



From Cash to Code: Examining the Legal Framework for the Future of Digital Currency in Pakistan

Balqees Amjad ^{1*}

¹School of International Law, Southwest University of Political Science and Law, China

* Corresponding Email: balqeesamjad1@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.07>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Pakistan's cash-heavy economy is rapidly moving toward digital finance, driven by fintech growth and the State Bank of Pakistan's Raast instant payment system, making it crucial to assess whether existing laws can support a future Digital Rupee or central bank digital currency (CBDC). This study evaluates how well Pakistan's current monetary and financial framework can accommodate CBDC, identifies regulatory and institutional gaps, and proposes reforms to protect monetary sovereignty, enhance financial inclusion, and maintain coherence across the financial system. This paper treats the shift "from physical cash to digital code" as a legal paradigm change that demands an updated understanding of legal tender, payments, and state-backed money in the digital age. Using doctrinal legal analysis, comparative case studies, and policy review, it examines whether Pakistan's existing rules can safely support CBDC design, issuance, and use. The study traces Pakistan's move from a predominantly cash-based economy to expanding digital rails, focusing on Raast and major private platforms such as Easypaisa, JazzCash, and licensed electronic money institutions (EMIs). It analyzes post-COVID-19 uptake of digital payments alongside persistent barriers such as low digital literacy and trust, especially among underserved groups. The paper also benchmarks Pakistan's emerging CBDC posture against international experiences, including China's e-CNY, the EU's Digital Euro, and Nigeria's eNaira, to highlight lessons on legal tender status, architecture, and inclusion. It then critically reviews key statutes i.e., the State Bank of Pakistan Act 1956, the Payment Systems and Electronic Funds Transfer Act 2007, the Foreign Exchange Regulation Act 1947, and the Prevention of Electronic Crimes Act 2016, showing that despite strong SBP authority, definitional gaps and overlapping mandates create legal uncertainty over digital assets, data protection, consumer redress, and cybersecurity. This study recommends targeted amendments to foundational monetary and payments legislation and the adoption of a dedicated "Digital Currency Act" that clearly defines the legal tender status of a Digital Rupee, allocates governance responsibilities, and embeds safeguards for privacy, cybersecurity, and user rights. It further argues that aligning Pakistan's framework with FATF, IMF, and BIS standards will allow the country to harness its growing digital infrastructure to foster inclusion, safeguard rights, and position itself as a regional leader in secure and equitable digital finance.

Keywords: Digital Currency; CBDC; Legal Framework; Pakistan; Financial Inclusion; FATF Compliance

1. Introduction

Over the past decade, Pakistan's financial landscape has undergone a remarkable transformation. A country once dominated by cash transactions is now witnessing a steady rise in [1]. What began as an experiment in financial technology has evolved into a nationwide movement toward digital finance [2]. This shift is not merely following a global trend but also it reflects Pakistan's need to expand financial inclusion, reduce transaction costs, strengthen transparency, and modernize its payment system [3]. However, the transition from physical cash to digital value is more than a technological upgrade; it is a fundamental legal and economic turning point [4]. It challenges long-held assumptions about what constitutes "money," who may issue it, and how it should be regulated. As digital platforms grow, so too do questions about the legal definition of tender, the authority to issue and control digital money, liability in cases of system failure or fraud, and data protection for users in an increasingly



interconnected ecosystem[5]. In short, Pakistan’s financial transformation demands a parallel modernization of law and regulation [6].

For decades, Pakistan’s reliance on cash has fueled a vast informal economy and deepened the divide between formal and informal finance [7]. Large segments of the population remain unbanked, hindered by limited access to banking services, social disparities, low financial literacy, and mistrust in institutions [8]. Recognizing these barriers, the State Bank of Pakistan (SBP) has taken decisive steps to promote digitalization through platforms like *Raast*, the country’s instant payment system, and mobile money services such as Easypaisa and JazzCash [9] [10]. Yet, while these innovations promise inclusion and efficiency, they also expose critical legal uncertainties for regulators, service providers, and the public. These uncertainties become even more complex when digital payments evolve into digital currency. Around the world, digital currencies are reshaping legal and monetary boundaries [11]. Cryptocurrencies like Bitcoin operate beyond state control, while central bank digital currencies (CBDCs) represent state-backed digital money designed to coexist with traditional cash [12, 13]. Pakistan now stands at this crossroads. The SBP has expressed justified caution toward unregulated crypto-assets due to their potential for money laundering, fraud, and financial instability [14]. At the same time, growing interest in a possible “Digital Rupee” signals Pakistan’s intent to innovate responsibly under a sovereign framework [15]. The central question is clear: How can the law encourage digital innovation without undermining monetary sovereignty, financial stability, and public trust? Existing legal frameworks, rooted in statutes such as the *State Bank of Pakistan Act 1956*, the *Foreign Exchange Regulation Act 1947*, the *Payment Systems and Electronic Funds Transfer Act 2007*, and the *Prevention of Electronic Crimes Act 2016*, provide a valuable foundation for currency and payment regulation [16]. Yet, these laws were conceived for a physical economy, not one where money might exist purely as digital code. Critical legal issues remain unresolved, including the definition of digital legal tender, issuance authority in the digital domain, treatment of digital tokens, and the delineation of regulatory responsibilities across banking, telecom, data, and cybersecurity regimes. A future Digital Rupee would, therefore, require more than incremental reform [17]. It demands a comprehensive legal architecture that clearly defines its legal tender status, governance mechanisms, convertibility, and distribution model [18, 19]. Such a framework must embed robust standards for consumer protection, dispute resolution, operational resilience, and cybersecurity [20, 21]. Comparative experience from other jurisdictions reveals that technological readiness alone is insufficient [22]; successful CBDC implementation must rest on strong legal certainty and cross-sector coordination [23, 24]. Any move toward a Digital Rupee must preserve monetary sovereignty and align with international obligations[25]. Currency issuance is a central act of state authority; its digital extension must be explicitly authorized in law and consistent with Pakistan’s commitments under global AML/CFT and financial integrity standards. As cross-border payments accelerate, legal clarity and international compliance will be essential to maintaining trust and stability [26, 27].

So, this research examines;

- Whether Pakistan’s current legal and institutional framework can effectively support the development of a Digital Rupee.
- Identifying the regulatory gaps, statutory limitations, and policy challenges that must be addressed to enable a secure and inclusive digital monetary system.
- How Pakistan’s “cash-to-code” transition is not only an economic or technological evolution but a defining legal moment.

2. Evolution of Currency and Digital Transformation in Pakistan

Pakistan’s shift from a cash-based to a digital financial ecosystem has been the result of a long historical and institutional journey shaped by economic realities, uneven access to banking, and rapid technological change. For decades, cash was the dominant means of exchange in Pakistan, valued not



only for its convenience but also for the trust and autonomy it provided in daily commerce. However, this reliance on physical currency reinforced a large informal economy, limited transaction documentation, and constrained the state's ability to broaden the tax base and extend formal financial services. The ongoing move "from cash to code" thus represents a structural shift in how money is used, regulated, and understood within the economy. Following independence in 1947, Pakistan initially relied on monetary institutions inherited from British India. With the establishment of the State Bank of Pakistan in 1948, the state began consolidating authority over currency issuance and monetary policy (SBP, 2023). Much of the twentieth century was defined by efforts to manage physical currency, maintain confidence in the Pakistani Rupee, control inflation, and foster monetary stability (World Bank, 2019). Despite expansion in formal banking, access remained concentrated in urban centers. In rural areas, limited infrastructure, low financial literacy, and mistrust in formal institutions kept large populations excluded from the regulated banking system, sustaining a heavy reliance on cash transactions[28].

