Journal of Law and Legal Reform
Vol. 7 Issue 3 (2026) 1785–1818
DOI: https://doi.org/10.15294/jllr.v7i3.44027
Online since: July 13, 2026

Journal of Law & Legal Reform
https://journal.unnes.ac.id/journals/jllr

Regulatory Sandbox for Ex-Ante Data Protection in the Digital Rupiah (CBDC) Pilot: A Doctrinal Comparison

Wardah Yuspin [a] ✉, Arief Budiono [a], Turdialiev Mukhammad Ali Polatjon ogli [b], Jompon Pitaksantayothin [c], Naeem Rakha Allah [b]

[a] Faculty of Law and Political Science, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia
[b] Tashkent State University of Law, Tashkent, Uzbekistan
[c] Hankuk University of Foreign Studies, South Korea

✉ Corresponding email: wy204@ums.ac.id

Abstract

The transformation of digital payments has prompted central banks to explore Central Bank Digital Currency (CBDC) as a new form of monetary infrastructure. However, CBDC is not merely a payment instrument; it also establishes a data processing regime, as transactions can be recorded, traced, and systematically processed. Existing studies on CBDC and privacy generally discuss design options or anonymity, but they rarely explain how personal data protection compliance should be tested before a CBDC pilot is expanded. This article addresses that gap by examining how the Digital Rupiah pilot can be designed as an ex-ante mechanism for testing compliance with Indonesia's Personal Data Protection Law. The novelty of this article lies in its proposal of a rights-based regulatory sandbox model that integrates CBDC architecture, tiered KYC, data minimization, access governance, and remedial mechanisms

into a single operational compliance framework. Using a normative legal approach and comparative method, this article interprets Indonesia's PDP Law. It compares it with Uzbekistan's data protection framework as an analytical mirror for assessing how processing controls and architectural requirements influence CBDC design. The article contributes to scientific knowledge by formulating a norm-to-control sandbox model that translates data protection principles into testable indicators, including purpose limitation, role-based access controls, audit trails, retention limits, and go/no-go compliance criteria. The findings show that the legitimacy of the Digital Rupiah pilot should not be measured only by technical performance or payment efficiency, but also by whether the sandbox can prove that data processing is lawful, proportionate, transparent, and auditable before wider implementation.

Keywords

CBDC, Digital Rupiah, Personal Data Protection, Regulatory Sandbox, Privacy.

HOW TO CITE:

Chicago Manual of Style Footnote:

[1] Wardah Yuspin, Arief Budiono, Turdialiev Mukhammad Ali Polatjon ogli, Jompon Pitaksantayothin, and Naeem Rakha Allah, "Regulatory Sandbox for Ex-Ante Data Protection in the Digital Rupiah (CBDC) Pilot: A Doctrinal Comparison," *Journal of Law and Legal Reform* 7, no 3 (2026): 1785–1818, https://doi.org/10.15294/jllr.v7i3.44027.

Chicago Manual of Style for Reference:

Yuspin, Wardah, Arief Budiono, Turdialiev Mukhammad Ali Polatjon ogli, Jompon Pitaksantayothin, and Naeem Rakha Allah. "Regulatory Sandbox for Ex-Ante Data Protection in the Digital Rupiah (CBDC) Pilot: A Doctrinal Comparison." *Journal of Law and Legal Reform* 7, no 3 (2026): 1785–1818. https://doi.org/10.15294/jllr.v7i3.44027.

Introduction

Central Bank Digital Currency (CBDC) is increasingly discussed as a new form of monetary infrastructure. In Indonesia, the Digital Rupiah is framed as part of payment system modernization and monetary sovereignty. Nevertheless, CBDC is not merely a digital version of cash. It may also create a new data processing regime because payment activities can be recorded, traced, linked, and analyzed more systematically than in physical cash transactions. This raises a central legal question: how can a regulatory sandbox be designed as an ex-ante mechanism to test compliance with personal data protection in the Digital Rupiah pilot, especially against the risks of transaction profiling and excessive surveillance[1]?

This question is important because CBDC creates a tension between monetary stability and privacy rights. On the one hand, the state has a legitimate interest in maintaining payment system integrity, preventing financial crime, and supporting monetary policy. On the other hand, the same infrastructure may expand the state's visibility over citizens' economic activities. If transaction data is collected and linked without strict limits, CBDC may create risks of abuse of power, transaction profiling, function creep, and excessive surveillance. These risks are not only technical. They are legal and institutional because they concern who controls transaction data, who may access it, for what purpose, and under what safeguards[2].

The existing literature on CBDCs moves in two broad directions. The first emphasizes traceability, security, and payment system integrity. This view can be found in studies that discuss the Digital Rupiah from the perspective of monetary sovereignty, cybercrime prevention, financial system resilience, and AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) compliance. The second

---

[1] Alma Wiranta, Robby MT, and Sovian Aritonang, "The Development of Digitalization of Rupiah Currency Towards National Security, Especially in Dealing With Cyber Crime and Financial Crime," *International Journal of Accounting and Economics Studies* 12, no. 6 (October 2025): 169–75, https://doi.org/10.14419/gbs8mw83.

[2] Fadhlina et al., "Perlindungan Data Pribadi Nasabah Dalam Transaksi Central Bank Digital Currency (CBDC) Dalam Rupiah Digital" 7, no. 1 (2024): 308–16.

emphasizes privacy, anonymity, and the risk of surveillance, especially in studies comparing CBDC design with cash-like privacy or examining public concerns about systems such as e-CNY[3]. Both perspectives are useful, but they often remain at the level of principles or design preferences. They do not sufficiently explain how personal data protection compliance should be tested before a CBDC pilot is expanded[4].

This article argues that a regulatory sandbox should not be understood only as an innovation-testing facility. In the context of CBDC, it should operate as a rights-based ex-ante compliance mechanism. This means that the sandbox must test not only technical performance, but also the legality, proportionality, transparency, security, and accountability of data processing. A technology-based sandbox may test whether the system works. A market-based sandbox may test whether the innovation is commercially or operationally feasible. A rights-based sandbox goes further by asking whether the system may lawfully process personal data, whether identity and transaction data are properly separated, whether access is restricted, whether retention is limited, and whether users have effective remedies[5].

The novelty of this article lies in the formulation of a norm-to-control sandbox model for the Digital Rupiah pilot. This model translates the principles of Indonesia's Personal Data Protection Law into operational test points, including purpose limitation, data minimization, tiered KYC, role-based access control, audit trails, retention limits, breach response, complaint handling, and go/no-go criteria before pilot expansion. In this model, compliance is not treated

---

[3] Vicko Taniady, Salsabiila Puteri Permatasari, and Reyka Widia Nugraha, "Crypto Asset-Trade Resilience During The Covid-19 Pandemic In Indonesia," *Jurnal Jurisprudence* 11, no. 1 (January 2022): 31–43, https://doi.org/10.23917/jurisprudence.v11i1.13340.

[4] Syahid Izzulhaq, Akhmad Syakir Kurnia, and Johan Beni Maharda, "Central Bank Digital Currency, Monetary Policy, And Macroeconomy: Evidence From Indonesia," *Bulletin of Monetary Economics and Banking* 27, no. 2 (May 2024): 241–64, https://doi.org/10.59091/2460-9196.2273.

[5] Raphael Auer et al., "CBDC Beyond Borders - Results from a Survey of Central Bankers," *Bank For International Settlements*, no. June (2021): 105–6.

as a post-launch administrative obligation but as a condition for pilot graduation[6].

This article uses Uzbekistan as the only comparative jurisdiction. The comparison is deliberately focused rather than broad. Uzbekistan is selected not because it represents the most advanced CBDC model, but because it offers a useful analytical mirror for Indonesia. Both jurisdictions are developing state-led digital transformations outside the EU legal tradition while strengthening their personal data protection frameworks[7]. Unlike the EU, whose GDPR model has become a dominant global benchmark, and unlike China, whose CBDC development is shaped by a different political and surveillance governance context, Uzbekistan provides a more proportionate comparison for examining how an emerging personal data protection regime may influence CBDC architecture, storage governance, processing control, and cross-border data transfer[8].

The contribution of this article is threefold. First, it reframes CBDC as both monetary infrastructure and data governance infrastructure. Second, it develops a rights-based sandbox model that connects CBDC architecture with personal data protection obligations. Third, it proposes concrete compliance indicators to determine whether the Digital Rupiah pilot should proceed, be corrected, or be stopped before wider implementation[9].

The legal discourse on CBDCs often stops at two extremes: one side emphasizes traceability as a prerequisite for public safety; the other emphasizes privacy protection as a limit on surveillance[10].

