EXAMINING PRIVACY TENSIONS IN RETAIL CENTRAL BANK DIGITAL CURRENCIES

Completed Research Paper

Martin Brennecke, University of Luxembourg, Luxembourg, martin.brennecke@uni.lu

Nadia Pocher, University of Luxembourg, Luxembourg, nadia.pocher@uni.lu

Muriel-Larissa Frank, University of Luxembourg, Luxembourg, muriel.frank@uni.lu

Abstract

Most central banks have moved from the exploration of retail central bank digital currencies (CBDCs) towards preparation and pilot initiatives. In designing retail CBDC systems, a major trade-off requires balancing the end-user preference for privacy with the protection of financial integrity. While end-user privacy and associated trade-offs are frequently discussed, related publications often focus on either technical (design-oriented) or social (adoption-oriented) aspects. As a result, the role of technologies in mitigating end-user privacy tensions emerging in these systems remains underexplored. Therefore, we first draw on socio-technical systems theory and a content analysis to identify and discuss end-user privacy tensions in retail CBDC systems. Second, we examine the role of technologies in mitigating such tensions. By shedding light on the socio-technical nature of these tensions and potential solutions in retail CBDC systems, our work supports central banks and policymakers but also provides a frame of reference for information systems researchers.

Keywords: Central bank digital currency, CBDC, Privacy, Socio-technical systems, Privacy-enhancing technologies.

1 Introduction

The majority of central banks are exploring the issuance of digital forms of sovereign money, known as central bank digital currencies (CBDCs) (Atlantic Council, 2025). As the maturity of these projects increases, academic research investigates not only various design choices (Genc & Takagi, 2024; Jabbar et al., 2023), but also how CBDCs are emerging financial services at the intersection of technology and real economy value processes (Alt et al., 2024). While some CBDC initiatives aim to improve interactions between financial institutions through wholesale systems (Allen et al., 2020; BIS, 2020), other initiatives focus on the retail side and the daily payments of citizens and businesses, with the idea of replicating the experience of physical cash (BIS-CGIDE, 2023). In this paper, we focus on retail CBDCs, where strong end-user privacy is essential to achieve broad acceptance by the general public (Baronchelli et al., 2022; Choi et al., 2023). Although the "cash-like" privacy feature ranks as a priority for potential end users (ECB, 2021; Tronnier et al., 2022), the prospect of a fully anonymous system of digital cash calls for regulatory safeguards in the area of anti-money laundering and counter-terrorist financing (AML/CFT) (BIS-IH, 2023a; IMF, 2023). This results in trade-offs that can be addressed through various technologies and tiered designs (EDPB & EDPS, 2023; Michalopoulos et al., 2025).

An examination of the current literature on privacy in retail CBDCs reveals that scholars primarily study either the technical (e.g., Brunnermeier & Landau, 2022; Gross et al., 2021; Wüst et al., 2022) or the social components (e.g., Choi et al., 2023; Jabbar et al., 2023; Tronnier et al., 2022), with little attention

given to the interplay between the two. Consequently, emerging privacy tensions are usually explored in isolation, leaving us unaware of their relationship with one another and the role of privacy-enhancing technologies (PETs) in mitigating them (see for example ECB, 2025; Lee et al., 2021). Failing to integrate a socio-technical perspective hampers the contribution of information systems (IS) research from its unique standpoint (Sarker et al., 2019), and leads to system inefficiencies (Bostrom et al., 2009). In particular, it may lead to overlook individual end-user privacy tensions and the role of technology in addressing them. Thus, we formulate the following research question: *Which tensions arise in retail CBDC systems with regard to end-user privacy and which technologies can mitigate them?*

At the core of our study lies the socio-technical systems (STS) theory (Bostrom & Heinen, 1977; Sarker et al., 2019). The socio-technical perspective is one of the foundational viewpoints of the IS discipline (Beath et al., 2013; Sarker et al., 2019), and enables the examination of end-user privacy tensions within retail CBDC systems, composed of organizations, institutions, end users, as well as technical components. To answer the first part of our research question, we qualitatively analyze publications by G20 central banks and the Bank for International Settlements (BIS). By means of deductive and inductive coding, we identify the bilateral tensions that emerge between stakeholders and components of socio-technical retail CBDC systems regarding end-user privacy. This highlights different stakeholder priorities and contributes to research on privacy design choices in retail CBDCs. To answer the second part of our research question, we conduct a structured literature review and qualitative analysis of both academic and grey literature. Using inductive coding, we identify technologies that are discussed to afford privacy in retail CBDC systems, and we analyze their impact on the mitigation of the previously identified bilateral tensions. By doing so, we showcase how the IS discipline is uniquely positioned to contribute to the informed design, development, and operation of retail CBDCs, including supporting stakeholders in better understanding their role in safeguarding end-user privacy.

In the remainder of this paper, we first present the theoretical underpinnings of our study, particularly the origins and discourses surrounding STS and retail CBDCs. We then provide an overview of the methodology we used to answer the two parts of our research question. Next, we elaborate on the implications of a socio-technical perspective for end-user privacy in retail CBDCs and identify the corresponding bilateral tensions. Then, we examine the emerging role of various technologies in mitigating such tensions and elaborate on related implementation challenges. Finally, we present contributions and limitations before concluding.

2 Background

2.1 Retail Central Bank Digital Currencies

Central bank money is a liability of a central bank, and typically comes in one of two forms: (a) fiat money or sovereign currency, what we typically refer to as physical cash, and (b) bank reserves or digital deposits, provided to authorized institutions (BIS, 2020). Following this distinction, a core classification of CBDCs distinguishes between retail and wholesale systems (Bindseil et al., 2021). In this paper, we focus on retail CBDCs, which intend to deliver digital fiat money to the public and thus raise the most concerns regarding end-user privacy (Baronchelli et al., 2022; Rennie & Steele, 2021). The most commonly foreseen architecture of a retail CBDC system is two-tier, where central banks issue the digital form of cash and intermediaries such as commercial banks facilitate access to it also in terms of distribution (Allen et al., 2020). Two-tier systems can vary when it comes to private sector involvement (BIS-CGIDE, 2023), and allow central banks to rely on established mechanisms of cooperation with financial institutions for tasks such as customer onboarding (Auer & Böhme, 2021; Carstens, 2021). Yet, unlike the digital forms of money that are traditionally handled by these institutions (e.g., commercial bank money and e-money), a retail CBDC is a liability of the central bank (ECB, 2025).

As of 2025, countries and monetary unions representing 98% of global gross domestic product (GDP) have explored or are exploring some type of CBDC (Atlantic Council, 2025). Among these, three retail CBDC systems have been launched – i.e., JAM-DEX in Jamaica, Sand Dollar in The Bahamas, and e-Naira in Nigeria. Meanwhile, 38 retail CBDC initiatives are in the pilot phase, including the European

Union (EU) investigation into a digital euro (ECB, 2023), coupled by the digital euro legislative package (European Commission, 2023), and the digital yuan (e-CNY) in China (Atlantic Council, 2025). Among G20 members, countries or monetary unions representing 50.06% of global GDP at purchasing power parity (PPP) are involved in retail CBDC projects that have reached the pilot stage.

Drivers for central banks to investigate retail CBDCs are diverse and evolved over time. They include safeguarding financial stability and the role of central banks amid a general decline in cash use in favor of digital means of payment (ECB, 2025). For smaller jurisdictions, it is a way of mitigating the risk of currency substitution (BIS, 2021). On a broader level, retail CBDC projects also aim to foster payment efficiency and financial inclusion (BIS-CGIDE, 2023). Among the key characteristics of these systems, end-user privacy, accessibility, security and resilience have emerged as top priorities (BIS-CGIDE, 2023; ECB, 2023). Yet, retail CBDCs should not become a tool to elude AML/CFT safeguards, such as limits to the use of cash, evade financial sanctions, or facilitate tax evasion (Michalopoulos et al., 2025).