The early 2000s marked a pivotal phase with the rise of mobile connectivity and affordable internet access. Technology began reshaping consumer behavior and introduced new possibilities for financial inclusion through digital channels[29]. Branchless banking emerged as a key innovation, driven by partnerships between banks, telecom operators, and microfinance institutions. Landmark services such as Easypaisa, launched in 2009, and JazzCash soon after, enabled millions of unbanked users to send and receive money, pay bills, and conduct essential transactions via mobile phones. This digitalization played a transformative role in expanding financial access and empowerment among previously excluded communities. Pakistan's digital payments landscape entered a more mature phase with the launch of Raast in 2021, an instant payment system spearheaded by the SBP to enable real-time, low-cost transactions across banks, fintechs, and government channels (SBP, 2021). Raast's integration with public payment programs has demonstrated how national payment infrastructure can foster inclusion, transparency, and efficiency (United Nations Capital Development Fund). Since its rollout, digital retail payments have increased significantly through mobile and internet banking platforms, establishing an operational backbone for potential innovations such as a central bank digital currency (CBDC)[30]. Concurrently, Pakistan's fintech sector has accelerated digital adoption by introducing user-friendly digital wallets, peer-to-peer platforms, and merchant payment tools. In response, the SBP introduced a licensing and regulatory framework for Electronic Money Institutions (EMIs), enabling non-bank entities to issue e-money under formal oversight (SBP, 2019). This framework has encouraged innovation while guiding the gradual transition toward a "cash-lite" economy. Nonetheless, digital growth raises governance challenges, including compliance with Know Your Customer (KYC) and anti-money laundering (AML) rules, and ensuring interoperability between banks, fintechs, and public payment systems (IMF, 2023).

Despite measurable progress, public adoption of digital payments remains uneven across regions and demographics. Urban youth have embraced cashless tools faster than rural or elderly populations, who continue facing barriers such as weak connectivity, lower digital literacy, and concerns about fraud[28, 31]. The COVID-19 pandemic temporarily accelerated digital payment adoption, yet long-term success hinges on consumer education, cybersecurity, and robust grievance redress mechanisms (World Bank, 2022). Current initiatives emphasizing digital literacy and women's participation underscore that financial transformation in Pakistan is as much a social challenge as it is technological[32]. Today, Pakistan's currency evolution stands at a critical threshold[33]. The nation possesses essential building blocks, branchless banking networks, EMI frameworks, and Raast infrastructure, but moving toward a sovereign digital currency will require more than technological readiness. Legal clarity, institutional coordination, and public trust are vital foundations for sustainable digital monetary transformation (SBP, 2023). Ultimately, Pakistan's journey from cash dependency toward digital enablement reflects a deeper evolution in governance, inclusion, and the very definition of money in a digital economy.



3. The Existing Legal and Regulatory Framework in Pakistan

The existing legal and regulatory framework in Pakistan provides a partial but incomplete foundation for governing digital finance and any future move toward a digital rupee [34]. Much of the core statutory architecture was designed for a cash-dominant, bank-centric system, and has been stretched through regulations and circulars to accommodate electronic payments rather than natively digital forms of money such as CBDCs or tokenized instruments. Within this framework, four statutes are particularly important: *the State Bank of Pakistan Act, 1956*; *the Payment Systems and Electronic Funds Transfer Act, 2007*; *the Foreign Exchange Regulation Act, 1947*; and *the Prevention of Electronic Crimes Act, 2016*, alongside the evolving regulatory role of the State Bank of Pakistan (SBP) itself.

The *State Bank of Pakistan Act, 1956* establishes SBP as the central bank and vests in it the core mandate of regulating the monetary and credit system, issuing currency, and securing monetary stability in Pakistan [35]. It gives SBP the exclusive authority to issue banknotes and defines the legal tender status of currency, framing the traditional architecture of sovereign money [36]. Over time, amendments have enhanced SBP's autonomy in monetary policy and its supervisory control over the banking sector, including powers over licensing, regulation, and oversight of banks and certain financial institutions [37]. This statute forms the constitutional backbone for any future digital currency, because questions such as who may issue a digital rupee, whether it is legal tender, and how it relates to existing forms of money are ultimately grounded in the SBP Act [38]. However, the Act was drafted long before digital currencies and does not explicitly define "digital currency" or "CBDC," leaving ambiguity over whether a digital rupee could be treated as a form of "currency" under the existing provisions or whether express legislative amendments would be required [39]. In practice, SBP has relied on its general powers to issue regulatory frameworks for payment systems and fintech, but those remain secondary legislation layered onto a statute built for physical cash and conventional deposits [40]. *The Payment Systems and Electronic Funds Transfer Act, 2007* (PS&EFT Act) is the central statute governing electronic payments and payment systems in Pakistan. It provides legal recognition and regulatory machinery for payment systems, payment instruments, and electronic funds transfers, empowering SBP to designate and supervise system operators and service providers [41]. Among other things, it allows SBP to prescribe standards for the safety, efficiency, and soundness of payment systems, and to oversee the operation of systems such as real-time gross settlement and retail payment schemes. The Act also embeds important consumer-protection features: it sets obligations on financial institutions regarding information disclosure, error resolution, and liability for unauthorized or incorrect electronic transfers, and it provides customers with civil remedies against service providers in cases of negligence or non-compliance. This framework has enabled the regulated roll-out of card networks, internet banking, mobile banking, and, more recently, instant payment platforms such as Raast, which rely on SBP's authority to designate and govern system operators and payment institutions [42]. Yet, the PS&EFT Act focuses on infrastructure, mechanisms, and responsibilities around electronic transfers, not on redefining what constitutes "money" itself [42]. It treats electronic funds transfer primarily as a means of moving existing monetary balances, typically deposits, rather than as a legal category of digital sovereign currency [43]. As a result, while the Act can readily be used to regulate wallets, payment switches, and digital payment schemes, it does not resolve core conceptual questions that would arise with a CBDC, such as whether digital units issued directly by SBP are to be treated as deposits, cash equivalents, or a distinct class of legal tender [44]. Nor does it directly address tokenized assets or smart-contract-based payment mechanisms, which are increasingly relevant for modern digital currency design [45]. The Foreign Exchange Regulation Act, 1947 (FERA) is a pre-independence statute that Pakistan retained and applies to regulate dealings in foreign exchange, payments to and from non-residents, and the movement of currency and certain financial instruments across borders [46]. It empowers the federal government and SBP to impose licensing requirements, control foreign currency accounts, restrict certain cross-border payments, and regulate the import and export of currency and



bullion [47]. FERA is important in the digital context because any cross-border use of digital currency or interaction with foreign digital assets would intersect with Pakistan's exchange-control regime. However, FERA's language is rooted in traditional concepts of "currency," "securities," and "foreign exchange," and does not expressly accommodate digital tokens, crypto-assets, or cross-border digital wallets [48]. In practice, SBP has drawn on its powers under banking and foreign-exchange law to instruct banks and payment providers not to facilitate trading or settlement in cryptocurrencies and unregulated virtual assets, citing concerns around money laundering, capital flight, and consumer protection, but the statute itself does not spell out how such instruments should be classified or treated [49]. If Pakistan were to issue a CBDC with cross-border functionality, or to formally regulate stablecoins and other digital instruments linked to foreign currencies, FERA would likely require updating or interpretive clarification to ensure consistent treatment and effective AML/CFT control [50].