---

[6] Novi Maryaningsih et al., "Central Bank Digital Currency: What Factors Determine Its Adoption?," *Buletin Ekonomi Moneter Dan Perbankan* 25, no. 1 (June 2022): 1–24, https://doi.org/10.21098/bemp.v25i1.1979.

[7] Indah Sri Utari et al., "A Criminological Perspective on Corruption as a Catalyst of Economic Breakdown: Socio-Legal Challenges in Indonesian Environmental Governance," *Jambe Law Journal* 9, no. 1 (2026): 205–47, https://doi.org/10.22437/jmj4ac47.

[8] Anneke Kosse and Ilaria Mattei, "The Potential of Central Bank Digital Currencies for Cross-Border Payments," no. 439 (2022): 1–7.

[9] Rafli Fadilah Muhammad and Rianda Dirkareshza, "Legalitas Penerapan Central Bank Digital Currency (CBDC) Di Indonesia," *Jurnal Usm Law Review* 6, no. 3 (November 2023): 913–30, https://doi.org/10.26623/julr.v6i3.7370.

[10] Ministry of Finance RI, "Getting to Know CBDC Better," 2023.

The existing legal discourse on CBDCs may be grouped into two dominant but incomplete tendencies. The first tendency emphasizes the public benefits of CBDC, including financial inclusion, payment efficiency, monetary resilience, and the possibility of publicly provided digital money. In the United States, for example, Crawford, Menand, and Ricks have supported the idea of a digital dollar, or "FedAccount," to improve access to safe public money. However, their proposals still leave unresolved questions about whether anonymous or cash-like payments can be preserved in a digital system[11]. The second tendency focuses on the risk that CBDCs may deepen the state's visibility into citizens' economic lives. Carrillo warns that new payment technologies may enable government agencies to surveil the public and strengthen social control, especially where privacy laws do not meaningfully restrict government acquisition of financial data[12]. These two tendencies show that the CBDC debate often oscillates between institutional efficiency and privacy protection. However, neither approach sufficiently explains how privacy safeguards should be tested before implementation. This is why a rights-based regulatory sandbox is necessary[13]. Unlike a technology-based sandbox that mainly tests system performance, or a market-based sandbox that prioritizes innovation and adoption, a rights-based sandbox requires the pilot to prove purpose limitation, data minimization, access control, anonymity thresholds, auditability, and remedies before the CBDC is expanded. In this sense, the sandbox becomes not only an innovation tool but also a legal mechanism for preventing surveillance risks before they become embedded in the monetary infrastructure[14].

In summary, this article aims to formulate a regulatory sandbox design for the Digital Rupiah pilot that links PDP Law principles to

---

[11] John Crawford, Lev Menand, and Morgan Ricks, "FedAccounts: Digital Dollars," *George Washington Law Review* 89, no. 1 (2021): 113–72.

[12] Raúl Carrillo, "Seeing Through Money: Democracy, Data Governance, and the Digital Dollar," *SSRN Electronic Journal*, 2023, 1207–1304, https://doi.org/10.2139/ssrn.4354085.

[13] Jennifer Devlin et al., "Digital Dollar : Privacy and Transparency Dilemma," 2025, 629–78.

[14] Federico Costantini et al., "Autonomous Vehicles in a GDPR Era: An International Comparison," 2020, 191–213, https://doi.org/10.1016/bs.atpp.2020.02.005.

operational control points and enriches the argument through a comparison with Uzbekistan, serving as an analytical mirror on how data protection regimes can force architectural aspects to be tested from the pre-pilot phase onward[15].

This research uses a qualitative doctrinal legal method supported by a focused comparative approach. There are four stages of the research: First, doctrinal legal analysis was conducted[16] to interpret and systematize relevant norms: the principle of personal data protection; the principle of restriction of rights, including necessity, suitability, and proportionality; and institutional authority related to the issuance and supervision of payment systems. Second, normative data mapping was conducted to identify data processing points that are most prone to profiling, purpose expansion, or excessive surveillance. Third, the study applied a sandbox analysis framework as an ex ante mechanism, namely by formulating a trial phase (pre-pilot, limited testing, evaluation, expansion), compliance prerequisites, oversight parameters, and accountability control points for data processing: purpose limitation, minimization, retention, transparency, access restriction, and remedial mechanisms. Fourth, a structured comparison with Uzbekistan, as a comparative jurisdiction, is conducted to examine how a data protection regime that emphasizes processing control and architectural aspects influences the digital policy design space[17].

The comparative method is limited to Uzbekistan as a single comparative jurisdiction. Uzbekistan was selected because it shares several structural characteristics with Indonesia, including its status as an emerging economy, a civil law legal system, and an ongoing digital

---

[15] Chenguo Zhang, "China's New Regulatory Regime Tailored for the Sharing Economy: The Case of Uber under Chinese Local Government Regulation in Comparison to the EU, US, and the UK," *Computer Law & Security Review* 35, no. 4 (August 2019): 462–75, https://doi.org/10.1016/j.clsr.2019.03.004.

[16] Indah Sri Utari et al., "Illegal Nickel Mining in Protected Forests: Challenges in Whistleblower and Justice Collaborator Protection in Indonesia," *Indonesian Journal of Environmental Law and Sustainable Development* 4, no. 2 (2025): 341–74, https://doi.org/10.15294/ijel.v4i2.38220.

[17] Patience Marange and Friedrich Hamadziripi, "Adapting Regulatory Compliance in Zimbabwe's Banking Sector to the Financial Technology Revolution: Lessons from South Africa," *Potchefstroom Electronic Law Journal* 29 (February 2026), https://doi.org/10.17159/1727-3781/2026/v29i0a21383.

financial transformation led by the central bank. Unlike jurisdictions such as China or Sweden, whose economic and institutional conditions differ substantially from those of Indonesia, Uzbekistan provides a more comparable regulatory environment for examining CBDC implementation. Furthermore, Uzbekistan has advanced to the pilot implementation stage of its Digital Soum, offering practical regulatory and institutional experience that Indonesia can evaluate as it develops its own Digital Rupiah framework. Consequently, Uzbekistan serves as an appropriate comparator for identifying best practices and regulatory lessons on the governance, legal framework, and risk management of CBDC implementation[18].

A. Institutional Position and Responsibility for Data Control in the Digital Rupiah Ecosystem

The finding confirms that CBDC should be understood as a monetary infrastructure that also shapes the data processing regime. With cash, relative anonymity is inherent, as each transaction occurs without a centralized record system that can be traced back to an individual's identity. In some modern non-cash instruments (cards, electronic money, transfers), recording does occur, but it is often scattered across various providers and not always integrated under a single authority. CBDC changes this configuration because it has the potential to provide a more structured and far-reaching layer of recordkeeping, especially if its architecture allows authorities to access transaction data directly or through tight integration with intermediaries[19].

The legal consequences are simple but profound[20], whereby the higher the traceability and integration, the greater the capacity to map

---

[18] Sendy Pratama Firdaus, "Measuring The Urgency Of A Digital Rupiah: A Socio-Legal Review," *Journal of Central Banking Law and Institutions* 4, no. 3 (September 2025): 505–32, https://doi.org/10.21098/jcli.v4i3.283.

[19] David K Linnan, "Central Bank Digital Currencies In The Indonesian Setting: Questions &Amp; Choices," *Journal of Central Banking Law and Institutions* 2, no. 2 (May 2023): 221–64, https://doi.org/10.21098/jcli.v2i2.45.

[20] Indah Sri Utari, Ridwan Arifin, and Ahmad Zaharuddin Sani Ahmad Sabri, "Why Did a Five-Year-Old Toddler Become a Victim of Murder? A Criminological and

citizens' economic behavior in granular detail. At a certain point, money is no longer just a medium of exchange, but also a rich source of data for inferring preferences, social relations, consumption habits, location, and even daily life patterns. Therefore, the legal analysis of CBDC should not stop at the legality of issuance or the validity of payment instruments; it must also address the legitimacy of data processing and the limits of surveillance[21].

This is where a classic problem in modern public law arises: surveillance can be justified for legitimate purposes, but overly powerful surveillance instruments tend to experience function creep. In the context of CBDCs, function creep can occur when transaction data originally collected for payment system integrity is then used for other purposes, such as fiscal surveillance, general law enforcement, or social policy, without clear boundaries. Even if the additional purposes are considered valid, such expansion still requires a clear legal basis, accountable procedures, and strict proportionality tests[22].

