,

sin embargo, de límites jurídicos al tratamiento de datos, privacidad por diseño, opciones accesibles y fuera de línea, ciberseguridad, interoperabilidad, supervisión independiente y recursos efectivos. La responsabilidad primaria del Estado emisor no excluye controles sobre el propio Estado; exige reglas claras de competencia, finalidad, proporcionalidad, auditoría y rendición de cuentas.

Blockchain habilita nuevos modelos de registro y ejecución programada, pero no es una moneda, un contrato jurídico ni una garantía automática de confianza. La inmutabilidad relativa, la trazabilidad y la automatización aportan valor cuando existen datos confia-



bles y gobernanza adecuada; también pueden consolidar errores, ampliar exposición de datos o dificultar reparación. Por ello, toda aplicación financiera debe identificar responsables, auditar código y datos, prever reversión o compensación y someterse a controles de seguridad y legalidad.

La tokenización crea una convergencia entre mercados tradicionales e infraestructuras digitales. Puede reducir fricciones y ampliar acceso, pero el token solo ofrece seguridad cuando el derecho representado, el emisor, la custodia, la transferencia y la jurisdicción están claramente definidos. La protección del inversionista, la integridad del mercado y la resiliencia sistémica deben acompañar la innovación; la mera existencia de gobernanza no elimina el riesgo, pero permite asignarlo, supervisararlo y responder.

Desde la seguridad humana, estas tecnologías producen simultáneamente beneficios y vulnerabilidades. El desafío no es decidir si son buenas o malas, sino cómo proteger a las personas: minimización de datos, privacidad y seguridad por diseño, continuidad operativa, canales alternativos, alfabetización financiera digital, evaluación de impacto, supervisión independiente, transparencia algorítmica, debido proceso y reparación. Esas medidas conectan la eficiencia financiera con la protección de la dignidad y del ejercicio de derechos.

La naturaleza digital de pagos, ahorro, inversión e identidad financiera convierte su continuidad en un asunto de seguridad nacional, porque una interrupción amplia puede afectar estabilidad económica y funciones esenciales. A la vez, es un asunto de seguridad humana porque el im-

pacto recae en salarios, alimentos, salud, remesas, patrimonio, privacidad y autonomía de las personas. Esta relación justifica integrar resiliencia de infraestructura, protección de datos, inclusión y gobernanza regulatoria en una misma política pública.

Los escenarios prospectivos no son predicciones, sino instrumentos para anticipar riesgos y adoptar decisiones. Después de identificar señales tempranas, los Estados deben establecer indicadores, responsables, umbrales de intervención, pruebas de resiliencia y revisiones periódicas. Para evitar concentración financiero-tecnológica, se proponen requisitos de interoperabilidad y portabilidad, límites a conflictos de interés, supervisión de proveedores críticos, competencia efectiva, auditorías independientes y capacidades públicas que reduzcan dependencia de una sola plataforma.

En conclusión, las CBDC, blockchain y la tokenización deben incorporarse al debate interdisciplinario sobre economía, tecnología, derecho, seguridad, defensa, ética pública y protección humana. La legitimidad social del orden financiero digital dependerá de que sus beneficios se midan también por inclusión, privacidad, resiliencia y capacidad de reparación, y no solo por velocidad o rentabilidad. Como líneas futuras de investigación se proponen: evaluar la preparación jurídica e institucional de República Dominicana para una CBDC; medir brecha y alfabetización financiera digital en grupos vulnerables; comparar modelos internacionales de privacidad; analizar concentración y dependencia de proveedores críticos; y desarrollar indicadores de impacto sobre las dimensiones económica, personal y política de la seguridad humana.



