Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Security and Privacy in Digital Payments: Blockchain, PIX, and Central Bank Digital Currencies (CBDCs)

Nilton Gomes Furtado

nilton.furtado@ua.pt

University of Aveiro

Daniel Ferreira Polonia

University of Aveiro

Julia Vasconcelos Furtado

University of Algarve

Systematic Review

Keywords: digital payment governance, central bank digital currencies, blockchain privacy, PIX, zero-knowledge proofs, privacy-enhancing technologies, systematic review, Digital Payment Governance Framework

Posted Date: November 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10939814/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

Background.

Digital payment systems, instant payment networks such as Brazil's PIX, public and permissioned blockchains, and Central Bank Digital Currencies (CBDCs) have become critical global financial infrastructure. Despite rapid adoption, persistent and unresolved trade-offs between security, privacy, and regulatory compliance remain inadequately addressed by existing governance frameworks, which are fragmented, system-specific, and rarely comparable across architectures.

Methods.

We conduct a PRISMA 2020-compliant systematic review of 50 highly relevant studies identified from 615 candidates (473 database records across Scopus, Web of Science, and Consensus AI; 142 via citation chaining) published between 2014 and 2025. Studies are thematically analysed across five governance dimensions: governance frameworks, privacy-enhancing technologies (PETs), regulatory compliance, decentralisation versus centralisation, and cryptographic mechanisms, and are positioned within a novel Digital Payment Governance Framework (DPGF) comprising three operationalisable axes.

Results.

PIX exemplifies a Regulatory Clarity Model (LoC-1 · PS-4 · CA-1): centralised control, low-default privacy, and a regulation-by-design compliance architecture. Public blockchains represent an Autonomy Model (LoC-5 · PS-2 · CA-5): decentralised governance, intermediate pseudonymity, and post-hoc compliance. CBDCs and permissioned blockchains exhibit a Hybrid Governance Model (LoC-2 · PS-2 · CA-2), combining central bank monetary authority with distributed execution and privacy-by-design potential. Zero-knowledge proofs and homomorphic encryption are the most adopted PETs but face unresolved scalability and metadata-privacy limitations. Hybrid governance architectures consistently demonstrate superior performance across composite governance indicators.

Conclusions.

The DPGF provides a structured, empirically grounded foundation for designing, evaluating, and comparing digital payment governance arrangements across architectures and jurisdictions. Five testable propositions derived from the framework constitute a research agenda for future empirical validation. Harmonised legal-technical frameworks that embed privacy-by-design at the protocol level represent the highest-priority governance innovation for next-generation payment infrastructure.

1. Introduction

The global digital payment ecosystem has undergone profound structural change in the decade since Bitcoin introduced decentralised ledger technology in 2008. Three distinct technological paradigms now coexist and

compete: centralised instant payment systems, exemplified by Brazil's PIX, launched by the Banco Central do Brasil (BCB) in November 2020 and now processing over three billion transactions monthly (BCB, 2024); public and permissioned blockchain networks used for payment settlement; and Central Bank Digital Currencies (CBDCs), with over 130 jurisdictions in active exploration or pilot phase as of 2025 (BIS, 2024). Each paradigm embodies fundamentally different design choices regarding control, privacy, and regulatory compliance, yet comparative governance analysis across all three remains sparse.

This structural divergence creates three interrelated problems that motivate the present review. First, governance frameworks are developed in isolation: CBDC literature rarely engages with PIX-type fast payment systems, and blockchain governance scholarship seldom incorporates comparative perspectives from central banks (Cong et al., 2024; Lee et al., 2021). Second, privacy-enhancing technologies (PETs), such as zero-knowledge proofs, homomorphic encryption, and proxy re-encryption, are evaluated within single-system contexts, preventing meaningful cross-architectural assessment of their effectiveness and scalability (Kaur, 2024; Xue et al., 2025). Third, the trade-offs between privacy, transparency, and regulatory compliance are consistently identified as central challenges but never formally modelled in a way that enables system comparison or generates testable propositions for empirical research (Sillaber & Eggen, 2024; Uhlig et al., 2023).

The specific contribution of this article is threefold. We conduct a PRISMA 2020-compliant systematic review synthesising 50 studies across the three system types (Section 3). We introduce the Digital Payment Governance Framework (DPGF), a three-axis analytical space that formalises the persistent trade-offs identified in the literature into operationalizable dimensions and positions PIX, public blockchains, and CBDCs within it (Section 2). We derive five testable propositions from the DPGF that constitute an empirical research agenda (Section 2.3), and we propose a cross-system indicator set enabling future measurement (Section 6). The article is structured as follows: Section 2 introduces the DPGF; Section 3 presents the methodology; Section 4 reports descriptive results; Section 5 presents the thematic synthesis; Section 6 presents the comparative governance analysis; Section 7 discusses theoretical and practical implications; Section 8 concludes.

2. Theoretical Framework: The Digital Payment Governance Framework (DPGF)

Digital payment governance has been theorised through multiple partial lenses: regulatory theory (Napieralska & Kępczyński, 2024), institutional economics (Shapoval, 2020), information systems privacy (Tronnier et al., 2023), and cryptographic engineering (Kiayias et al., 2022). No existing framework integrates these perspectives into a single analytical space that is simultaneously applicable to centralised, decentralised, and hybrid payment architectures. The DPGF is designed to fill this gap.

The DPGF builds on three established theoretical traditions. The Locus of Control axis draws on Ostrom's (1990) institutional analysis of polycentric governance and on Tirole's (2015) theory of platform regulation, both of which distinguish the authority to set rules from the capacity to enforce them, a distinction this article extends to digital payment protocol governance. The Privacy Spectrum axis is grounded in Acquisti et al.'s (2016) economics of privacy, specifically their demonstration that privacy valuations are context-dependent

and non-monotonic with respect to disclosure levels, and in Nissenbaum's (2004) contextual integrity theory, which holds that information flows are appropriate when they match the normative expectations of the context in which they originate. The Compliance Architecture axis is anchored in Baldwin et al.'s (2012) regulatory design framework, which treats ex ante rule-embedding and ex post enforcement as fundamentally different regulatory strategies with distinct cost, precision, and adaptability profiles. By grounding each axis in prior theory, the DPGF generates propositions that are theoretically motivated rather than merely empirically induced and that connect digital payment governance to broader bodies of evidence in regulatory economics, privacy theory, and institutional analysis.

2.1 Framework Design Logic

Three empirical observations recur across the 50 reviewed studies, regardless of technological architecture: (i) control over system rules and enforcement is always distributed across some set of actors, but the distribution varies radically, from a single central authority to a diffuse protocol community; (ii) the disclosure level of transactional and identity data exists on a spectrum, not as a binary, and can be engineered at multiple architectural layers; and (iii) compliance obligations can be embedded structurally at the time of system design or enforced retroactively at system boundaries. These three observations map onto three independent axes, each with a measurable 1–5 scale.

The DPGF positions any digital payment governance arrangement as a coordinate triple (LoC, PS, CA) within a three-dimensional analytical space (Fig. 1). The axes are orthogonal by design: a system can simultaneously have centralised governance (LoC-1), intermediate privacy (PS-3), and post-hoc compliance (CA-5). This orthogonality is an analytical advantage over frameworks that conflate governance centralisation with a compliance approach, as many policy documents do. Table 1 formalises each axis.

Table 1
Digital Payment Governance Framework (DPGF), Axis Definitions

DPGF Axis	Governance Question	Poles (1 → 5)	Operationalisation
Axis 1, Locus of Control (LoC)	Who holds ultimate authority over system rules, enforcement and upgrade decisions?	LoC-1: Fully centralised (single authority) ↔ LoC-5: Fully decentralised (protocol community)	Number of veto actors; amendment procedure; enforcement locus; upgrade governance
Axis 2, Privacy Spectrum (PS)	What is the default disclosure level of transaction and identity data?	PS-1: Full anonymity (cash-like) ↔ PS-5: Full transparency (fully auditable ledger)	Default pseudonymity; availability of ZKPs/HE; selective disclosure mechanisms; tiered privacy
Axis 3, Compliance Architecture (CA)	When and how are regulatory obligations embedded in the system?	CA-1: Regulation-by-design (ex ante, protocol-level) ↔ CA-5: Post-hoc compliance (boundary-layer enforcement)	Smart contract enforcement; built-in AML/KYC; audit trail architecture; upgrade rigidity

DPGF axes and their operationalisation. LoC = Locus of Control; PS = Privacy Spectrum; CA = Compliance Architecture.