These findings reinforce the argument that the risk of privacy violations in CBDCs is systemic. Violations do not necessarily arise as isolated incidents, but rather as designs that allow for excessive data processing to become the norm. Therefore, risk control cannot wait until the ex post enforcement phase after abuse has occurred, control must be integrated from the pilot phase as a condition for policy legitimacy[23].

In CBDC pilots, central banks not only act as monetary authorities but also as key actors in data governance. In data protection law, the first question that determines compliance architecture is who is the data

---

Legal Perspective," *Indonesian Journal of Criminal Law Studies* 8, no. 2 (2023), https://doi.org/10.15294/ijcls.v8i2.48591.

21 Alejandro Billyjoe Mau Bere, Richard Win Putra, and Linda Kusumaning Wedari, "Investigation of Digital Rupiah Acceptance Using UTAUT-3 Model," *Indonesian Journal of Electrical Engineering and Computer Science* 35, no. 3 (September 2024): 1710, https://doi.org/10.11591/ijeecs.v35.i3.pp1710-1721.

22 Wahyu Yun Santoso et al., "Design Elements And Risks Of Central Bank Digital Currency In Tailoring A Prudent 'Rupiah Digital," *Diponegoro Law Review* 8, no. 2 (October 2023): 141–58, https://doi.org/10.14710/dilrev.8.2.2023.141-158.

23 Umi Khaerah Pati and Heri Indrajat, "Regulating Fintech in the CBDC Era: Addressing Competitive Fragility and Preserving State-Owned Banking Stability," *Journal of Indonesian Legal Studies* 10, no. 1 (August 2025): 257–94, https://doi.org/10.15294/jils.v10i1.19342.

controller, who is the processor, and how are responsibilities divided? In conventional payment systems, data control is often spread across banks, payment system operators, and third parties[24]. In CBDC, this division could change because the central bank becomes both the issuer and the manager of the main infrastructure[25].

If Bank Indonesia is in the position of data controller (or joint controller) for certain processing activities, then the principles of the PDP Law must be translated into operational obligations[26]. These obligations not only require a legitimate basis for processing, but also concern purpose limitation, accuracy, minimization, retention, security, and the fulfillment of data subject rights. In the context of CBDC, data subject rights should not be viewed as mere administrative access, but rather as a mechanism to limit informational power[27].

The allocation of institutional responsibilities is an essential element of accountability under the Personal Data Protection Law. Although Bank Indonesia establishes the Digital Rupiah architecture and determines the public purposes of CBDC processing, licensed intermediaries, including banks and payment service providers, also determine significant aspects of customer onboarding, identity verification, authentication, and wallet administration. Accordingly, the Digital Rupiah ecosystem should be governed through a joint controllership model rather than treating Bank Indonesia as the sole

---

[24] Indah Sri Utari et al., "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online," *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025), https://doi.org/10.15294/ciils.v4i2.35309.

[25] And Lillian F. Mills Kelvin K. F., "Financial Gatekeepers and Investor Protection: Evidence from Criminal Background Checks," *Journal of Accounting Research* 57, no. 2 (May 2019): 491–543, https://doi.org/10.1111/1475-679X.12265.

[26] Indra Ardiansyah et al., "Taking Restitution Seriously?: Victim-Oriented Gaps in the Criminal Justice System," *IJCLS (Indonesian Journal of Criminal Law Studies)* 10, no. 1 (2025), https://doi.org/10.15294/ijcls.v10i1.19636.

[27] Wardah Yuspin et al., "The Accountability Principle in Personal Data Protection in Sweden and Indonesia," *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (October 2025): 667–94, https://doi.org/10.53955/jsderi.v3i3.97.

controller[28]. Under this model, Bank Indonesia acts as the joint controller for monetary infrastructure, transaction validation, and ledger governance; licensed intermediaries act as joint controllers for customer-facing processing activities. At the same time, technology vendors and cloud service providers operate solely as processors acting under documented instructions. The regulatory sandbox should require a documented allocation of these responsibilities before pilot deployment and verification. Such an approach transforms accountability from a general principle into a verifiable governance mechanism. It reduces the risk of overlapping responsibilities, regulatory gaps, and the concentration of control over CBDC transaction data[29].

The regulatory sandbox should serve not only as a technological testing environment but also as a mechanism to detect and prevent function creep in the processing of CBDC transaction data[30]. Function creep arises when personal data collected for payment settlement, fraud prevention, or AML/CFT compliance is subsequently used for purposes that exceed the original legal basis. Articles 16, 20, and 28 of Law No. 27 of 2022 on Personal Data Protection require that personal data be processed only for specific and lawful purposes, supported by an appropriate legal basis, and protected against unauthorized access. Accordingly, a CBDC sandbox should operationalize these principles by testing purpose-based access controls, role-based authorization, immutable audit trails, data retention limits, and mechanisms for rejecting requests that fall outside the authorized processing purpose. Through these legal and technical controls, the sandbox can identify instances of function creep before the Digital Rupiah is deployed nationwide, thereby ensuring that the CBDC ecosystem complies with

---

[28] Ata Fauzie Yuspin, Wardah, "The Effectiveness of Spin off As a Breakthrough in Promoting Islamic Banking in Indonesia," *The Journal of Social Sciences Research*, no. 6 (December 2018): 213–16, https://doi.org/10.32861/jssr.spi6.213.216.

[29] Zhang, "China's New Regulatory Regime Tailored for the Sharing Economy: The Case of Uber under Chinese Local Government Regulation in Comparison to the EU, US, and the UK."

[30] Indah Sri Utari et al., "Rethinking Filicide through Freudian Psychoanalysis: A Comparative Perspective on Indonesian and Spanish Criminal Cases," *Jurnal IUS Kajian Hukum Dan Keadilan* 14, no. 2 (2026): 587–620, https://doi.org/10.29303/ius.v14i2.1997.

the principles of legality, proportionality, accountability, and data protection[31].

Regarding risks that may arise during the implementation of CBDC, the comparative evidence suggests that the risks of transaction profiling, excessive surveillance, and potential abuse of power are not inherent to CBDCs themselves. Instead, these risks depend on the legal and institutional framework governing access to transaction data[32]. China's e-CNY demonstrates how a CBDC with broad traceability capabilities can spark sustained debate about financial surveillance and profiling[33]. In contrast, Sweden's e-krona illustrates how comprehensive data protection laws, independent oversight, and constitutional safeguards can constrain the same technological capabilities[34]. For Indonesia, the principal challenge is therefore not the Digital Rupiah technology itself, but whether the existing legal framework, including Bank Indonesia's CBDC regulations and the Personal Data Protection Law, provides sufficiently specific safeguards on data access, retention, proportionality, and independent oversight to prevent misuse of transaction information. This comparative perspective provides a strong doctrinal basis for arguing that CBDC governance should be evaluated through the lens of constitutional principles, administrative accountability, and data protection law rather than solely on technological design alone[35].

---

[31] Arief Budiono et al., "Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice," *Journal of Human Rights, Culture and Legal System* 3, no. 3 (November 2023): 441–75, https://doi.org/10.53955/jhcls.v3i3.127.

[32] Mutia Enggarwati and Inda Fresti Puspitasari, "Central Bank Digital Currency and Financial Stability in Indonesia: Analysis on Vector Error Correction Model (VECM) Approach," *Proceeding ISETH (International Summit on Science, Technology, and Humanity)*, January 2024, 1533–42, https://doi.org/10.23917/iseth.4364.

[33] Utari et al., "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online."

[34] S Maghfira and W Yuspin, "Legal Analysis of Central Bank Digital Currency (CBDC) Regulation in the Indonesian Payment System: A Comparative Study with the Implementation of E-CNY in ...," *Journal of Legal and Social Changes* 1, no. 1 (2025): 1–13.

[35] Zahrashafa Mahardika, Rizky Banyualam Permana, and Nadia Maulisa, "Going Digital Rupiah: Some Considerations From Sovereignty And Cybersecurity

B. Regulatory Sandbox as an Ex-Ante Compliance Mechanism: A Rights-Based Sandbox Model for the Digital Rupiah Pilot

The principle of proportionality should operate as the legal language of the CBDC sandbox. It converts abstract debates on privacy and public interest into measurable tests. In CBDC design, the main question is not whether traceability exists; rather, it is whether it can be achieved. The more precise question is how much traceability is lawful, necessary, and controllable[36].

Proportionality can be tested through three questions. First, the necessity test asks whether a specific type of data is genuinely required for a legitimate purpose. For example, full identity data may not be necessary for every low-value transaction. A tiered identity model may be more appropriate. Second, the suitability test asks whether the chosen data processing method is effective for the stated objective. If the purpose is AML/CFT, the system must show a rational link between data collection and risk detection. It should not merely accumulate personal data. Third, the least intrusive means test asks whether the same objective can be achieved through less privacy-invasive tools. These tools may include pseudonymization, separation of identity and transaction data, role-based access, and documented authorization procedures[37].