2.2 A Socio-Technical View on Retail CBDCs

The socio-technical perspective assumes that IS consist of both a social and a technical part, nested in a complex environment (Bostrom & Heinen, 1977; Oosthuizen & Pretorius, 2016). The technical system is composed of business processes and physical systems with the purpose of solving tasks or achieving goals that are defined by humans (Bostrom & Heinen, 1977). Conversely, the social system consists of people embedded in organizational structures (Bostrom & Heinen, 1977). Six bilateral interactions can be found between those components (Bostrom & Heinen, 1977; Oosthuizen & Pretorius, 2016). Both components are highly interdependent, resulting in complex relationships that must be jointly optimized in order for the IS to be purposeful and successful (Sarker et al., 2019).

We see initial confirmation that the socio-technical view is relevant in the field of decentralized finance (Augustin et al., 2023; Brennecke et al., 2022), as it allows to examine not only the technical features, but also how the system in which they are embedded enables value creation. Aligning with these perspectives, we consider retail CBDC systems to be composed of the social and the technical, which encompass a human dimension embedded in formative structures as well as a physical system dimension and processes (see Figure 1). This understanding reinforces the positioning of CBDCs as digital financial services at the intersection of increasingly decentralized, adaptive, and hybrid information technologies and real economy value processes as highlighted by Alt et al. (2024).

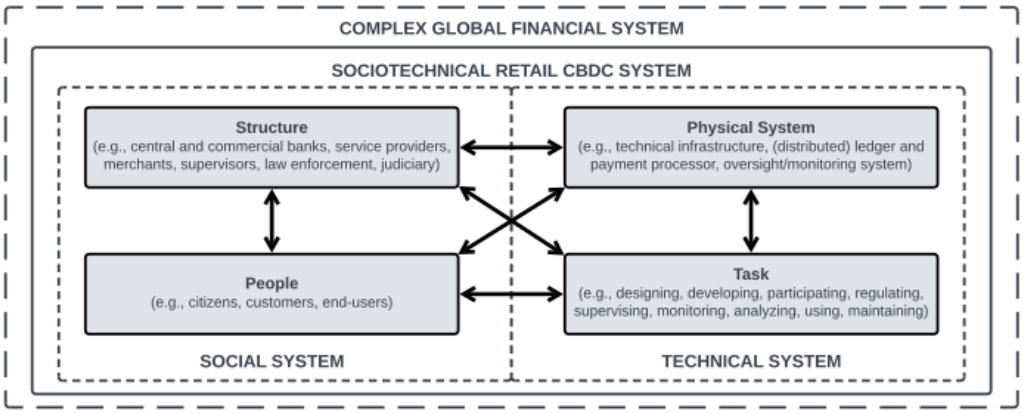

Figure 1. Retail CBDC System as an STS. Own figure based on our qualitative analysis, as well as on Bostrom and Heinen (1977) and Oosthuizen and Pretorius (2016).

Structure. Following Bostrom & Heinen (1977), structure refers to the organizational boundaries and governance. As their name indicates, retail CBDC systems revolve around the central bank of a given monetary area. Within the boundaries of monetary and central bank laws, it is typically this central bank that, in cooperation with the corresponding national government or supranational bodies, sets the rules for issuance, system development, and design (European Commission, 2023). Further, the structure of a retail CBDC system is strongly linked to its surrounding legal and regulatory frameworks, governance,

and design choices (Allen et al., 2020; Genc & Takagi, 2024). The involved organizations will likely include at least central bank(s), commercial banks, payment processors, payment service providers (PSPs), merchants (physical & online shops), financial authorities and supervisors, law enforcement agencies, and the judiciary (BIS-IH, 2023d; ECB, 2023).

People. The second dimension within the social system refers to people and their skills, values, and attitudes (Bostrom & Heinen, 1977). Retail CBDC systems include a strong human dimension, represented by citizens, customers, and end users. These are the core stakeholders in retail CBDC systems, distinguishing them from wholesale CBDCs systems (BIS-IH, 2022). In 2021, during a public consultation on a digital euro, a survey among 8,221 respondents indicated that citizens strongly prioritize privacy and security in a retail CBDC (ECB, 2021). The survey also indicated that financial and ease-of-use aspects, such as the usability without incurring additional costs and throughout the currency area, were top priorities (ECB, 2021). While priorities may vary by currency area, people generally consider privacy, security, economic efficiency, and usability to be key features of a successful retail CBDC system (ECB, 2023). Academic research has also highlighted that both technical safeguards (Gross et al., 2021; Michalopoulos et al., 2025), as well as trust in and credibility of central banks are expected to positively influence retail CBDC adoption (Frank et al., 2026; Tronnier et al., 2022).

Physical System. Building on prior understandings of STSs in various subdomains of IS (Bostrom & Heinen, 1977; Sarker et al., 2019), the physical system includes the underlying technologies of a retail CBDC system, including its hardware and software elements. Hardware includes, but is not limited to, the general technical infrastructure, such as servers, as well as the physical buildings that house them (Bank of Japan, 2024). The hardware side further includes payment terminals and devices on the side of commercial banks and merchants, as well as components such as secure elements (SEs) and trusted execution environments (TEEs) potentially used by customers to initiate (offline) payments (Michalopoulos et al., 2025). Second, in the case of retail CBDC systems, software includes its code base and interfaces, systems for transaction documentation and settlement, as well as financial oversight and data sharing systems (BIS-IH, 2022; ECB, 2019). The software and tools used in the system would likely interact using standards, application programming interfaces (Bank of England, 2023), and other interface functions (BIS-CGIDE, 2023).

Task. Making use of physical systems, people and organizations within a retail CBDC system execute and, in turn, enable a variety of tasks. Primarily, retail CBDCs are used to execute retail payments. To enable this task, stakeholders are initially involved in designing and developing the system and infrastructure, in many cases based on active stakeholder engagement (ECB, 2021, 2023; Federal Reserve Board, 2022). Once this core infrastructure is rolled out, participants will focus on maintaining the system before turning towards developing and rolling out additional features (ECB, 2023, 2025). Building on this core infrastructure, financial service providers and other actors may want to create related applications and services or even be involved in the governance and change processes surrounding the system (BIS-IH, 2023d; Schaaf et al., 2025). Stakeholders at the financial oversight level will further engage in regulation, supervision, and monitoring (EDPB & EDPS, 2023). The judiciary, law enforcement agencies, and supervisory authorities oversee and supervise the functioning of the system and ensure checks-and-balances (Reserve Bank of Australia & Treasury, 2024). Depending on the design choices, authorities may audit technology and governance elements, and/or supervise the involved financial institutions (Banco Central do Brasil, 2024; BIS-IH, 2023d).

2.3 Information Privacy and Retail CBDCs

Focusing on information privacy, which combines personal communication and data privacy, Smith et al. (1996) identified four dimensions: data collection, unauthorized secondary use of data, improper access, and errors. Subsequent research has applied these dimensions to measure privacy concerns related to mobile payment solutions (Chen & Nath, 2008). Building on Smith et al. (1996), in the context of retail CBDCs, these dimensions relate to concerns regarding (i) the collection and storage of extensive amounts of end-user data, (ii) transaction information and behaviors being used for other purposes than previously intended, either by internal and external actors (e.g., prohibition of commercial re-use and

supervisory access), (iii) individual end-user data being readily available to unauthorized individuals, and (iv) an inadequate protection against deliberate and accidental errors in personal data of end users.

