Digital Payment Systems and International Trade Laws: Harmonizing Rules for Cross-Border Fintech Solutions

---

1. Abstract

Digital payment systems now power how countries trade with each other by making global commerce faster while becoming more accessible and creative. We cannot achieve full global economic growth because different nations do not have the same trade rules and regulations. This paper studies the connection between digital payment systems and international trade laws through analyzing the main problems of diverse rules, security threats, and currency market fluctuations. This analysis focuses on blockchain and IoT innovations that show great potential for improving cross-border payments yet their full adoption remains limited by unclear regulations. Collaborated rules and broader technology use will create a global financial platform that serves businesses and users effectively.

2. Introduction

The global digital payments market is projected to reach $14.78 trillion by 2027, growing at a CAGR of 13.10% from 2022 to 2027.[11] Fintech innovations such as cross-border UPI (Unified Payments Interface), blockchain-based remittances, and central bank digital currencies (CBDCs) are transforming international transactions, making them faster, cheaper, and more accessible. However, as digital payment systems expand beyond borders, regulatory fragmentation remains a critical challenge, with varying compliance requirements across jurisdictions creating inefficiencies, legal uncertainties, and risks of financial crime.

Despite the World Trade Organization (WTO) and Financial Action Task Force (FATF) promoting standardization in digital financial services, countries continue to impose inconsistent Anti-Money Laundering (AML), Know Your Customer (KYC), and data protection laws. For instance, India's UPI expansion into the UAE, Singapore, and France has highlighted the need for mutual regulatory recognition and interoperability, yet global alignment remains elusive. According to the Bank for International Settlements (BIS), inefficiencies in cross-border payments cost businesses and individuals over $120 billion annually in transaction fees and compliance delays.[2]

[2]This research explores the intersection of digital payment systems and international trade laws, analyzing the gaps in regulatory harmonization and proposing policy recommendations for seamless cross-border fintech solutions. By assessing existing trade agreements, financial regulations, and emerging digital currency frameworks, this paper aims to provide a roadmap for governments, financial institutions, and fintech firms to align digital payment policies with global trade norms, ensuring both security and efficiency.

As cross-border digital transactions reshape international commerce, the question remains: Can global regulators keep pace with fintech innovation, or will fragmented trade laws hinder the future of seamless financial connectivity?

---

[1] Statista. (n.d.). *Digital payments - Worldwide*. Statista. Retrieved February 24, 2025, from https://www.statista.com/outlook/fmo/digital-payments/worldwide

[2] JPMorgan. (n.d.). *mCBDCs: Unlocking $120 billion value in cross-border payments*. Retrieved February 24, 2025, from https://www.jpmorgan.com/kinexys/documents/mCBDCs-Unlocking-120-billion-value-in-cross-border-payments.pdf

I. Advancements of Digital Payments Systems

Since the introduction of the digital payment solutions, buyers and sellers can make or receive payment in a matter of an instance and such transactions can be operated from any part of the world. This reduces both time and loss of business opportunities that could be the result of delayed payment clearances. In general, the monetary sum associated with digital payment systems is higher, but transaction or platform costs are typically lower most of the time. This makes the management of the business within the global market cost effective and feasible . These systems adopt the concept of encrypting technology so that the business transactions will be secure.The digital payment system features a choice which allows different currency transactions between partners and customers operating internationally. With the emerging technologies like Blockchain , Internet of Things (IoT) and Artificial Intelligence, digital payment systems are becoming a more transparent, efficient and reliable source of payment. Hence, continuous technological development sets digital payment systems to be essential components of international commerce while building powerful economic growth and enhancing business-consumer connection on a global scale.

II. Role of Digital Payment Systems in International Trade

The expansion of digital payment systems has significantly influenced international trade by enhancing transaction efficiency, reducing costs, and increasing financial accessibility. These systems provide businesses with secure, scalable, and streamlined payment solutions, minimizing dependence on conventional banking infrastructure and mitigating financial and geographical constraints.

A key advantage of digital payment systems is their ability to facilitate seamless cross-border transactions. Emerging fintech solutions, particularly blockchain-based cryptocurrencies like Bitcoin and Stellar, help address challenges associated with fluctuating currency exchange rates. By enabling peer-to-peer (P2P) transactions without intermediaries, these systems enhance transaction speed and efficiency while reducing reliance on traditional financial institutions. This decentralized approach strengthens liquidity and financial stability in global markets.