2.2 DPGF Positioning of the Three Systems

Figure 1 presents the DPGF as a radar diagram, positioning PIX, public blockchains, and CBDCs/permissioned blockchains within the three-axis space. Table 2 unpacks the rationale for the positioning of each axis. Scores are derived from the comparative governance analysis across 20 domains (Section 6) and from convergent evidence in the 50 reviewed studies. Positioning is analytical, not evaluative: no axis pole is inherently superior, and optimal scores are context-dependent.

Table 2
DPGF Positioning: PIX vs Public Blockchain vs CBDC/Permissioned Blockchain

DPGF Axis	PIX (Brazil)	Public Blockchain	CBDC / Permissioned BC	Key Trade-off
LoC	LoC-1. BCB mandates all rules; PSPs are operational delegates. No community veto.	LoC-5. Protocol-level consensus; forks as a governance mechanism; no authority can compel compliance.	LoC-2. The central bank retains monetary authority; the consortium or intermediary executes operations.	Efficiency vs resilience to regulatory capture
PS	PS-4. Full auditability by BCB and PSPs; no cryptographic mechanism for user-controlled selective disclosure.	PS-2. Pseudonymity by default; ZKPs, ring signatures, CoinJoin available but not mandated.	PS-2. Privacy-by-design possible; tiered anonymity (small TX → higher privacy) via ZKPs and Pedersen commitments.	User autonomy vs AML/KYC compliance
CA	CA-1. AML/KYC obligations are structurally inseparable from participation; mandatory PSP compliance.	CA-5. The protocol layer is compliance-agnostic; obligations are imposed only at the VASP/PSP boundary.	CA-2. Smart contract enforcement; programmable compliance; built-in holding limits and AML triggers.	Rule precision vs regulatory adaptability
DPGF Profile	Regulatory Clarity Model (LoC-1 · PS-4 · CA-1)	Autonomy Model (LoC-5 · PS-2 · CA-5)	Hybrid Governance Model (LoC-2 · PS-2 · CA-2)	No single optimal; context-dependent

System positioning across the three DPGF axes. No single profile is optimal; trade-offs are context-dependent.

2.3 Testable Propositions Derived from the DPGF

A systematic review at this venue must generate propositions that future empirical studies can test. The following five propositions are derived from the DPGF axes and their interactions, operationalised via the indicator set in Section 6 (Table 5):

- P1 (LoC → Regulatory Efficiency): Governance arrangements with lower LoC scores exhibit faster regulatory response times and higher PSP compliance rates, but higher surveillance risk as measured by linkability indices. Jurisdictions implementing centralised payment systems (LoC-1 to LoC-2) are expected to outperform decentralised systems (LoC-4 to LoC-5) on MTTR and compliance rates, at the cost of higher linkability.

- P2 (PS → User Trust): Arrangements with intermediate PS scores (PS-2 to PS-3), implementing selective anonymity with regulatory auditability, generate higher user trust (NPS) than arrangements at extremes, following an inverted-U functional form. The mechanism operates through two competing channels: (i) increasing anonymity toward PS-1 reduces surveillance anxiety but amplifies institutional concern about illicit use, eroding systemic trust; (ii) increasing transparency toward PS-5 reduces illicit-use concern but amplifies individual financial surveillance anxiety, eroding user trust. The intermediate range (PS-2 to PS-3) minimises the sum of both trust-eroding forces. This inverted-U prediction is consistent with Acquisti et al. (2016), who show that privacy valuations peak at intermediate disclosure levels, and with Nissenbaum (2004), whose contextual integrity framework holds that payment transactions are contextually appropriate only when disclosure matches the norms of the financial context, that is, neither the full anonymity of physical cash (PS-1, which may raise illicit-use concerns) nor the full transparency of a public ledger (PS-5, which raises surveillance concerns).
- P3 (CA → Compliance Cost): Regulation-by-design architectures (CA-1 to CA-2) reduce per-transaction compliance cost relative to post-hoc enforcement architectures (CA-4 to CA-5), but increase system inflexibility to regulatory change, manifested as higher implementation cost of regulatory updates.
- P4 (Hybrid Governance Advantage): Governance arrangements with intermediate scores across all three axes (LoC-2 to LoC-3, PS-2 to PS-3, CA-2 to CA-3) demonstrate superior performance on composite governance indices, combining fraud rate, MTTR, linkability index and user trust, relative to systems at extremes.
- P5 (PET Scalability Constraint): Adoption of advanced PETs (ZKPs, homomorphic encryption) reduces the linkability index but increases transaction latency nonlinearly, imposing a scalability ceiling that constrains their feasibility at national payment volume scales without hardware acceleration or batching protocols.

3. Methodology

3.1 Research Protocol and Registration

This review follows the PRISMA 2020 reporting guidelines (Page et al., 2021). The research question, formulated in PICO format, is: What governance frameworks, privacy-enhancing technologies, and cryptographic mechanisms are effective in mitigating security and privacy risks in PIX, public/permissioned blockchains, and CBDCs, under what regulatory conditions, and with what trade-offs between privacy, transparency and compliance? The review was not pre-registered. Methodological decisions and any post-hoc analytical choices are disclosed transparently in the limitations section (Section 7.3).

DPGF Scoring Protocol. The scores assigned to each system on the three DPGF axes (Table 2) were derived through a structured domain-mapping procedure applied to the 20 governance domains in Table 3. For each domain, two reviewers independently assigned a sub-score to each system on the relevant axis: LoC sub-scores reflect the number and independence of veto actors, amendment procedures, and enforcement locus; PS sub-scores reflect default disclosure level, mandatory adoption of PETs, and selective disclosure mechanisms; CA sub-scores reflect whether compliance obligations are embedded at protocol level (CA-1), enforced at system boundaries (CA-5), or distributed between these extremes. System-level axis scores

represent the median of domain sub-scores. Disagreements on sub-scores were resolved by discussion; where consensus was not reached, the midpoint was adopted. The full sub-score matrix is available as Supplementary Material S3. Sensitivity analysis showed that varying each system score by ± 1 does not alter the qualitative ordering of DPGF profiles or the directional predictions of Propositions P1–P5.

3.2 Eligibility Criteria

Inclusion and exclusion criteria were defined a priori and applied consistently across all screening stages. Table 4 presents the full set of criteria.

Table 4
Eligibility Criteria, PRISMA 2020 Compliant

Category	Criterion	Description	Rationale
INCLUSION	**Theme scope**	Studies explicitly addressing security, privacy and/or governance in digital payments	Ensures alignment with research question
INCLUSION	**Target systems**	At least one of: PIX (Brazil), public/permissioned blockchains used for payments, CBDCs (retail/wholesale)	Ensures comparability across governance arrangements
INCLUSION	**Outcomes/indicators**	Reports at least one measurable indicator of security, privacy, governance or operations	Enables structured synthesis
INCLUSION	**Study types**	Quantitative/qualitative empirical, case studies, technical evaluations, regulatory analyses with metrics	Favours evidence useful for synthesis
INCLUSION	**Source quality**	Peer-reviewed journals, conferences, regulator/CB technical reports with transparent methodology	Ensures minimum methodological rigour
INCLUSION	**Time window**	2014–2025 (blockchain); 2020–2025 (PIX); CBDC pilots/production from 2017	Aligns with technological maturity
INCLUSION	**Language**	Portuguese, English or Spanish	Maximises Ibero-American coverage
EXCLUSION	**Inadequate scope**	Primary focus outside digital payments or without a link to security/privacy/governance	Avoids topic dilution
EXCLUSION	**Absent method**	No method, data, metrics or verifiable evidence	Avoids high risk of bias
EXCLUSION	**Duplication**	Duplicate or preliminary version where consolidated final version exists	Avoids redundancy

Inclusion and exclusion criteria were applied at title/abstract and full-text screening stages.