Since the seminal publication by Smith et al. (1996), a large body of related work on information privacy has accumulated both within and outside IS, as highlighted in the literature review by Bélanger and Crossler (2011). Notably, privacy concerns have been used as a proxy to measure privacy and as a way to mitigate related fears. In commerce, the absence of trust may lead individuals to call for state intervention in the form of regulation (Smith et al., 2011). In particular, Nissenbaum (2009) gives an account of (online) privacy that is rooted in appropriate flows of personal information, which are those that comply with contextual informational norms. In IS research, Tronnier (2024) applied Nissenbaum's theory of contextual integrity in the context of retail CBDCs, while other researchers have focused on privacy in digital payments (Bandara et al., 2020). To this day, however, it remains difficult to identify a definition of privacy that is valid over time and across disciplines. As a result, privacy is a multilevel and multifaceted concept, with notions ranging from ISO 24775-2:2021 to those of privacy by design and by default mandated by the EU General Data Protection Regulation (EDPB & EDPS, 2023).

A key design trade-off in retail CBDCs is the balancing of end-user privacy with certain levels of financial transparency, notably for AML/CFT (Allen et al., 2020). Financial transparency is based on identifiability, i.e., the link to real-world identities (Pfitzmann & Hansen, 2010), which is not guaranteed in fully anonymous designs. It is also tied to auditability (ECB, 2019), which assumes certain data access in given circumstances and by specific actors, without breaching confidentiality (ECB & Bank of Japan, 2020). Although retail CBDCs have prompted fear of mass surveillance (Baronchelli et al., 2022; Rennie & Steele, 2021), their levels of privacy can be protected and balanced with other safeguards in various ways and to different extents (Gross et al., 2021; Lamberty et al., 2024; Wüst et al., 2022). On the one hand, privacy-enhancing techniques do not necessarily imply full anonymity or affect identifiability (Bank of Canada, 2025). On the other hand, allowing a set of anonymous transactions does not mean the entire system is anonymous (Mancini-Griffoli et al., 2018). Indeed, the high level of privacy desired by prospective retail CBDC end users (ECB, 2021; Jabbar et al., 2023; Tronnier et al., 2022) may comply with the AML/CFT risk-based approach when implemented selectively (Michalopoulos et al., 2025).

3 Methodology

To answer the first part of our research question, we collected and analyzed publications by both central banks and the BIS. While central bank publications allowed us to account for jurisdictional details, BIS publications added cross-jurisdictional considerations to the overall picture. For the former, we decided to focus on central banks of G20 countries, as they would be responsible for the issuance of retail CBDCs in countries accounting for 85% of gross world product (G20, 2025). To ensure representation, coverage, and relevance, we searched the website of each G20 country's central bank for central bank digital currenc* or CBDC*, as well as the name of the local proposed retail CBDC. We collected and organized all resulting records for later analyses. For the latter, we identified all retail CBDC projects in which the BIS has been or is currently involved. We then excluded all records published prior to 2018, the year in which investigations into retail CBDCs reached sufficient sophistication to enable qualitative analysis (Mancini-Griffoli et al., 2018). Overall, we included 37 records, encompassing a total of 1,497 pages. This selection features a wide variety of document types, including but not limited to reports, statements, policy documents, and guidelines. Since few retail CBDC initiatives have reached the roll-out stage, the literature underlying this part of our analysis is primarily based on work-in-progress initiatives of central banks and the BIS. We acknowledge that it may thus include biases, tied to regulatory and political aspects, institutional mandates, and special interests.

Following Neuendorf (2017), we then conducted a qualitative content analysis based on a total of 37 publications. These included eight publications by the BIS and a total of 25 publications by G20 central banks and related bodies. Our coding strategy was both deductive and inductive. On the one hand, it was deductive to the extent that we built our analysis on the core tenets of STS theory as described above (Oosthuizen & Pretorius, 2016), establishing a coding system that distinguishes between the social system (including the dimensions of structure and people) and the technical system (including the

dimensions of physical system and tasks). On the other hand, it was inductive, as we identified 24 subcodes, falling into the four dimensions of socio-technical systems.

To answer the second part of our research question, we conducted a structured literature review using the PRISMA approach (Page et al., 2021). First, we identified relevant literature using the following search string on both Scopus and the AIS eLibrary: "("central bank digital currenc*" OR CBDC*) AND privacy". This search yielded 188 and 45 records, respectively, for a total of 233 records. We then manually excluded duplicates (n=3) and non-peer-reviewed items (n=50), resulting in a total of 180 records included in the screening phase. Second, in the screening phase, we excluded records published prior to 2018 (n=5), as per the reasoning above, records not available in English (n=4), as well as posters and minitrack descriptions (n=2). For the abstract screening, two authors independently screened the abstracts and included records related to retail CBDC systems that indicated a design-orientation or a design-relevance from a privacy perspective. During the full-text screening, two authors independently screened the full texts of the remaining 49 records. They excluded conference publications for which journal versions had been published (n=2), as well as records that did not refer to technologies with the potential to mitigate end-user privacy problems (n=18). In case of differing assessments by the two screening authors, all authors jointly discussed whether to include or exclude a given record based on the previously defined inclusion criteria. Finally, in the inclusion phase, we included 29 relevant records.

Following Corbin and Strauss (2008), we then conducted a three-step coding process on the included 29 records plus the 37 institutional reports previously identified. In a first step of open coding, we assigned codes to small text segments directly relating to the mitigation of privacy trade-offs. In a second step of axial coding, we reviewed the previously identified open codes looking at the relationship between them and we grouped the emerged patterns into broader categories with a focus on technology-enabled objectives that support privacy in various ways (e.g., data minimization, data segregation, secret computation). In a third step of selective coding, we reviewed the axial codes and reassessed all records using the identified codes and categories. Subsequently, we focused on pinpointing technologies and technology groups affording the most promising features, according to these sources, to mitigate the bilateral privacy tensions between the components of the socio-technical retail CBDCs. We also derived four challenges associated with the implementation of these technologies in retail CBDCs.

4 Identification of Privacy Tensions in Retail CBDC Systems

In this section, we draw from our qualitative analysis as well as STS theory to analyze the implications for end-user privacy of the interplay between the STS components of a retail CBDC system. To do so, we examine all six bilateral interactions and outline how end-user privacy tensions arise from them.

First, at the intersection of *People and Tasks*, the privacy levels afforded by a given retail CBDC system are expected to have a strong impact on the way in which people would perform activities such as paying in physical and online stores, exchanging value peer-to-peer, and saving money. Privacy features would naturally foster or hinder the execution of these tasks. Importantly, if retail CBDCs were to replace physical cash entirely (a solution that is explicitly avoided in most projects), the scale of the impact on end users' tasks would rise considerably, as they would lose access to any possible means of payment of fully anonymous nature. Further, the high degree of privacy that is reportedly a condition for end users to adopt the retail CBDC (Tronnier et al., 2022) will directly impact which tasks can be executed by public authorities requiring data access to fulfil their tasks and obligations such as monitoring and auditing but also enforcing laws and regulations (Bank of Japan, 2023). Conversely, if people believe that the execution of such tasks is prioritized over their privacy preferences, end users may be reluctant to participate in retail CBDC systems (Reserve Bank of India, 2022).