The Prevention of Electronic Crimes Act 2016, constitutes Pakistan's principal cyber-crime statute, criminalizing conduct such as unauthorized access to information systems, data interception, electronic fraud, electronic forgery, and offenses relating to identity and information misuse [51]. It provides law-enforcement agencies with powers to investigate, search, and seize electronic evidence and establishes penalties for a range of offenses that can target or exploit digital financial platforms, including online banking systems and payment infrastructure [52]. In the context of digital currency, PECA would be relevant to prosecuting hacking of CBDC wallets, manipulation of transaction records, phishing schemes targeting digital-wallet users, and other cyber-enabled financial crimes [53]. Its broad definitions of "information system" and "data" allow its application to financial platforms even though it is technology-neutral [54]. However, PECA is fundamentally a criminal-law instrument; it does not provide prudential standards or operational requirements for financial institutions, nor does it establish a sector-specific framework for incident reporting, resilience, or cyber-risk management in payment and currency systems [54]. Thus, while it complements financial regulation by providing sanctions against harmful conduct, it does not itself regulate how digital currency infrastructure must be designed or governed. Within this statutory landscape, the State Bank of Pakistan plays a central regulatory and policymaking role [55]. Under the SBP Act and related laws, it licenses and supervises banks, microfinance institutions, payment system operators, payment service providers, exchange companies, and, more recently, electronic money institutions (EMIs) and digital banks. SBP has issued a dedicated regulatory framework for EMIs, allowing non-bank entities to offer e-money and wallet services subject to capital, governance, and risk-management requirements. It has also published a licensing and regulatory framework for digital banks, aimed at fostering branchless, technology-driven banking models under strict prudential oversight. On the infrastructure side, SBP oversees key systems including the real-time gross settlement system and the instant payment system Raast, leveraging its PS&EFT powers to designate and regulate system operators and ensure interoperability, security, and efficiency [56]. Regarding virtual assets, SBP has taken a cautious, restrictive policy stance. Through circulars and public advisories, it has directed banks and regulated entities not to facilitate trading, custody, or settlement services for cryptocurrencies and related tokens, citing concerns over volatility, consumer risks, and potential misuse for money laundering and terrorism financing, as well as the absence of a formal legal framework for such assets. At the same time, SBP has participated in policy discussions about exploring a central bank digital currency, aligning with emerging international practice, and has signaled interest in studying CBDC models, including potential benefits for payments efficiency and financial inclusion [57]. This dual posture, promoting digitalization of regulated financial services while restricting unregulated private digital assets, reflects the tension between innovation and risk management that will shape any future legal framework for a digital rupee [58]. Despite these building blocks, the existing financial-law framework reveals several significant gaps and limitations when examined through the lens of a future digital currency system. One fundamental gap is the absence of



explicit legal definitions and categories for digital currency, CBDCs, and virtual assets in primary legislation. Neither the SBP Act nor the PS&EFT Act clearly specifies what constitutes digital legal tender, how it relates to physical currency and bank deposits, or what obligations public bodies and private parties would have to accept it in discharge of debts [59]. Without such clarity, a CBDC implementation would rely heavily on regulatory interpretation and could be vulnerable to legal challenges, especially regarding issues such as priority in insolvency, treatment under existing contract law, and interaction with tax and accounting rules. A second limitation concerns data governance, privacy, and surveillance. Large-scale digital currency systems, particularly retail CBDCs, generate granular transaction data that can be highly revealing of individuals' economic behavior. Pakistan currently lacks a comprehensive, enacted personal data protection law, although draft legislation has been proposed; existing statutes such as PECA focus on criminalizing unauthorized access or misuse rather than on proactive rules for collection, processing, retention, and sharing of financial data [60]. Any future digital currency framework will have to reconcile SBP's legitimate needs for oversight and AML/CFT compliance with constitutional and human-rights concerns about privacy and state surveillance, which are not yet fully articulated in financial legislation [61]. Third, the legal treatment of private digital assets and crypto-based instruments remains largely regulatory and policy-driven rather than statutory [62]. SBP's directions have effectively constrained the involvement of regulated entities with cryptocurrencies, but there is no specific statute that categorizes virtual assets, sets licensing requirements for virtual asset service providers, or defines their relationship to existing categories such as "securities" or "commodities." This can create legal uncertainty, especially in light of evolving international standards such as those issued by the FATF, which expect jurisdictions to establish clear regulatory regimes for virtual assets and associated service providers [63]. A fourth gap lies in the framework's limited adaptation to programmable money, smart contracts, and decentralized infrastructures. The PS&EFT Act contemplates centralized operators and service providers and assigns them responsibilities for ensuring accuracy, security, and reversals, but it does not expressly address complex arrangements where transactions are executed automatically based on code, or where decentralized validators share responsibility. Questions about liability allocation, dispute resolution, error correction, and legal finality of transactions in such environments would need more tailored statutory treatment if Pakistan were to adopt advanced digital currency features. Fifth, cross-border dimensions of digital currency are insufficiently captured by FERA's traditional categories. If Pakistani residents were to hold foreign CBDCs or stablecoins, or if a Pakistani CBDC were used abroad, complex questions would arise about exchange control, capital-account management, and cross-border AML/CFT supervision that FERA, in its current form, only partially addresses. Addressing these cross-border aspects is crucial not only for financial stability but also for maintaining correspondent-banking relationships and compliance with global standards. Finally, existing coordination mechanisms among SBP, SECP, FBR, and cyber-crime and data-protection authorities have not yet been fully re-engineered for a digital-currency environment that cuts across monetary law, securities regulation, cyber-security, taxation, and consumer protection [64]. Fragmented mandates may lead to regulatory overlaps, inconsistencies, or gaps when dealing with complex digital products that span payments, investment features, and data processing [65]. An effective legal framework for digital currency will require clearer allocation of responsibilities, formal coordination channels, and possibly new institutional arrangements or joint regulatory bodies. Overall, Pakistan's current legal and regulatory framework is robust enough to support incremental digitalization of payments and the growth of regulated digital financial services, but it remains incomplete for a fully fledged digital currency ecosystem. The move "from cash to code" will therefore demand a deliberate legislative agenda: clarifying the legal nature of digital sovereign money, updating exchange-control and payment laws, embedding privacy and data-governance safeguards, designing statutory regimes for virtual assets, and strengthening inter-agency coordination. Without these reforms, any CBDC or comprehensive digital



currency framework would rest on a legal foundation that is functional but not fully fit for purpose in the new monetary era [66].

4. Legal Challenges in the Digital Currency Ecosystem

Digital currency creates legal pressure because most financial laws were written for a world of physical cash, paper instruments, and bank-centred transactions [67]. Code-based money operates through apps, networks, and automated systems that do not fit neatly into older legal categories [68]. In Pakistan, the challenge is sharper because digital payments are growing fast, yet primary legislation has not fully caught up with CBDCs, private digital assets, and programmable payment tools. As a result, uncertainty appears at the points where law normally provides clarity: definitions, jurisdiction, privacy, consumer rights, and liability [69].

4.1 Ambiguities in legal definition and status

The first and most basic problem is definitional. Many legal systems, including Pakistan's, do not clearly define "digital currency," "virtual assets," or "CBDC" in primary statutes [70]. Monetary law still tends to describe "currency" and "legal tender" with reference to notes and coins, while electronic payment laws focus on moving balances rather than creating a new form of sovereign money. This creates uncertainty about how a future Digital Rupee would be treated in law: is it the same as cash, a new category of legal tender, or simply another electronic value instrument? These questions matter because legal status affects contracts, discharge of debts, insolvency priority, taxation, and accounting treatment. For private digital assets, the classification problem is even more complex [71]. A cryptocurrency or stablecoin may be treated as a commodity, a security, a payment instrument, or a sui generis asset, each label triggering different licensing duties, investor disclosures, and consumer safeguards. Where statutes are silent, regulators often rely on circulars or case-by-case decisions. That approach can discourage responsible innovation, while leaving enough "grey space" for unregulated actors to operate. It also places courts in a difficult position when disputes arise over ownership, collateral enforcement, fraud recovery, or the legal effect of smart-contract obligations [72].

4.2 Jurisdictional and enforcement challenges

Digital currency systems routinely operate across borders. Users may be in one country, service providers in another, and infrastructure (servers, nodes, cloud services) scattered globally. This reality complicates jurisdiction, applicable law, and enforcement [73]. Traditional conflict-of-laws tools, such as the place of contracting, performance, or location of assets, are harder to apply when assets exist as entries on ledgers accessible from anywhere. For regulators and law enforcement agencies, cross-border structure creates practical limits. A wallet provider or exchange may serve Pakistani users through an app without being locally licensed. Authorities may struggle to compel compliance, obtain records, freeze assets, or enforce sanctions. International cooperation mechanisms exist, but they often move slowly compared to the speed of digital transactions, and they are poorly suited to decentralized systems with no identifiable operator. This gap can be exploited for fraud, money laundering, or sanctions evasion through "jurisdiction shopping." Even in a CBDC context, cross-border use raises difficult questions. If non-residents can hold or transact in a Digital Rupee, Pakistan would need clear rules on court jurisdiction, regulatory cooperation, and exchange-control treatment, areas where traditional foreign exchange laws were not drafted with digital units in mind [74].