Additionally, digital payment systems contribute to greater financial inclusion, particularly for individuals and businesses in remote or underserved regions. Traditional banking networks often fail to reach these populations, limiting their participation in the global economy. However, digital wallets and mobile-based payment platforms provide an accessible alternative, allowing users to engage in international trade and benefit from improved financial literacy. By bridging this gap, digital payments foster economic growth and create opportunities for small and medium-sized enterprises (SMEs).

The efficiency of financial transactions has also improved significantly with the adoption of digital payment technologies. Traditional banking methods involve manual verifications, lengthy processing times, and administrative delays, all of which hinder international trade. In contrast, digital transactions occur in real time, ensuring faster settlements and better cash flow

management. This increased efficiency reduces disruptions in supply chains, enhances operational agility, and promotes business continuity in global commerce.

Cost reduction is another major benefit of digital payment systems. Traditional international money transfers are often associated with high fees due to intermediary charges, foreign exchange markups, and compliance costs. Digital payment technologies, particularly blockchain-based solutions, lower transaction costs by eliminating intermediaries and streamlining the payment process. This affordability is especially beneficial for SMEs seeking to expand their trade activities without incurring excessive financial burdens.

Security and fraud prevention mechanisms within digital payment systems further strengthen their role in international trade. Advanced encryption protocols, cryptographic authentication, and AI-driven fraud detection tools ensure transaction integrity and protect businesses from cyber threats. Multi-factor authentication and real-time monitoring systems enhance financial security, fostering confidence in digital transactions and reducing the risks associated with cybercrime.

Furthermore, digital payments generate valuable data insights that businesses can utilize to make strategic decisions. By analyzing transactional trends, consumer behavior, and market demands, companies can optimize their product offerings, refine pricing strategies, and enhance customer engagement. Access to such data-driven intelligence allows businesses to stay competitive, adapt to evolving market conditions, and strengthen their global trade strategies.

3. AML and KYC Landscape

KYC refers to the procedure that helps banks and other financial institutions determine if a customer is who they claim to be and assess the level of risk associated with engaging with that customer. AML, or Anti-Money Laundering, pertains to the strategies employed to prevent money laundering, fraud, and other related financial crimes. Both KYC and AML are particularly crucial in high-risk environments, especially within the banking sector, where activities may often involve illegal or illicit funds.

Digital payment system rapid adoption has created new routes for money laundering along with fraudulent actions. Cyberspace provides criminals with advantages of maintaining anonymity , global accessibility and faster transactions through digital payment systems.Thus, in the world of the digital payment system - AML (Anti-Money Laundering) and KYC (Know Your Customer) act as critical compliance rules to authenticate users and track financial activity which detects unusual payments thus protecting the payment system through legitimized transaction activity.

I. India

In India, anti-money laundering (AML) regulations are primarily governed by the *Prevention of Money Laundering Act, 2002* (PMLA), which mandates that designated institutions and entities implement robust mechanisms to detect and prevent money laundering activities. The key AML regulatory authorities include the Reserve Bank of India (RBI), the Enforcement Directorate (ED), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Financial Intelligence Unit of India (FIU).

The *Prevention of Money Laundering (Maintenance of Records) Amendment Rules, 2023* were introduced to enhance AML compliance by requiring entities to adopt more stringent reporting measures, particularly concerning beneficial ownership. A significant development under this amendment is the explicit inclusion of cryptocurrencies and other virtual digital assets (VDAs) within the AML framework, reflecting India's evolving regulatory approach to financial technology and digital transactions.

The RBI has undertaken several initiatives to strengthen AML measures, particularly through amendments to its *KYC Master Directions*. These updates emphasize the importance of periodic KYC revisions and mandate real-time updates to ensure the accuracy and integrity of financial records. Additionally, the *Comprehensive Sanctions Screening* framework now obligates regulated entities (REs) to screen customers against 14 *United Nations Security Council (UNSC) Sanctions Lists* and the *Unlawful Activities (Prevention) Act, 1967* (UAPA). Furthermore, the threshold for identifying beneficial ownership has been reduced to 10%, reinforcing due diligence obligations[3].

To ensure enhanced compliance, the *Central KYC (CYKC) Registry* imposes strict documentation and verification standards for REs. The RBI has also intensified its enforcement measures, with penalties for non-compliance increasing by 88% over the past three years[4]. The primary infractions pertain to KYC and AML compliance deficiencies, underscoring persistent challenges faced by financial institutions in aligning with regulatory expectations. For instance, regulatory action against Paytm Payments Bank, arising from alleged KYC violations and money laundering concerns, highlights the critical importance of adherence to compliance protocols.

Additionally, the *Financial Action Task Force (FATF)* has recommended that India strengthen due diligence procedures concerning bank accounts associated with politically exposed persons (PEPs), including local politicians, government officials, and their relatives. These recommendations call for enhanced monitoring of financial transactions and require senior banking officials to approve the opening of new accounts for PEPs to mitigate the risks of corruption and bribery.