3.3 Search Strategy

Systematic electronic searches were conducted in two primary bibliographic databases: Scopus (search date: 15 March 2025; n = 289 records) and Web of Science Core Collection (search date: 15 March 2025; n = 184 records), yielding 473 records after deduplication across the two databases. As a supplementary source for grey literature and recent preprints, Consensus AI (search date: 20 March 2025) was queried using the same conceptual terms; 142 additional records were identified through this channel combined with citation chaining. Consensus AI was treated as a supplementary source only: each candidate was verified against Scopus or Web of Science metadata before inclusion and subjected to identical eligibility criteria. Results from primary databases and the supplementary channel are reported separately in the PRISMA 2020 flow diagram (Fig. 2). The following Boolean search string was applied to Scopus and WoS:

(TITLE-ABS-KEY("digital payment" OR "instant payment" OR "PIX" OR "CBDC" OR "central bank digital currency" OR "blockchain") AND TITLE-ABS-KEY("security" OR "privacy" OR "governance") AND TITLE-ABS-KEY("framework" OR "cryptography" OR "zero-knowledge" OR "regulation" OR "AML" OR "KYC")) AND PUBYEAR > 2013

The temporal window was 2014–2025 for blockchain and CBDC studies, and 2020–2025 for PIX-specific studies (reflecting the system's operational launch). Snowball searching (backward citation chaining from reference lists, and forward citation chaining using Google Scholar) was applied to all studies meeting full-text inclusion criteria.

3.4 Screening and Data Extraction

Title and abstract screening was conducted by two independent reviewers (reviewer identities redacted for double-blind peer review), with inter-rater agreement assessed using Cohen’s kappa ($\kappa = 0.78$, 95% CI [0.71, 0.85], indicating substantial agreement per Landis and Koch 1977). Disagreements were resolved by consensus or third-party arbitration. Full-text assessment was applied to all records passing abstract screening. Figure 2 presents the PRISMA 2020 flow diagram.

A structured extraction template covering 19 fields was applied to all 50 included studies: study identifier, publication year, country/region, target system context, blockchain type, use case, study type, data sources, sample size or scope, primary threats analysed, governance domains covered, reported indicators, metrics and units, observed values, measurement window, calculation methodology, limitations, main conclusions, and additional references. Full extraction data are available as Supplementary Material S2.

4. Descriptive Results: Study Landscape

4.1 Temporal Distribution

Publication volume grew substantially over the review period, reflecting accelerating institutional and academic interest in digital payment governance. Studies published between 2020 and 2022 account for 28% of the corpus (n = 14), driven primarily by early CBDC design literature and initial blockchain security evaluations. The period 2023–2025 accounts for 72% (n = 36), with 2024 representing the single most productive year (n = 18 studies, 36% of the corpus). This concentration reflects the maturation of CBDC pilot programmes in major economies (China, European Union, Nigeria, Brazil), the entry into force of the EU's

Markets in Crypto-Assets (MiCA) regulation in December 2024 and growing scholarly attention to PIX as a model for fast payment systems internationally.

4.2 Geographic and Systemic Coverage

The reviewed literature is geographically concentrated but diverse in systemic focus. Europe (EU institutions and member states) accounts for the largest share of CBDC-focused studies (n = 12), reflecting the European Central Bank's digital euro research programme. Brazil features prominently as the primary PIX context (n = 7 studies), with three additional studies examining PIX as a comparative reference in broader payment system reviews. The United States (n = 6), China (n = 4), and multi-jurisdictional comparative studies (n = 9) complete the geographic profile.

By system focus: blockchain-focused studies represent the plurality (n = 21, 42%), followed by CBDC-centred studies (n = 20, 40%), with the remaining nine studies (18%) addressing fast payment systems including PIX, or conducting cross-system comparisons. Mixed-system studies tend to be the most methodologically sophisticated, integrating governance framework analysis with cryptographic evaluation.

4.3 Study Type Distribution

Methodological approaches within the corpus are predominantly technical or legal-analytical. Technical and empirical studies, including cryptographic protocol analyses, threat modelling, proof-of-concept implementations, and simulation studies, constitute 32 of the 50 included papers (64%). Governance and legal analyses, including regulatory framework reviews, comparative legal analyses, and policy evaluations, account for the remaining 18 studies (36%). Purely quantitative empirical studies with real-world transaction data are notably scarce (n = 4), constituting a critical gap the proposed indicator set (Section 6) is designed to address.

5. Thematic Synthesis

The 50 included studies converge on five major governance themes: (T1) governance frameworks balancing privacy and regulatory compliance; (T2) integration of privacy-enhancing technologies; (T3) blockchain and consensus mechanisms for security and transparency; (T4) privacy and security challenges specific to CBDCs; and (T5) emerging cryptographic techniques and post-quantum security. The following subsections synthesise evidence within each theme, identifying points of convergence, divergence, and unresolved tension.

5.1 Governance Frameworks Balancing Privacy and Regulatory Compliance (27/50 Studies)

The dominant theme in the literature concerns the design of governance frameworks that satisfy AML/CFT requirements while preserving user privacy, a tension consistently identified as the central challenge in digital payment governance (Kaur, 2024; Sillaber & Eggen, 2024; Kiayias et al., 2022). Three governance design philosophies emerge from the evidence.

Regulation-by-design approaches embed legal requirements directly into technological architectures, arguing that ex ante compliance integration is both more effective and more privacy-preserving than post-hoc enforcement (Pocher & Veneris, 2021; Napieralska & Kępczyński, 2024). The PEReDi CBDC design (Kiayias et al., 2022) operationalises this through distributed cryptographic protocols that enable selective disclosure to authorised regulators without compromising user anonymity for ordinary transactions. This approach achieves the strongest theoretical privacy-compliance balance but remains at proof-of-concept stage with limited empirical validation.

Hybrid governance models, exemplified by HybCBDC (Lamberty et al., 2024) and the Ethereum-based consortium design of Tunzina et al. (2024), combine centralised regulatory oversight with decentralised transaction recording. These models sacrifice some decentralisation benefits for regulatory tractability and represent the emerging practical consensus among central bank researchers. Fifteen of the 50 reviewed studies advocate hybrid models explicitly, making this the single most supported governance position in the corpus.

Selective de-anonymisation models (Sahu et al., 2023; Jia et al., 2023) distribute the power to reveal user identities across multiple regulatory actors, using threshold cryptography and zero-knowledge proofs to prevent unilateral surveillance while enabling lawful disclosure. These models address the political economy of privacy governance but introduce significant operational complexity and have not been tested at production scale.

5.2 Privacy-Enhancing Technology Integration

A substantial portion of the literature documents the integration of PETs into payment governance frameworks. Zero-knowledge proofs (ZKPs) are the most widely adopted cryptographic primitive, appearing in 18 of the 50 studies. Their application ranges from transaction validity proofs (Islam & In, 2024) to regulatory compliance demonstrations without data disclosure (Popov et al., 2024) to identity verification (Garcia & Ueyama, 2024). The zk-LTARK scheme (Islam & In, 2024) represents the state of the art, providing 128-bit security with lower proof sizes and faster verification than prior constructions, though its computational overhead remains a barrier to deployment at PIX-scale transaction volumes.

Homomorphic encryption appears in 10 studies, primarily in CBDC contexts where it enables computation on encrypted transaction data for regulatory reporting without decryption. Khalid et al. (2023) combine homomorphic encryption with secure multi-party computation for dynamic consent management, achieving GDPR compliance without centralised data collection. The practical limitation is computational cost: fully homomorphic encryption remains three to four orders of magnitude slower than plaintext computation, restricting its application to low-frequency batch operations rather than real-time payment processing.

Ring signatures and proxy re-encryption appear in six and four studies respectively, primarily in blockchain-payment contexts. Xue et al. (2025) combine ring signatures with Merkle tree structures and verifiable timestamps to achieve traceable anonymity, enabling regulatory disclosure while protecting transaction unlinkability, but note that timestamp privacy remains an unresolved vulnerability. This finding directly informs DPGF Proposition P5: PET adoption creates latency penalties that scale non-linearly with privacy guarantees.

