Journal of Interdisciplinary Research in Artificial Intelligence and Society,
2026, 2(1), Article 5
eISSN: 3117-793X

Review paper

Law and Politics of AI-Enabled Central Bank Digital Currency Governance: A Critical Integrative Review of Commercial Bank Deposit Stability, Digital Rights, Surveillance Risk, Democratic Accountability, and Global Justice in Emerging Economies

Shahida Sharmin*

Dhaka Commerce College, BANGLADESH

***Corresponding Author**: shahida.sharmin12@gmail.com

Citation: Sharmin, S. (2026). Law and politics of AI-enabled central bank digital currency governance: A critical integrative review of commercial bank deposit stability, digital rights, surveillance risk, democratic accountability, and global justice in emerging economies. journal of interdisciplinary research in artificial intelligence and society. *Journal of Interdisciplinary Research in Artificial Intelligence and Society, 2*(1), Article xx. https://doi.org/10.20897/jirais/19193

Published: August 25, 2026

ABSTRACT

Central bank digital currency (CBDC) is often presented as a technical response to declining cash use, private payment concentration, financial exclusion, and the rise of tokenized money. This critical integrative review argues that an AI-enabled CBDC is also a constitutional and political institution: it reallocates control over money, payment data, bank funding, and the conditions of economic participation. Integrating monetary, legal, financial-stability, digital-rights, AI-governance, and global-justice scholarship published across 2023–2026 with foundational theory, the review develops four findings. First, CBDC does not have a fixed effect on commercial bank deposits; deposit substitution, liquidity transformation, run risk, and credit supply depend on remuneration, holding limits, access architecture, interoperability, and the central bank's crisis backstop. Second, transaction-level data create a distinctive surveillance risk that cannot be resolved by encryption alone because lawful access, institutional separation, retention, inference, and remedy are legal choices. Third, AI can improve fraud detection, operational resilience, and supervisory intelligence, but it can also make financial exclusion, automated suspicion, and policy discretion less visible and harder to contest. Fourth, in emerging economies, digital divides, weak oversight, foreign technology dependence, and cross-border data flows turn CBDC design into a question of distributive and international justice. The review's originality lies in treating AI adoption as a governance-dependent institutional process rather than a purely technical or behavioral outcome. It proposes a rights-preserving framework based on legislative authorisation, public participation, tiered privacy, cash coexistence, prudential safeguards, human review, independent oversight, algorithmic audit, interoperability, and accessible offline capability. It concludes that CBDC should be judged not by technical novelty or adoption speed, but by whether it preserves monetary trust while limiting the concentration of economic and informational power.

Keywords: central bank digital currency, financial stability, digital rights, surveillance, democratic accountability, emerging economies

The debate over central bank digital currency has moved from monetary theory into the domain of public law and political economy. A retail CBDC is a digital form of central bank money made available to households and firms, while a wholesale CBDC is designed mainly for settlement among financial institutions. Both differ from

bank deposits because they are direct liabilities of the central bank. That difference gives CBDC a distinctive public-money function, but it also creates a new institutional relationship between citizens, central banks, commercial banks, payment intermediaries, and technology providers. The question is therefore not simply whether a CBDC can make payments faster. It is who may observe, restrict, verify, suspend, or contest the use of money, and under what legal authority (Latif & Yasin, 2025; Amin et al., 2026).

The policy momentum is substantial. The 2023 Bank for International Settlements (BIS) survey reported that 94 percent of responding central banks were exploring a CBDC, while the 2024 survey found that 91 percent of 93 respondents were exploring either a retail CBDC, a wholesale CBDC, or both (Di Iorio et al., 2024; Illes et al., 2025; Latif et al., 2026). This activity does not establish that issuance is necessary or welfare-enhancing. It shows instead that central banks are treating digital public money as part of a wider struggle over the future architecture of payments. In emerging market and developing economies, motivations commonly include financial inclusion, payment efficiency, resilience, and monetary sovereignty, but the same settings may have weaker connectivity, data-protection enforcement, cyber capacity, and democratic checks.

The central claim of this review is that CBDC governance should be evaluated as a legally bounded distribution of monetary and informational power. An AI-enabled CBDC is not merely a wallet with machine-learning tools attached. It is a sociotechnical system in which data collection, identity verification, transaction monitoring, risk scoring, liquidity management, and policy communication can be combined at scale. The addition of AI can improve detection and resilience, yet it can also convert discretionary judgments into automated classifications that are difficult for affected persons to understand or challenge. The core issue is therefore not whether AI is used, but whether the legal and institutional design makes its use proportionate, auditable, contestable, and compatible with democratic rights (Sindhura et al., 2025).

The review addresses four linked questions. First, how might CBDC design affect commercial bank deposits, bank funding, credit supply, and financial stability? Second, what legal and political risks arise when transaction data become a durable public record available for analytics and surveillance? Third, how should central bank independence be reconciled with legislative authorisation, public accountability, and individual remedies? Fourth, what does a just CBDC architecture require when emerging economies face unequal access to devices, networks, identity systems, technical expertise, and international bargaining power? The analysis treats these questions as mutually dependent. Deposit stability affects the political legitimacy of issuance; privacy affects adoption and trust; accountability affects the credibility of safeguards; and cross-border architecture affects sovereignty and distributive outcomes (Yasin & Latif, 2025).

The contribution is fourfold. First, the review brings monetary economics and financial-stability analysis into direct conversation with digital constitutionalism, privacy, and surveillance studies. Second, it reframes AI governance as an institutional question within payment infrastructure rather than an isolated model-risk problem. Third, it develops an emerging-economy lens that treats inclusion, sovereignty, and global justice as substantive design criteria rather than secondary implementation concerns. Fourth, it extends AI-adoption research by showing that adoption in a public financial infrastructure is legitimate and sustainable only when legal authority, data governance, accountability, and contestability are designed alongside technical capability. The argument is not that CBDCs should be rejected. It is that their legitimacy depends on whether they preserve the social functions of money while preventing a centralisation of economic and informational authority those citizens cannot meaningfully oversee.

REVIEW APPROACH AND ANALYTICAL FRAMEWORK

Scope and method

This article uses a critical integrative review rather than a systematic review or meta-analysis. An integrative review is appropriate because the relevant evidence is distributed across monetary models, banking studies, legal scholarship, policy papers, human-rights instruments, and research on algorithmic governance. The method seeks analytical integration: it compares the assumptions, concepts, and policy implications of these literatures and identifies tensions that remain hidden when each field is read in isolation. The review focuses on retail CBDC governance, while drawing on wholesale CBDC and cross-border arrangements where they illuminate legal authority, bank settlement, data flows, or geopolitical power.

The evidence base was assembled through targeted searches of peer-reviewed journal literature and major institutional repositories, including the Bank for International Settlements, International Monetary Fund, OECD, World Bank, central-bank, United Nations, Financial Stability Board, and national standards sources. Search concepts combined CBDC and related terms with commercial-bank deposits, financial stability, bank runs, privacy, surveillance, data governance, artificial intelligence, accountability, financial inclusion, monetary sovereignty, adoption, and emerging economies. Priority was given to peer-reviewed international journal articles and authoritative reports published from 2023 through 2026, while foundational works on privacy, accountability,

development, and public money were retained when they supplied concepts required for interpretation. Sources were included when they contributed a theoretical mechanism, legal principle, empirical finding, policy framework, or comparative case relevant to the four questions. Sources were excluded when they treated CBDC only as a technical ledger without addressing institutional consequences or when they made unsupported predictions about adoption. Because this is a critical integrative review rather than a systematic review or meta-analysis, the synthesis is interpretive and does not claim a complete census of the literature or a pooled effect estimate.

The synthesis proceeded in three stages. First, the literature was organised around four domains: monetary and banking stability; digital rights and surveillance; democratic accountability and institutional design; and global justice in emerging economies. Second, each domain was examined for mechanisms rather than slogans. For example, deposit stability was traced through funding costs, liquidity transformation, run incentives, and central-bank facilities; privacy was traced through data collection, access, retention, inference, and remedy. Third, the domains were recombined to identify design choices that produce cross-domain trade-offs. This method does not claim a statistical estimate of the average effect of CBDC. It provides a theoretically disciplined account of why effects are conditional and why safeguards must be designed together.