These regulatory developments reflect India's ongoing efforts to align with international AML standards while addressing emerging financial risks. However, challenges remain in ensuring effective implementation and enforcement of these measures across diverse financial institutions.

[3] https://www.aiprise.com/blog/ubo-reporting-beneficial-ownership-guidelines

[4] https://www.business-standard.com/finance/news/rbi-penalties-surge-88-in-last-3-years-kyc-and-aml-top-violations-list-124060600486_1.html

II. China

The *Anti-Money Laundering Act, 2025* (AMLA 2025) in China introduces comprehensive measures aimed at strengthening anti-money laundering (AML) compliance among financial institutions, payment service providers, and triangular merchants. A key aspect of this legislative development is the formal recognition of crypto assets and technological platforms as financial instruments, necessitating enhanced regulatory oversight. The AMLA 2025 prescribes stringent customer identification protocols, risk assessment frameworks, and real-time transaction monitoring mechanisms to mitigate financial crimes effectively.

A notable advancement in the amended framework is the integration of advanced technologies in customer due diligence (CDD) processes. The law explicitly acknowledges the role of artificial intelligence (AI) and data analytics as essential tools for detecting suspicious transactions and improving the overall effectiveness of AML measures. These technological innovations are expected to enhance compliance capabilities and facilitate more robust enforcement mechanisms.

In parallel, China's *Personal Data Protection Law (PDPL)*, which came into effect on November 1, 2021, plays a pivotal role in shaping Know Your Customer (KYC) and AML procedures. The PDPL imposes strict requirements on the collection, processing, and international transfer of personal data, necessitating operational compliance solutions that ensure the protection of user data during identification and verification processes. The regulation mandates explicit user consent, sets clear limitations on data retention periods, and imposes restrictions on cross-border data transfers, thereby influencing the design and implementation of AML compliance frameworks.

Despite these regulatory advancements, significant challenges persist within China's AML enforcement landscape. One of the primary concerns is the limited scope of predicate offenses under the existing AML framework, which has been criticized for potentially hindering comprehensive enforcement against diverse money laundering schemes. Additionally, financial institutions have encountered substantial difficulties in implementing effective KYC procedures, leading to regulatory penalties. For instance, in 2023, the *People's Bank of China (PBOC)* imposed fines on several institutions primarily for non-compliance with KYC requirements[5].

Moreover, the rapid evolution of financial technology and socio-economic activities has contributed to the increasing complexity and sophistication of money laundering schemes. This dynamic landscape has raised concerns regarding the adequacy of existing AML regulations in addressing contemporary financial crime risks. While the AMLA 2025 aims to enhance financial integrity, its practical implementation and effectiveness in combating emerging threats will depend on the adaptability of regulatory authorities and financial institutions.

[5] https://www.lexology.com/library/detail.aspx?g=65cb8699-6363-47a0-91fa-7b352e18e52c

III. European Union (EU)

The European Commission, in collaboration with the European Supervisory Authorities (ESAs), has developed guidelines and recommendations to assist national authorities in understanding and implementing regulatory expectations under the European Union's anti-money laundering (AML) framework. A key initiative in this regard is the establishment of the *Anti-Money Laundering Authority (AMLA)*, which seeks to enhance cooperation among *Financial Intelligence Units (FIUs)* and coordinate national regulatory bodies to ensure private-sector compliance with EU AML and counter-terrorist financing (CFT) standards. Through a series of strategic measures, AMLA aims to reinforce the EU's capacity to combat financial crimes effectively.

The *Sixth Anti-Money Laundering Directive (6AMLD)* represents a significant regulatory advancement in the EU's AML/CFT strategy. One of its most notable provisions is the imposition of criminal liability on legal entities, holding corporate bodies accountable for failures in preventing AML/CFT violations. Under 6AMLD, companies found in breach of these regulations may face severe penalties, including monetary fines or permanent closure. Additionally, the directive mandates stricter measures to enhance collaboration among FIUs and align national regulatory approaches, ensuring uniform application of AML standards across EU member states.

A key aspect of 6AMLD is the elevation of criminal accountability for both individuals and corporate entities. Entities and individuals found guilty of AML violations may be subject to imprisonment for up to four years, alongside financial penalties reaching €5 million.[6] Given the increasing role of digital assets in financial transactions, 6AMLD also introduces *Enhanced Due Diligence (EDD)* requirements, mandating more rigorous oversight of cross-border transactions involving crypto-asset service providers. These provisions reflect the EU's efforts to adapt AML regulations to emerging financial risks while reinforcing legal accountability.