4.3 Data protection and privacy issues

Digital currency systems generate detailed transactional data that may be more granular than ordinary banking records. In a retail CBDC, particularly an account-based model, transaction trails can reveal personal patterns of spending, location, and lifestyle [75]. This creates a legal balancing task: enabling AML/CFT compliance and financial oversight without turning digital money into a tool of excessive surveillance. In many developing jurisdictions, including Pakistan, data protection regimes remain incomplete or unevenly enforced. Where clear rules are missing, individuals may not know who can



access their transaction data, for what purpose, and for how long. If the legal framework allows broad access without oversight, adoption may weaken due to fear of monitoring [76]. If privacy is designed too strongly without risk controls, it may conflict with FATF expectations and weaken AML/CFT enforcement. Another layer concerns data localization and cross-border data flows: when digital currency platforms use foreign cloud infrastructure, questions arise about which laws apply, how regulators can access data, and what remedies exist if data is misused or leaked. Without clear statutory safeguards, trust, the currency of digital finance can erode quickly [77].

4.4 Consumer rights and dispute resolution mechanisms

Digital currency ecosystems challenge consumer protection because users often interact with apps, wallets, and automated processes rather than traditional bank branches [77]. Funds may be stored in wallet structures instead of bank accounts, and transactions may involve multiple intermediaries like banks, EMIs, payment switches, technology vendors, and sometimes smart-contract code. When something goes wrong unauthorized transfers, system outages, mistaken payments, or fraud, the question becomes: who is legally responsible, and what remedy does the user have? Existing electronic transfer rules offer a starting point, but they were not drafted for complex digital value chains or self-executing transactions. Smart contracts create a particularly difficult problem: if a transfer occurs due to faulty code, an oracle error, or an automated trigger, the law may not clearly allocate loss between developer, platform, intermediary, and user. Cross-border services complicate matters further because platforms may be licensed under foreign standards or not effectively supervised at all. For a CBDC, policymakers must decide how far statutory protections will go, whether certain losses are guaranteed, how mistaken or fraudulent transfers will be handled, and which forum (courts, ombudsman, arbitration, specialized tribunals) will provide accessible and timely dispute resolution [78].

4.5 Cybersecurity threats and liability concerns

Because digital currency systems rely on information infrastructure, cybersecurity is not a side issue—it is a core legal risk. Threats include hacking of wallets, phishing and identity theft, malware targeting user devices, insider abuse, denial-of-service attacks, and vendor-chain vulnerabilities [79]. A major incident can undermine confidence in payments and, at worst, affect financial stability. Pakistan’s cybercrime law provides tools to punish attackers, but criminal law alone does not create a prevention framework. It does not set minimum resilience standards, define institutional duties, or clearly allocate liability when breaches occur. This leaves urgent legal questions open: What cybersecurity standards must intermediaries meet? Who compensates users when losses result from weak safeguards or third-party failures? In a CBDC system, how will responsibility be shared between the SBP, banks, EMIs, and technology providers? If liability rules are weak, providers may underinvest in security; if rules are overly strict, they may avoid participation or innovation. A credible framework therefore needs clear standards for resilience, mandatory incident reporting, audit requirements, compensation rules where fault exists, and viable insurance or guarantee mechanisms, supported by cooperation with international best practices because cyber risks do not respect borders.

4.6 Overall implications

These challenges show that digital currency is not simply an “upgrade” of payments. It is a structural change that tests the boundaries of monetary law, private law, criminal enforcement, and data governance. If the legal system remains unclear on status, jurisdiction, privacy, consumer protection, and cybersecurity liability, digital currency initiatives may struggle to earn trust, withstand disputes, or deter misuse. For Pakistan, the solution cannot be purely reactive or circular-based. It requires proactive legislative reform, clear regulatory mandates, and coordinated institutional strategy so that the move from cash to code strengthens, rather than destabilizes, the legal order around money [80].

5. CBDC and Its Legal Implications



A CBDC sits at the centre of Pakistan’s debate on how to modernize money while protecting monetary stability and legal certainty [81]. A Digital Rupee would not be merely a new payment service; it would be a new form of sovereign money issued under state authority. That makes it legally different from wallets, EMIs, or private tokens, and it means its legitimacy must be anchored in clear law [82]. If designed and governed properly, a Digital Rupee can strengthen inclusion and efficiency. If launched without statutory clarity and safeguards, it can trigger uncertainty, litigation, and loss of public confidence in the rupee itself. The policy case for a Digital Rupee typically rests on five connected objectives: expanding financial inclusion, improving payment efficiency, reducing cash handling costs and informality, strengthening monetary policy transmission, and responding strategically to private digital assets and foreign CBDCs. Pakistan still has a large unbanked and underbanked population, and a retail CBDC could offer a low-cost, risk-free payment option backed directly by the SBP, especially if designed with tiered wallets and simplified onboarding for low-risk users. A Digital Rupee could also support instant settlement at low cost, complementing national infrastructure such as Raast and strengthening e-commerce and government-to-person transfers [83]. Over time, digital money can reduce the fiscal burden of printing, transporting, and securing cash, while also curbing counterfeiting and improving transparency in financial flows, provided privacy safeguards are strong enough to sustain trust. A CBDC may further improve monetary policy monitoring by providing more timely aggregate data and, depending on design, potentially offering new tools for targeted interventions, though interest-bearing or programmable features raise sensitive legal and political questions. Finally, a Digital Rupee can protect monetary sovereignty by offering a regulated alternative if unregulated crypto-assets, stablecoins, or foreign CBDCs begin to substitute for the rupee in domestic transactions [84].

Because a CBDC changes the form of state money, it requires a firm legal foundation for issuance authority, legal tender status, and user rights. In Pakistan, this inevitably engages the SBP Act and the legal meaning of “legal tender.” The law would need to expressly define the Digital Rupee as a central bank liability, clarify SBP’s exclusive authority to issue and redeem it, and specify its relationship with physical rupees and bank deposits, including convertibility and redemption rights. Without explicit statutory backing, a Digital Rupee could face uncertainty in contractual disputes, insolvency scenarios, and questions about whether public or private actors must accept it as payment [85]. Clear legislation would also protect monetary sovereignty by affirming that rupee-denominated digital legal tender remains a state monopoly even when money becomes code. Legal implications also flow from governance choices. Pakistan would need to adopt a workable operating model: a direct CBDC (SBP provides wallets/accounts), an intermediated model (banks/EMIs distribute wallets under SBP oversight), or a hybrid model (SBP runs the core ledger while intermediaries provide customer-facing services). Intermediated or hybrid models are generally more consistent with maintaining the role of banks and avoiding sudden disintermediation [85]. Whatever model is chosen, the legal framework must allocate responsibilities and liabilities clearly across SBP, intermediaries, and technology providers, covering KYC/AML duties, cybersecurity standards, dispute handling, error correction, and operational resilience [86].

Cross-border functionality introduces further legal risk. If the Digital Rupee can be held by non-residents or used abroad, exchange control, capital flow management, and external stability concerns arise [87]. Pakistan’s foreign exchange rules would need modernization to address offshore wallet use, conversion rules, holding limits, and reporting obligations [82]. Without such provisions, digital channels could increase capital flight risks or open enforcement gaps. Finally, CBDC design has constitutional and rights implications. The level of traceability and programmability determines how much the state can observe or influence private transactions. CBDC law must therefore balance legitimate oversight needs with privacy, due process, and property protections, supported by clear limits, oversight mechanisms, and remedies.



International experience reinforces these lessons. China's e-CNY shows the value of explicit statutory backing and centralized governance, while also raising warnings about surveillance if privacy safeguards are weak [88]. The EU's Digital Euro approach highlights the importance of rights-based design, institutional coordination, and legal safeguards to protect stability and avoid crowding out private payments [88]. Nigeria's eNaira demonstrates that even with a legal basis, adoption depends on public trust, clear communication, and smooth user experience especially in developing contexts [89]. Across models, the common thread is clear: CBDC works best when law and design move together, providing legal legitimacy, predictable governance, and enforceable protections.