Analytical framework

The analytical framework treats CBDC governance as a relationship among four forms of power. Monetary power concerns who issues money, who intermediates credit, and who absorbs liquidity risk. Informational power concerns who can see, combine, infer, and retain transaction data. Administrative power concerns who can classify users, enforce rules, suspend accounts, and operate the system. Geopolitical power concerns whose standards, cloud infrastructure, identity systems, and cross-border rails shape the currency. AI acts as a multiplier across all four forms: it can make supervision more capable, but it can also widen the scale, speed, and opacity of public decisions.

This framework yields a demanding standard for policy evaluation. A technically secure system may still be unlawful if it collects excessive data or provides no remedy. A privacy-preserving system may still be unjust if it excludes people without smartphones or formal identity documents. A stable system may still be democratically unacceptable if the central bank can change programmable rules without legislative scrutiny. Conversely, a system with modest adoption may still improve welfare if it strengthens competition, preserves access to public money, and provides resilient offline payments. The evaluative question is therefore whether the complete institutional arrangement is proportionate, inclusive, accountable, and resilient, not whether one feature performs well in isolation.

Recent evidence and analytical gap

Recent evidence confirms that the field has moved beyond purely conceptual speculation but remains fragmented across disciplines. In financial-stability research, Ahnert et al. (2023) and Ponce and Taroco (2026) show that remuneration, holding limits, and liquidity arrangements can change the direction of the CBDC–bank-stability relationship, while Heitmann et al. (2025) provide new cross-country bank-level evidence of higher stability after CBDC launch. In inclusion and emerging-market research, Tan (2024), Dunbar and Treku (2024), Fan et al. (2025), and Le (2025) show that infrastructure, intermediation, openness, and institutional capacity condition whether digital public money broadens access or creates new dependency. In legal and rights research, Soana and de Arruda (2024), Murphy et al. (2024), Belikoff and Blazsek (2025), and Zafar (2026) show that privacy, financial integrity, data access, and regulatory authority are inseparable design questions.

The recent AI literature adds a second layer. Araujo et al. (2024), the Financial Stability Board (2024), and the Bank for International Settlements (2025) identify operational benefits from AI adoption in central banking and finance, but also risks involving model error, confidentiality, third-party concentration, cyber resilience, and systemic correlation. The reviewed literature rarely joins these AI-adoption concerns to the legal, monetary, and distributive consequences of a CBDC. This review responds by treating AI as a multiplier of four forms of power—monetary, informational, administrative, and geopolitical—and by asking how that multiplier changes bank intermediation, rights, accountability, and justice at the same time. Its originality is therefore analytical and institutional: it offers a framework for comparing CBDC choices across jurisdictions without assuming that a design that is workable in an advanced economy is automatically legitimate or feasible in an emerging economy.

CBDC AS A CONSTITUTIONAL AND INSTITUTIONAL CHOICE

Monetary authority and legal basis

CBDC issuance changes the legal object that citizens receive and the legal relationship that supports payment finality. If the token or account is a direct central-bank liability, the issuing institution must have authority to create

it, make it available to the public, operate or procure the payment platform, govern intermediaries, and resolve disputes. These questions are not formalities. The absence of a clear mandate can create uncertainty about legal tender, settlement finality, central-bank balance-sheet exposure, data responsibilities, and the rights of users against intermediaries. Legal scholarship and IMF analysis therefore treat statutory authorisation as a precondition rather than a post-launch compliance task (Bossu et al., 2020; Bechara et al., 2025; Latif et al., 2026).

The legal basis should distinguish at least three layers. The first is monetary law: what counts as currency or central-bank money and whether the CBDC has legal-tender status. The second is public-administration law: what the central bank may do directly, what it may delegate to commercial banks or payment providers, and how discretion is supervised. The third is private law: the contractual, property, consumer-protection, error-resolution, and liability rules governing wallets, transfers, fraud, outages, and insolvency. Treating these layers as one technology problem risks allowing operational documents or vendor contracts to perform functions that should be determined through legislation.

The legal debate also exposes a constitutional tension. Central-bank independence protects monetary policy from short-term political pressure, but a public payment platform may exercise powers that affect privacy, association, equality, property, and access to basic economic life. Independence cannot mean immunity from public law. A central bank may need operational autonomy to run a payment system while remaining bound by statutory purposes, procedural safeguards, transparency duties, judicial review, independent data oversight, and legislative control over major changes in the rights architecture. Digital constitutionalism is useful here because it asks how public and private digital infrastructures should be constrained by legality, rights, separation of powers, and contestability (Celeste, 2019; Kowsar et al., 2025). The public-money dimension also matters: the equivalence between private and public money is institutionally contingent, not a reason to treat their legal and political consequences as identical (Brunnermeier & Niepelt, 2019).

The 2024 BIS survey illustrates why this distinction matters for emerging economies. Among responding emerging market and developing economy central banks working on CBDC, the share reporting legal authority to issue a retail CBDC was materially higher than in advanced economies, but a large minority still lacked a clear basis or remained uncertain about it (Illes et al., 2025). A formal mandate is not equivalent to a complete framework. It must be accompanied by rules for data access, institutional separation, procurement, resilience, consumer protection, and the distribution of losses when a system fails.

Institutional architecture and AI-enabled governance

A two-tier model is often proposed in which the central bank issues the liability and private intermediaries provide wallets, customer service, onboarding, and payment interfaces. The model can preserve commercial-bank relationships and use existing compliance capacity, but it does not eliminate public responsibility. The central bank still defines technical standards, access criteria, transaction limits, data schemas, and the conditions under which intermediaries may act. A public-private architecture may also diffuse accountability: users may be unable to determine whether a denial or outage was caused by the central bank, a bank, a payment service provider, an identity vendor, a cloud operator, or an AI model.

AI enters this architecture through fraud detection, anti-money-laundering analytics, cyber defence, demand forecasting, liquidity monitoring, customer support, and supervisory technology. Central banks are already exploring machine learning for statistics, macroeconomic analysis, payment oversight, supervision, and financial-stability work (Araujo et al., 2024). These applications can be valuable because payment systems produce high-volume, high-frequency data that are difficult to review manually. However, a model that flags an unusual transfer is not merely an efficiency tool if the flag causes a wallet freeze, a reporting obligation, or a refusal of service.

AI-enabled governance should therefore be divided into at least two categories. Operational AI supports system reliability, fraud detection, and service delivery; its errors can cause financial loss, service interruption, or discriminatory friction. Policy AI supports decisions about limits, risk thresholds, monetary operations, and supervisory prioritisation; its errors can affect macroeconomic conditions and the distribution of state attention. The second category demands heightened safeguards because it can influence the rules under which the first category operates. In both categories, model performance must be assessed against distributional effects, false positives, false negatives, data drift, adversarial behaviour, and dependence on external providers.

The National Institute of Standards and Technology (2023) frames trustworthy AI through governance, mapping, measurement, and management across the system life cycle. The OECD principles and UNESCO's global recommendation similarly connect robustness, transparency, accountability, and human rights to democratic values (OECD, 2019, 2023; UNESCO, 2021). Emerging binding rules, such as the European Union's Artificial Intelligence Act, illustrate how risk-based duties can be translated into enforceable governance requirements even though their jurisdictional reach is limited (European Union, 2024). These frameworks are useful but not self-executing. CBDC statutes and supervisory rules should translate them into enforceable duties: documented purposes, data minimisation, independent validation, human review, incident reporting, model inventories,

procurement controls, and a right to obtain reasons and seek correction when an automated process materially affects access to money.