Despite these regulatory advancements, financial institutions operating within the EU face considerable compliance challenges due to variations in AML rules across member states. A *PwC survey* indicates that nearly half of organizations across Europe, the Middle East, and Africa (EMEA) perceive AML requirements as lacking clarity and consistency[7]. The financial burden associated with AML and Know Your Customer (KYC) compliance remains a critical concern. Notably, Sir Howard Davies, former chairman of *NatWest*, criticized the UK's AML framework for imposing an estimated £30 billion annual cost on banks without yielding significant convictions, calling for urgent reform[8].

Moreover, the evolving nature of financial crimes necessitates the integration of advanced technological solutions into AML operations. The *European Central Bank (ECB)* has

---

[6] https://www.signicat.com/blog/aml6-sixth-anti-money-laundering-directive#:~:text=The%20minimum%20penalty%20for%20crimes,authorities%20to%20impose%20exemplary%20sanctions.

[7] https://www.pwc.lu/en/press/press-releases-2024/aml-survey-2024.html

[8] https://www.thetimes.com/business-money/companies/article/anti-money-laundering-rules-hamper-banks-says-former-natwest-chairman-ccdtknngf

acknowledged that legacy technologies are often inadequate in addressing modern AML risks, while emerging technologies present opportunities to enhance compliance effectiveness. However, financial firms continue to struggle with managing vast amounts of transactional data, underscoring the need for regulatory bodies to facilitate the adoption of sophisticated data analytics and AI-driven AML solutions.

In response to the growing demand for secure and transparent payment mechanisms, financial technology firms are actively developing innovative solutions that enhance the efficiency, security, and accessibility of cross-border transactions.

4. Blockchain and Cross-Border Digital Payments

Blockchain technology has emerged as a transformative tool in the cross-border payment ecosystem. By facilitating secure and transparent database sharing across distributed networks, blockchain enables efficient transaction recording and asset tracking for businesses. Compared to traditional payment networks, blockchain-based payment systems offer significantly faster processing times by eliminating intermediaries, thereby reducing transaction delays and operational inefficiencies.

One of the key advantages of blockchain technology in digital payments is its cost-effectiveness. The removal of intermediaries lowers processing fees, making international transactions more affordable for businesses and consumers. Additionally, as a decentralized system, blockchain allows for global transactions without the complexities associated with traditional foreign exchange mechanisms, thereby streamlining cross-border payments.

Blockchain's security framework relies on sophisticated cryptographic techniques, distributed ledger technology, and decentralization, which collectively enhance fraud prevention and ensure transaction integrity. Every node in a blockchain network maintains a copy of the distributed ledger, and transactions are sequentially verified through a consensus mechanism before being recorded. This structural complexity makes it difficult for any single entity to manipulate transaction data, ensuring transparency and reducing the risk of fraudulent activities.

Security and Compatibility in Blockchain-Based Payments

Blockchain payment systems implement advanced security measures, such as encryption protocols and private key authentication, to safeguard user data. Each transaction requires the use of a private key, adding an extra layer of security that significantly reduces the risk of unauthorized access or cyberattacks. This dual-layer security mechanism enhances data protection and reinforces the resilience of blockchain-based financial systems.

Moreover, blockchain technology is designed to accommodate diverse currency systems, supporting both digital assets and fiat currencies within a unified framework. This adaptability facilitates seamless integration with existing financial and accounting infrastructures, ensuring compatibility with conventional payment systems. To optimize cross-border payment processes, blockchain developers prioritize interoperability with legacy financial systems, allowing blockchain-based transactions to function alongside traditional banking mechanisms.

5. Internet of Things (IoT)

The Internet of Things (IoT) refers to any physical device among tools and accessories along with equipment or vehicles which combine sensor units for information processing through automated communication. Beneficial information goes from sensors in connected devices using the Internet of Things framework to target devices which address these needs. Through its operation the IoT platform assesses which information holds value and which information should be discarded. The analysis of collected data through pattern recognition enables spotting potential incidents together with developing recommended actions.

IoT payments represent a revolutionary shift in the financial industry, where consumers do not initiate transactions but instead get alerts when their smart devices make significant purchases. The aggregation of large volumes of financial activities and data has sparked an increased demand for IoT services in the global fintech landscape. Additionally, the need for IoT is expanding in other industries, such as manufacturing, logistics, and healthcare. Payments based on IoT automate transaction processes, eliminating the necessity for human involvement while enhancing speed, convenience, and efficiency. IoT-driven payments confirm transactions using encrypted data, thereby reducing the risk of fraud. Transaction expenses are minimized due to the removal of manual operations and intermediaries. IoT-based payment methods deliver a seamless transaction experience to customers, enabling them to make quicker and more efficient payments.