Second, between *People and Physical System*, we observe that end users see embedded strong privacy guarantees as a prerequisite for their use of retail CBDC systems (ECB, 2021; Tronnier et al., 2022). These end-user privacy preferences may conflict with requirements that must be embedded in the retail CBDC system to safeguard integrity and stability for its integration in the broader financial system – e.g., a retail CBDC system and executed transactions should be auditable and verifiable (Wang et al., 2022). From another perspective, a fully online retail CBDC system would not meet the expectations of

many prospective end users to be able to pay also in the absence of Internet connectivity (Reserve Bank of Australia & Treasury, 2024), where the possibility to transact offline is associated with higher privacy guarantees (ECB, 2021). In the absence of such safeguards, citizens would incur, at the hands of the system, what Rennie & Steele (2021, p. 10) refer to as a "[l]oss of anonymity [that] is closely associated with traditional concepts of privacy that resist intrusion." Further, different citizens and businesses may have varying priorities, expectations and understandings of how which privacy features are or can be embedded in the physical system, leading to conflicting design preferences but also difficulty in understanding the privacy level embedded and afforded by the system.

Third, at the junction of *People and Structure* lies one of the core privacy risks in retail CBDCs, namely that of end users and their spending behaviors becoming subject to (large-scale) surveillance (Lamberty et al., 2024), leading to what Rennie & Steele (2021) refer to as "loss of liberty." This privacy concern relates to citizens' trust in their government, the central bank, and their respective political and legal underpinnings (Frank et al., 2026; Reserve Bank of India, 2022). The governance of retail CBDC systems depends on how it is regulated and on how checks and balances are embedded in its governance structure (Bank of England, 2023; Reserve Bank of Australia & Treasury, 2024; Reserve Bank of India, 2022). While people's preferences influence how privacy is designed in the system's structure, the latter will also attract or repel individuals depending on whether it mitigates their privacy concerns (Jabbar et al., 2023). An example is the need for citizens' trust that the use of collected data will align with the promises made (ECB, 2023, 2025). Or more specifically, which data is collected by whom, and how effectively governance structures mitigate the risks of unauthorized secondary use and improper access. Rennie & Steele (2021, p. 10) refer to this as a "[l]oss of individual control over personal information [that] aligns with contemporary ideas of data protection, including protecting information from misuse, such as through unauthorized commercialization." Tensions also arise between the privacy preferences of end users and financial institutions or third parties who may have an interest to use transaction data to improve services (BIS-IH, 2023c; Central Bank of the Republic of Türkiye, 2023) as well as for value creation and monetization (Auer et al., 2022; Schaaf et al., 2025).

Fourth, between *Structure and Physical System*, researchers have long discussed how organizational structures and requirements impact the design of physical systems (Harvey, 1968). Domain-specific discussions, frequently driven by decentralization technologies such as distributed ledgers, converged on the realization that decentralization might indeed increase the costs incurred related to the operation of systems but may be desirable for organizational reasons (Bank Indonesia, 2022). We consider similar tensions to also hold in the case of retail CBDCs, where privacy trade-offs between governance and the physical system seem inevitable. The decision on the level of privacy to be guaranteed at the infrastructure level directly impacts the extent to which an authorized secondary use of data can both create value in the overall system but also contribute to mitigating AML/CFT risks. It thereby directly relates to and heavily impacts the organizational functions of stakeholders such as regulators, supervisors, law enforcement agencies (Reserve Bank of India, 2022).

Fifth, considering *Physical System and Tasks*, the goal is typically to design a physical system in a way that enables effective and efficient execution of the foreseen tasks (Zigurs & Buckland, 1998). In retail CBDCs, the possible privacy features embedded in the physical system would impact numerous tasks, such as paying (e.g., offline and/or online) but also auditing and monitoring with varying levels of granularity (ECB, 2025). Theoretically, a digital means of payment would naturally offer better ways to safeguard against financial crime than cash (Lamberty et al., 2024). Yet, this inherent feature of the physical system leads to privacy tensions that are crucial for other tasks, such as end users paying with and adopting the digital currency. From the perspective of the tasks to be performed, the concept of privacy itself may become granular when evaluated against various frameworks – e.g., from an AML/CFT perspective, a fully private transaction is one that cannot be related to an identifiable individual (Michalopoulos et al., 2025). Hence, to determine if specific privacy features enable or hinder certain tasks, it is important to pinpoint what data needs to be available (and in what form) to uphold the performance of the given task, and how certain tasks can be performed with the least amount of data.

Sixth, amid *Structure and Tasks*, the impact of a system's governance on end-user privacy largely impacts the execution of tasks themselves. Specifically, the structure of a retail CBDC system may be

designed to put privacy front-and-center, potentially leading to intra- and inter-organizational information barriers between central banks, commercial banks, and supervisors. However, these barriers might lead to inefficiencies and distrust in the overall system (Bannister, 2001). For instance, between commercial banks and other PSPs tensions may emerge between the need to protect sensitive personal and commercial data and the collaboration among each other to enhance their AML/CFT, anti-fraud and cybersecurity posture (Bank of England, 2023). It is in the interaction of structure and tasks that organizations can lay the governance rules against unauthorized data collection, improper access, and unauthorized secondary data use (Bank of England, 2023; Smith et al., 1996). The political and legal environment that houses a retail CBDC is thus of utmost importance in shaping the governance elements that impact the execution of privacy-sensitive tasks – e.g., which parties are involved in auditing, monitoring, following which procedures and in which boundaries.

5 Towards the Mitigation of the Bilateral Privacy Tensions

As outlined in Section 3, we identified a selection of publications that discuss and propose privacy solutions related to retail CBDC designs. These privacy solutions are both of technical and social nature, as, differently from physical cash, in cashless payments privacy is a matter of technical, organizational, and legal design (Ballaschk & Paulick, 2021). In this section, we focus on technologies, mostly PETs, as well as on their role in mitigating the bilateral privacy tensions identified above. As our analysis demonstrates, these technologies can attend simultaneously to multiple bilateral tensions, albeit to varying degrees. We map them to the bilateral tensions they can most relevantly contribute to mitigate. Importantly, these technologies are also often recommended to be applied concurrently, and their application in the retail CBDC context is largely still at a theoretical and prototype level. Their implementation is still challenging in terms of performance, maturity, complexity and effectiveness (Bank of Canada, 2025). The pairing of tensions and solutions, with their main aspects highlighted below, is at the core of the contribution of this work (see Table 1 for a summary of our findings).

5.1 The Role of Technologies

At the intersection between *People and Task (1)*, privacy preferences of end users are expected to strongly influence tasks such as paying in physical or online stores, ultimately fostering or hindering retail CBDC adoption. The level of privacy also has a strong impact on the tasks performed by stakeholders such as supervisors, law enforcement and auditors, up to making these tasks impossible in scenarios of strong anonymity. A mitigating role is played by technologies that support the execution of traditional financial sector tasks, such as supervising, onboarding and monitoring, in a privacy-preserving way – i.e., to achieve "auditable privacy" (Lee et al., 2021). Promising PETs to this end are zero-knowledge proofs (ZKPs), which are discussed for their role in maintaining verifiability and enabling compliance checks despite minimizing data sharing by enabling selective disclosure (Lamberty et al., 2024; Michalopoulos et al., 2025), but also crypto primitives such as Pedersen commitments (ECB & Bank of Japan, 2020; Pocher & Veneris, 2022), as well as blind and ring signatures (Goodell et al., 2021; Kiayias et al., 2022; Lee et al., 2021). ZKPs are also discussed for verifiable credentials and decentralized identifiers, which allow to selectively share digital identity records, e.g., for onboarding (Bank of Canada, 2025). While this is in line with the principle of data minimization, it could also reduce the amount of data available for supervision, monitoring and auditing, making it difficult to trace the origin of funds or identify patterns of money laundering (Bank of Canada, 2025).