DEPOSIT STABILITY AND COMMERCIAL-BANK INTERMEDIATION

Why CBDC can intensify disintermediation

Commercial banks perform maturity transformation by funding relatively illiquid assets with callable deposits. A retail CBDC offers a public, highly liquid alternative that may be safer than an individual bank deposit, especially during stress. If households and firms move a significant share of transactional balances from banks to CBDC wallets, banks may lose low-cost deposit funding and respond by raising deposit rates, substituting wholesale funding, reducing lending, increasing fees, or taking more risk. The effect is not mechanically determined by the existence of CBDC. It depends on whether users view the CBDC as a payment instrument, a store of value, or a safe haven.

The theoretical literature identifies this trade-off. Agur et al. (2022) and Latif et al. (2026) show that the design of CBDC relative to cash and deposits affects the allocation of users among payment instruments and the degree of pressure on bank intermediation. Keister and Sanches (2023) emphasise that improved exchange efficiency can coexist with deposit crowd-out, higher bank funding costs, and lower investment, while Ahnert et al. (2024) synthesise the wider monetary and financial-stability trade-offs. The concern is especially acute when CBDC is interest-bearing, unlimited, frictionless to acquire, and directly accessible during a bank panic. Under those conditions, the currency can function as an always-open exit from commercial-bank liabilities.

Digital technology can also change the speed of a run. A transfer from a bank deposit to a CBDC wallet may be completed continuously, remotely, and at low cost. A model trained on payment flows may identify stress earlier, but it may also accelerate the reaction of users if risk signals become public or if algorithmic alerts trigger simultaneous precautionary withdrawals. The speed of movement matters because a bank can be solvent over a longer horizon yet unable to liquidate assets quickly enough to meet a concentrated demand for withdrawal. CBDC can thus reduce some frictions that previously slowed a run while increasing the value of timely supervision and credible liquidity support.

Why stability effects are conditional

The disintermediation argument is not one-sided. A CBDC can make banks less fragile if it reduces excessive maturity transformation, improves payment settlement, and gives authorities better information about liquidity conditions. Keister and Monnet (2022) model two countervailing effects: CBDC can increase the incentive to run from a weak bank, but it can also reduce banks' exposure to runs and help authorities identify weak institutions sooner. Fernández-Villaverde et al. (2021) likewise show that a central bank may be more stable than private banks during panic conditions, although large-scale public intermediation raises questions about credit allocation and institutional capacity.

Other models reach more cautionary conclusions. Kim and Kwon (2023) and Yellamma et al. (2025) show that CBDC deposits can reduce bank credit supply and increase the likelihood of panic unless the central bank recycles or lends the funds back to banks. Schilling et al. (2024) identify a trilemma among efficient allocation, financial stability, and price stability when the central bank becomes involved in financial intermediation. The implication is that a CBDC cannot be evaluated through a single slogan such as 'CBDC causes bank runs' or 'CBDC improves stability.' The result depends on remuneration, caps, liquidity facilities, deposit insurance, resolution rules, collateral policy, and the central bank's ability to communicate credible limits.

Empirical evidence now complicates the theoretical picture. Luu et al. (2023) find a positive association between CBDC adoption and bank stability, and Heitmann et al. (2025) similarly report higher bank stability after launch in a dynamic-panel study. These results are important but should not be read as universal causal proof: jurisdictions that pilot or launch a CBDC may already have stronger institutions, and aggregate bank-stability measures may not capture distributional effects on small banks or credit supply. Ahnert et al. (2023) and Ponce and Taroco (2026) show why design parameters—especially remuneration, holding limits, and liquidity arrangements—can reverse the direction of the stability effect. The appropriate conclusion is conditional rather than binary: CBDC can stabilise the system when its design preserves intermediation and credible liquidity support, but it can accelerate safe-haven migration when it is frictionless and weakly constrained.

Emerging-economy transmission

Recent work also shows why emerging-economy transmission cannot be inferred from advanced-economy models alone. Dunbar and Treku (2024) demonstrate that access to a CBDC is not equivalent to meaningful access to banking: inclusion depends on whether infrastructure, intermediaries, and user protections reduce practical

barriers. Fan et al. (2025) highlight the constraints faced by small open economies, while Le (2025) places CBDC alongside cryptocurrency competition and monetary sovereignty in emerging markets. These studies reinforce the need to test deposit migration, foreign-currency substitution, connectivity, and intermediary concentration jointly rather than treating adoption as a uniform shock.

The banking implications may be sharper in emerging economies because deposits are often a central source of domestic credit, capital markets are thinner, foreign-currency liabilities are more important, and lender-of-last-resort capacity is more constrained. A shift into CBDC could improve safety for depositors while increasing funding costs for small banks that already face limited access to wholesale markets. The distributional effect may be uneven: large banks and telecommunications firms may capture the new payment business, while rural banks, credit cooperatives, and informal agents lose transaction revenue or customer data.

The policy response should be proportionate and context-specific. Holding limits can reduce the use of CBDC as a savings substitute, but limits may also harm households that need a safe account when banks are inaccessible. Nonremuneration can preserve the distinction between money and savings, but it may reduce adoption when inflation is high. Tiered accounts can broaden access for low-risk users, but they must not create a second-class form of money with unreliable service or excessive surveillance. Liquidity facilities can prevent a bank run, but they may socialise risk and weaken incentives for prudent management. The point is not to select one universal feature. It is to connect each feature to a public objective, a measurable risk, and a transparent review process.

A prudent framework would require pre-launch stress testing of deposit migration under ordinary use, rumors, cyber incidents, payment outages, inflation shocks, and bank-specific distress. Testing should include small and rural banks, households with limited digital access, and foreign-currency substitution scenarios. The results should inform caps, emergency conversion rules, central-bank lending, deposit insurance communication, and a sunset or revision mechanism. Commercial banks should not be protected from competition merely because CBDC exists; they should be protected from destabilising design and abrupt institutional change. In this sense, deposit stability is a condition of legitimate public-money innovation, not a veto against it.

Table 1 summarises the principal CBDC design variables, their deposit-stability channels, and the corresponding policy responses. **Figure 1** illustrates how these design choices influence conversion behaviour, bank funding, credit provision, run dynamics, and liquidity outcomes.

Table 1

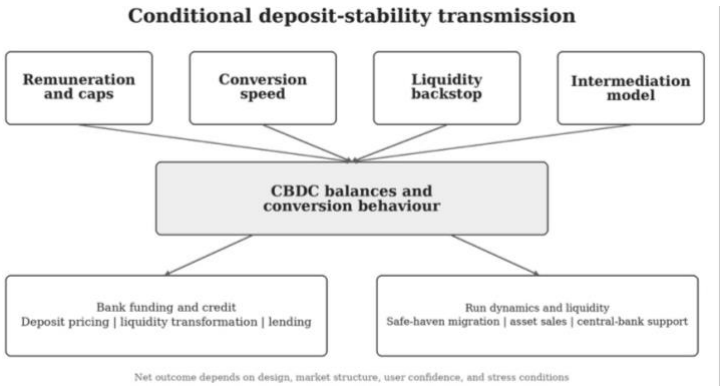
CBDC design and deposit-stability channels

Design variable	Stability channel	Response
Remuneration and caps	Deposit substitution	Calibrate through stress tests
Conversion speed	Faster safe-haven movement	Tiered limits and monitoring
Liquidity backstop	Cbdc drains bank funding	Pre-arranged lending facilities
Intermediation model	Credit-supply pressure	Two-tier delivery and review

Note. Author's synthesis.

Figure 1

CBDC design, bank funding, credit, and liquidity outcomes



Note. Author's synthesis.

DIGITAL RIGHTS, SURVEILLANCE, AND DATA GOVERNANCE

Privacy as constitutional infrastructure

Cash does more than settle a transaction. It allows people to transact without creating a permanent, centrally searchable record of every purchase, association, donation, or movement. A CBDC can reproduce some of that

privacy, but it cannot do so by default if its architecture links identity, wallet, device, merchant, location, and transaction history. Privacy is therefore not a narrow consumer preference. It is an enabling condition for autonomy, association, dissent, and equal participation in social life. Garratt and van Oordt (2021) describe payment privacy as a public good because individuals do not bear all of the social costs when privacy is weakened. Nissenbaum (2010) further shows that privacy depends on appropriate flows of information, not on secrecy in the abstract.