A consistent limitation across PET studies is the gap between theoretical construction and real-world deployment. Of the 18 ZKP studies reviewed, 14 present proofs-of-concept or simulations; only four evaluate performance under realistic transaction loads. This empirical gap is the primary obstacle to confident policy recommendations on PET adoption.

5.3 Blockchain and Consensus Mechanisms

Blockchain-focused studies address two distinct governance problems: the security of the underlying consensus mechanism, and the governance of smart contracts that implement payment logic. On consensus, the reviewed literature evaluates three principal mechanisms. Proof-of-Authority (PoA), used in consortium blockchain CBDC designs (Islam & In, 2024), provides high throughput and energy efficiency but requires trust in the authority set, a centralisation that conflicts with the stated decentralisation rationale of many CBDC proposals. Proof-of-Stake (PoS), adopted in Mandal and Shill's (2024) NFC payment integration, achieves better decentralisation but introduces long-range attack vulnerabilities in permissionless settings. Byzantine Fault Tolerance (BFT) variants (Kiayias et al., 2022; Zhao, 2024) provide formal resilience guarantees against malicious actors but have known scalability limitations at network sizes exceeding a few hundred validators.

Cross-chain interoperability emerges as a critical security vulnerability in 2024 literature. Augusto et al. (2024) identify billions of dollars lost to exploits in cross-chain bridge protocols, attributing the losses to inadequate key management, absent formal verification, and governance gaps in upgrade procedures. This finding has direct implications for CBDCs seeking interoperability with existing blockchain payment networks, the governance of the bridge interface may be more consequential than the governance of either connected system.

5.4 Privacy and Security Challenges Specific to CBDCs

CBDC-specific literature converges on a set of challenges that distinguish CBDCs from both traditional payment systems and existing cryptocurrencies. Mass surveillance risk is the most frequently cited concern: unlike commercial bank payment data, CBDC transaction data would be directly accessible to central banks, creating comprehensive financial surveillance capabilities without the intermediary layer that currently limits regulatory data access (Chan, 2023; Uhlig et al., 2023). Several authors invoke Foucauldian panopticon imagery to describe the potential chilling effects on financial behaviour.

The offline payment problem, enabling CBDC transactions without network connectivity while maintaining security and preventing double-spending, remains technically unsolved at scale. Sillaber and Eggen (2024) evaluate seven proposed offline CBDC mechanisms and find that all require either a trust anchor (degrading to a form of centralisation) or a synchronisation mechanism (limiting the duration of offline capability). This is a design constraint with governance implications: systems requiring synchronisation create audit windows that reduce privacy.

Hans et al. (2023) apply the STRIDE threat modelling framework to blockchain-based CBDC designs and identify 39 distinct threat vectors, spanning spoofing, tampering, repudiation, information disclosure, denial of service, and privilege escalation. Their taxonomy provides the most systematic security threat coverage in the corpus and serves as a foundation for the proposed indicator set in Section 6.

5.5 Emerging Cryptographic Techniques and Post-Quantum Security

A smaller but strategically important subset of studies addresses the long-term security of payment infrastructure against quantum computing threats. Li et al. (2023) propose a post-quantum blockchain payment framework using hash-based one-time addresses and lattice-based signatures, achieving theoretical resistance to Grover's and Shor's algorithms at the cost of larger transaction sizes and slower verification. Bahar (2025) extends this to a full CBDC design, the Quantum-Resilient Privacy Ledger (QRPL), though the work remains entirely conceptual, with no implementation or performance data.

The post-quantum transition timeline is contested but policy-relevant: the National Institute of Standards and Technology (NIST) finalised its first post-quantum cryptographic standards in 2024, creating implementation obligations for financial infrastructure operators. The reviewed literature suggests that PIX and most current CBDC designs rely on elliptic curve cryptography (ECC) that would be compromised by a sufficiently powerful quantum computer, a threat with a commonly cited horizon of 10–20 years. The governance implication is that payment system architects must begin planning for cryptographic agility now, even if quantum threats are not yet operationally active.

6. Comparative Governance Analysis: PIX, Blockchain, and CBDCs

This section applies the DPGF to the three system types across 20 governance domains, drawing on the thematic synthesis in Section 5 and the extraction data from all 50 included studies. The analysis operationalises the DPGF positioning summarised in Table 2 and Fig. 1, providing the evidentiary foundation for the Propositions P1–P5.

6.1 Full Comparative Table, Governance Domains

Table 3
Comparative Governance Analysis Across 20 Domains

Governance Domain	PIX (Brazil)	Blockchain (Public/Permissioned)	CBDCs (Retail/Wholesale)
Regulatory Authority / Operator	BCB regulates; PSPs operate. Unified enforcement.	No single operator; VASPs/PSPs at protocol boundaries. Consortium model in permissioned.	Central bank (direct or two-tier). Strong institutional authority.
Primary Legal Basis	BCB regulations + Brazilian financial law. Mandatory for PSPs.	Fragmented national laws; VA guidance; consortium rules (permissioned).	Monetary law + CBDC-specific framework; high legislative specificity.
Governance Model	Centralised, unified rules, regulatory enforcement.	Public: open/protocol. Permissioned: consortium. Off-chain enforcement.	Centralised in CB; may delegate to intermediaries.
AML / KYC	Mandatory via PSPs at onboarding, monitoring, reporting.	Absent at protocol level (public); mandated in permissioned by consortium rules.	Mandatory, standardised; risk-based tiering; real-time monitoring.
Identity & Onboarding	Identity verified by PSPs; public key directories.	Custodial wallets (KYC by provider) or self-custody (pseudonymous). DIDs in permissioned.	Anchored to national registries; tiered wallet verification.
Data Protection (LGPD/GDPR)	PSPs under LGPD; data minimisation and purpose limitation.	On-chain public data requires off-chain handling; providers are subject to LGPD/GDPR.	Privacy-by-design mandated; BC sets legal safeguards.
Transparency & Auditability	Audit logs held by PSPs/BCB; regulatory audit.	Public: high on-chain auditability. Permissioned: member/third-party audit.	High auditability for monetary policy; centralised or shared ledger.
Privacy-by-Design	Minimisation policies; access control at PSP level.	ZKPs, rotating addresses, private channels; sensitive data off-chain.	Normative selective anonymity; conditional privacy per public policy.
Access Control	Via licensed PSPs; strong authentication; operational limits.	Public: open protocol access. Permissioned: role-based permissioning.	CB-defined policy; authorised wallets/APIs.
Custody & Key Management	PSP-managed custody (custodial).	Self-custody or third-party; HSM and MPC	Licensed intermediary custody; HSM and

Governance Domain	PIX (Brazil)	Blockchain (Public/Permissioned)	CBDCs (Retail/Wholesale)
		in professional operators.	segregation requirements.
Incident Response	Standardised detection/communication/remediation under BCB.	Public: community and providers. Permissioned: consortium procedures.	CB and participant runbooks; continuity requirements.
Fraud Prevention	Risk models, real-time transaction monitoring via PSPs.	Analytics at VASPs/PSPs; on-chain flagging; risk heuristics.	Centralised real-time analysis; intermediary cooperation.
Reversibility / Contestation	Formal dispute/reversal via PSPs and arrangement rules.	Public: generally irreversible; off-chain forensics. Permissioned: configurable.	Policy-conditioned reversal; CB holds blocking and chargeback authority.
Compliance & Reporting	Periodic/ad hoc reports to BCB; audits and certifications.	VASPs/PSPs; contractual reporting in permissioned.	Standardised CB reporting; risk, usage and stability metrics.
Interoperability & Standards	Standardised APIs; open finance integration; messaging standards.	Public: open standards. Permissioned: consortium standards; bridge due diligence.	ISO 20022 and legacy system integration; international standards.
Smart Contract Governance	Limited (dynamic QR code via PSPs); contracts outside core.	Critical: audits, formal verification, bug bounties, upgrade management.	Controlled and audited; contracts under CB policy and formal testing.
Sanctions & Block Lists	National/international lists via PSPs.	VASPs/PSPs at endpoints. Native enforcement in permissioned.	Centralised enforcement; blocking, listing and access policies.
Transaction Limits & Safeguards	Per-profile/schedule/value limits set by BCB and PSPs.	No native limits in public protocol; providers impose risk limits.	Tiered wallet limits; systemic risk policies.
Offline Operation & Continuity	Continuity via PSPs and redundant infrastructure; no native offline.	Some networks support channels/rollups; true offline rare.	Some CBDC designs provide offline payments with limits and later sync.
Financial Inclusion & Accessibility	Wide access via simplified accounts, standardised UX, low cost.	Direct access without banks (self-custody) but technical barriers; custodial solutions broaden access.	CB inclusion policies: tiering, simplified wallets, exemptions.