Between *People and Physical System (2)*, preferences of different end users may reflect contrasting priorities to be enabled, and expectations to be met, through design features of retail CBDCs. These preferences may also need to be balanced with the requirements for a safe integration of the retail CBDC system into the broader financial system (ECB, 2025). A core expectation of end users is that they will maintain their ability to pay anonymously and offline. Against this backdrop, our findings suggest that technologies that allow for tiering approaches of selective privacy levels may play a key role, as they follow the principle "lower risk and lower value, more privacy" and vice versa (ECB, 2025; People's Bank of China, 2021; Reserve Bank of Australia & Treasury, 2024). Concretely, tiering may be based

on the risk level associated to end users, for example affording more privacy-enhancing options to low-risk end users, such as increased offline spending limits, while limiting offline spending for high-risk end users. Tiering can also be based on transaction amounts, easing offline transfers of smaller values only; or on counterparties, such as requiring business-to-business transfers to be performed online. Tiering can also be based on combinations of these criteria (Michalopoulos et al., 2025). This arguably gives end users more control over their privacy, as they have multiple options at their disposal (Bank of England, 2023; ECB, 2025; Rennie & Steele, 2021). Technologies discussed in this context relate to both online and offline retail CBDC systems and range from hardware-based solutions, such as SEs and TEEs, to software-based solutions, including blind signatures, ring signatures, Pedersen commitments, ZKPs, and secure multi-party computation (SMPC) (Atangana et al., 2025; Lamberty et al., 2024; Lee et al., 2021; Wang et al., 2022; Wüst et al., 2022). Relatedly, several sources point to leveraging features of distributed ledgers (combined with PETs), and to the provision of non-custodial wallets and corresponding secure management of credentials (Bank of Canada, 2025; Bizama et al., 2025; Goodell et al., 2021). Frequently, token-based models are described as more conducive to privacy than account-based (Bizama et al., 2025; Goodell et al., 2021), although recent work indicates the limits of this distinction (Michalopoulos et al., 2025; Wüst et al., 2022).

Between *People & Structure (3),* tensions emerge from the risk that end users and their spending behaviors could be subject to (large-scale) surveillance, but also that financial institutions or third parties may have an interest to monetize data generated in retail CBDC systems. This tension is strongly related to which entity collects data, and how effectively data governance structures can mitigate the risks of unauthorized secondary use and improper access (Bank of Japan, 2023). At this level, the focus is primarily on ensuring that central banks and governments will not have access to the end users' personal data and are able to limit access from private financial institutions as well (Bank of England, 2023; Bank of Japan, 2023; ECB, 2025). A key role is played by technologies that enable organizations to maintain control over their data while also allowing authorities to perform aggregate monitoring. Federated learning, SMPC and homomorphic encryption (HE) emerge as crucial in this respect (Bank of Canada, 2025; Bank of Japan, 2023). In this context, some features of distributed ledgers, e.g., transparency and immutability, may enhance the verifiability of confidential computations when combined with PETs. Differential privacy is a non-cryptographic way of making aggregated data and statistics available without revealing identities (Bank of Japan, 2023). Threshold cryptography may further mitigate risks of data misuse by allowing privacy revocation only under specific circumstances (Ballaschk & Paulick, 2021; Kiayias et al., 2022), while verifiable credentials would reduce the risk of oversharing identity data (Bank of England, 2023; Bank of Japan, 2023; Central Bank of the Republic of Türkiye, 2023).

Between *Structure & Physical System (4)*, we can observe how trade-offs emerging between specific privacy-related design features of the physical system may heavily impact the activities of stakeholders such as regulators, supervisors and law enforcement, potentially forcing changes to their organizational setup. At the same time, safeguards in the physical system, such as those against unauthorized access (Lamberty et al., 2024), are crucial to protect the organizational functions of such stakeholders. At this level, special attention shall be paid, in the development and maintenance of the software infrastructure, to both security and privacy (Bank of Japan, 2023). Further, in both offline and online scenarios, solutions such as SEs, TEEs, and ZKPs, allow to hard-code governance and regulatory rules, albeit with varying level of computational capabilities and flexibility (Michalopoulos et al., 2025). As outlined at the intersection of structure and tasks (since it is primarily related to the organizational tasks), certain technologies allow organizations to fulfill their mandates by leveraging privacy-preserving data sharing and collaborative computation, e.g., through SMPC, HE, federated learning, and differential privacy.

Between *Physical System & Task (5)*, a retail CBDC system's privacy features strongly depend on the tasks the system is designed to afford. In theory, digital payments offer more efficient ways to safeguard against financial crime than what happens with cash payments. Yet, this capability also leads to privacy tensions that are crucial for other tasks such as end users paying and adopting the CBDC. This has led to the development of the previously mentioned tiered models, with solutions that, by enabling offline payment (e.g., through SEs, TEEs), also allow end users to pay offline with a higher degree of privacy. Meanwhile, performing data analysis in TEEs – but also in confidential computing environments and

leveraging SMPC and HE – can uphold supervisory tasks while supporting privacy (Bank of Canada, 2025; Bank of Japan, 2023). ZKPs further allow to provide proofs of compliance (Michalopoulos et al., 2025) and transaction settlement in a privacy-preserving way (Wüst et al., 2022).

Between *Structure & Task (6)*, the influence of a retail CBDC system's governance on end-user privacy may reflect various priorities and largely impacts the execution of tasks themselves. On the one end, tasks such as AML/CFT and anti-fraud monitoring could be performed collaboratively by the involved institutions. On the other end, the fear of sharing sensitive personal or commercial data may lead to information silos between central and commercial banks and supervisors. This is where governance rules are key to ensure a suitable level of privacy and collaboration, to avoid hampering tasks that are crucial for financial integrity, such as supervision and oversight, which require data access. Several technologies are examined to mitigate this tension by enabling collaborative tasks while keeping sensitive data secret from other organizations (Bank of Japan, 2023). The chief example is federated learning, sometimes complemented with differential privacy (Bank of Japan, 2023). Other examples include SMPCs and HE which allow organizations to perform analytical tasks collaboratively without revealing raw data (Bank of Canada, 2025). Some features of distributed ledgers, combined with PETs, may also be conducive to this. Pedersen commitments and HE may also allow the central bank to supervise commercial banks while protecting the privacy of their transactions (Wang et al., 2022). Further, (searchable) public-key encryption has been proposed to support lawful access and audit tasks while keeping the remaining data encrypted (Bank of Japan, 2023). Overall, privacy tensions related to (e.g., supervisory) tasks are emerging as particularly difficult to mitigate, with fewer technologies reportedly able to attend to them effectively (Table 1). Yet ZKPs emerge as promising, maintaining verifiability and minimizing data sharing via selective disclosure (Michalopoulos et al., 2025).

Bilateral tensions (→) & Technologies (↓)	**(1) People and task**	**(2) People and physical system**	**(3) People and structure**	**(4) Structure and physical system**	**(5) Physical system and task**	**(6) Structure and task**
Secure elements		x		x	x	
Trusted execution environments		x		x	x	
Zero-knowledge proofs	x	x	x	x	x	x
Secure multi-party computation and threshold cryptography		x	x	x	x	x
Homomorphic and searchable encryption		x	x	x	x	x
Differential privacy			x		x	x
Verifiable credentials and decentralized ID	x	x	x			
Blind/ring signatures, stealth addresses, Pedersen commitment	x	x	x			x
Federated learning			x	x		x
Distributed ledgers	x	x	x	x	x	x

Table 1. (Groups of) technologies that have been discussed to address the privacy tensions between different components of socio-technical retail CBDC systems.

5.2 Implementation Challenges

From a theoretical standpoint, the discussed technologies and their combinations have emerged as promising solutions to address many bilateral socio-technical privacy tensions in retail CBDC systems. Their implementation, however, is challenging especially in critical infrastructures. Four core areas of

concern emerge from the (prospective) use of these technologies in retail CBDC systems, pertaining to cost and scalability, reliance on foreign manufacturers, security, as well as maturity and interoperability.