The legal risk arises at several points in the data life cycle. Data may be collected during onboarding, generated during payment, enriched through device or location information, inferred through behavioral models, shared with intermediaries or law-enforcement agencies, retained for long periods, and used for purposes that were not visible at the time of payment. Each step can be lawful in isolation yet collectively produce a system of continuous financial observation. Solove's (2006) taxonomy helps show why the harm may involve aggregation, identification, exclusion, and secondary use rather than disclosure alone; Jiang (2023), Soana and de Arruda (2024), and Zafar (2026) similarly emphasise that CBDC privacy depends on architecture, institutional separation, and legal governance, not only on confidentiality during transmission. A privacy analysis that focuses only on encryption at the point of transfer misses the broader question of who can assemble the record, who can authorise access, and what inferences can be drawn from it.

The international human-rights framework reinforces this concern. The right to privacy protects against arbitrary or unlawful interference, while freedom of expression, association, equality, and participation may be chilled by pervasive monitoring (Office of the United Nations High Commissioner for Human Rights, 2018; United Nations, 1966). CBDC governance should therefore apply legality, necessity, proportionality, purpose limitation, data minimisation, security, independent authorisation, and effective remedy. A general promise that data will be used responsibly is inadequate where a central bank or service provider has technical access to detailed economic behaviour.

AI-enabled surveillance and function creep

AI changes the surveillance problem because it turns records into predictions. A transaction history can be used not only to verify whether a payment occurred but to classify a person's income stability, political associations, health-related purchases, religious giving, or likelihood of future conduct. A model may infer risk from correlations that the person never supplied and cannot inspect. This makes privacy harm more than unauthorised disclosure. It includes the loss of contextual boundaries and the possibility that an inferred profile becomes the basis for a denial, investigation, or restriction.

The risk of 'function creep' is particularly strong in a national payment infrastructure. A system introduced to reduce fraud may later support tax enforcement, social-benefit conditions, capital controls, sanctions screening, credit scoring, public-order monitoring, or commercial data analytics. Some secondary uses may be legitimate, but legitimacy cannot be assumed because the data already exist. A new purpose changes the balance of rights and interests. It should require a new legal basis, public justification, impact assessment, and a way for affected persons and legislatures to contest the change. Otherwise, technical reuse can become an informal expansion of state power.

The AI layer can also transform selective surveillance into population-scale surveillance. Rule-based monitoring generally specifies known indicators; machine-learning systems can search for anomalies across the entire payment population. False positives may be concentrated among migrants, informal workers, low-income households, small merchants, or users whose transaction patterns differ from the training data. A risk score can then reproduce existing inequalities while appearing neutral because it is generated by a statistical model. Benjamin (2019), Couldry and Mejias (2019), and Zuboff (2019) help explain why data extraction and automated classification can make inequality and surveillance computationally durable even when a system is not explicitly designed to discriminate.

A rights-preserving approach should distinguish anonymous or pseudonymous payment from unlawful payment. Anti-money-laundering rules require risk-based controls, not unlimited visibility into every transaction. Wang (2023) shows that the optimal privacy design depends on the interaction between anonymity, interest, laundering incentives, and output. Murphy et al. (2024) and Belikoff and Blazsek (2025) similarly emphasise that institutional arrangements, collection rules, access controls, storage policies, design choices, and privacy-enhancing technologies must be considered together. The legal objective is not absolute anonymity. It is constrained, reviewable, and proportionate access that preserves ordinary transactional privacy while enabling targeted investigation under due process.

Privacy-preserving design and accountability

Privacy by design should begin with institutional separation. The entity that operates the payment interface need not have access to the complete transaction history; the central bank need not have direct visibility into

identifiable retail activity; and law-enforcement access need not be routed through the monetary-policy function. Separation reduces the risk that a single authority can combine issuance, identity, transaction analytics, enforcement, and rule changes. It also creates clearer lines of responsibility for warrants, audits, complaints, and data breaches.

Technical measures can support this separation. They include tokenisation, pseudonymous identifiers, selective disclosure, threshold or tiered privacy, secure multiparty computation, zero-knowledge proofs, hardware-secured offline limits, and privacy-preserving analytics. These tools should not be treated as magic solutions. They can fail through poor implementation, metadata leakage, reidentification, weak governance, or exceptional-access rules. Technical claims must be independently tested, publicly documented to the extent consistent with security, and linked to legal guarantees that prevent the quiet expansion of access. The privacy promise should be measurable through retention periods, access logs, audit results, error rates, and the number and type of disclosures.

User trust is also an empirical issue. Choi et al. (2025) find that willingness to use CBDC varies with the degree of privacy protection and with information about privacy benefits. Recent adoption studies add that uptake is shaped by institutional and behavioral conditions: Bai et al. (2025) provide initial evidence from China, while An et al. (2024) show that emotional and technology-acceptance factors influence digital-currency use. These studies are valuable, but they mainly treat adoption as an individual or firm-level behavioral outcome. This review extends that conversation by arguing that users adopt public digital money sustainably only when privacy, access, remedy, and institutional trust are credible. User preference surveys do not settle the legal question. Individuals may accept surveillance because they have no practical alternative, because the consequences are uncertain, or because the payment system is necessary for wages and public benefits. Consent in a public infrastructure cannot substitute for structural limits on state power.

The minimum safeguard is an enforceable right to know, understand, and challenge. Users should receive accessible explanations of data categories, model-supported decisions, disclosure rules, retention periods, and human-review channels. A person whose wallet is frozen or whose transaction is denied should be able to obtain a reason, correct inaccurate information, and obtain timely review. Independent data-protection authorities, ombudspersons, courts, legislatures, and civil-society auditors should be able to inspect the system. These mechanisms convert privacy from a promise into an accountability relation.

Table 2 maps each stage of the AI-enabled CBDC data lifecycle to its principal AI function and required safeguard. **Figure 2** traces the progression from data collection and inference through automated decision-making, human review, remedy, and independent oversight.

Table 2

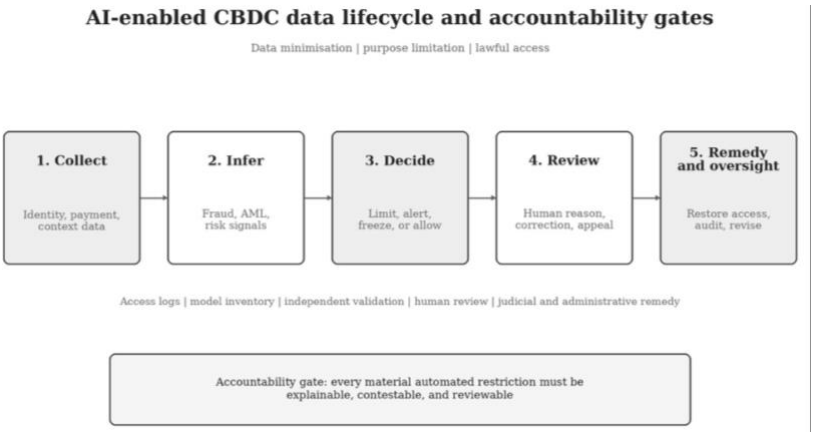
AI-enabled CBDC data lifecycle and safeguards

Lifecycle stage	AI function	Safeguard
Onboarding	Identity and eligibility	Purpose limits; non-digital route
Monitoring	Fraud and AML flags	Threshold validation; error audits
Decision	Freeze or transfer review	Reasons; human review; appeal
Retention and sharing	Linkage and analytics	Retention limits; access logs
Model change	Recalibration or update	Independent test; public notice

Note. Author's synthesis.

Figure 2

AI-enabled CBDC data lifecycle and accountability gates



Note. Author's synthesis.