6. International Regulatory Standards and Compliance

International standards shape Pakistan's choices because digital currencies move quickly across borders and can affect correspondent banking, market access, and reputational standing. Any credible Digital Rupee framework must align with FATF expectations, cross-border payments work led by BIS/CPMI and the IMF, and the emerging global principles on CBDC legal soundness and financial stability [34]. These standards do not remove Pakistan's policy discretion, but they set boundaries for what is internationally acceptable particularly on supervision, transparency, and risk controls.

6.1 FATF, AML/CFT, and data protection

FATF sets the global baseline for AML/CFT, including rules for virtual assets and virtual asset service providers (VASPs). Its guidance expects countries to identify risks, license or register relevant service providers, supervise them, and enforce core duties such as customer due diligence, recordkeeping, and suspicious transaction reporting [34]. FATF also emphasizes the "travel rule," requiring originator and beneficiary information to accompany transfers, and extends attention to stablecoins and peer-to-peer risks. Pakistan's exit from the FATF grey list reflects strengthened AML/CFT systems, but it also means Pakistan must ensure that digital currency design does not reopen risk channels, such as anonymous large-value transfers or weak intermediary controls [90]. Data protection is closely linked to AML/CFT because compliance requires processing sensitive identity and transaction information. International practice is moving toward a balance: enabling necessary monitoring while restricting access, limiting retention, strengthening security, and ensuring proportionality. For Pakistan, this requires clear rules on who can access CBDC transaction data, under what legal authority, and subject to which oversight and remedies, so that AML/CFT objectives are met without creating unchecked surveillance risks [91].

6.2 Cross-border payments, FX control, and CBDC

CBDCs are increasingly discussed in global work on improving cross-border payments, particularly under BIS/CPMI and IMF initiatives. These bodies note that CBDCs can reduce cost and settlement delays, but only if systems are designed for interoperability and backed by strong governance and legal coordination [92]. "Multi-CBDC" models ranging from compatible domestic systems to shared platforms, raise complex legal issues such as settlement finality, applicable law, access criteria, data sharing, and dispute resolution across jurisdictions. For Pakistan, cross-border design matters because remittances and trade flows are central to the economy. A Digital Rupee that can integrate safely into cross-border channels could improve speed and cost, but it would also require exchange-control modernization. Traditional statutes like the Foreign Exchange Regulation Act were not written for foreign CBDCs or offshore digital wallets. International guidance suggests that if non-residents can hold CBDC or cross-border transfers become frictionless, states must reassess capital flow tools, consider holding limits, and ensure consistent treatment of digital and traditional instruments for balance of payments and FX reporting. Without alignment, cross-border digital channels could undermine capital account policies or enable opaque outflows [93].

6.3 Alignment with IMF/BIS policy standards

The IMF and BIS stress that CBDCs must be legally sound, financially stable, and internationally cooperative. A clear legal foundation is treated as non-negotiable: the law must identify CBDC as a



central bank liability, clarify legal tender status where intended, and define the rights and duties of users and intermediaries [94]. These bodies also warn that poorly designed CBDCs can destabilize bank funding, accelerate run[95]s, or weaken monetary policy if users can move at speed from deposits into central bank money without safeguards. In cross-border contexts, IMF/BIS work emphasizes respect for monetary sovereignty and warnings against unintended currency substitution, particularly for smaller or developing economies. Legal frameworks are therefore expected to include tools such as tiered access, holding caps for non-residents, and cooperation agreements that specify applicable law, data sharing, and crisis protocols. For Pakistan, alignment implies designing the Digital Rupee within amended central banking and payments law, embedding stability protections, and handling cross-border use through structured agreements rather than unregulated market expansion [96].

6.4 Overall compliance implications for Pakistan

International standards create both discipline and opportunity [97]. FATF rules constrain anonymity and demand strong intermediary supervision; IMF/BIS principles require legal clarity and stability safeguards; cross-border payment standards push interoperability and governance. Pakistan's strengthened AML/CFT regime provides a strong base, but compliance will require translating standards into enforceable domestic rules. For a Digital Rupee, this means embedding FATF-consistent controls for intermediaries and any licensed VASPs, modernizing foreign exchange and payments legislation to cover digital flows, aligning data governance with privacy safeguards, and ensuring cross-border features comply with settlement finality and cooperation principles [98]. A Digital Rupee built on these standards is more likely to be trusted domestically and accepted internationally [95].

7. Ethical, Socio-Economic, and Inclusion Dimensions

Digital money changes not only how people pay, but also who can participate safely and effectively in the financial system. In Pakistan, where inequalities in income, gender, geography, and literacy already shape access to banking and technology, inclusion is not a side benefit, it is a core test of legitimacy. Digital finance has expanded access through mobile wallets and branchless banking, reducing travel costs and lowering barriers for small transactions [99]. A Digital Rupee could deepen this progress by offering low-cost state-backed value, integrating with social protection payments, and supporting tiered wallets that bring excluded users into formal channels. But without careful design, a “digital by default” approach can widen inequality and expose vulnerable groups to new risks. Gender remains a critical fault line. Women are less likely to own phones, control SIM registration, or hold independent accounts, and social norms can limit their digital autonomy. If digital currency assumes personal device ownership and independent credentials, women may be pushed into dependence on male relatives or informal intermediaries, reducing control over their own funds. Rural communities face similar structural barriers: weaker connectivity, fewer agents, limited merchant acceptance, and lower digital literacy. For these groups, cash may remain more practical unless legal and policy measures actively close access gaps. The risk is that the benefits of digitalization concentrate in cities while rural areas remain excluded or become dependent on informal “helpers” who charge fees and create exploitation risks [100].

Digital literacy is another determinant of fairness [101]. The shift from cash to code creates a divide between users who can navigate apps and protect credentials and those who cannot. Low literacy users, the elderly, people with disabilities, and remote communities face higher exposure to scams, coercion, and social engineering [102]. They also face practical barriers when disputes occur: where to complain, how to prove unauthorized transfers, and how to secure timely reversal or compensation. Economic inequality compounds these issues, as poorer users may share devices, switch off data to save costs, or rely heavily on agents, reducing privacy and increasing vulnerability [103]. These realities mean that digital currency does not automatically empower; empowerment depends on rights-based legal safeguards. Inclusive legal and policy approaches must therefore be built into the framework. Law should preserve meaningful choice, including continued cash use and non-smartphone access channels



during a long transition. Tiered KYC and risk-based onboarding should be legally supported so low-risk wallets can be opened more easily while higher tiers carry stronger AML/CFT controls. Consumer protection rules should be updated for wallet-based environments, requiring clear disclosures in plain language, fee transparency, accessible confirmations (SMS/voice), time-bound complaint handling, and compensation where provider fault exists. Privacy and data minimization principles should limit unnecessary collection and sharing, with special care for shared device contexts. Accessibility requirements should ensure interfaces work for disabilities and low-literacy users. Agent regulation is essential because agents remain the main access point in many areas; conduct rules, fee display obligations, and shared institutional liability are needed so users are not left without recourse. Finally, social protection integration should prioritize beneficiary control, especially for women, so that digital payments strengthen autonomy rather than enable capture by third parties [104]. Participation and oversight matter too: consultation with civil society and consumer groups, and independent ombudsman mechanisms, can improve trust and accountability. In Pakistan's case, inclusion is the bridge between technical feasibility and public legitimacy [105].

8. Policy Recommendations and Legal Reform Agenda

Pakistan requires a coherent reform agenda to move from incremental digitization toward a legally grounded digital currency regime [106]. The objective should be to integrate a future Digital Rupee into the monetary system without undermining stability, rights, or innovation, while closing the gaps that current statutes and regulatory practice leave exposed. Reform should focus on legal clarity, institutional capacity, and coordinated governance so that digital finance evolves within predictable, enforceable rules. A first pillar is targeted amendment of core monetary and payments laws. The State Bank of Pakistan Act should be updated to define the "Digital Rupee" as a central bank liability and, where intended, as legal tender alongside notes and coins [107]. It should clarify issuance and redemption authority, convertibility with physical rupees, and the state monopoly over rupee-denominated digital legal tender. The Payment Systems and Electronic Funds Transfer Act should be modernized to explicitly cover CBDC wallets, tokenized payment instruments, and smart-contract settlement features, while strengthening liability rules for multi-party digital value chains and automated errors. Foreign exchange law should be revised to address cross-border holdings and transfers of Digital Rupee units, foreign CBDCs, and stablecoins, including clear rules for non-resident access, offshore wallets, conversion, reporting, and capital flow limits. These changes would reduce uncertainty for remittances, trade, and cross-border fintech services while protecting external stability [108].