Systematic comparison of PIX, blockchain (public/permissioned), and CBDCs (retail/wholesale) across 20 governance domains. Evidence derived from 50 included studies and protocol extraction template (19 fields).

6.2 Axis 1, Locus of Control: Who Governs?

PIX represents the most unambiguous case of centralised governance (LoC-1) in the corpus. The BCB exercises rulemaking, enforcement, and sanctioning authority; PSPs are operational delegates operating under mandatory compliance regimes, with no meaningful discretion over system rules. This architecture delivers measurable governance benefits: regulatory response time is low (BCB can issue binding normative within days), PSP compliance rates are high (BCB reporting indicates near-universal participation), and incident response is coordinated. The governance cost is concentration risk: systemic failures, regulatory capture, or infrastructure compromise at the BCB would simultaneously affect all over 3 billion monthly transactions processed in 2024 (BCB, 2024).

Public blockchains occupy the opposite pole (LoC-5). Protocol changes require broad community consensus through improvement proposal processes (BIPs for Bitcoin, EIPs for Ethereum), which can take years and may be contentious. This resilience to unilateral governance decisions is the primary claimed advantage of decentralised systems, and it is genuine: no single actor can compel compliance or alter the system's rules. The governance cost is enforcement incapacity: AML/KYC requirements can only be applied at the VASP/PSP boundary, creating a structural arbitrage that is exploited by cross-chain bridge attacks (Augusto et al., 2024). Regulatory response to emerging threats (e.g., sanctioned-address screening) requires international VASP coordination rather than protocol change.

CBDCs and permissioned blockchains occupy intermediate LoC positions (LoC-2 to LoC-3). The central bank retains monetary authority and rulemaking power, but implementation is distributed across intermediary institutions. The HybCBDC architecture (Lamberty et al., 2024) exemplifies LoC-2: the central bank sets all parameters, but transaction recording occurs on a distributed ledger operated by licensed intermediaries, reducing single points of infrastructure failure while preserving regulatory control. This is the governance design with the strongest empirical support in the reviewed literature.

6.3 Axis 2, Privacy Spectrum: What Can Be Seen?

PIX's PS-4 positioning reflects a deliberate regulatory design choice rather than a technical constraint. The BCB has access to all PIX transaction data through PSP reporting obligations; this surveillance capability is framed as a financial crime prevention tool and has contributed to a documented reduction in money laundering via traditional payment channels (BCB, 2023). Users exercise privacy through LGPD protections governing PSP data handling, but not through the payment protocol itself. The absence of any cryptographic privacy mechanism in PIX is a functional governance decision: the system is optimised for transparency and auditability at the expense of user financial privacy.

Public blockchain pseudonymity (PS-2 to PS-3) is widely misunderstood as stronger than it is in practice. Address pseudonymity provides meaningful privacy only so long as addresses are not linked to identities through on- or off-ramp KYC, transaction graph analysis, or timing correlations. Tabet and Kayssi (2024) demonstrate that even sophisticated mixing services reduce, but do not eliminate, linkability, and Xue et al. (2025) show that timestamp metadata leakage enables re-identification in a substantial proportion of

attempted anonymous transactions. The practical privacy level of public blockchain payments used through standard wallets is therefore closer to PS-3 than to PS-1.

CBDCs offer the most architecturally sophisticated privacy design space. Tiered anonymity, where small transactions are treated as effectively anonymous (PS-1 to PS-2), medium transactions as pseudonymous (PS-3), and large transactions as fully transparent (PS-5), can be implemented through ZKPs and Pedersen commitments (Chan, 2023; Kiayias et al., 2022). This approach mirrors the cash-versus-bank-transfer distinction in traditional finance and represents the strongest alignment with the contextual integrity principle (Tronnier et al., 2023). However, the metadata privacy problem identified in Section 5.2 also applies to CBDC designs: even a transaction whose amount is cryptographically hidden may be linkable through timing and frequency patterns.

6.4 Axis 3, Compliance Architecture: How Is Regulation Embedded?

PIX's regulation-by-design architecture (CA-1) means that regulatory obligations are structurally inseparable from system participation. PSPs cannot process PIX transactions without implementing real-time transaction monitoring, suspicious activity reporting, and mandatory KYC onboarding. This structural embedding eliminates compliance arbitrage within the PIX ecosystem and enables near-real-time regulatory enforcement, the BCB can freeze PIX keys associated with illicit activity within minutes through PSP coordination. The governance cost is inflexibility: every regulatory update requires coordinated implementation across all 800 + PSPs, leading to implementation lag and heterogeneous compliance timelines.

Public blockchain's post-hoc compliance architecture (CA-5) creates the structural vulnerabilities documented in Section 5.1. The compliance-agnostic protocol layer means that any actor who can access the blockchain without transiting a regulated interface, through direct node operation or privacy-enhancing overlays, can transact outside the compliance perimeter. Privacy pool architectures (Popov et al., 2024) represent the most promising approach to introducing voluntary compliance signalling at the protocol level, enabling users to demonstrate that their funds did not pass through sanctioned addresses without revealing their full transaction history. Widespread adoption of this approach would effectively move compliance architecture from CA-5 toward CA-3 to CA-4 without requiring protocol changes.

CBDC smart contract enforcement (CA-2) is the most technically promising compliance architecture in the corpus. Holding limits, transaction thresholds, sanctions screening, and AML triggers encoded in the protocol layer can enforce compliance without requiring PSP reporting intermediaries for every transaction. Tunzina et al. (2024) demonstrate this in an Ethereum-based CBDC pilot, achieving real-time compliance enforcement at 10,000 transactions per second. The governance risk is smart contract vulnerability: a bug in a compliance-enforcement contract could either block legitimate transactions or fail to flag illicit ones, and the formal verification requirements for production-grade smart contracts remain expensive and time-consuming.

6.5 Proposed Measurable Indicators for Cross-System Comparison

A persistent limitation in the reviewed literature is the absence of standardised, cross-system indicators enabling empirical comparison of governance effectiveness across PIX, blockchain, and CBDC architectures. Table 5 proposes a 13-indicator set that operationalises the DPGF Propositions P1–P5 and is grounded in the governance domain analysis in Table 3.

Table 5
Proposed Cross-System Governance Effectiveness Indicators

Dimension	Indicator	Operationalisation	Applicable System
Security	**Fraud rate per million transactions**	N fraudulent TX / total TX × 1,000,000 per channel and period	PIX, Blockchain, CBDC
Security	**Mean Time to Recover (MTTR)**	Average hours to detect, contain and recover from critical incidents	All systems
Security	**Code audit coverage (%)**	Proportion of critical components externally audited per year	Blockchain, CBDC
Privacy	**Data breach incidents**	Number of breaches per year per 1M users; severity measured in records affected	All systems
Privacy	**DPIA compliance (%)**	Percentage of services with up-to-date Data Protection Impact Assessment and implemented mitigations	All systems
Privacy	**Linkability index**	Estimated probability of user re-identification from transactional metadata (timing, amount, address)	Blockchain, CBDC
Governance	**Regulatory response time**	Days between risk identification and normative update or regulatory guidance	PIX, CBDC
Governance	**PSP/operator compliance (%)**	Participants demonstrating full compliance with applicable requirements per audit cycle	PIX, CBDC
Governance	**Reporting quality score**	Composite score of completeness, timeliness and consistency of required regulatory reports	All systems
Operational	**System availability**	Uptime percentage and number of critical outages per year	All systems
Operational	**Dispute resolution time**	Average calendar days to resolve user-initiated payment disputes	PIX, CBDC
Adoption/Trust	**Complaint rate per 100k TX**	Registered user complaints per 100,000 transactions by channel	All systems
Adoption/Trust	**User trust, Net Promoter Score**	Periodic standardised surveys with end users and merchants	All systems

Proposed measurable indicators for empirical validation of DPGF Propositions P1–P5. Indicators are designed for cross-system comparability and can be operationalised using regulatory reporting data, transaction logs, and periodic user surveys.