DEMOCRATIC ACCOUNTABILITY AND GLOBAL JUSTICE

Central-bank independence versus democratic control

CBDC governance makes the boundary between monetary policy and general administration more visible. A central bank may be independent when setting interest rates, yet it may exercise ordinary administrative power when deciding who can access an account, how data are shared, what fees intermediaries may charge, or which transfers are blocked. Those decisions affect rights and distributive outcomes even when they are described as operational matters. Accountability must therefore follow the function being performed, not the institutional label of the actor performing it.

Public accountability requires answerability, transparency, review, and consequences. Scott (2000) and Latif and Yasin (2025) distinguishes the institutional relationships through which regulators can be called to account, while Bovens et al. (2014) and Dube et al. (2025) emphasize the importance of a forum before which an actor must explain and justify conduct. Black (2008) and Latif et al. (2025) add that legitimacy and accountability become more difficult when authority is distributed across a polycentric regulatory regime. A CBDC statute should specify which forum reviews which decision: legislatures should review mandates, major design changes, and public-resource commitments; independent regulators should supervise data protection, competition, and consumer protection; courts should review legality and rights violations; and auditors should examine security, procurement, model risk, and operational resilience.

Participation should occur before technical specifications become fixed. Consultation limited to banks, vendors, and central-bank experts may produce a technically coherent system that fails to reflect the needs of informal workers, women, rural users, persons with disabilities, migrants, and small merchants. Public deliberation should address whether cash remains available, how offline payments work, what identification is necessary, whether public benefits can be received without a smartphone, and what happens during outages or political emergencies. Participation is not a referendum on cryptography. It is a way to identify the social functions that the system must preserve.

Inclusion, exclusion, and distributive justice

Financial inclusion is a plausible rationale for CBDC, but it should not be equated with digitisation. The Global Findex reports major growth in account ownership and digital payments while also documenting persistent gaps by income, gender, education, age, and geography (Demirgüç-Kunt et al., 2022). A CBDC can lower transaction costs, provide a public-money anchor, and support low-cost transfers. It can also reproduce exclusion when access depends on a phone, network, electricity, biometric identity, literacy, or an intermediary that charges fees or rejects users.

Tan (2024) shows that CBDC can improve financial inclusion under conditions that address the barriers faced by excluded users. Dunbar and Treku (2024) and Latif, Mussayeva, et al. (2026) likewise caution that access outcomes depend on the surrounding banking and payment ecosystem. Those conditions are not automatically created by issuance. They include low-cost access, usable interfaces, agent networks, consumer protection, financial literacy, interoperability, offline functionality, and a reliable method for recovery when a device is lost. Inclusion also requires that users can hold and use the currency without being forced to surrender more personal data than similarly situated users of cash or ordinary payment instruments.

A capability approach is helpful because it asks what people are substantively able to do rather than whether an account technically exists (Sen, 1999; Latif et al., 2026). On this view, a CBDC is inclusive only if individuals can make and receive payments, preserve reasonable privacy, understand important decisions, obtain redress, and participate without unreasonable exposure to surveillance or technological dependency. Distributional analysis should examine who gains from lower fees and better access, who bears infrastructure costs, whose data are used for model training, and who is most likely to be falsely flagged or disconnected. An architecture that improves aggregate efficiency while narrowing the practical freedom of vulnerable groups is not automatically just.

Cash coexistence is therefore a justice requirement, not a sentimental preference. Cash serves as a fallback during outages, a low-tech instrument for people excluded from digital systems, and a privacy-preserving means of exchange. Removing it before a CBDC is demonstrably accessible shifts transition risk onto those least able to absorb it. A rights-respecting policy should preserve cash for as long as there is a meaningful social need, provide non-digital support, and treat accessibility as an ongoing public obligation rather than a temporary pilot feature.

6.3 Cross-border power and global governance

The international dimension of CBDC creates both opportunity and asymmetry. Interoperable CBDC arrangements could reduce the cost and delay of remittances, trade settlement, and regional payments. They could also reconfigure correspondent banking, capital-flow management, sanctions enforcement, and currency

competition. BIS analysis identifies multiple ways to connect CBDC systems, from common standards to shared infrastructure, but each option distributes control over data, access, compliance, and settlement differently (Auer et al., 2022). Cross-border convenience is therefore inseparable from questions of sovereignty and jurisdiction.

Emerging economies may gain from faster remittances and reduced dependence on expensive intermediaries, yet they may also become dependent on foreign cloud platforms, identity providers, cryptographic standards, and analytics vendors. Fan et al. (2025) and Le (2025) show why the benefits and risks of openness are particularly acute in small and emerging markets. The data generated by domestic payments may be processed outside the issuing country or combined with foreign databases. A system that is formally sovereign but operationally dependent can narrow policy autonomy. Global justice requires attention to who sets technical standards, who bears cyber and outage risks, whose laws govern data access, and whether smaller countries have a meaningful voice in international arrangements.

The IMF's CBDC handbook emphasises that cross-border design, legal foundations, stakeholder engagement, and risk containment should be considered from the outset rather than after domestic issuance (International Monetary Fund, 2025; Latif et al., 2026). This is especially important where currency substitution and dollarisation pressures are present. A CBDC may support the domestic unit of account, but it may also make foreign digital money easier to access if interoperability is poorly designed. Policy should seek open and reciprocal standards, local capacity building, transparent governance of shared infrastructure, and safeguards against cross-border surveillance. The objective is not technological autarky. It is the ability of emerging economies to participate in digital monetary networks without surrendering the capacity to protect their people and pursue legitimate public policy.

Table 3 identifies the principal justice risks facing emerging economies and presents context-sensitive responses concerning access, affordability, sovereignty, cross-border data, and participation.

Table 3

Emerging-economy justice risks and responses

Justice dimension	Main risk	Response
Access	Device, network, or identity exclusion	Offline wallets; cash; agents
Affordability	Fees and data costs	Basic low-cost tier; consumer rules
Sovereignty	External infrastructure dependence	Open standards; local capacity
Cross-border data	Foreign access and function creep	Jurisdiction rules; oversight
Participation	Marginalized groups absent	Inclusive consultation; impact review

Note. Author's synthesis.

AN INTEGRATED GOVERNANCE FRAMEWORK

Design principles

The preceding analysis suggests that CBDC governance should be organised around a bundle of mutually reinforcing principles. The first is legality: issuance, access, data processing, programmability, and exceptional powers must have a clear statutory basis. The second is public purpose: every material feature should be linked to an articulated objective and reviewed against evidence of benefit. The third is proportionality: surveillance, identity requirements, restrictions, and model complexity should not exceed what is necessary to address a defined risk. The fourth is coexistence: CBDC should complement rather than prematurely displace cash, bank deposits, and accessible private payment options. The fifth is contestability: users and affected communities must be able to understand, challenge, and obtain correction of decisions. The sixth is institutional pluralism: no single actor should control issuance, identity, data, enforcement, and model oversight.

These principles produce a practical governance matrix. Deposit stability requires calibrated holdings, nonpunitive remuneration, liquidity facilities, resolution planning, and transparent stress testing. Digital rights require data minimisation, tiered privacy, separation of functions, selective disclosure, retention limits, and independent access controls. AI governance requires a model inventory, data provenance, validation, bias testing, cyber resilience, human review, and incident reporting. Democratic accountability requires legislative authorisation, public participation, independent supervision, auditability, judicial remedy, and a mechanism for revising rules. Global justice requires interoperability on fair terms, offline access, local capacity, and protection against technological and jurisdictional dependency.

Legal and institutional safeguards

The safeguards should be written into the life cycle of the system rather than placed in an ethics statement. At the authorisation stage, legislation should define the CBDC's legal nature, central-bank mandate, user rights,

intermediary duties, cash status, data purposes, and emergency powers. At the design stage, authorities should conduct financial-stability, human-rights, data-protection, accessibility, gender, and distributional impact assessments. At the pilot stage, evaluation should include ordinary and stress scenarios, independent red-team testing, public reporting, and evidence from users who face access barriers. At the production stage, oversight should continue through audits, model monitoring, incident disclosure, complaint data, and periodic legislative review.