Beyond amendments, Pakistan would benefit from a dedicated Digital Currency and Virtual Assets Act to bring coherence and transparency to the regulation of both sovereign and private digital instruments. Such legislation could define categories (CBDC, stablecoins, other crypto-assets), set licensing and conduct rules for intermediaries and VASPs, establish prudential and governance requirements for digital currency infrastructure, and integrate consumer protection, AML/CFT duties, and cybersecurity obligations into a single statutory scheme rather than scattered circulars. This would move Pakistan from ad hoc restriction toward predictable, enforceable regulation that can deter misuse while enabling lawful innovation [109].

Legal reform must also strengthen institutions and coordination mechanisms [110]. Within the SBP, specialized capacity on digital currency, data governance, and cyber risk should be resourced with clear mandates [111]. Regulatory sandboxes and pilots should be formalized with explicit authority to admit firms, impose conditions, and grant time-bound waivers within defined limits [112]. CBDC pilots should have legally clear status, participant rights, and liability rules so that testing does not create confusion about whether pilot units are "real money." Inter-agency coordination should be institutionalized through a Digital Finance and Currency Coordination Council involving SBP, SECP, FBR, consumer and competition bodies, cybercrime agencies, and data protection authorities. Its role



should include harmonizing overlapping rules, sharing supervisory information, and coordinating systemic incident responses, with regular public reporting to build confidence. Judicial and professional capacity building is also necessary: courts will be asked to interpret new categories of money, resolve disputes involving smart contracts and wallets, and allocate liability after cyber incidents. Training programs, guidance materials, and potentially specialized benches or tribunals can improve consistency and competence in fintech dispute resolution [113].

To guide drafting, Pakistan can adopt clear legislative principles that translate into model clauses [114]. A legal certainty clause should declare the Digital Rupee as a form of currency issued by SBP and, where intended, legal tender equivalent in value to physical rupees. A state monopoly clause should prohibit any private actor from issuing rupee-denominated digital instruments claiming legal tender status, supported by penalties for counterfeit or unauthorized issuance. Intermediated distribution clauses should authorize SBP to designate licensed banks and EMIs as intermediaries and permit tiered wallet categories with proportionate KYC, balance caps, and risk-based functionality [115]. Data governance clauses should restrict CBDC data processing to necessary purposes, impose minimization and retention limits, and require oversight safeguards for access to detailed individual records. Consumer protection clauses should impose duties of fair treatment, transparent fees, accessible disclosures, time-bound complaint resolution, and compensation rules for unauthorized or erroneous transfers caused by provider fault or system failure. Cybersecurity and resilience clauses should mandate minimum standards, independent audits where appropriate, and incident reporting obligations, alongside clear sanctions for non-compliance. Cross-border clauses should empower SBP to permit or restrict non-resident access and cross-border use consistent with FX and capital flow policy. Finally, technology-neutral drafting should ensure the law does not lock Pakistan into a specific platform, while still requiring security, reliability, and verifiability standards. Taken together, these reforms provide a realistic legal pathway for Pakistan's transition from cash to code [116]. By updating foundational statutes, enacting focused digital currency legislation, strengthening institutions, and embedding rights-based safeguards, Pakistan can create a Digital Rupee framework that supports innovation and inclusion while protecting sovereignty and stability [117].

9. Conclusion

Pakistan's transition from cash to code is a defining change in its monetary and legal architecture. While existing laws support the digitization of payments, they do not yet provide a complete framework for CBDCs, digital legal tender, or the governance of virtual assets. Key legal risks, uncertain definitions, cross-border enforcement gaps, privacy and data governance weaknesses, consumer protection limitations, cybersecurity exposure, and incomplete alignment with international standards, must be addressed if Pakistan is to avoid regulatory fragmentation and loss of public trust. Global experience shows that successful digital currency projects are grounded in explicit statutory authority, credible governance, and rights-sensitive safeguards. A Digital Rupee can strengthen inclusion, reduce cash-handling costs, and enhance payment efficiency, but only if the SBP's issuance authority and the currency's legal status are clearly defined, intermediaries are properly regulated, and privacy and consumer rights are protected. With a coherent legislative agenda, structured pilots, and strong institutional coordination, Pakistan can build a hybrid regime where sovereign digital money coexists with regulated private innovation turning "cash to code" into a legally secure path toward inclusive growth and digital sovereignty.

References

1. Rizvi, S.K.A., B. Naqvi, and F. Tanveer, *Is Pakistan ready to embrace Fintech innovation?* 2018.
2. Siddik, M.N.A. and S. Kabiraj, *Digital finance for financial inclusion and inclusive growth*, in *Digital transformation in business and society: Theory and cases*. 2019, Springer. p. 155-168.
3. Javed, M. and W. Zhuquan, *Analysis of accounting reforms in the public sector of Pakistan and adoption of cash basis IPSAS*. *Universal Journal of Accounting and Finance*, 2018. **6**(2): p. 47-53.



4. Garnaut, R., *Macro-economic implications of the turning point*. China Economic Journal, 2010. **3**(2): p. 181-190.
5. Afzal, J., *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.
6. Hanif, M.N., *Restructuring of financial sector in Pakistan*. 2002.
7. Mughal, K.S. and F.G. Schneider, *How informal sector affects the formal economy in Pakistan? A lesson for developing countries*. South Asian Journal of Macroeconomics and Public Finance, 2020. **9**(1): p. 7-21.
8. Adelaja, A.O., et al., *Advancing financial inclusion through fintech: Solutions for unbanked and underbanked populations*. World Journal of Advanced Research and Reviews, 2024. **23**(01): p. 427-438.
9. Bokhari, H. *Digital financial inclusion of the informal sector: the case of Raast Platform in Pakistan*. in *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*. 2022.
10. Nesse, P.J., et al. *Growth of mobile financial services key learnings from literature, industry analysis and cases. in 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. 2017. IEEE.
11. Belke, A. and E. Beretta, *From cash to central bank digital currencies and cryptocurrencies: a balancing act between modernity and monetary stability*. Journal of Economic Studies, 2020. **47**(4): p. 911-938.
12. Dow, S., *Monetary reform, central banks, and digital currencies*. International Journal of Political Economy, 2019. **48**(2): p. 153-173.
13. Afzal, J., *Globalization of Economy and Regulatory Laws of Digital Currency*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 113-124.
14. Meighan, S.J., *The Regulation of Crypto-assets for Anti-Money Laundering*. 2024.
15. Ghauri, B.S.U., G.R. Nafees, and S.A. Anwer, *Navigating Socio Economic and Security Challenges: An exploration of Central Bank Digital Currency (CBDC) Implementation in Pakistan*. Journal of Indian Studies, 2024. **10**(1): p. 49-76.
16. Akhtar, S., *Assessing the Cybercrime Legislation in Pakistan: a Comparative Study of European Union and Pakistani Cybercrime Laws*. Available at SSRN 4555751, 2023.
17. Manzoor, R., et al., *Digital financial services in Pakistan: opportunities, challenges and suggestions*. J Financ Econ, 2021. **6**(2): p. 1-6.
18. Feichtner, I., *Public Law's Rationalization of the Legal Architecture of Money: What Might Legal Analysis of Money Become?* German Law Journal, 2016. **17**(5): p. 875-906.
19. Afzal, J., *Decentralized Currencies and Digital Economy: Stability and Implications of Digital Currency*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 97-112.
20. Ballaji, N., *Consumer Protection in the Era of Digital Payments: Legal Challenges and Solutions*. Beijing L. Rev., 2024. **15**: p. 1268.
21. Afzal, J., *Digital Security Legislation Trends to Facilitate Digital Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 53-64.
22. Bruno, I., et al. *Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services*. in *Proceedings of the 13th international conference on theory and practice of electronic governance*. 2020.
23. Rachmad, Y.E., *Global Regulations for CBDC: Bridging Uniformity in International Policy*. The United Nations and the Nobel Peace Prize Awards, 2025.
24. Afzal, J., *Potential of International Law and Digital Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 147-166.
25. Afzal, J., *International Law and the Globalization of the Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 1-18.
26. Zetsche, D.A., et al., *DLT-based enhancement of cross-border payment efficiency—a legal and regulatory perspective*. Law and Financial Markets Review, 2021. **15**(1-2): p. 70-115.
27. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024: Springer.
28. Akbar, F., et al., *The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis*. International Journal of Discovery in Social Sciences, 2025. **1**(1).
29. Gabor, D. and S. Brooks, *The digital revolution in financial inclusion: international development in the fintech era*, in *Material cultures of financialisation*. 2020, Routledge. p. 69-82.
30. Afzal, J., *International Law and Emerging Economic Issues*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 79-95.
31. Afzal, J., et al., *Review of various Aspects of Digital Violence*. Journal of Engineering, Science and Technological Trends, 2024. **1**(2).