This proportionality test is important because CBDC traceability is often treated as a technical inevitability. In fact, traceability has degrees. A CBDC can be designed with stronger anonymity for low-risk payments and stronger identification for higher-risk transactions. The sandbox is therefore the proper place to test whether privacy protection and AML/CFT can be balanced in practice. This balance cannot be

---

Perspectives," *Journal of Central Banking Law and Institutions* 2, no. 1 (January 2023): 25–54, https://doi.org/10.21098/jcli.v2i1.42.

[36] Linnan, "Central Bank Digital Currencies In The Indonesian Setting: Questions &Amp; Choices."

[37] Mau Bere, Putra, and Wedari, "Investigation of Digital Rupiah Acceptance Using UTAUT-3 Model."

justified only through policy statements. It must be proven through system design, audit evidence, and independent review[38].

This article proposes a rights-based sandbox model. This model differs from a technology-based sandbox and a market-based sandbox. A technology-based sandbox mainly asks whether the system works. A market-based sandbox asks whether the innovation is commercially viable and useful for consumers. A rights-based sandbox asks a different question: whether the pilot is lawful, proportionate, and accountable before it is expanded. In this model, rights protection is not an external compliance layer. It becomes a condition for the CBDC pilot's legitimacyt[39].

The core mechanism of this model is the purpose lock. Purpose lock means that every category of personal data must be linked to a specific, lawful, and pre-approved purpose. It should be enforced in three ways. First, through code, by embedding purpose tags, access limits, retention rules, and automated rejection of unauthorized queries into the system. Second, through contract, by requiring joint-controller agreements, processor agreements, vendor clauses, and a prohibition on secondary use. Third, through institutional oversight, requiring approval from an independent evaluation committee before any new purpose, data category, or access channel is added[40].

The go/no-go decision should not be made only by the system operator. An independent evaluation committee should review it. For the Digital Rupiah sandbox, this committee may include Bank Indonesia, OJK, the PDP supervisory institution once established, PPATK for AML/CFT issues, BSSN for cybersecurity, an external IT auditor, and academic or consumer representatives. Its authority should include verifying compliance evidence, requiring remediation, recommending suspension, and issuing a reasoned recommendation before pilot expansion. This structure is consistent with the logic of sandbox supervision, risk-based monitoring, reporting, and evaluation

---

38 Santoso et al., "Design Elements And Risks Of Central Bank Digital Currency In Tailoring A Prudent 'Rupiah Digital."

39 Pati and Indrajat, "Regulating Fintech in the CBDC Era: Addressing Competitive Fragility and Preserving State-Owned Banking Stability."

40 Kelvin K. F., "Financial Gatekeepers and Investor Protection: Evidence from Criminal Background Checks."

under POJK No. 3/2024, as well as with the accountability, DPIA, security, and supervisory provisions under the PDP Law[41].

Table 1. Simplified Rights-Based Sandbox Stages for Digital Rupiah

No.	Stage	Main test focus	Specific legal basis	Evidence / pass-fail output	Responsible actors
1	Pre-pilot Design and governance	Data-flow map, role allocation, purpose lock, DPIA, tiered KYC/privacy design.	POJK 3/2024: Arts. 8(3), 9(4)-(5), 10(1). PDP Law: Arts. 16(2), 18, 20, 27-28, 34, 53-54.	Approved testing plan; data-flow map; role matrix; DPIA; purpose-lock register. Fail: unclear purpose, access role, or data category.	Bank Indonesia as lead; banks/PSPs; DPO; legal-compliance team; external privacy/IT auditor.
2	Limited pilot Controlled testing	Small-scale transactions, pseudonymization, role-based access, audit log, retention, breach response, AML/CFT scenarios.	POJK 3/2024: Arts. 11(2)-(7), 12, 13(1)-(4), 26(2)(d)-(f). PDP Law: Arts. 31, 35-39, 46, 51-52.	Pilot report; access-log test; blocked unauthorized access; retention/deletion test; AML/CFT results. Fail: access bypass or use outside approved purpose.	Bank Indonesia; banks/PSPs; PPATK for AML/CFT; BSSN for cybersecurity; independent auditor.
3	Compliance evaluation Go / no-go	Residual risk, proportionality test, function-creep review, incident review, and user-rights review.	POJK 3/2024: Arts. 13(4)-(5), 14, 18, 19. PDP Law: Arts. 34, 47, 57-60.	Independent evaluation report; remediation list; proportionality assessment; go/no-go recommendation. No-go: unresolved	Independent evaluation committee: BI, OJK, PDP supervisory institution, PPATK, BSSN, external

[41] Fitri Handayani, "Design And Legal Aspect Of Central Bank Digital Currency: A Literature Review," *Journal of Central Banking Law and Institutions* 1, no. 3 (September 2022): 509–36, https://doi.org/10.21098/jcli.v1i3.35.

				high-risk issue or unauthorized purpose expansion.	auditor, consumer/academic representative.
4	Gradual expansion Graduation and oversight	Expansion standards, periodic audit, complaint handling, transfer control, post-pilot monitoring, and continuous AML/CFT review.	POJK 3/2024: Arts. 15-16, 20, 23-24, 26, 29, 47-49. PDP Law: Arts. 42-46, 55-60.	Graduation report; audit schedule; public transparency summary; complaint/remedy channel; cross-border transfer assessment. Fail: no permanent oversight after expansion.	Bank Indonesia; OJK; PDP supervisory institution; PPATK; BSSN; banks/PSPs; consumer protection unit.

(Source note: The table uses POJK No. 3 of 2024 as the sandbox governance reference and Law No. 27 of 2022 on Personal Data Protection as the data-rights reference. For Digital Rupiah, the table is proposed as a rights-based model because Bank Indonesia remains the primary monetary authority).

The table should be read as an operational sequence. The pre-pilot phase tests whether the CBDC design is lawful before any real transaction occurs. The limited pilot tests whether the legal design works inside the system. The evaluation phase determines whether the remaining risks are acceptable. The graduation phase ensures oversight continues after the pilot expands[42].

In this structure, proportionality is no longer a general principle. It becomes a pass/fail test. A CBDC pilot may proceed only when the system proves that data collection is necessary, access is limited, retention is controlled, and rights can be exercised effectively. This is the main

[42] Nadia Spatari, "Building Safe Digital Environments for Children: AI Regulatory Sandbox and Pilot Project Insights," in *2025 12th International Conference on Future Internet of Things and Cloud (FiCloud)* (IEEE, 2025), 459–66, https://doi.org/10.1109/FiCloud66139.2025.00070.

contribution of the rights-based sandbox model. It shifts CBDC governance from a reactive model, in which violations are addressed after harm occurs, to an ex ante model, in which legality and rights protection are tested before wider deployment[43].

C. Comparative Lessons from Uzbekistan: Compliance that Touches Architecture Data Governance by Design

Uzbekistan is used as an analytical mirror, not to be imitated wholesale. The value of comparison lies in how data protection regimes compel digital policies to consider architectural aspects. Relatively strict data protection regimes encourage very concrete questions: where is the data stored, who operates the data center, what are the conditions for cross-border transfers, and how do registration or processing control mechanisms work[44].

Uzbekistan's Law No. ZRU-547 defines personal data in Article 4 as information recorded on electronic, paper, or other media that relates to a specific person or enables identification. This is relevant to CBDC because identity data, wallet data, transaction metadata, and biometric KYC data may fall within this definition. Article 5 also sets out the basic principles, including the legality of purpose, accuracy, confidentiality, security, and protection of the individual, society, and the state[45].

For limitations, the strongest articles are Articles 10, 12, 18, and 19. Article 10 says personal data should be collected only as necessary and

---

[43] Thiago Moraes, "Regulatory Sandboxes for Trustworthy Artificial Intelligence – Global and Latin American Experiences," *International Review of Law, Computers & Technology* 39, no. 1 (January 2025): 55–74, https://doi.org/10.1080/13600869.2024.2351674.

[44] Lerong Lu, "The Law of Fintech: How Artificial Intelligence and Innovative Technologies Contribute to a Sustainable Financial Industry and Its Effective Regulation," in *Artificial Intelligence, Finance, and Sustainability* (Cham: Springer Nature Switzerland, 2024), 243–63, https://doi.org/10.1007/978-3-031-66205-8_10.