7. Discussion

7.1 Theoretical Implications

The DPGF makes three theoretical contributions to the digital payment governance literature. First, it establishes that the governance space of digital payment systems is three-dimensional, not one-dimensional. Prior frameworks tend to arrange systems on a single centralisation-decentralisation axis (Cong et al., 2024) or a single privacy-transparency axis (Uhlig et al., 2023). The DPGF demonstrates that control, privacy, and compliance architecture are independently variable, a finding with direct implications for system design, since optimising on one axis does not constrain the others in the way that simpler frameworks imply.

Second, the DPGF resolves a persistent terminological confusion in the literature between governance decentralisation and compliance architecture. Several studies conflate decentralised governance (LoC-5) with post-hoc compliance (CA-5), as if decentralised systems were inherently incapable of regulation-by-design. The privacy pool architectures (Popov et al., 2024) and distributed CBDC designs (Kiayias et al., 2022) demonstrate that high-LoC systems can achieve CA-1 to CA-2 through cryptographic compliance embedding, a design space the existing literature inadequately maps.

Third, the DPGF positions PIX as a theoretically important governance anchor, not merely as a regional payment system but as the clearest real-world example of the Regulatory Clarity Model (LoC-1 · PS-4 · CA-1) at national scale. This positioning enables researchers to test Proposition P4 (Hybrid Governance Advantage) by comparing PIX's governance outcomes on the proposed indicators against CBDC and blockchain payment pilots as they mature.

7.2 Practical Implications

For central bank policymakers designing CBDCs, the review's primary practical implication is that tiered anonymity, implementing PS-1 to PS-2 for small transactions and PS-4 to PS-5 for large transactions, is both technically feasible and politically defensible, combining cash-like privacy for everyday purchases with regulatory transparency for high-value transfers. The technical foundation exists (ZKPs, Pedersen commitments, threshold cryptography), and the governance model has precedent in existing cash/bank-transfer distinctions. The critical missing element is a standardised, legally recognised threshold above which selective disclosure is triggered, a policy design question rather than a technical one.

For regulators governing blockchain payment systems, the structural post-hoc compliance problem (CA-5) is unlikely to be resolved through VASP regulation alone. The reviewed literature suggests two complementary strategies: cryptographic compliance signalling at protocol level (privacy pools, association sets), which moves compliance architecture from CA-5 toward CA-3 without protocol changes; and cross-chain governance standards for bridge protocols, which address the highest-risk attack surface identified by Augusto et al. (2024). Neither strategy requires banning pseudonymous transactions, a politically contentious and enforcement-impractical approach.

For payment system designers, the PET scalability constraint (Proposition P5) has concrete engineering implications. ZKP verification times at national payment scale, PIX processes over 100 million transactions per day, require either hardware acceleration (application-specific integrated circuits for ZKP verification),

batching protocols that amortise proof generation costs across many transactions, or a tiered architecture where ZKPs are applied selectively to high-value transactions rather than universally. These are known engineering approaches; the governance contribution of the present review is to specify the threshold conditions under which each approach becomes operationally necessary.

7.3 Limitations

Three limitations bound the generalisability of the present findings. First, the empirical base is thin: of the 50 included studies, only four evaluate governance mechanisms using real-world transaction data. The remaining 46 rely on theoretical constructions, proof-of-concept implementations, simulations, or analysis of regulatory documents. The proposed indicator set (Table 5) is designed precisely to generate the empirical base that currently does not exist, but its operationalisation requires data-access agreements with payment system operators that researchers do not currently have.

Second, the review's geographic coverage is uneven. CBDC literature is disproportionately European and Chinese; PIX literature is almost exclusively Brazilian; blockchain payment governance literature is globally distributed but concentrates on English-language publications. Major emerging-market implementations, India's UPI, Nigeria's eNaira, Kenya's M-Pesa ecosystem, are underrepresented, limiting the transferability of findings to these contexts.

Third, the DPGF's three axes are analytically orthogonal by construction, but empirically they may be correlated. Central banks that choose high centralisation (LoC-1) may systematically also choose high transparency (PS-4 to PS-5) for political reasons unrelated to the technical architecture, in which case P1 and P2 would be confounded in observational data. Experimental or quasi-experimental designs would be required to disentangle the axes' independent effects.

8. Conclusions and Future Research

This systematic review has synthesised 50 studies on digital payment governance across PIX, blockchain, and CBDC architectures and introduced the Digital Payment Governance Framework (DPGF) as a structured analytical instrument for comparing governance arrangements across systems that have, until now, been analysed in isolation.

The review's central finding is that no architecture optimally resolves the three-way tension between regulatory oversight, user privacy, and compliance efficiency. PIX demonstrates that the Regulatory Clarity Model achieves national-scale operationalisation of regulation-by-design compliance with high PSP compliance rates, at the cost of minimal default privacy. Public blockchains demonstrate that the Autonomy Model achieves censorship resistance and user autonomy, at the cost of structural compliance gaps at scale. CBDCs and permissioned blockchains demonstrate that the Hybrid Governance Model can theoretically achieve intermediate positions on all three axes, but that the gap between theoretical design and empirical validation remains the most significant limitation in the field.

The five DPGF Propositions (P1–P5) constitute a structured research agenda. Testing P1 requires comparative data on regulatory response time and PSP compliance rates across jurisdictions implementing different LoC scores. Testing P2 requires standardised user trust surveys across payment system types.

Testing P3 requires transaction-level compliance cost data from payment operators. Testing P4 requires a composite governance index aggregating the 13 proposed indicators. Testing P5 requires controlled performance benchmarks of ZKP and homomorphic encryption implementations at realistic transaction volumes.

The most urgent policy recommendation to emerge from this review is the development of a governance interoperability standard, a common framework enabling cross-system comparison of governance outcomes using the indicator set proposed in Table 5. Without such a standard, the field will continue to produce governance recommendations that are system-specific, empirically unvalidated, and non-comparable. The DPGF provides the conceptual foundation; the next step is institutional adoption by BIS, ECB, and BCB as a comparative evaluation tool for the second generation of digital payment governance design.

Declarations

Ethical approval

This article is a systematic review of previously published literature. It does not contain any studies with human participants or animals performed by any of the authors. Ethical approval was therefore not required.

Informed consent

This article does not contain any studies with human participants performed by any of the authors. Informed consent was therefore not applicable.

Competing interests

The authors declare no competing interests.

Author contributions and funding

Redacted for double-blind peer review. Full statements are provided in the cover letter.

Author Contribution

N.G.F.: Investigation, Methodology, Writing (original draft), Writing (review and editing). D.F.P.: Investigation, Methodology. J.V.F.: Supervision, Writing (review and editing). All authors read and approved the final manuscript.

Data availability

All datasets and materials underpinning this systematic review are provided as supplementary files with this submission and are available to the editors and referees: Supplementary Material S1 (completed PRISMA

2020 checklist); Supplementary Material S2 (data extraction form, the completed 19-field extraction dataset and the full list of the 50 included studies); Supplementary Material S3 (DPGF sub-score matrix, synthesis tables and sensitivity analysis); Supplementary Material S4 (full search strategies for all databases and sources consulted, with search dates and record counts); and Supplementary Material S5 (exported records, title/abstract and full-text screening logs with the inclusion and exclusion criteria applied, reasons for exclusion and the inter-rater agreement calculation). The PRISMA 2020 flow diagram is presented as Fig. 2. There are no restrictions on sharing these materials. Upon acceptance, the same files will be deposited in a public repository with a persistent identifier.