32. Javed, A., M.Z. Ashraf, and S. Shahbaz, *Digital Transformation and Its Influence on Women's Economic Empowerment in Pakistan*. Sustainable Futures, 2025. **10**: p. 101092.
33. Jalil, A. and H. Hina, *Monetary Policy Crafting a Path for Pakistan's Economic Stability*. 2024: Pakistan Institute of Development Economics.
34. Khan, R.U., K. Ullah, and M. Atiq, *Regulatory constraints, responsibilities and consultation (CRC) for legal institutionalization of cryptocurrencies in Pakistan*. Qualitative Research in Financial Markets, 2024. **16**(4): p. 680-708.
35. Arby, M.F., *State Bank of Pakistan: Evolution, functions and organization*. 2004.
36. Huber, J., *Modern Money and Sovereign Currency*. Real-world Economics Review, 2014. **66**: p. 38-57.
37. Javed, S.A., *First Response to the SBP Amendment Act 2021*. 2021.
38. Alexander, K., *The european central bank and banking supervision: The regulatory limits of the single supervisory mechanism*. European Company and Financial Law Review, 2016. **13**(3): p. 467-494.
39. Dordevic, L., et al., *Strengthening bank regulation and supervision: National progress and gaps*. 2021, International Monetary Fund.
40. Chaudhuri, R. and Graber, *Central Bank Independence, Regulations, and Monetary Policy*. 2018: Springer.
41. Shahin, W. and E. El-Achkar, *Banking and monetary policies in a changing financial environment: A regulatory approach*. 2016: Routledge.
42. Hossain, A.A., *Central banking and monetary policy in the Asia-Pacific*, in *Central Banking and Monetary Policy in the Asia-Pacific*. 2009, Edward Elgar Publishing.
43. Ricks, M., *Money as infrastructure*. Colum. Bus. L. Rev., 2018: p. 757.
44. Goldfinger, C., *Intangible economy and electronic money*. The future of money, 2002: p. 87-122.
45. Helleiner, E., *Electronic money: a challenge to the sovereign state?* Journal of international affairs, 1998: p. 387-409.
46. Brunnermeier, M.K., H. James, and J.-P. Landau, *The digitalization of money*. 2019, National Bureau of Economic Research.
47. Caliskan, K., *Data money: The socio-technical infrastructure of cryptocurrency blockchains*. Economy and Society, 2020. **49**(4): p. 540-561.
48. Melecky, M., *Choosing The Currency Structure Of Foreign-Currency Debt: A Review Of Policy Approaches*. Journal of International Development, 2012. **24**(2): p. 133-151.
49. Eichengreen, B. and D.J. Mathieson, *The Currency Composition of Foreign Exchange Reserves Retrospect and Prospect*. 2000.
50. Thimann, C., *Global roles of currencies*. International Finance, 2008. **11**(3): p. 211-245.
51. Ahmad, W., U. Asghar, and M. Afzal, *An analysis of the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan: Challenges and recommendations*. Research Consortium Archive, 2025. **3**(2): p. 836-852.
52. Akhlaq, M., *Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan*. PCL Student Journal of Law, 2021. **5**(1): p. 30-66.
53. Arshad Khan, E., *The prevention of electronic crimes act 2016: An analysis*. LUMS LJ, 2018. **5**: p. 117.
54. Haq, I.U. and S.M. Zarkoon, *Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan*. Pakistan's Multidisciplinary Journal for Arts & Science, 2023: p. 43–62-43–62.
55. Aleem, Y., M. Asif, and M.U. Ashraf, *The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan*. Ilkogretim Online, 2021. **20**(2).
56. Mehmood, M., *The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan*. Annals of Human and Social Sciences, 2025. **6**(1): p. 35-44.
57. Aziz, B. and S.H. Bhatti, *Securing the Cyberspace for E-Commerce Industry of Pakistan: A Consumer Protection Perspective*. Journal of Law & Social Studies (JLSS), 2023. **5**(1): p. 30-41.
58. Fehr, C., C. LiCalzi, and T. Oates, *Computer crimes*. Am. Crim. L. Rev., 2016. **53**: p. 977.
59. CRIME, F.A.C. and C. LAW, *BORBA PROTIV CYBER KRIMINALA: KRIVIČNOPRAVNI I KRIMINALISTIČKI ASPEKT*.
60. Batool, S., et al., *Good governance via E-Governance: moving towards digitalization for a digital economy*. Review of applied management and social sciences, 2021. **4**(4): p. 823-836.
61. Taylor, N., *State surveillance and the right to privacy*. Surveillance & Society, 2002. **1**(1): p. 66-85.
62. Ferreira, A. and P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*. Computer Law & Security Review, 2021. **43**: p. 105632.
63. Jovanić, T. *An overview of regulatory strategies on crypto-asset regulation-challenges for financial regulators in the Western Balkans*. in Tatjana Jovanić, *An Overview of Regulatory Strategies on Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans*, in: *EU Financial*