Programmability deserves special caution. Programmable payments can automate conditions such as delivery, escrow, or benefit distribution. Programmable money can attach restrictions to what a unit may be used for, where it may be spent, or when it expires. The latter can be useful in narrowly defined public programmes, but it also creates a route for coercion and political control. Restrictions should be authorised by law, specific in purpose, time-limited, reviewable, and subject to due process. General-purpose money should not become conditional money through software updates that avoid legislative scrutiny. The same rule applies to AI-generated risk thresholds: a model update that changes who is investigated or excluded is a substantive governance event, not a routine technical patch.

The framework should also assign responsibility across the public-private ecosystem. The central bank should remain accountable for core monetary and payment-system functions even when delivery is outsourced. Intermediaries should be responsible for customer service, error correction, and compliance within clear legal limits. Technology providers should be subject to security, audit, documentation, localisation, and subcontracting requirements. Independent authorities should have access to logs, model documentation, and testing environments. Users should have a single accessible channel for complaints, even if responsibility is later allocated among several actors. Accountability that requires a user to identify the correct layer of a complex architecture is not meaningful accountability.

Practical implications for implementation

For central banks, the practical implication is to treat CBDC issuance as a gated public-infrastructure programme rather than a technology launch. Before a pilot, the authority should publish the legal mandate, intended public purposes, data map, model inventory, intermediary responsibilities, cash-coexistence plan, and measurable exit criteria. Before expansion, it should test deposit migration under ordinary use, rumors, cyber incidents, outages, inflation shocks, and bank-specific distress; report false-positive and false-negative rates for AI-supported controls; and demonstrate that human review and appeal channels can restore access within a timeframe compatible with economic life. The Bank for International Settlements (2025) and the Financial Stability Board (2024) support this emphasis on adaptive governance, model-risk controls, and monitoring of third-party dependencies.

For legislatures and independent regulators, the implication is to allocate responsibility before implementation. Legislation should define the CBDC's legal nature, data purposes, programmable-payment limits, emergency powers, user rights, and remedies. Independent data-protection, competition, consumer-protection, and audit bodies should have access to logs, model documentation, procurement records, and testing environments. A single public complaint channel should be available even when the system is delivered through several private intermediaries. Belikoff and Blazsek (2025) and Zafar (2026) reinforce the need to connect technical architecture to enforceable legal duties rather than relying on nonbinding ethical statements.

For commercial banks, wallet operators, and technology providers, the implication is operational and contractual. They should maintain clear responsibility for onboarding, error correction, security, customer service, data separation, model validation, incident reporting, and subcontractor oversight. Intermediaries should not be rewarded for maximising data extraction or automated rejection. Procurement contracts should require interoperability, audit access, portability, continuity planning, localisation where legally justified, and disclosure of material model changes. For emerging-economy policymakers and international standard-setters, implementation should prioritise offline access, agent networks, local technical capacity, open and reciprocal standards, and cross-border rules that prevent foreign infrastructure from becoming an unreviewable substitute for domestic governance.

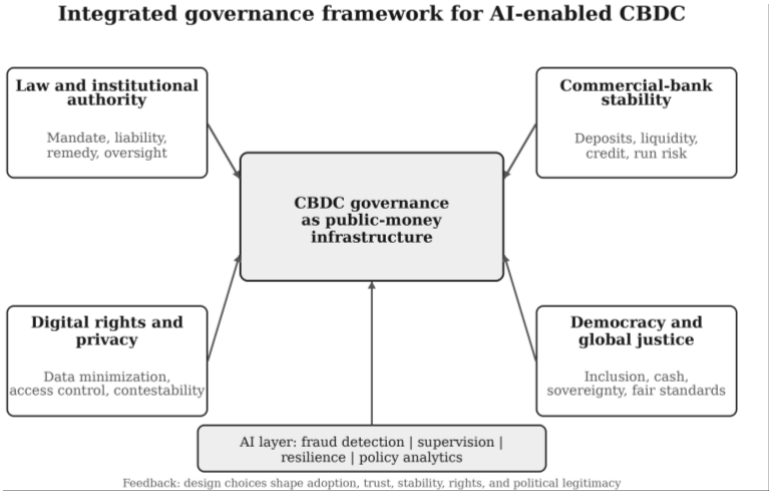
Table 4 consolidates the primary risks and minimum safeguards across the five domains of AI-enabled CBDC governance. **Figure 3** integrates deposit stability, digital rights, AI governance, democratic control, and global justice within a unified governance framework.

Table 4
Integrated AI-enabled CBDC governance priorities

Governance domain	Primary risk	Minimum safeguard
Deposit stability	Deposit migration	Caps; liquidity support
Digital rights	Persistent surveillance	Privacy tiers
AI governance	Opaque flags	Model inventory; review
Democratic control	Rule changes	Statutory limits; review
Global justice	Infrastructure dependency	Interoperability

Note. Author's synthesis.

Figure 3
Integrated governance framework for AI-enabled CBDC



Note. Author's synthesis based on the literature reviewed in the manuscript.

RESEARCH AGENDA

Broader contribution to global AI-adoption research

Although this article is not an AI-adoption survey, it contributes to global AI-adoption research by shifting the unit of analysis from software uptake to institutionally mediated capability. Central banks may adopt AI because it improves forecasting, fraud detection, supervision, and resilience, but legitimate adoption also requires legal authority, data minimisation, model validation, human review, and redress. Adoption is therefore not complete when a model is deployed; it is sustainable only when users, intermediaries, regulators, and affected communities can understand and contest its operation. This interpretation connects the governance concerns identified by Araujo et al. (2024), the Financial Stability Board (2024), and the Bank for International Settlements (2025) with the trust and privacy concerns identified in CBDC adoption research.

The framework also generalises beyond CBDCs. Across jurisdictions, AI adoption in public and financial infrastructures depends on four conditions: mission alignment, informational and data governance, administrative accountability, and geopolitical or technical sovereignty. The balance differs across advanced and emerging economies, which explains why findings from one institutional setting cannot be transferred automatically to another. Privacy, fairness, inclusion, and remedy are not external ethical constraints added after adoption; they are determinants of trust and sustained use. The broader contribution is thus a political-economy lens that complements behavioral models of technology acceptance and encourages future research to examine who gains authority, who bears risk, and who can contest AI-mediated decisions.

Future research agenda

The literature is rich in models and design proposals but relatively thin in evidence from live deployments and emerging-economy stress conditions. The recent growth of empirical adoption and AI-governance research does not remove this limitation because pilot exposure, actual wallet balances, model deployment, and stress-period behaviour are still measured inconsistently. Future research should therefore move beyond binary questions about whether CBDC or AI is good or bad. First, comparative bank-level studies should distinguish pilot exposure, actual wallet balances, deposit substitution, bank size, ownership, market concentration, and the availability of lender-of-

last-resort facilities. Natural experiments should examine whether payment modernisation through fast-payment systems produces similar effects without changing the liability structure of money.

Second, researchers should build linked legal-technical datasets. A CBDC design should be coded not only by ledger type, remuneration, and holding limits but also by statutory authority, data-access rules, retention periods, oversight independence, judicial remedies, cash obligations, and the legal status of intermediaries. Such data would make it possible to test whether strong legal safeguards correlate with adoption, trust, resilience, or lower privacy concerns. It would also help separate technological properties from institutional properties.

Third, AI-specific research should measure error and distributional effects in realistic payment environments. Studies should test whether fraud and AML models have higher false-positive rates for informal workers, remittance recipients, cross-border traders, rural users, or people with shared devices. Research should examine how model drift, adversarial transactions, synthetic identities, and cloud outages affect both safety and access. Human review should be evaluated as an institutional process, not assumed to correct automation bias. Finally, research should investigate how users understand explanations and whether complaint channels actually restore access within a timeframe compatible with economic life.