First, the implementation of these technologies currently entails high deployment and operational costs, which hinders scalability. High deployment costs are discussed for specialized hardware and software, especially around TEEs and SEs (Michalopoulos et al., 2025). At the same time, operational costs are highlighted in relation to ZKPs, MPCs and distributed ledgers, given their computation and communication costs (Atangana et al., 2025; Bank of Canada, 2025; Bank of Japan, 2024; Lee et al., 2021). For instance, some ZKP approaches have higher computational overhead at larger proof sizes (Bank of Canada, 2025), MPC complexity increases with the number of participants (Michalopoulos et al., 2025), and distributed ledgers are less efficient than traditional ones (Lee et al., 2021). Hence, their inclusion in payment systems entails scaling risks (Bank of Canada, 2025; Bank of Japan, 2023).

Second, many currency areas currently lack the domestic capacities to produce specialized hardware. If these areas include technologies such as TEEs and SEs in the design of their retail CBDC systems, they are likely to introduce dependencies on specialized foreign hardware manufacturers (Michalopoulos et al., 2025). Therefore, the inclusion of such technologies would, in many cases, conflict with one of the main reasons for introducing retail CBDCs, namely safeguarding monetary sovereignty (ECB, 2025).

Third, the implementation of many of these technologies poses security risks, including vulnerabilities to novel attack vectors (BIS-IH, 2023b). In TEEs, SEs, and ZKPs, for instance, attackers may be able to extract information from the observation of computation and communication activities in side-channel attacks, as well as through physical means (BIS-IH, 2023b; Michalopoulos et al., 2025). In the case of differential privacy, the extent to which information is both protected and useful relies on the careful calibration of the noise added (Bank of Japan, 2023), and federated learning approaches can be susceptible to data manipulation and inference (Bank of Canada, 2025).

Lastly, from a practical standpoint, the maturity of several of these technologies is limited because they have not been implemented in production environments and tested at a large scale (Bank of Canada, 2025; BIS-IH, 2023c). This makes their implementation in retail CBDC particularly risky, as it could lead to reliability and performance issues that are critical in financial systems (Bank of Canada, 2025). Additionally, many of the considered technologies and their related protocols are not yet sufficiently covered by standards to support their interoperability with each other or with legacy systems (Bank of Canada, 2025). This lack of standardization, e.g., in the case of ZKPs, SMPCs, and some signature implementations, makes it challenging to develop systems complying with laws and regulations.

To address these trade-offs, central banks and researchers are exploring combinations of technologies that balance scalability, sovereignty, security and interoperability with the required privacy guarantees (Bank of Japan, 2023). As PETs evolve from a technical niche to being piloted in the context of CBDC systems, the key challenge for central banks shifts from achieving end-user privacy to balancing it with the protection of financial integrity and other design goals without introducing novel attack vectors.

6 Discussion

6.1 Contributions

In this work, we identify and structure socio-technical end-user privacy tensions emerging in retail CBDC systems and discuss the technologies that have been proposed to mitigate them. While prior IS publications on CBDCs addressed trust (e.g., Frank et al., 2026), privacy (e.g., Tronnier et al., 2022), and design (e.g., Currie & Seddon, 2023) in relation to individual socio-technical components, they do not position STS theory (Bostrom & Heinen, 1977; Oosthuizen & Pretorius, 2016) at the center of analysis. To the best of our knowledge and based on our qualitative analysis of academic and institutional publications, we thus offer the first account of end-user privacy in retail CBDC systems based explicitly on STS theory. This approach advances existing research from a threefold perspective. First, by focusing on the components of the social and technical systems, we highlight the differences in perspectives on privacy between end users and organizations, notably of central and commercial banks, as well as third parties. We also emphasize how privacy elements affect differently the system's

infrastructure and the tasks to be performed. Second, we shed light on the privacy tensions that are harder to mitigate, particularly those that are task-related, where the implementation of PETs may hinder key functionalities such as payment, data sharing, and oversight. Third, this is the first work to identify which technologies are discussed to address each of the bilateral end-user privacy tensions, and highlight those, such as ZKPs, that have emerged as promising solutions for addressing all these tensions.

Against this backdrop, the contributions of our work are also empirical (Ågerfalk & Karlsson, 2020), and explanatory (Gregor, 2006). They are empirical, as – in response to the first part of our research question – we provide a detailed account of the socio-technical components and their interactions in the context of emerging retail CBDC systems based on both research- and practice-oriented sources. We then elaborate on the impact of these socio-technical components on the design of CBDC systems, particularly with respect to (information) privacy. This work is also explanatory, as – in response to the second part of our research question – we delineate which technologies have been proposed to mitigate end-user privacy tensions between the socio-technical components of retail CBDC systems.

6.2 Implications for Domain and Research Practice

Our work has direct implications for domain practice and has the potential to inform design and decision-making processes related to retail CBDCs. First, it helps institutions recognize the value of investigating the functionalities of the discussed technologies and mitigating existing implementation challenges, such as limited standardization. Second, it sheds light on the composite problem of ensuring end-user privacy while accounting for design goals that include but are not limited to the protection of financial integrity, ultimately providing socio-technical scientific backing to the combination of PETs as well as tiered privacy approaches. Third, it enables regulators and supervisors to consciously engage in the required collaborative work to ensure that emerging retail CBDCs system can co-create and harness value that is meaningful to all system participants while safeguarding end-user privacy. It helps central banks gain a holistic understanding of the dimensions at play when designing novel retail CBDC systems and improving existing proposals, and it aids financial service providers in better understanding their roles within retail CBDC systems and the corresponding impact on end-user privacy. In two-tiered models in particular, these institutions will be crucial in the distribution of CBDCs as well as in making it accessible to citizens. Finally, it could help all stakeholders reduce frictions in retail CBDC adoption.

For research practice, our explanation of the social and the technical systems within retail CBDC systems highlights the impact that the integration of social and technical understandings has on some of the fundamental aspects of retail CBDC design and adoption. Indeed, it is precisely this interplay that simultaneously acknowledges people's desire for privacy, the systems through which it might be achieved, and the structures involved in governing it. Based on both parts of our qualitative analyses, the IS discipline is uniquely well-positioned to address these challenges and contribute to the empirically informed design, development, and operation of future retail CBDC systems.

Against this backdrop, we encourage IS researchers and practitioners to increasingly focus on the concept of data governance while trying to balance privacy with financial integrity. In doing so, they can move beyond more rigid privacy approaches that demand no data to be collected at all. Thus, rather than attempting to revolutionize the concept of end-user privacy in retail CBDC systems with respect to traditional digital payments, they may focus on more feasible improvements in how collected data is governed or used. This nuanced interpretation may help with interoperability and cross-border models, especially since regulatory frameworks on privacy and data protection are still fragmented.

6.3 Limitations and Future Research

As any research endeavor, this work has shortcomings and should be evaluated in consideration of at least four limitations. These, however, also give rise to future research opportunities aiming to further improve the design and development of retail CBDC systems through the joint optimization of the social and the technical system. First, we focus on the socio-technical components and interactions, as well as on the technologies proposed to mitigate end-user privacy tensions in retail CBDC systems. However, a more detailed discussion of the affordances and limitations of these technologies in the context of

privacy tensions in retail CBDCs, as well as their critical assessment beyond the academic and institutional publications analyzed, were out of the scope of this work. Future IS research could then investigate the impact of specific technologies on specific privacy tensions in design-oriented studies. Second, this work takes an information privacy perspective on end-user privacy. While this is an established lens that balances conceptual and practical considerations, future research could employ alternative lenses, initially building on concepts such as information risks, and moving towards applied privacy engineering methods such as LINDDUN. Third, this work sheds light on the socio-technical components and interaction of retail CBDC systems, which enabled us to discuss end-user privacy with a focus on design choices in proposed retail CBDC systems. Although fully and broadly implemented retail CBDC systems are still rare, both the digital yuan pilot and the digital euro (as soon as it reaches a sufficient technology readiness level), could offer opportunities for further engagement taking a socio-technical perspective. Fourth, this work builds on publications from research and domain practice, which may be biased and influenced by organizational interests. Future research could thus investigate to which extent real-world retail CBDC systems will be able to live up to their stated goals and ambitions.