[45] Nodirbek Inoyatov, "Artificial Intelligence And Autonomous Vehicles: Issues Of Legal Subjectivity In The Digital Era," *Jurisprudence* 5, no. 2 (April 2025): 38, https://doi.org/10.51788/tsul.jurisprudence.5.2./ECZK6798.

sufficient for the owner or operator's task. Article 12 says data must be used only for the previously stated purposes. Article 18 provides the legal grounds for processing, while Article 19 requires that the processing purpose be consistent with the purpose stated at the time of collection. These provisions support your argument for purpose lock-in in the CBDC sandbox[46].

For data security and localization, use Article 27 and Article 27^1. Article 27 requires legal, organizational, and technical measures to protect personal data, including measures to ensure confidentiality, integrity, and the prevention of unlawful processing. Article 27^1 was amended by Law No. O'RQ-1125 of 26 March 2026. The current version no longer imposes blanket localization for all personal data. It requires certain categories of data, such as biometric data, genetic data, and telecommunications users' data, to be stored in Uzbekistan. Other personal data may be stored or processed abroad if specific conditions are met, such as equivalent protection, standard contractual clauses, binding corporate rules, or recognized international standards[47].

The direct sandbox basis is Article 67^1 of the Law on the Central Bank of the Republic of Uzbekistan, Law No. O'RQ-582. This article defines the special legal regime, or regulatory sandbox, as a controlled, limited environment for testing new financial products, technologies, and services. It also states that the Central Bank determines the procedure for introducing and terminating the sandbox. The sandbox may last up to three years and must include evaluation criteria and target indicators[48].

The implementing regulation is Central Bank Resolution No. 3391 of 4 October 2022, titled Regulation on the Procedure for Introducing a Special Legal Regime in the Field of Financial Services[49]. It

---

[46] Naeem AllahRakha, "Digital Law Nexus 2025," *Uzbek Journal of Law and Digital Policy* 3, no. 2 (April 2025), https://doi.org/10.59022/ujldp.319.

[47] Budiono et al., "Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice."

[48] Sharipov Firdavs Kholnazarovich, "Legal Foundations And Practical Proposals For Applying Artificial Intelligence Technologies In Uzbekistan's Legislative Process," *International Journal of Law And Criminology* 5, no. 12 (December 2025): 12–16, https://doi.org/10.37547/ijlc/Volume05Issue12-03.

[49] Ardiansyah et al., "Taking Restitution Seriously?: Victim-Oriented Gaps in the Criminal Justice System."

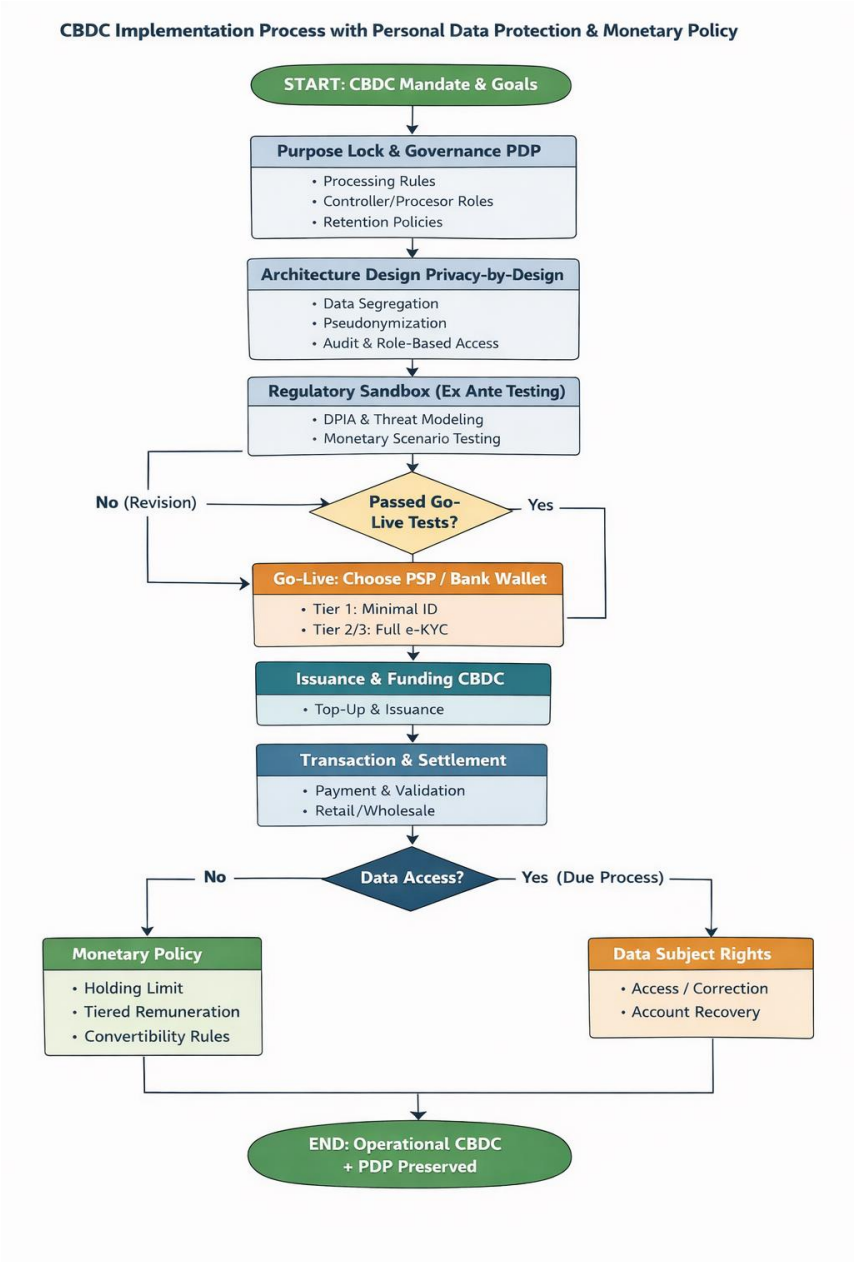
regulates the creation, cancellation, and operation of the sandbox. It also requires the temporary testing arrangement to include the tested service, the testing period, applicable exemptions and restrictions, evaluation criteria, consumer protection rules, AML/CFT requirements, and reporting obligations to the Central Bank[50].

These three instruments do not stand alone. Role-based access provides technical limits; SoD provides institutional limits; oversight provides normative limits. If one is missing, the system tends to become more invasive to improve effectiveness. Therefore, the sandbox must verify the combination of all three before expanding the pilot. To gain a comprehensive understanding of how a sandbox can be used as a testing environment to implement digital rupiah and data protection, see the following table[51].

[50] AllahRakha, "Digital Law Nexus 2025."

[51] Rafael Brown, Jon Truby, and Imad Antoine Ibrahim, "Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation," *European Studies* 9, no. 1 (August 2022): 61–90, https://doi.org/10.2478/eustu-2022-0003.

Flowchart 1. CBDC Implementation Process with Personal Data Protection and Monetary Policy



(Sources: Author's elaboration based on Indonesia's PDP Law (Law No. 27/2022) and OJK Regulation POJK No. 3/2024 on Implementation of Financial Sector Technology Innovation)

Flowchart 1 illustrates the proposed implementation process of CBDC within a personal data protection framework. The process begins with the legal mandate and policy objectives of CBDC. At this stage, the central bank must define the monetary goals, payment system objectives, and the public-interest justification for issuing a CBDC. These objectives are important because they determine the lawful basis and the limits of data processing[52].

The next stage is purpose lock and PDP governance. This stage requires clear processing rules, a division of roles between the controller and the processor, and retention policies. The purpose of data collection must be fixed from the beginning. Data should not later be used for unrelated objectives without legal review and proper authorization[53].

After that, the CBDC architecture must apply privacy-by-design. This means privacy protection is built into the system, not added after it is completed. The architecture should include data segregation, pseudonymization, audit trails, and role-based access. These mechanisms reduce the risk of profiling, excessive surveillance, and unauthorized access[54].

The scheme then places the CBDC system inside a regulatory sandbox. The sandbox works as an ex ante testing mechanism. It tests the system before wider implementation. This stage includes DPIA, threat modelling, and monetary scenario testing. The objective is to prove that the system is technically reliable, legally compliant, and proportionate[55].

The go-live test becomes the main decision point. If the system fails, it must return to the revision stage. If the system passes, it may proceed to a controlled go-live phase through PSPs or bank wallets. At this stage, tiered identity is important. Low-risk transactions may use

---

[52] Handayani, "Design And Legal Aspect Of Central Bank Digital Currency: A Literature Review."

[53] Camila Amalia, "Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment," *Journal of Central Banking Law and Institutions* 1, no. 2 (May 2022), https://doi.org/10.21098/jcli.v1i2.19.