Fourth, global-justice research should examine the politics of standards, procurement, and data flows. Cross-border CBDC arrangements should be assessed for their effects on remittance costs, capital-flow management, sanctions, currency substitution, and the bargaining power of smaller central banks. Qualitative work with communities that are commonly underrepresented in financial technology design is essential. A policy framework that lacks their experience may misclassify inconvenience, exclusion, or surveillance as acceptable implementation friction. The next generation of CBDC scholarship should therefore treat legal capacity, technical sovereignty, and democratic participation as variables that shape monetary outcomes.

CONCLUSION

CBDC governance sits at the intersection of money, law, data, and political authority. The critical literature does not support a universal prediction that retail CBDC will either destabilise commercial banks or produce safer finance. Deposit effects depend on design and institutional capacity. Nor does it support the idea that privacy can be added after launch through an encryption layer. Privacy is shaped by identity, data access, institutional separation, retention, inference, and remedy. AI can improve detection, resilience, and policy analysis, but it can also scale surveillance, obscure responsibility, and automate exclusion. The review's broader contribution is to show that these are not separate technical, monetary, or ethical problems: they are interacting dimensions of public-infrastructure governance.

For emerging economies, the stakes are particularly high. CBDC may reduce payment costs, strengthen a domestic public-money anchor, and broaden access. It may also deepen dependence on external infrastructure, place new pressure on bank funding, and create a concentrated record of economic life in settings where legal and democratic safeguards are uneven. Global justice therefore requires more than universal access to a wallet. It requires an institutional ability to refuse unnecessary surveillance, preserve cash and offline alternatives, contest automated decisions, supervise technology providers, and participate fairly in cross-border rulemaking.

The appropriate policy standard is consequently constitutional and developmental rather than merely technical. Before issuing a CBDC, authorities should demonstrate a clear legal mandate, a credible public purpose, a rights-preserving data architecture, a tested stability strategy, accessible alternatives, and accountable AI governance. After issuance, they should publish evidence, invite scrutiny, correct failures, and revise the system when distributional or rights impacts are unacceptable. A legitimate CBDC does not maximise data, automation, or adoption. It preserves the trust-producing functions of public money while preventing the concentration of monetary and informational power from becoming invisible, irreversible, or immune from democratic control. This standard gives global AI-adoption research a concrete institutional test: adoption should be evaluated not only by efficiency or uptake, but also by legality, contestability, inclusion, resilience, and the fair distribution of technological power.

Acknowledgement

The Authors express their sincere gratitude to Dhaka Commerce College, Dhaka-1216, Bangladesh for the institutional support.

Funding

This research received no external funding.

Ethical statement

This study is a critical integrative review based on published and publicly available literature and policy documents. It did not involve human participants, animals, or identifiable personal data; therefore, ethics approval was not required.

Competing interests

The author declares no competing interests.

Author contributions

The author was responsible for conceptualisation, methodology, literature analysis, writing, review and editing, and final approval of the manuscript.

Data availability

No original dataset was generated or analysed. All sources used in the review are cited in the manuscript and are publicly accessible through the reference links where available.

AI disclosure

In preparing this manuscript, the author used OpenAI Codex (GPT-5) for language refinement, readability improvement, and Word-formatting assistance. Following the use of this service, the author reviewed and edited the content as necessary and takes full responsibility for the content of the published article.

Biographical sketch

Shahida Sharmin is an Assistant Professor at Dhaka Commerce College, Dhaka, Bangladesh. Her scholarly interests include central bank digital currency, financial stability, digital rights, artificial intelligence governance, and public policy in emerging economies.

Disclaimer/Publisher's Note

REFERENCES (APA7)

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., Assenmacher, K., Hoffmann, P., Leonello, A., Monnet, C., & Porcellacchia, D. (2024). The economics of central bank digital currency. *International Journal of Central Banking*, *20*(4), 221–274.

Ahnert, T., Hoffmann, P., Leonello, A., & Porcellacchia, D. (2023). *Central bank digital currency and financial stability* (ECB Working Paper Series No. 2783). European Central Bank. https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2783~0af3ad7576.en.pdf

Amin, M. B., Latif, W. B., Desai, A., Salehin, M., Debnath, G. C., & Kőmíves, P. M. (2026). Beyond the service-quality trap: Blockchain traceability, AI orchestration and rebound-aware governance for sustainable platform value. *Acta Innovations*, *62*, 613–621. https://www.actainnovations.com/index.php/pub/article/view/766

An, L., Wang, Y., Yan, Y., & Ma, C. (2024). The role of emotional factors in the acceptance of digital currency: An extended study of a technology acceptance model. *Finance Research Letters*, *62*, 105090. https://doi.org/10.1016/j.frl.2024.105090

Araujo, D. K. G. de, Doerr, S., Gambacorta, L., & Tissot, B. (2024). *Artificial intelligence in central banking* (BIS Bulletin No. 84). Bank for International Settlements. https://www.bis.org/publ/bisbull84.htm

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., & Shin, H. S. (2022). Central bank digital currencies: Motives, economic implications, and the research frontier. *Annual Review of Economics*, *14*, 697–721.

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

Bank for International Settlements. (2025). *Governance of AI adoption in central banks*. https://www.bis.org/publ/othp90.htm

Bechara, M., Dumitrescu-Pasecinic, A., & Kubota, T. (2025). *Selected legal considerations for central bank digital currencies* (IMF Fintech Note 2025/006). International Monetary Fund.

Belikoff, V., & Blazsek, V. (2025). A systematisation of legal-regulatory risks related to central bank digital currencies: A comparative analysis of the US, the UK and China. *Law and Financial Markets Review*, *18*(2), 73–101. https://doi.org/10.1080/17521440.2025.2526326

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. Polity.

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Regulation & Governance*, *2*(2), 137–164. https://doi.org/10.1111/j.1748-5991.2008.00034.x

Bossu, W., Itatani, M., Margulis, C., Rossi, A. D. P., Weenink, H., & Yoshinaga, A. (2020). *Legal aspects of central bank digital currency: Central bank and monetary law considerations* (IMF Working Paper No. 20/254). International Monetary Fund. https://doi.org/10.5089/9781513561622.001

Bovens, M., Goodin, R. E., & Schillemans, T. (Eds.). (2014). *The Oxford handbook of public accountability*. Oxford University Press.

Brunnermeier, M. K., & Niepelt, D. (2019). On the equivalence of private and public money. *Journal of Monetary Economics*, *106*, 27–41. https://doi.org/10.1016/j.jmoneco.2019.07.004

Celeste, E. (2019). Digital constitutionalism: A new systematic theorization. *International Review of Law, Computers & Technology*, *33*(1), 76–99. https://doi.org/10.1080/13600869.2019.1562604

Choi, S., Kim, B., Kim, Y.-S., & Kwon, O. (2025). Central bank digital currency and privacy: A randomized survey experiment. *International Economic Review*, *66*(2), 823–847. https://doi.org/10.1111/iere.12746

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. https://doi.org/10.1596/978-1-4648-1897-4

Di Iorio, A., Kosse, A., & Mattei, I. (2024). *Embracing diversity, advancing together: Results of the 2023 BIS survey on central bank digital currencies and crypto* (BIS Papers No. 147). Bank for International Settlements.

Dube, R., Agarwal, K., Rahman, A., Kannarasu, V., Latif, W. B., & Balaji, V. (2025, February). The impact of AI on economic forecasting: A case study of currency exchange rate prediction. In *2025 International Conference on Technology Enabled Economic Changes (InTech)* (pp. 755–760). IEEE. https://doi.org/10.1109/InTech64186.2025.11198571

Dunbar, K., & Treku, D. N. (2024). Examining the impact of a central bank digital currency on the access to banking. *International Review of Financial Analysis*, *93*, 103220. https://doi.org/10.1016/j.irfa.2024.103220

European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Fan, R., Walker, T. B., & Wright, A. (2025). Central bank digital currency in small open economies. *Latin American Journal of Central Banking*, *6*(2), 100151. https://doi.org/10.1016/j.latcb.2024.100151

Fernández-Villaverde, J., Sanches, D., Schilling, L., & Uhlig, H. (2021). Central bank digital currency: Central banking for all? *Review of Economic Dynamics*, *41*, 225–242. https://doi.org/10.1016/j.red.2020.12.004

Financial Stability Board. (2024). *The financial stability implications of artificial intelligence*. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

Garratt, R. J., & van Oordt, M. R. C. (2021). Privacy as a public good: A case for electronic cash. *Journal of Political Economy*, *129*(7), 2157–2180. https://doi.org/10.1086/714133

Heitmann, D., Koch, J.-A., Islam, M. S., & Eva, S. A. (2025). The impact of central bank digital currencies on the financial stability of banks: Dynamic panel estimation. *Finance Research Letters*, *84*, 107791. https://doi.org/10.1016/j.frl.2025.107791

Illes, A., Kosse, A., & Mattei, I. (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.