REFERENCIAS

- Adrian, T. (2026). *Tokenized finance* (IMF Notes No. 2026/001). International Monetary Fund. <https://doi.org/10.5089/9798229042468.068>
- Bank for International Settlements. (2023). III. Blueprint for the future monetary system: Improving the old, enabling the new. En *BIS Annual Economic Report 2023*. <https://www.bis.org/publ/arpdf/ar2023e3.htm>
- Bank for International Settlements. (2025). III. The next-generation monetary and financial system. En *BIS Annual Economic Report 2025*. <https://www.bis.org/publ/arpdf/ar2025e3.htm>
- Bank for International Settlements. (2026, 27 de mayo). *Project Agora: Exploring tokenisation of wholesale cross-border payments*. BIS Innovation Hub. <https://www.bis.org/about/bisih/topics/fmis/agora.htm>
- Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5), 1754–1797. <https://doi.org/10.1093/rfs/hhz007>
- F/m Investments. (2026, 10 de marzo). *TBIL ETF tokenized shares: F/m Investments' SEC application—Investor & industry Q&A*. <https://www.fminvest.com/news/tbil-etf-tokenized-shares-fm-investments-sec-application-investor-industry-qa>
- Financial Stability Board. (2024). *The financial stability implications of tokenisation*. <https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/>
- Fink, L. (2025). *Larry Fink's 2025 annual chairman's letter to investors*. BlackRock. <https://www.blackrock.com/corporate/investor-relations/2025-larry-fink-annual-chairmans-letter>
- Illes, A., Kosse, A., & Wierst, P. (2025). *Advancing in tandem: Results of the 2024 BIS survey on central bank digital currencies and crypto* (BIS Papers No. 159). Bank for International Settlements. <https://www.bis.org/publ/bppdf/bispap159.htm>
- International Monetary Fund. (2024). *Global Financial Stability Report, April 2024: The last mile-Financial vulnerabilities and risks*. <https://www.imf.org/en/publications/gfsr/issues/2024/04/16/global-financial-stability-report-april-2024>
- International Monetary Fund. (2025). *Central bank digital currency: Further navigating challenges and risks* (Policy Paper No. 2025/041). <https://doi.org/10.5089/9798229032360.007>
- International Monetary Fund. (s. f.). *Central bank digital currency (CBDC): Virtual handbook*. Recuperado el 2 de junio de 2026, de <https://www.imf.org/en/topics/digital-payments-and-finance/central-bank-digital-currency/virtual-handbook>
- International Organization of Securities Commissions. (2025). *Tokenization of financial assets: Final report*. <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD809.pdf>
- Organisation for Economic Co-operation and Development. (2025). *Supporting informed and safe use of digital payments through digital financial literacy*. OECD Publishing. <https://doi.org/10.1787/21de47d1-en>
- Programa de las Naciones Unidas para el Desarrollo. (1994). *Human Development Report 1994: New dimensions of human security*. Oxford University Press. <https://hdr.undp.org/content/human-development-report-1994>



- Programa de las Naciones Unidas para el Desarrollo. (2022). *New threats to human security in the Anthropocene: Demanding greater solidarity*. <https://hdr.undp.org/content/2022-special-report-human-security>
- República Dominicana. (2013). Ley núm. 172-13, sobre protección integral de los datos personales. Gaceta Oficial núm. 10737.
- Santana González, R. (2021). Costo económico de los ciberataques no tipificados en las leyes dominicanas. *Revista Seguridad, Ciencia & Defensa*, 5(5), 32–39. <https://doi.org/10.59794/rscd.2019.v5i5.59>
- Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153–174. <https://doi.org/10.20955/r.103.153-74>
- Securities and Exchange Commission. (2026, 28 de enero). *Statement on tokenized securities*. <https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities>
- Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, 50(9), 14–17. <https://doi.org/10.1109/MC.2017.3571047>
- World Bank. (2023). *The global state of financial inclusion and consumer protection: 2022 report*. <https://documents1.worldbank.org/curated/en/099013124180517721/pdf/P16239315d0da60591bd9c1b6325ce5c6ef.pdf>
- World Economic Forum. (2025, 21 de mayo). *Asset tokenization in financial markets: The next generation of value exchange*. <https://www.weforum.org/publications/asset-tokenization-in-financial-markets-the-next-generation-of-value-exchange/>