[54] Linnan, "Central Bank Digital Currencies In The Indonesian Setting: Questions &Amp; Choices."

[55] Dita Anis Zafani and Moh. Musfiq Arifqi, "Cahsless Society on GoPay: An Islamic Economic Perspective," *Journal of Islamic Economic Laws* 9, no. 1 (March 2025): 141–58, https://doi.org/10.23917/jisel.v3i2.11904.

minimal identity verification, while higher-risk transactions require full electronic KYC[56].

The next stages concern CBDC issuance, funding, transaction, and settlement. These stages show that CBDC is not only a data system. It is also part of the monetary infrastructure. Therefore, it must support top-up, issuance, payment validation, and settlement for retail or wholesale use[57].

The final part of the scheme separates monetary policy functions from data access requests. Monetary policy tools, such as holding limits, tiered remuneration, and convertibility rules, may operate without exposing individual transaction data. However, when access to personal data is requested, it must follow due process. Data subjects must also retain their rights, including the right to access, correct, and recover their accounts[58].

Overall, the scheme shows that CBDC implementation should not be treated only as a technological project. It must be governed as a legal and institutional process. The main objective is to ensure that CBDC supports monetary policy while preserving personal data protection[59].

D. CBDC Architecture Options and Privacy Implications: Account-Based, Token-Based, and Hybrid Models

This discussion needs to touch on architectural choices, as architecture determines the data points and the degree of traceability.

---

[56] Ampuan Situmeang, Hari Sutra Disemadi, and Irvan Ricardo Marsudi, "Contextualizing Consumer Data Protection within the Operational Principles of Banking: A Legal Inquiry," *Legal Spirit* 8, no. 2 (August 2024): 365–78, https://doi.org/10.31328/ls.v8i2.5458.

[57] Niza Nur Azizah, "Analisis Sadd Al-Dzariah Terhadap Problematika Akibat Percerain Yang Dilakukan Di Luar Prosedur Pengadilan (Studi Kasus Di Kampung Banjarsari Kecamatan Baradatu Kabupaten Way Kanan)," 2022, 6.

[58] Frédéric Tronnier and Weihua Qiu, "How Do Privacy Concerns Impact Actual Adoption of Central Bank Digital Currency? An Investigation Using the e-Cny in China," *Quantitative Finance and Economics* 8, no. 1 (2024): 126–52, https://doi.org/10.3934/QFE.2024006.

[59] Izzulhaq, Kurnia, and Maharda, "Central Bank Digital Currency, Monetary Policy, And Macroeconomy: Evidence From Indonesia."

Simply put, CBDC designs often fall into three models: account-based, token-based, and hybrid[60]. Each model creates a different relationship between identity, transaction data, and regulatory control. This is important because CBDC architecture is not only a technical choice. It also determines the level of privacy, traceability, and legal risk in the system.

CBDC architecture may be classified into account-based, token-based, and hybrid models. This classification is important because each model creates a different relationship between user identity, transaction validation, privacy protection, and regulatory control. The table below summarizes the privacy and regulatory implications of each model[61].

Table 2. CBDC Architecture Models and Privacy–Regulatory Implications

Model	Core character	Privacy implication	Main regulatory benefit	Main legal risk
Account-based model	CBDC is held in an account linked to the user's identity.	Privacy is weaker because identity and transaction data are easier to connect.	Strong for KYC, AML/CFT, monitoring, and recovery.	Profiling, surveillance, and function creep.
Token-based model	CBDC works like digital cash. The system verifies the token, not always the full identity.	Privacy is stronger because not every transaction needs full identity linkage.	Useful for cash-like and low-value payments.	Fraud, token loss, and hidden traceability through later control mechanisms.

[60] Tjerk Timan and Zoltan Mann, "Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies," in *The Elements of Big Data Value* (Cham: Springer International Publishing, 2021), 153–75, https://doi.org/10.1007/978-3-030-68176-0_7.

[61] Mohamad Faisal Zulmy, Monica Vivi Kurniawati, and Setiadi Yazid, "The Conceptual Design E-Wallet for Rupiah Digital," *Jurnal Ilmu Komputer Dan Informasi* 18, no. 1 (June 2024): 29–45, https://doi.org/10.21609/jiki.v18i1.1309.

Hybrid model	CBDC combines identity-based and token-like features through tiered KYC and tiered privacy.	Privacy is balanced. Low-risk payments may use limited identity, while high-risk payments require stronger verification.	Balances privacy protection with AML/CFT and financial integrity.	Tier creep, where stricter identity rules slowly expand to all transactions.

(Source: Author's elaboration based on the World Bank's CBDC technical) note on account/token-based design and privacy–AML/CFT trade-offs, the IMF's discussion on CBDC data use and privacy risks, the EDPS analysis on CBDC privacy and token-based/offline design, and FATF guidance on risk-based AML/CFT and customer due diligence)

The account-based model gives regulators the strongest control. It is easier to identify users, monitor transactions, and recover accounts. However, this model also creates the highest privacy risk. When identity and transactions are directly linked, the system may enable profiling or excessive surveillance[62].

The token-based model gives stronger privacy. It is closer to cash logic because the system focuses on the validity of the payment instrument. However, this model is harder to supervise. It may create difficulties for AML/CFT, fraud prevention, and recovery when tokens are lost or misused[63].

The hybrid model offers a middle position. It allows low-value or low-risk transactions to be processed with limited identity. Higher-risk transactions still require stronger KYC. This model is more consistent with proportionality because not all users are treated as high risk.

[62] Brown, Truby, and Ibrahim, "Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation."

[63] Jamilya Panabergenova, Mambetbay Tleumuratov, and Sharafatdin Shamshetov, "Legal Aspects of Implementing Artificial Intelligence Systems in the Management of Energy Supply Companies in the Republic of Uzbekistan: Regulatory Challenges and Development Prospects," 2025, 030065, https://doi.org/10.1063/5.0305916.

However, it must be carefully controlled so that tiered privacy does not slowly disappear[64].

In academic terms, the hybrid model is the most balanced architecture for CBDC. A fully account-based model may be too intrusive. A fully token-based model may be too weak for regulatory controls. The hybrid model allows privacy and financial integrity to coexist. Its success depends on clear thresholds, strong access control, and sandbox testing before wider implementation[65].

Finally, the article emphasizes the importance of ongoing transparency after the sandbox phase. Many digital policies lose legitimacy not at launch, but when the public no longer receives adequate information about how data is managed. Therefore, the design of the Digital Rupiah should include mechanisms for periodic reporting on privacy and security: summaries of audit findings, statistics on data access requests by authorities (in aggregate form), the number of incidents and responses, and updates on mitigation controls.

Such reports do not have to disclose sensitive information that could jeopardize security; rather, they should provide transparency at the governance level. With ongoing transparency, the public can see that data protection is not a one-time project, but rather an ongoing commitment. In turn, this mechanism strengthens the effectiveness of monetary policy by increasing trust and encouraging user participation.

Conclusion

This article concludes that CBDC should be understood as both a monetary infrastructure and a data infrastructure. Its design affects the circulation of money, but it also determines how identity, transaction data, and public authority are connected. This is why CBDC implementation cannot be assessed only through technical readiness. It

---

[64] Meenakshi Shunmugam, Satya Rajesh Kunchaparthy, and Baby Kalpana, "High Protection Bank Locker Security Alert System Using Voice Authentication Based on Wireless Sensor Network," 2023, 020027, https://doi.org/10.1063/5.0115687.

[65] Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia," *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (August 2019): 145–60, https://doi.org/10.24246/jrh.2019.v3.i2.p145-160.

must also be assessed through legality, proportionality, accountability, and protection of personal data.

In Indonesia, the legal foundation for Digital Rupiah is already explicit. Law No. 7 of 2011 on Currency, as amended by Law No. 4 of 2023, recognizes Rupiah digital as one form of Rupiah. It also gives Bank Indonesia exclusive authority to manage Digital Rupiah through planning, issuance, circulation, and administration. The same provision requires attention to monetary stability, payment-system stability, innovation, inclusion, cybersecurity, and personal data protection. This confirms that CBDC implementation in Indonesia must be linked to the PDP Law, especially the principles of lawful, limited, specific, and transparent processing.

This article, therefore, argues that the regulatory sandbox is essential at every stage of CBDC development. In the pre-pilot phase, the sandbox should test the legal basis, purpose lock, data-flow map, and institutional role division. In the limited pilot phase, it should test tiered KYC, data minimization, access control, retention, cybersecurity, AML/CFT controls, and user remedies. In the evaluation phase, it should produce a clear go/no-go decision. In the expansion phase, it should become a continuing oversight mechanism. In this way, the sandbox functions as an ex ante compliance mechanism, rather than merely a space for technological experimentation.