- Regulation and Markets-Beyond Fragmentation and Differentiation (Eds. I. Bajakić, M. Božina Beroš), Conference Proceedings, Zagreb. 2020.*
64. Iqbal, F., et al., *The dual impact of digital currencies on economy and environment: Insights into the role of monetary control*. International Journal of Business and Economic Affairs, 2024. **9**(4): p. 22-44.
 65. Putrevu, J. and C. Mertzanis, *The adoption of digital payments in emerging economies: challenges and policy responses*. Digital Policy, Regulation and Governance, 2024. **26**(5): p. 476-500.
 66. Matsuura, J.H., *Digital Currency: An International Legal and Regulatory Compliance Guide*. 2016: Bentham Science Publishers.
 67. Monye, O.F., *Rethinking the legal and institutional framework for digital financial inclusion in Nigeria*. 2021.
 68. Stracca, L., *Digitalization Comes to Money*, in *Redefining the Monetary Standard in the Digital Age: Digital Innovations and the Future of Monetary Policy*. 2025, Springer. p. 55-98.
 69. Ganne, E., *Can Blockchain revolutionize international trade?* 2018: World Trade Organization Geneva.
 70. Hrytsai, S., *The place of virtual assets in the structure of digital financial technology*. International Science Journal of Management, Economics & Finance, 2022. **1**(3): p. 34-48.
 71. Wendehorst, C., *Proprietary rights in digital assets and the conflict of laws*, in *Blockchain and Private International Law*. 2023, Brill Nijhoff. p. 101-127.
 72. Muradyan, S.V., *Digital assets: Legal regulation and estimation of risks*. Journal of Digital Technologies and Law, 2023. **1**(1).
 73. Geva, B. and M. Muraj, *The Digitization of Money: Stablecoins and CBDC*. Banking & Finance Law Review, vol. 40, no. 1, 2024, pp. 115-141., 2023.
 74. Zatti, F. and R.G. Barresi, *Digital assets and the law: Fiat money in the era of digital currency*. 2024: Taylor & Francis.
 75. Gruschka, N., et al. *Privacy issues and data protection in big data: a case study analysis under GDPR*. in *2018 IEEE international conference on big data (big data)*. 2018. IEEE.
 76. Changchit, C., *Data protection and privacy issue*. Journal of Information Privacy and security, 2008. **4**(3): p. 1-2.
 77. Bygrave, L.A., *Privacy and data protection in an international perspective*. Scandinavian studies in law, 2010. **56**(8): p. 165-200.
 78. Cortés, P., *Online dispute resolution for consumers in the European Union*. 2010: Taylor & Francis.
 79. Shad, M.R., *Cyber threat landscape and readiness challenge of Pakistan*. Strategic Studies, 2019. **39**(1): p. 1-19.
 80. Saleem, B., et al., *A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap*. International Cybersecurity Law Review, 2024. **5**(4): p. 533-561.
 81. Mu, Y. and A. Mu, *CBDC: Concepts, benefits, risks, design, and implications*. Benefits, Risks, Design, and Implications (October 1, 2022), 2022.
 82. Hassan, A., S.S. Rao, and B. Amjad, *Risk Factors of Criminal Recidivism into Criminal Activities*. Global Legal Studies Review, 2023. **8**(2): p. 117-123.
 83. Handayani, F. and F. Yuliana, *Design and legal aspect of central bank digital currency: a literature review*. Journal of Central Banking Law and Institutions, 2022. **1**(3): p. 509-536.
 84. Rachmad, Y.E., *Redefining Money: Implementation and Challenges of CBDC in the Digital Era*. The United Nations and the Nobel Peace Prize Awards, 2025.
 85. Infante, S., et al., *The macroeconomic implications of CBDC: A review of the literature*. 2022.
 86. Dupuis, D., K. Gleason, and Z. Wang, *Money laundering in a CBDC world: a game of cats and mice*. Journal of Financial Crime, 2022. **29**(1): p. 171-184.
 87. Nosheen, M., T. Mumtaz, and B. Amjad, *Gendered Dynamics and Economic Influences in Transboundary Mountain Ecology: A Case Study of the Himalayan Region*. Journal of Asian Development Studies, 2024. **13**(4): p. 349-367.
 88. Wang, H., *China meets digital currency: E-CNY and its implications for businesses*. The Law Gazette (November 2021 issue, Forthcoming), UNSW Law Research Paper, 2021(21-77).
 89. Oluwaleke, E.A., D. Akhimie, and O. Olonade, *Awareness and Understanding of Enaira in Nigeria*. Acta Universitatis Danubius. Oeconomica, 2023. **19**(5).
 90. Nosheen, M., K. Farooq, and B. Amjad, *The role of islamic finance in promoting entrepreneurship and economic growth*. International Journal of Social Sciences Bulletin, 2024. **2**(4): p. 2006-2014.
 91. Khan, A., et al., *Regulatory strategies for combatting money laundering in the era of digital trade*. Journal of Money Laundering Control, 2025. **28**(2): p. 408-423.
 92. He, D., *Digitalization of cross-border payments*. China Economic Journal, 2021. **14**(1): p. 26-38.
 93. Bindseil, U. and G. Pantelopoulos, *Towards the holy grail of cross-border payments*. 2022: ECB Working Paper.



94. Wouters, J. and J. Odermatt, *Comparing the 'four pillars' of global economic governance: A critical analysis of the institutional design of the FSB, IMF, World Bank, and WTO*. *Journal of International Economic Law*, 2014. **17**(1): p. 49-76.
95. Bennett, D., S.A. Asjad Naqvi, and W.P. Schmidt, *Constraints on compliance and the impact of health information in rural Pakistan*. *Health Economics*, 2015. **24**(9): p. 1065-1081.
96. Walter, A., *Emerging Countries in Global Financial Regulatory Standard Setting: What Is to Be Done?* 2019.
97. Akhtar, S., H. Hussain, and R.Y. Hussain, *Contributing role of regulatory compliance and Islamic operations in bank risk: Evidence from Pakistan*. *Nankai Business Review International*, 2021. **12**(4): p. 618-635.
98. Amjad, B., et al., *Towards Automation and Digital Justice: A Review of Digital Twin Technology for Automation in Justice System*. *Journal of Asian Development Studies*, 2025. **14**(3): p. 49-62.
99. Paccoud, I., et al., *Socio-ethical challenges and opportunities for advancing diversity, equity, and inclusion in digital medicine*. *Digital health*, 2024. **10**: p. 20552076241277705.
100. Mordini, E., et al., *Ethics, e-inclusion and ageing*. *Stud. Ethics L. & Tech.*, 2009. **3**: p. 1.
101. Celik, I., *Exploring the determinants of artificial intelligence (Ai) literacy: Digital divide, computational thinking, cognitive absorption*. *Telematics and Informatics*, 2023. **83**: p. 102026.
102. Amjad, B., A. Saeed, and A. Amjad, *Social responsibility of corporate sector: a comparative analysis between Pakistan and United Kingdom (UK)*. *Pakistan Social Sciences Review*, 2024. **8**(2): p. 01-16.
103. Aydin, M., *Does the digital divide matter? Factors and conditions that promote ICT literacy*. *Telematics and Informatics*, 2021. **58**: p. 101536.
104. Nasah, A., et al., *The digital literacy debate: An investigation of digital propensity and information and communication technology*. *Educational Technology Research and Development*, 2010. **58**(5): p. 531-555.
105. Anurogo, D., et al., *Digital Literacy 5.0 to enhance multicultural education*. *Multicultural Islamic Education Review*, 2023: p. 95-104.
106. Esposito, M., Y. Akbar, and F.X. Campbell, *Digitalization in Emerging Economies*. 2025: Cambridge University Press.
107. Ranjan, A. and I. Talbot, *Challenge, Continuity, and Change in Pakistan*. 2025: Taylor & Francis.
108. Aslam, A. and M.A. Shah, *Tec (h) tonic shifts: taxing the "digital economy"*. 2020: International Monetary Fund.
109. Jaswal, B.A., *Digitization of archival collections by libraries in Pakistan: Issues, strategies, challenges and opportunities*. *Pakistan Journal of Information Management and Libraries*, 2016. **17**: p. 97-108.
110. Pomaza-Ponomarenko, A., et al., *Legal reform and change: research on legal reform processes and their impact on society. Analysis of factors that facilitate or hinder legal change, including political, social, and economic factors*. *Journal of Law and Sustainable Development*, 2023. **11**(10): p. e1854-e1854.
111. Pomaza-Ponomarenko, A., et al., *Dynamics of legal transformatis: Assessment of impact on society and analysis of determinations of changes in the legislative sphere*. *Multidisciplinary Reviews*, 2024. **7**.
112. Richman, D., *Institutional Coordination and Sentencing Reform*. *Tex. L. Rev.*, 2005. **84**: p. 2055.
113. Zainutdinova, E.V., *Models of legal regulation of digital rights and digital currency turnover*. *Legal Issues Digit. Age*, 2023. **4**: p. 93.
114. Yanto, S.E. and F. Santiago, *The Legal Vacuum in Law Enforcement of Digital Currency Crimes by the Police*. *Journal of World Science*, 2024. **3**(12): p. 1576-1586.
115. Pranevičienė, K., M. Sadzevičius, and N. Gaubienė, *Recovery of Digital Assets and Cryptocurrencies in Civil Enforcement Proceedings: Key Challenges*. *Prawo i Więż*, 2025. **55**(2).
116. Etuge, N., *Digital currency and the law: the way forward For a stable regulatory framework in Cameroon's monetary and financial system*. *The Law Brigade (Publishing) Group*, 2022.
117. Deryugina, T., *Problems of determining the legal nature of digital currency*. *Perm U. Herald Jurid. Sci.*, 2024. **64**: p. 274.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable



Declaration of AI Use: The author declares that the AI tool "ChatGPT" was used to assist with drafting in the preparation of this manuscript. All content was critically reviewed, verified, and edited by the author, who take full responsibility for the accuracy and integrity of the work.