International Monetary Fund. (2025). *Central bank digital currency (CBDC) virtual handbook*. https://www.imf.org/en/topics/digital-payments-and-finance/central-bank-digitalcurrency/virtual-handbook

Jiang, J. (2023). Privacy implications of central bank digital currencies. *Seton Hall Law Review*, *54*, 69–130.

Keister, T., & Monnet, C. (2022). Central bank digital currency: Information and stability. *Journal of Economic Dynamics and Control*, *142*, 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

Kim, Y.-S., & Kwon, O. (2023). Central bank digital currency, credit supply, and financial stability. *Journal of Money, Credit and Banking*, *55*(1), 297–321. https://doi.org/10.1111/jmcb.12913

Kowsar, A. M., Roy, S. S., & Latif, W. (2025). Digital trust and checkout choices: Empirical evidence on online consumer behavior in Asia. *Journal of Information Systems and Management (JISMA)*, *4*(6), 25–35. https://jisma.org/index.php/jisma/article/view/1204

Latif, W. B., Amin, M. B., Debnath, G. C., Salehin, R., & Al Mamun, M. A. (2026). The phenomenon of strategic catalysts and barriers in education technology entrepreneurship: A multi-case study and comparative analysis. *Corporate and Business Strategy Review*, *7*(2), 196–204. https://doi.org/10.22495/cbsrv7i2art18

Latif, W. B., Amin, M. B., Islam, M. A., & Gazi, M. A. I. (2026). Artificial intelligence and big data in green marketing analytics. In S. Mushtaq, K. Beta, V. Rana, & B. Shameem (Eds.), *Driving digital consumer value with green marketing approaches* (pp. 1–28). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-2600-0562-0.ch001

Latif, W. B., Laila, I., Ahmed, T. B., Islam, F., Rahman, M. M., Uddin, M. M., & Nusrat, F. (2026). Transformational leadership as corporate strategy in the healthcare industry. *Corporate and Business Strategy Review*, *7*(3), 28–35. https://doi.org/10.22495/cbsrv7i3art3

Latif, W. B., Mussayeva, I., Amin, M. B., Shafiqu, M. S. I., Debnath, G. C., Islam, M. N., Kowsar, A. M., & Salehin, R. (2026). Big data-driven marketing analytics and customer engagement: A design-science demonstration for business performance. *Business Performance Review*, *4*(3), 44–54. https://doi.org/10.22495/bprv4i3p4

Latif, W. B., Mussayeva, I., Chowdhury, S., Yakub, S., Amin, M. B., Nusrat, F., & Salehin, R. (2026). Data science, artificial intelligence, and the third wave of digital era governance for public health technology: Corporate law and governance implications at macro and micro levels. *Corporate Law & Governance Review*, *8*(3), 170–181. https://doi.org/10.22495/clgrv8i3p16

Latif, W. B., & Yasin, I. M. (2025a, October 2). From disparities to sustainability: Embedding artificial intelligence and digital health literacy into learning health systems. In *Proceedings of the 25th International Conference of Public Health Sciences: Transforming Global Health in the Digital Era with AI-Driven Solutions for NCDs* (Vol. 25, Issue 1, p. 40). https://www.researchgate.net/publication/396521537_From_Disparities_to_Sustainability_Embedding_Artificial_Intelligence_and_Digital_Health_Literacy_into_Learning_Health_Systems

Latif, W. B., & Yasin, I. M. (2025b). From disparities to sustainability: Embedding artificial intelligence and digital health literacy into learning health systems—A critical review article. *Pacific Journal of Medical Research*, *2*(4), 167–173. https://doi.org/10.70818/pjmr.v02i04.0122

Latif, W. B., Yasin, I. M., Amin, M. B., Debnath, G. C., & Al Mamun, M. A. (2026). Machine intelligence for predictive, adaptive curriculum design in higher education. *TEM Journal*, *15*(2), 1988–1998. https://doi.org/10.18421/TEM152-86

Latif, W. B., Yasin, I. M., & Nusrat, F. (2025). Digital health literacy as an equity lever for AI-enabled noncommunicable disease care: A thematic synthesis. In *Proceedings of the 25th International Conference of Public Health Sciences* (Vol. 1, No. 1, pp. 33–46). College of Public Health Sciences, Chulalongkorn University. https://doi.org/10.58837/CHULA.PCD.2025.2

Le, A. H. (2025). Central bank digital currency and cryptocurrency in emerging markets. *International Economics*, *181*, 100577. https://doi.org/10.1016/j.inteco.2024.100577

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

Murphy, K., Sun, T., Zhou, Y. S., Tsuda, N., Zhang, N., Budau, V., Solomon, F., Kao, K., Vucinic, M., & Miggiani, K. (2024). *Central bank digital currency data use and privacy protection* (IMF Fintech Note 2024/004). International Monetary Fund. https://doi.org/10.5089/9798400286971.063

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

OECD. (2023). *Central bank digital currencies (CBDCs) and democratic values* (OECD Business and Finance Policy Papers No. 31). OECD Publishing. https://doi.org/10.1787/f3e70f1f-en

Office of the United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age*(Report A/HRC/39/29). United Nations.

Ponce, J., & Taroco, S. (2026). CBDC's design implications for financial stability. *Latin American Journal of Central Banking*, *7*(1), 100188. https://doi.org/10.1016/j.latcb.2025.100188

Schilling, L., Fernández-Villaverde, J., & Uhlig, H. (2024). Central bank digital currency: When price and bank stability collide. *Journal of Monetary Economics*, *145*, 103554. https://doi.org/10.1016/j.jmoneco.2024.01.007

Scott, C. (2000). Accountability in the regulatory state. *Journal of Law and Society*, *27*(1), 38–60. https://doi.org/10.1111/1467-6478.00146

Sen, A. (1999). *Development as freedom*. Alfred A. Knopf.

Sindhura, K., Rajagopal, N. K., Latif, W. B., Kumar, J. R., Kayande, R. A., & Sakthivel, S. (2025). Leveraging big data and machine learning for real-time economic monitoring and forecasting. In *2025 International Conference on Technology Enabled Economic Changes (InTech)* (pp. 789–794). IEEE. https://doi.org/10.1109/InTech64186.2025.11198446

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*, 467–486. https://doi.org/10.1057/s41261-024-00241-2

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Tan, B. J. (2024). Central bank digital currency and financial inclusion. *Journal of Macroeconomics*, *81*, 103620. https://doi.org/10.1016/j.jmacro.2024.103620

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Wang, Z. (2023). Money laundering and the privacy design of central bank digital currency. *Review of Economic Dynamics*, *51*, 604–632. https://doi.org/10.1016/j.red.2023.06.004

Yasin, I. M., & Latif, W. B. (2025). The strategic emergence of BRICS in business, policy and economics: Reimagining global trade and development. *Pacific Journal of Business Innovation and Strategy*, *2*(3), 1–4. https://doi.org/10.70818/pjbis.2025.v02i03.074

Yellamma, M., Latif, W. B., Koilraj, M., Manjula, M., Peneti, S., & Vedaansh, M. (2025). Real-time gesture recognition for human-robot interaction using mmWave radar and deep learning. In *2025 IEEE 5th International Conference on ICT in Business, Industry & Government (ICTBIG)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICTBIG68706.2025.11323973

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

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.