The article proposes a hybrid rights-based model for CBDC governance. The hybrid architecture is suitable because it balances privacy and financial integrity. Low-value, low-risk transactions can use limited identity verification. Higher-risk transactions may require stronger KYC and traceability measures. This model is more proportionate than a fully account-based model, which may create excessive profiling risks. It is also more controllable than a purely token-based model, which may weaken AML/CFT supervision. However, the hybrid model must be governed through a rights-based framework. This means that every phase must test purpose limitation, minimization, retention, role-based access, audit trails, independent review, and effective remedies.

The comparison with Uzbekistan strengthens this conclusion. Uzbekistan has not yet provided a CBDC-specific legal framework equivalent to Indonesia's Digital Rupiah provisions. However, its

Central Bank Law provides a special regulatory sandbox for testing new financial operations, technologies, and services in a controlled, limited environment. This regime includes a defined testing period, evaluation criteria, target indicators, and post-test analysis. Uzbekistan's Personal Data Law also requires that processing purposes be legally determined and that any change of purpose be subject to consent or legal control. These rules show that CBDC preparation must address both financial innovation and data protection from the design stage.

References

AllahRakha, Naeem. "Digital Law Nexus 2025." *Uzbek Journal of Law and Digital Policy* 3, no. 2 (April 2025). https://doi.org/10.59022/ujldp.319.

Amalia, Camila. "Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment." *Journal of Central Banking Law and Institutions* 1, no. 2 (May 2022). https://doi.org/10.21098/jcli.v1i2.19.

Ardiansyah, Indra, Anis Widyawati, Indah Sri Utari, and Moh. Fadhil. "Taking Restitution Seriously?: Victim-Oriented Gaps in the Criminal Justice System." *IJCLS (Indonesian Journal of Criminal Law Studies)* 10, no. 1 (2025). https://doi.org/10.15294/ijcls.v10i1.19636.

Auer, Raphael, Codruta Boar, Giulio Cornelli, Jon Frost, Henry Holden, and Andreas Wehrli. "CBDC Beyond Borders - Results from a Survey of Central Bankers." *Bank For International Settlements*, no. June (2021): 105–6.

Azizah, Niza Nur. "Analisis Sadd Al-Dzariah Terhadap Problematika Akibat Percerain Yang Dilakukan Di Luar Prosedur Pengadilan (Studi Kasus Di Kampung Banjarsari Kecamatan Baradatu Kabupaten Way Kanan)," 2022, 6.

Benuf, Kornelius, Siti Mahmudah, and Ery Agus Priyono. "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia." *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (August 2019): 145–60. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160.

Brown, Rafael, Jon Truby, and Imad Antoine Ibrahim. "Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation." *European Studies* 9, no. 1 (August 2022): 61–90. https://doi.org/10.2478/eustu-2022-0003.

Budiono, Arief, Absori Absori, Kelik Wardiono, Wardah Yuspin, and Said Saidakhrarovich Gulyamov. "Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice." *Journal of Human Rights, Culture and Legal System* 3, no. 3 (November 2023): 441–75. https://doi.org/10.53955/jhcls.v3i3.127.

Carrillo, Raúl. "Seeing Through Money: Democracy, Data Governance, and the Digital Dollar." *SSRN Electronic Journal*, 2023, 1207–1304. https://doi.org/10.2139/ssrn.4354085.

Costantini, Federico, A, Send mail to Costantini F., ;, Nikolas Thomopoulos, B, ;, et al. "Autonomous Vehicles in a GDPR Era: An International Comparison," 191–213, 2020. https://doi.org/10.1016/bs.atpp.2020.02.005.

Crawford, John, Lev Menand, and Morgan Ricks. "FedAccounts: Digital Dollars." *George Washington Law Review* 89, no. 1 (2021): 113–72.

Devlin, Jennifer, Amy Stein, Peter Molk, Kathy Hwang, Ben Johnson, Chris Hampson, Tsang Cheng-yun, et al. "Digital Dollar : Privacy and Transparency Dilemma," 2025, 629–78.

Enggarwati, Mutia, and Inda Fresti Puspitasari. "Central Bank Digital Currency and Financial Stability in Indonesia: Analysis on Vector Error Correction Model (VECM) Approach." *Proceeding ISETH (International Summit on Science, Technology, and Humanity)*, January 2024, 1533–42. https://doi.org/10.23917/iseth.4364.

Fadhlina, Resentia, Syarifahah Fatimahtazzuhrah Rukhsal Assegaf, Herpandu Hadiwibowo, Alicia Shafa Azzahra, Amilah, Regina, and Devita. "Perlindungan Data Pribadi Nasabah Dalam Transaksi Central Bank Digital Currency (CBDC) Dalam Rupiah Digital" 7, no. 1 (2024): 308–16.

Firdaus, Sendy Pratama. "Measuring The Urgency Of A Digital Rupiah: A Socio-Legal Review." *Journal of Central Banking Law and Institutions* 4, no. 3 (September 2025): 505–32. https://doi.org/10.21098/jcli.v4i3.283.

Handayani, Fitri. "Design And Legal Aspect Of Central Bank Digital Currency: A Literature Review." *Journal of Central Banking Law and Institutions* 1, no. 3 (September 2022): 509–36. https://doi.org/10.21098/jcli.v1i3.35.

Inoyatov, Nodirbek. "Artificial Intelligence And Autonomous Vehicles: Issues Of Legal Subjectivity In The Digital Era." *Jurisprudence* 5, no. 2 (April 2025): 38. https://doi.org/10.51788/tsul.jurisprudence.5.2./ECZK6798.

Izzulhaq, Syahid, Akhmad Syakir Kurnia, and Johan Beni Maharda. "Central Bank Digital Currency, Monetary Policy, And Macroeconomy: Evidence From Indonesia." *Bulletin of Monetary Economics and Banking* 27, no. 2 (May 2024): 241–64. https://doi.org/10.59091/2460-9196.2273.

Kelvin K. F., And Lillian F. Mills. "Financial Gatekeepers and Investor Protection: Evidence from Criminal Background Checks." *Journal of Accounting Research* 57, no. 2 (May 2019): 491–543. https://doi.org/10.1111/1475-679X.12265.

Kholnazarovich, Sharipov Firdavs. "Legal Foundations And Practical Proposals For Applying Artificial Intelligence Technologies In Uzbekistan's Legislative Process." *International Journal of Law And Criminology* 5, no. 12 (December 2025): 12–16. https://doi.org/10.37547/ijlc/Volume05Issue12-03.

Kosse, Anneke, and Ilaria Mattei. "The Potential of Central Bank Digital Currencies for Cross-Border Payments," no. 439 (2022): 1–7.

Linnan, David K. "Central Bank Digital Currencies In The Indonesian Setting: Questions &Amp; Choices." *Journal of Central Banking Law and Institutions* 2, no. 2 (May 2023): 221–64. https://doi.org/10.21098/jcli.v2i2.45.

Lu, Lerong. "The Law of Fintech: How Artificial Intelligence and Innovative Technologies Contribute to a Sustainable Financial Industry and Its Effective Regulation." In *Artificial Intelligence, Finance, and Sustainability*, 243–63. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-66205-8_10.

Maghfira, S, and W Yuspin. "Legal Analysis of Central Bank Digital Currency (CBDC) Regulation in the Indonesian Payment System: A Comparative Study with the Implementation of E-CNY in …."

Journal of Legal and Social Changes 1, no. 1 (2025): 1–13.

Mahardika, Zahrashafa, Rizky Banyualam Permana, and Nadia Maulisa. "Going Digital Rupiah: Some Considerations From Sovereignty And Cybersecurity Perspectives." *Journal of Central Banking Law and Institutions* 2, no. 1 (January 2023): 25–54. https://doi.org/10.21098/jcli.v2i1.42.

Marange, Patience, and Friedrich Hamadziripi. "Adapting Regulatory Compliance in Zimbabwe's Banking Sector to the Financial Technology Revolution: Lessons from South Africa." *Potchefstroom Electronic Law Journal* 29 (February 2026). https://doi.org/10.17159/1727-3781/2026/v29i0a21383.

Maryaningsih, Novi, Suahasil Nazara, Febrio Nathan Kacaribu, and Solikin M Juhro. "Central Bank Digital Currency: What Factors Determine Its Adoption?" *Buletin Ekonomi Moneter Dan Perbankan* 25, no. 1 (June 2022): 1–24. https://doi.org/10.21098/bemp.v25i1.1979.