7 Conclusions

When conceptualizing retail CBDC systems through a socio-technical lens, it becomes apparent that attempts to capture the system from a purely social or purely technical perspective overlook crucial aspects relating to the design, roll-out, and maintenance of retail CBDCs as well as the roles of the stakeholders involved. With privacy being a top priority for prospective end users, our analysis indicates that the governance level – including technical and managerial governance as well as in terms of public governance and regulation – plays a key role in the design and success of these systems. Our findings show that the discussed technologies address an average of four privacy tensions between the socio-technical components of retail CBDC systems, with ZKPs and distributed ledgers, especially in combination, being reportedly conducive to mitigating all six bilateral tensions. While, as our analysis has demonstrated, this appears promising to enable these systems to balance end-user privacy and financial integrity, moving forward it will crucial that both researchers and practitioners prioritize the resolution of the implementation challenges of these technologies. In summary, we conclude that accounting for the socio-technical components outlined above is a necessary step to achieve a holistic assessment of the end-user privacy level of a retail CBDC system. Yet, this undoubtedly adds a layer of complexity to ongoing activities of research and development. Given the granular nature of privacy, researchers and practitioners are encouraged to expand their understanding of privacy when designing and assessing retail CBDC solutions, reaching beyond a straightforward social or technical perspective.

Acknowledgements

This work was funded in part by the PayPal-FNR PEARL Chair in Digital Financial Services (ref. 13342933/Gilbert Fridgen), and by the FutureFinTech National Centre of Excellence in Research and Innovation (ref. 16570468, with Ministry of Finance). It was supported by Spuerkeess. For open access, the authors applied a CC BY 4.0 license to any author accepted manuscript arising from this submission.

References

Ågerfalk, P. J., & Karlsson, F. (2020). Artefactual and empirical contributions in information systems research. *European Journal of Information Systems*, *29*(2), 109–113. https://doi.org/ghzjw7

Allen, S., Capkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., John, S., Miller, A., Prasad, E., Wüst, K., & Zhang, F. (2020). *Design choices for central bank digital currency: Policy and technical considerations*. NBER. https://www.nber.org/papers/w27634

Alt, R., Fridgen, G., & Chang, Y. (2024). The future of fintech—Towards ubiquitous financial services. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-023-00687-8

Atangana, O., Khoukhi, L., Barbier, M., & Manno, J. D. (2025). Securing offline CBDC transactions: DigiVault card and MarkoPayChain with mobile phone integration. *28th ICIN Conference*, 33–40. https://doi.org/10.1109/ICIN64016.2025.10942801

Atlantic Council. (2025). *CBDC tracker*. https://www.atlanticcouncil.org/cbdctracker/

Auer, R., & Böhme, R. (2021). *Central bank digital currency: The quest for minimally invasive technology*. BIS. https://www.bis.org/publ/work948.pdf

Auer, R., Böhme, R., Clark, J., & Demirag, D. (2022). Mapping the privacy landscape for central bank digital currencies: Now is the time to shape what future payment flows will reveal about you. *Queue*, *20*(4), 16–38. https://doi.org/10.1145/3561796

Augustin, N., Durani, K., Kollmer, T., & Eckhardt, A. (2023). Examining the use of blockchain technology in virtual worlds: A socio-technical systems perspective. *56th HICSS*. https://doi.org/10.24251/HICSS.2023.732

Ballaschk, D., & Paulick, J. (2021). The public, the private and the secret: Thoughts on privacy in central bank digital currencies. *Journal of Payments Strategy & Systems*, *15*(3). https://doi.org/qxhg

Banco Central do Brasil. (2024). *BCB updates the guidelines of the digital Brazilian real and releases the directives of its pilot project*. https://www.bcb.gov.br/en/pressdetail/2466/nota

Bandara, R., Fernando, M., & Akter, S. (2020). Privacy concerns in e-commerce: A taxonomy and a future research agenda. *Electronic Markets*, *30*(3), 629–647. https://doi.org/qdg8

Bank Indonesia. (2022). *Project Garuda: Navigating the architecture of digital rupiah*. https://www.bi.go.id/en/rupiah/digital-rupiah/Documents/White-Paper-CBDC-2022_en.pdf

Bank of Canada. (2025). *Privacy-enhancing technologies for CBDC solutions*. https://doi.org/qxz8

Bank of England. (2023). *The digital pound: A new form of money for households and businesses?* https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper

Bank of Japan. (2023). *Privacy enhancing technologies: Payments and financial services in a digital society*. https://www.boj.or.jp/en/research/brp/psr/data/psrb230120.pdf

Bank of Japan. (2024). *Central bank digital currency experiments—Progress on the pilot program*. https://www.boj.or.jp/en/paym/digital/dig240531a.pdf

Bannister, F. (2001). Dismantling the silos: Extracting new value from IT investments in public administration. *Information Systems Journal*, *11*(1), 65–84. https://doi.org/c8fm49

Baronchelli, A., Halaburda, H., & Teytelboym, A. (2022). CBDCs risk becoming a digital leviathan. *Nature Human Behaviour*, *6*(7), 907–909. https://doi.org/10.1038/s41562-022-01404-9

Beath, C., Berente, N., Gallivan, M., & Lyytinen, K. (2013). Expanding the frontiers of IS research. *Journal of the Association for Information Systems*, *14*(4). https://doi.org/10.17705/1jais.00330

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/ggc3wp

Bindseil, U., Panetta, F., & Terol, I. (2021). *Central bank digital currency: Functional scope, pricing and controls*. ECB. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op286~9d472374ea.en.pdf

BIS. (2020). *Central bank digital currencies: Foundational principles and core features*. https://www.bis.org/publ/othp33.htm

BIS. (2021). *CBDCs: Financial stability implications*. https://www.bis.org/publ/othp42_fin_stab.pdf

BIS-CGIDE. (2023). *High-level technical requirements for a functional CBDC architecture*. https://www.bis.org/publ/othp82.pdf

BIS-IH. (2022). *Project Aurum: A prototype for two-tier CBDC*. https://www.bis.org/publ/othp57.htm

BIS-IH. (2023a). *Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders*. https://www.bis.org/publ/othp66.pdf

BIS-IH. (2023b). *Project Polaris: A handbook for offline payments with CBDC (#1)*. https://www.bis.org/publ/othp64.pdf

BIS-IH. (2023c). *Project Polaris: A high-level design guide for offline payments with CBDC (#4)*. https://www.bis.org/publ/othp79.pdf

BIS-IH. (2023d). *Project Sela: An accessible and secure retail CBDC ecosystem*. https://www.bis.org/publ/othp74.htm

Bizama, G. R., Goodell, G., Speed, C., Revans, J., & Bowler, R. D. (2025). A non-custodial wallet for digital currency: Design challenges and opportunities. *Journal of Payments Strategy & Systems*, *19*(3), 247. https://doi.org/10.69554/KRMP9840

Bostrom, R. P., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. *Journal of Management Information Systems*, *26*(1), 17–48. https://doi.org/10.2753/MIS0742-1222260102

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: the causes. *MIS Quarterly*, *1*(3), 17–32. https://doi.org/10.2307/248710