References

1. Augusto A, Belchior R, Correia M, Vasconcelos A, Zhang L, Hardjono T (2024) SoK: Security and privacy of blockchain interoperability [extended version]. TechRxiv. https://doi.org/10.36227/techrxiv.24595764.v2
2. Bahar SW (2025) Quantum-resilient privacy ledger (QRPL): A sovereign digital currency for the post-quantum era. arXiv preprint. http://arxiv.org/abs/2507.09067v2
3. BIS (Bank for International Settlements) (2024) CBDC tracker: Country overview. https://www.bis.org/cbdc
4. Banco Central do Brasil (2023) PIX: Relatório de gestão 2023. https://www.bcb.gov.br
5. Banco Central do Brasil (2024) PIX: Estatísticas mensais, outubro 2024. https://www.bcb.gov.br
6. Chan WMT (2023) A privacy-preserving central bank ledger for central bank digital currency. arXiv preprint. https://doi.org/10.48550/arxiv.2311.16105
7. Cong LW, Easley D, Prasad E (2024) Demystifying electronic payment systems and digital currencies. Oxf Res Encyclopedia Econ Finance. https://doi.org/10.1093/acrefore/9780190625979.013.826
8. Garcia RD, Ueyama J (2024) Blockchain-based data governance for privacy-preserving in multi-stakeholder settings. In Proceedings of SBRC 2024. https://doi.org/10.5753/sbrc_estendido.2024.1638
9. Hans J, Khan S, Svetinovic D (2023) Blockchain CBDC security threats using STRIDE. In Proceedings of BCCA 2023. https://doi.org/10.1109/bcca58897.2023.10338905
10. Islam MM, In HP (2024) An auditable, privacy-preserving, transparent unspent transaction output model for blockchain-based central bank digital currency. IEEE Open J Comput Soc 1–12. https://doi.org/10.1109/ojcs.2024.3486193
11. Jia W, Xie T, Wang B (2023) A privacy-preserving scheme with multi-level regulation compliance for blockchain. Res Square preprint. https://doi.org/10.21203/rs.3.rs-3274117/v1
12. Kaur G (2024) The privacy paradox of CBDCs. Advances in Finance, Accounting, and Economics Book Series. 194–207. https://doi.org/10.4018/979-8-3693-1882-9.ch012
13. Khalid MI, Ahmed M, Helfert M, Kim J (2023) Privacy-first paradigm for dynamic consent management systems. Electronics 12(24):4973. https://doi.org/10.3390/electronics12244973
14. Kiayias A, Kohlweiss M, Sarencheh A (2022) PEReDi: Privacy-enhanced, regulated and distributed central bank digital currencies. In Proceedings of ACM CCS 2022. https://doi.org/10.1145/3548606.3560707
15. Lamberty R, Kirste D, Kannengießer N, Sunyaev A (2024) HybCBDC: A design for central bank digital currency systems enabling digital cash. IEEE Access. https://doi.org/10.1109/access.2024.3458451

16. Lee Y, Son B, Park S, Lee J, Jang H (2021) A survey on security and privacy in blockchain-based central bank digital currencies. J Internet Serv Inform Secur 11(3):1–27. https://doi.org/10.22667/jisis.2021.08.31.016
17. Li L, Lu X, Wang K (2023) A post-quantum privacy-enhancing blockchain-based transaction framework with access control. In Proceedings of ICDSP 2023. https://doi.org/10.5121/csit.2023.130809
18. Mandal S, Shill PC (2024) Ensuring security and efficiency in digital payments using blockchain with NFC. In Proceedings of ICKECS 2024. https://doi.org/10.1109/ickecs61492.2024.10616703
19. Napieralska A, Kępczyński P (2024) Balancing transparency and privacy in central bank digital currencies. Advances in Finance, Accounting, and Economics Book Series. 208–223. https://doi.org/10.4018/979-8-3693-1882-9.ch013
20. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, Moher D (2021) The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 372:n71. https://doi.org/10.1136/bmj.n71
21. Pocher N, Veneris A (2021) Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme. IEEE Trans Netw Serv Manage 19(2):1776–1788. https://doi.org/10.1109/tnsm.2021.3136984
22. Popov V, Gross A, Krupin M, Koreli G (2024) Blockchain privacy and self-regulatory compliance: Methods and applications. Int J Cryptocurrency Res 4(1):64–78. https://doi.org/10.51483/ijccr.4.1.2024.64-78
23. Sahu N, Gajera M, Chaudhary A, Ivey-Law H (2023) SeDe: Balancing blockchain privacy and regulatory compliance by selective de-anonymisation. arXiv preprint. https://doi.org/10.48550/arxiv.2311.08167
24. Shapoval Y (2020) Central bank digital currencies: Experience of pilot projects and conclusions for the NBU. Economy and Forecasting, 2020(4), 103–121. https://doi.org/10.15407/ECONFORECAST2020.04.097
25. Sillaber C, Eggen M (2024) Privacy in payments: What a CBDC can do better than commercial bank money. Z für Bankrecht und Bankwirtschaft 36(4):267–276. https://doi.org/10.15375/zbb-2024-0407
26. Tabet S, Kayssi A (2024) A privacy-preserving method for Ethereum transactions. In Proceedings of 3ICT 2024. https://doi.org/10.1109/3ict64318.2024.10824304
27. Tronnier F, Biker P, Löbner S (2023) An evaluation of information flows in digital euro transactions using contextual integrity theory. In Proceedings of PrivaCI 2023. https://doi.org/10.1145/3590777.3590779
28. Tunzina T, Chayon MAK, Jitu PG, Ankon MU, Joy SN, Shaha RK, Islam MM, Hussain M, Hassan MM, Pham PH (2024) Blockchain-based central bank digital currency: Empowering centralised oversight with decentralised transactions. IEEE Access. https://doi.org/10.1109/access.2024.3517147
29. Uhlig H, Alonso M, Frost J (2023) Privacy in digital payments, Escaping the panopticon. Georget J Int Affairs 24:174–180. https://doi.org/10.1353/gia.2023.a913643
30. Xue L, Huang H, Xiao F, Li Q, Wang Z (2025) A privacy-enhanced traceable anonymous transaction scheme for blockchain. IEEE Trans Inf Forensics Secur. https://doi.org/10.1109/tifs.2025.3526049
31. Zhang ZW (2024) CBDC security. Future of Business and Finance, 73–92. https://doi.org/10.1007/978-3-031-58002-4_5
32. Zhao J (2024) Blockchain-enabled privacy-preserving federated learning algorithms in edge computing. In Proceedings of CCSB 2024. https://doi.org/10.1109/ccsb63463.2024.10735574

33. Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. J Econ Lit 54(2):442–492. https://doi.org/10.1257/jel.54.2.442
34. Baldwin R, Cave M, Lodge M (2012) Understanding regulation: Theory, strategy, and practice, 2nd edn. Oxford University Press
35. Landis JR, Koch GG (1977) The measurement of observer agreement for categorical data. Biometrics 33(1):159–174. https://doi.org/10.2307/2529310
36. Nissenbaum H (2004) Privacy as contextual integrity. Wash Law Rev 79(1):119–158
37. Ostrom E (1990) Governing the commons: The evolution of institutions for collective action. Cambridge University Press. https://doi.org/10.1017/CBO9780511807763
38. Schär F (2021) Decentralized finance: On blockchain- and smart contract-based financial markets. Fed Reserve Bank St Louis Rev 103(2):153–174. https://doi.org/10.20955/r.103.153-74
39. Tirole J (2015) Market failures and public policy. Am Econ Rev 105(6):1665–1682. https://doi.org/10.1257/aer.15000024
40. Zetzsche DA, Annunziata F, Arner DW, Buckley RP (2020) The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. Capital Markets Law J 16(2):203–225. https://doi.org/10.1093/cmlj/kmab005