Mau Bere, Alejandro Billyjoe, Richard Win Putra, and Linda Kusumaning Wedari. "Investigation of Digital Rupiah Acceptance Using UTAUT-3 Model." *Indonesian Journal of Electrical Engineering and Computer Science* 35, no. 3 (September 2024): 1710. https://doi.org/10.11591/ijeecs.v35.i3.pp1710-1721.

Ministry of Finance RI. "Getting to Know CBDC Better," 2023.

Moraes, Thiago. "Regulatory Sandboxes for Trustworthy Artificial Intelligence – Global and Latin American Experiences." *International Review of Law, Computers & Technology* 39, no. 1 (January 2025): 55–74. https://doi.org/10.1080/13600869.2024.2351674.

Muhammad, Rafli Fadilah, and Rianda Dirkareshza. "Legalitas Penerapan Central Bank Digital Currency (CBDC) Di Indonesia." *Jurnal Usm Law Review* 6, no. 3 (November 2023): 913–30. https://doi.org/10.26623/julr.v6i3.7370.

Panabergenova, Jamilya, Mambetbay Tleumuratov, and Sharafatdin Shamshetov. "Legal Aspects of Implementing Artificial Intelligence Systems in the Management of Energy Supply Companies in the Republic of Uzbekistan: Regulatory Challenges and Development Prospects," 030065, 2025.

https://doi.org/10.1063/5.0305916.

Pati, Umi Khaerah, and Heri Indrajat. "Regulating Fintech in the CBDC Era: Addressing Competitive Fragility and Preserving State-Owned Banking Stability." *Journal of Indonesian Legal Studies* 10, no. 1 (August 2025): 257–94. https://doi.org/10.15294/jils.v10i1.19342.

Santoso, Wahyu Yun, Araya Anggara Putra, Laras Susanti, and Faiz Rahman. "Design Elements And Risks Of Central Bank Digital Currency In Tailoring A Prudent 'Rupiah Digital." *Diponegoro Law Review* 8, no. 2 (October 2023): 141–58. https://doi.org/10.14710/dilrev.8.2.2023.141-158.

Shunmugam, Meenakshi, Satya Rajesh Kunchaparthy, and Baby Kalpana. "High Protection Bank Locker Security Alert System Using Voice Authentication Based on Wireless Sensor Network," 020027, 2023. https://doi.org/10.1063/5.0115687.

Situmeang, Ampuan, Hari Sutra Disemadi, and Irvan Ricardo Marsudi. "Contextualizing Consumer Data Protection within the Operational Principles of Banking: A Legal Inquiry." *Legal Spirit* 8, no. 2 (August 2024): 365–78. https://doi.org/10.31328/ls.v8i2.5458.

Spatari, Nadia. "Building Safe Digital Environments for Children: AI Regulatory Sandbox and Pilot Project Insights." In *2025 12th International Conference on Future Internet of Things and Cloud (FiCloud)*, 459–66. IEEE, 2025. https://doi.org/10.1109/FiCloud66139.2025.00070.

Taniady, Vicko, Salsabiila Puteri Permatasari, and Reyka Widia Nugraha. "Crypto Asset-Trade Resilience During The Covid-19 Pandemic In Indonesia." *Jurnal Jurisprudence* 11, no. 1 (January 2022): 31–43. https://doi.org/10.23917/jurisprudence.v11i1.13340.

Timan, Tjerk, and Zoltan Mann. "Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies." In *The Elements of Big Data Value*, 153–75. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-68176-0_7.

Tronnier, Frédéric, and Weihua Qiu. "How Do Privacy Concerns Impact Actual Adoption of Central Bank Digital Currency? An

Investigation Using the e-Cny in China." *Quantitative Finance and Economics* 8, no. 1 (2024): 126–52. https://doi.org/10.3934/QFE.2024006.

Utari, Indah Sri, Ridwan Arifin, Ali Masyhar, Valerio Sebastian, and Souad Ezzerouali. "Rethinking Filicide through Freudian Psychoanalysis: A Comparative Perspective on Indonesian and Spanish Criminal Cases." *Jurnal IUS Kajian Hukum Dan Keadilan* 14, no. 2 (2026): 587–620. https://doi.org/10.29303/ius.v14i2.1997.

Utari, Indah Sri, Ridwan Arifin, and Ahmad Zaharuddin Sani Ahmad Sabri. "Why Did a Five-Year-Old Toddler Become a Victim of Murder? A Criminological and Legal Perspective." *Indonesian Journal of Criminal Law Studies* 8, no. 2 (2023). https://doi.org/10.15294/ijcls.v8i2.48591.

Utari, Indah Sri, Muhammad Azil Maskur, Benny Sumardiana, Diandra Preludio Ramada, and Nizamuddin Alias. "Illegal Nickel Mining in Protected Forests: Challenges in Whistleblower and Justice Collaborator Protection in Indonesia." *Indonesian Journal of Environmental Law and Sustainable Development* 4, no. 2 (2025): 341–74. https://doi.org/10.15294/ijel.v4i2.38220.

Utari, Indah Sri, Diandra Preludio Ramada, Salman Alfarisi, and Nizamuddin Alias. "A Criminological Perspective on Corruption as a Catalyst of Economic Breakdown: Socio-Legal Challenges in Indonesian Environmental Governance." *Jambe Law Journal* 9, no. 1 (2026): 205–47. https://doi.org/10.22437/jmj4ac47.

Utari, Indah Sri, Diandra Preludio Ramada, Ubaidillah Kamal, Ratih Damayanti, and Nizamuddin Alias. "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online." *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025). https://doi.org/10.15294/ciils.v4i2.35309.

Wiranta, Alma, Robby MT, and Sovian Aritonang. "The Development of Digitalization of Rupiah Currency Towards National Security, Especially in Dealing With Cyber Crime and Financial Crime." *International Journal of Accounting and Economics Studies* 12, no. 6 (October 2025): 169–75. https://doi.org/10.14419/gbs8mw83.

Yuspin, Wardah, Ata Fauzie. "The Effectiveness of Spin off As a Breakthrough in Promoting Islamic Banking in Indonesia." *The*

Journal of Social Sciences Research, no. 6 (December 2018): 213–16. https://doi.org/10.32861/jssr.spi6.213.216.

Yuspin, Wardah, Kelik Wardiono, Arief Budiono, Andria Luhur Prakoso, and Trisha Rajput. "The Accountability Principle in Personal Data Protection in Sweden and Indonesia." *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (October 2025): 667–94. https://doi.org/10.53955/jsderi.v3i3.97.

Zafani, Dita Anis, and Moh. Musfiq Arifqi. "Cahsless Society on GoPay: An Islamic Economic Perspective." *Journal of Islamic Economic Laws* 9, no. 1 (March 2025): 141–58. https://doi.org/10.23917/jisel.v3i2.11904.

Zhang, Chenguo. "China's New Regulatory Regime Tailored for the Sharing Economy: The Case of Uber under Chinese Local Government Regulation in Comparison to the EU, US, and the UK." *Computer Law & Security Review* 35, no. 4 (August 2019): 462–75. https://doi.org/10.1016/j.clsr.2019.03.004.

Zulmy, Mohamad Faisal, Monica Vivi Kurniawati, and Setiadi Yazid. "The Conceptual Design E-Wallet for Rupiah Digital." *Jurnal Ilmu Komputer Dan Informasi* 18, no. 1 (June 2024): 29–45. https://doi.org/10.21609/jiki.v18i1.1309.

Acknowledgment

The authors gratefully acknowledge the financial support provided under the Research Contract Letter for Funding and Implementation of National Muhammadiyah Research Grants (RISETMU) Batch IX 2025 Number: 0259.898/I.3/D/2025. This research was funded and facilitated through the Muhammadiyah National Research Grant (RISETMU) program, whose support has been instrumental in enabling the successful completion of this study. The authors also extend sincere appreciation to the academic advisors, institutional leaders, and all parties who contributed guidance, administrative assistance, and constructive input throughout the research process.

Funding Information

This research was funded by the "*Majelis Pendidikan Tinggi, Penelitian, dan Pengembangan (Diktilitbang) Pimpinan Pusat Muhammadiyah under the Hibah Riset Nasional Muhammadiyah Batch IX Tahun 2025*", based on Research Contract Number 0259.898/I.3/D/2025. The total grant amount awarded for this study was Rp 20,000,000 (Twenty Million Rupiah), disbursed in two stages: 70% upon initial verification and 30% after completion of all research obligations, including submission of the final report and required research outputs.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

None.