Brennecke, M., Guggenberger, T., Sachs, A., & Urbach, N. (2022). The human factor in blockchain ecosystems: A sociotechnical framework. *17th WI Tagung*. https://hdl.handle.net/10993/55251

Brunnermeier, M., & Landau, J.-P. (2022). *The digital euro: Policy implications and perspectives*. EP. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)703337

Carstens, A. (2021). Digital currencies and the future monetary system. *Hoover Institution Policy Seminar*, *89*(1). https://www.bis.org/speeches/sp210127.pdf

Central Bank of the Republic of Türkiye. (2023). *Digital Turkish lira—First phase evaluation report*. https://www.tcmb.gov.tr/

Chen, L., & Nath, R. (2008). Determinants of mobile payments: An empirical analysis. *Journal of International Technology and Information Management*, *17*(1), 9–20. https://doi.org/qdwx

Choi, S., Kim, B., Kim, Y.-S., & Kwon, O. (2023). *Central bank digital currency and privacy: A randomized survey experiment*. BIS. https://www.bis.org/publ/work1147.htm

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3rd ed.). SAGE. https://doi.org/10.4135/9781452230153

Currie, W., & Seddon, J. (2023). Unpacking the societal and institutional risks of crypto assets: The policy-innovation nexus. *44th ICIS*. https://aisel.aisnet.org/icis2023/practitioner/practitioner/3/

ECB. (2019). *Exploring anonymity in central bank digital currencies*. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.el.pdf

ECB. (2021). *Eurosystem report on the public consultation of a digital euro*. https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

ECB. (2023). *Progress on the investigation phase of a digital euro—Fourth report*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.degov230713-fourth-progress-report-digital-euro-investigation-phase.en.pdf

ECB. (2025). *Progress on the preparation phase of a digital euro—Closing progress report*. https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.deprp202510.en.pdf

ECB & Bank of Japan. (2020). *Balancing confidentiality and auditability in a distributed ledger environment*. https://www.boj.or.jp/en/paym/fintech/data/rel200212a2.pdf

EDPB & EDPS. (2023). *Joint opinion 02/2023 on the proposal for the establishment of a digital euro*. https://www.edpb.europa.eu/system/files/2023-10/edpb_edps_jointopinion_022023_digitaleuro_en.pdf

European Commission. (2023). *Digital euro. Proposal for a regulation of the European parliament and of the council on the establishment of the digital euro*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0369

Federal Reserve Board. (2022). *Money and payments: The USD in the age of digital transformation*. https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

Frank, M., Pocher, N., & Tharwat, A. (2026). The influence of institutional trust on the adoption of the digital euro. *59th HICSS Proceedings*, 2206–2215. https://hdl.handle.net/10125/111661

G20. (2025). *About G20*. https://g20.org/about-g20/g20-members/

Genc, H. O., & Takagi, S. (2024). A literature review on the design and implementation of central bank digital currencies. *International Journal of Economic Policy Studies*, *18*(1). https://doi.org/qdz9

Goodell, G., Al-Nakib, H. D., & Tasca, P. (2021). A digital currency architecture for privacy and owner-custodianship. *Future Internet*, *13*(5), 130. https://doi.org/10.3390/fi13050130

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611–642. https://doi.org/10.2307/25148742

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). *Designing a central bank digital currency with support for cash-like privacy*. https://ssrn.com/abstract=3891121

Harvey, E. (1968). Technology and the structure of organizations. *American Sociological Review*, *33*(2), 247–259. https://doi.org/10.2307/2092391

IMF. (2023). *CBDC: initial considerations*. https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/11/14/Central-Bank-Digital-Currency-Initial-Considerations-541466

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: a privacy calculus perspective. *Research in International Business and Finance*, *64*(1). https://doi.org/10.1016/j.ribaf.2022.101826

Kiayias, A., Kohlweiss, M., & Sarencheh, A. (2022). PEReDi: Privacy-enhanced, regulated and distributed central bank digital currencies. *Conference on Computer and Communications Security*, 1739–1752. https://doi.org/10.1145/3548606.3560707

Lamberty, R., Kirste, D., Kannengießer, N., & Sunyaev, A. (2024). HybCBDC: A design for central bank digital currency systems enabling digital cash. *IEEE Access*, *12*, 137712–137728. https://doi.org/10.1109/ACCESS.2024.3458451

Lee, Y., Son, B., Park, S., Lee, J., & Jang, H. (2021). A survey on security and privacy in blockchain-based central bank digital currencies. *Journal of Internet Services and Information Security*, *11*(3), 16–29. https://doi.org/10.22667/JISIS.2021.08.31.016

Mancini-Griffoli, T., Peria, M. S. M., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2018). *Casting light on CBDC*. IMF. https://doi.org/10.5089/9781484384572.006

Michalopoulos, P., Olowookere, O., Pocher, N., Sedlmeir, J., Veneris, A., & Puri, P. (2025). Privacy and compliance design options in offline central bank digital currencies. *IEEE Transactions on Network and Service Management*, *22*(5), 3748–3763. https://doi.org/10/qdz8

Neuendorf, K. A. (2017). *The content analysis guidebook*. Sage.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. SUP.

Oosthuizen, R., & Pretorius, L. (2016). Assessing the impact of new technology on complex sociotechnical systems. *South African Journal of Industrial Engineering*, *27*(2), 15–29. https://doi.org/10.7166/27-2-1144

Page, M. J., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1). https://doi.org/10.1186/s13643-021-01626-4

People's Bank of China. (2021). *Progress of research & development of E-CNY in China*. http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Pocher, N., & Veneris, A. (2022). Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme. *IEEE Transactions on Network and Service Management*, *19*(2), 1776–1788. https://doi.org/10.1109/TNSM.2021.3136984

Rennie, E., & Steele, S. (2021). Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency. *Law, Technology and Humans*, *3*(1), 6–17. https://doi.org/10.5204/lthj.1745

Reserve Bank of Australia & Treasury. (2024). *CBDC and the future of digital money in Australia*. https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/pdf/cbdc-and-the-future-of-digital-money-in-australia.pdf

Reserve Bank of India. (2022). *Concept note on central bank digital currency*. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *MIS Quarterly*, *43*(3), 695–719. https://doi.org/10.25300/MISQ/2019/13747

Schaaf, V., Lautenschlager, J., Voucko-Glockner, H., Plank, T., Guggenberger, T., & Urbach, N. (2025). A multivocal literature review on capturing value propositions for private organizations in a CBDC ecosystem. *Communications of the Association for Information Systems*, *57*, 289–317. https://doi.org/10.17705/1CAIS.05712

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Tronnier, F. (2024). Using contextual integrity to uncover acceptability of information flows in central bank digital currency transactions. *57th HICSS*. https://doi.org/10.24251/HICSS.2023.708

Tronnier, F., Harborth, D., & Hamm, P. (2022). Investigating privacy concerns and trust in the digital euro in Germany. *Electronic Commerce Research and Applications*, *53*. https://doi.org/gsg2mn

Wang, Y.-R., Ma, C.-Q., & Ren, Y.-S. (2022). A model for CBDC audits based on blockchain technology: Learning from the DCEP. *Research in International Business and Finance*, *63*, 101781. https://doi.org/10.1016/j.ribaf.2022.101781

Wüst, K., Kostiainen, K., Delius, N., & Capkun, S. (2022). Platypus: A central bank digital currency with unlinkable transactions and privacy-preserving regulation. *Conference on Computer and Communications Security*, 2947–2960. https://doi.org/10.1145/3548606.3560617

Zigurs, I., & Buckland, B. K. (1998). A theory of task/technology fit and group support systems effectiveness. *MIS Quarterly*, *22*(3), 313–334. https://doi.org/10.2307/249668