Figures

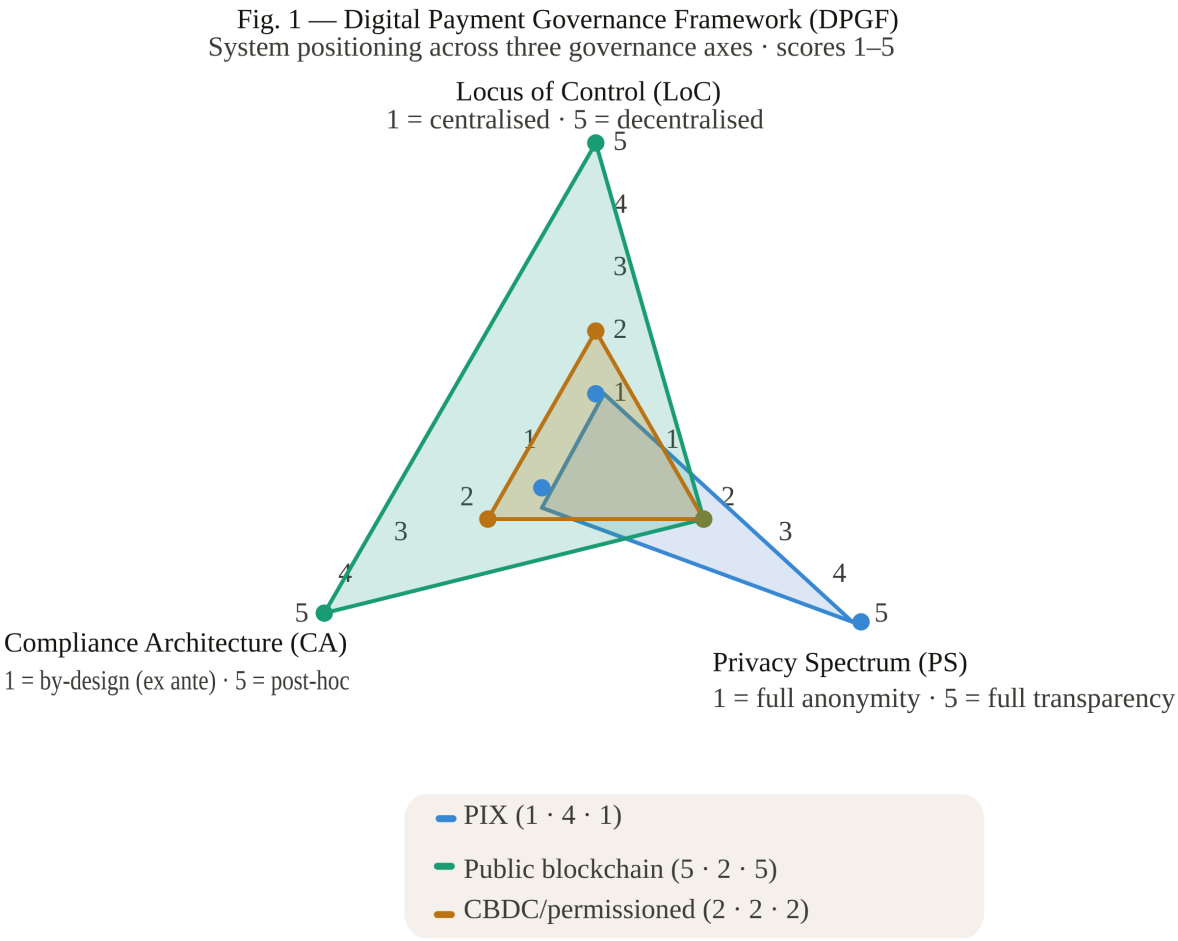


Figure 1

Digital Payment Governance Framework (DPGF), three-system positioning. Scores on each axis (1–5) reflect the comparative governance analysis of 20 domains. PIX = Regulatory Clarity Model (1·4·1); Public Blockchain = Autonomy Model (5·2·5); CBDC/Permissioned = Hybrid Governance Model (2·2·2). LoC = Locus of Control; PS = Privacy Spectrum; CA = Compliance Architecture.

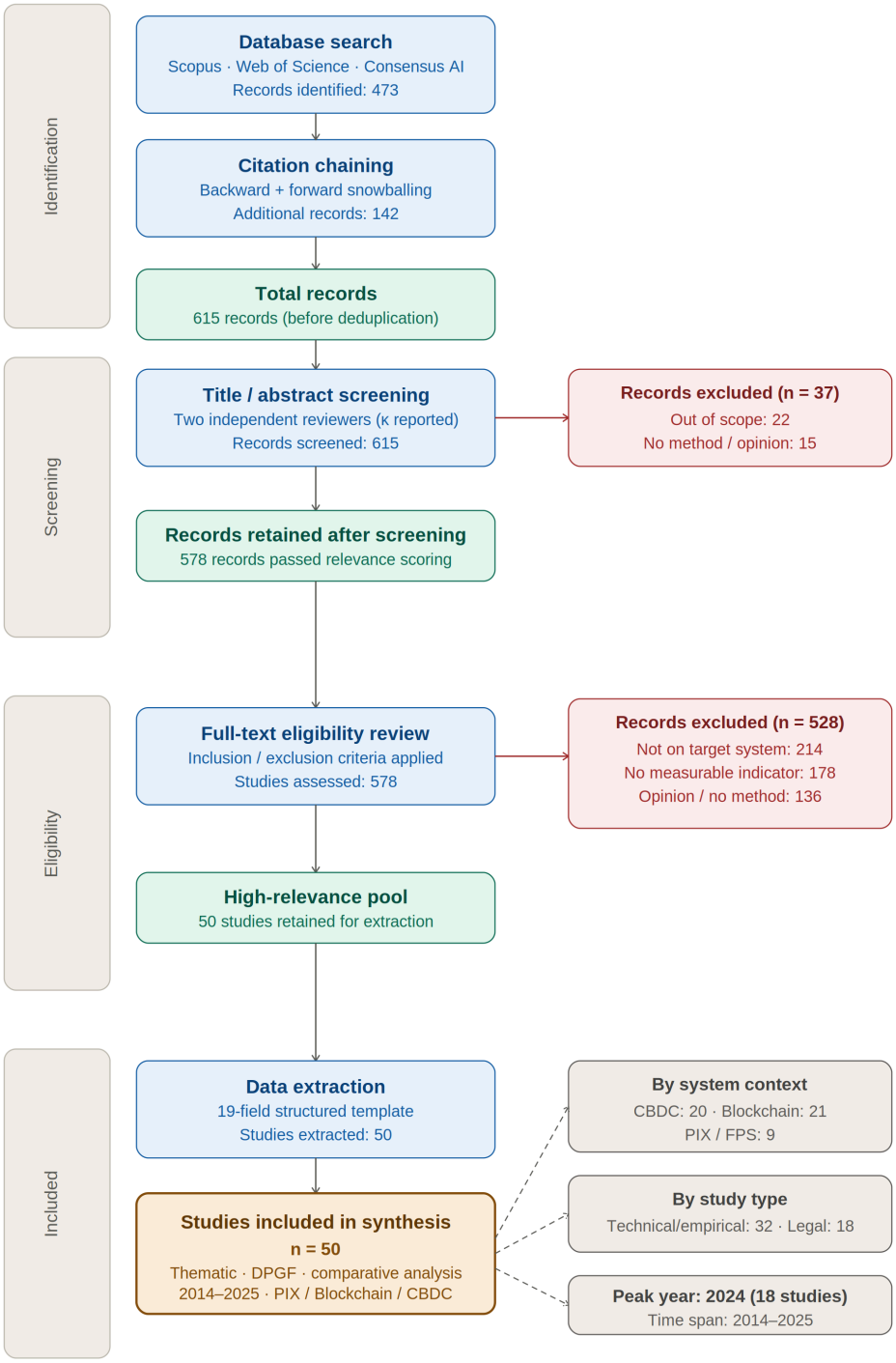


Fig. 2 — PRISMA 2020 flow diagram · systematic review selection process

Security and Privacy in Digital Payments: Blockchain, PIX, and CBDCs

Figure 2

PRISMA 2020 flow diagram. Records identified via Scopus, Web of Science, and Consensus AI (n = 473) supplemented by citation chaining (n = 142); total pool n = 615. Final included studies: n = 50. FPS = fast payment systems; CBDC = central bank digital currency.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- QuadroGovernancaPagamentos.xlsx
- HSSCInternalcheckerPRISMAkappaen.xlsx
- HSSCS1PRISMA2020checklist.docx