Digital payment systems derive usefulness from IoT by permitting users to make contactless transactions with any device that holds connectivity including mobile phones, wearables and smart home systems thus bypassing traditional payment tools and speeding up checkouts and improving security through biometric verification and improved convenience. IoT payments demonstrate great potential as a next-generation cashless payment technology because of its various advantageous characteristics. This method provides security benefits and time-saving features for all participants who take part in the payment transaction process. However it is advised that consumers should exercise caution with their payments through connected devices despite the implemented security measures. A user should thoroughly check both the device and app authenticity before providing their personal data or financial details. People should review their account statements frequently to recognize any doubtful transactions. Using proper safety measures alongside risk awareness leads to secure cashless payment transactions while protecting both security and privacy.

For the banking industry, the Internet of Things (IoT) offers the advantage of handling data, enabling businesses to access essential information for accurate credit risk evaluation. By implementing sensors and utilizing machine-to-machine communication protocols, data analysts can obtain figures to develop a comprehensive profile that addresses requirements from KYC and AML regulations to fraud detection. The synergy between fintech and IoT companies can delve deeply into analyzing a client's daily activities and even actively engage in them. Such capabilities include features where customers can connect their wearable devices to banking applications for tracking expenses, setting spending limits weekly or monthly, or even freezing accounts once the specified limit is reached. With these applications, the need for physical cards may diminish, significantly enhancing the convenience of shopping.

Financial service organizations that integrate IoT in the foreseeable future can enhance their data collection and storage methods, create a more robust risk assessment framework, discover new avenues

to engage with their customers, and thus boost customer interaction. Financial institutions can leverage IoT devices to refine their operations, enhance efficiency, and ultimately reduce expenses. This technology also provides immediate insights and analytics, enabling companies to make more informed choices. In addition, IoT can aid financial services firms in customizing their offerings and delivering more pertinent solutions tailored to individual client needs and preferences. Moreover, embracing IoT can bolster cybersecurity by consistently monitoring and identifying potential threats in real time.

6. International Trade Agreements on Digital Payment Systems

I. World Trade Organization

Over the course of five years in the WTO, 80 nations such as China, Japan, Singapore, Australia, Brazil, Saudi Arabia etc., have achieved significant milestones regarding cross-border internet transactions, ratifying a draft set of common regulations and standards for global online trading. However, some countries, including the United States, have not fully engaged in the initiative. Formalized on July 26, 2024, this framework aims to establish guidelines facilitating the international exchange of goods and services, promoting regulatory collaboration, and simplifying global commerce.

WTO member nations commit to aligning their legal systems with the principles of the 1996 UNCITRAL Model Law on Electronic Commerce. This ensures that electronic and paper-based information are treated equally, granting electronic contracts the same legal validity as traditional written agreements. The treaty encourages the transition from physical documentation to digital trade forms, urging nations to eliminate paper-based customs processes in favor of digital documentation.

Given the increasing reliance on electronic payments in global trade, WTO members are also working toward safe, efficient, and competitively priced payment methods that meet international interoperability standards. To address the risks of fraudulent activities in e-commerce, the agreement defines misleading commercial practices and mandates consumer protection measures to ensure e-commerce offers equivalent safeguards as traditional commerce. The treaty also requires WTO nations to enhance cybersecurity frameworks, develop national response mechanisms, and coordinate efforts in identifying cyber threats.

Despite these advancements, several challenges persist like:

a. **Fragmentation:** Differing national data governance laws complicate the implementation of unified digital payment standards.
b. **Inclusion of Developing Nations:** Technological and infrastructural limitations hinder equitable participation in digital trade.
c. **Regulatory Lag:** Digital payment innovations often outpace the development of legal frameworks, complicating governance and enforcement.

To address these issues, international cooperation is essential in creating adaptive regulatory frameworks and providing capacity-building programs to assist developing nations in navigating digital trade complexities.

II. World Economic Forum (WEF)

The **Digital Trade Initiative** by WEF aims to foster an equitable global digital trade system through:

a. Regulatory Collaboration
b. E-commerce and Payment Ecosystems
c. Trade-enabling Technologies

The **Digital Economy Agreement Leadership (DEAL)** provides a networking platform for regulatory bodies, industry stakeholders, and policymakers. A key project under this is the **ASEAN Digital Economy Agreement Leadership (DEAL)**, supporting ASEAN's Digital Economy Framework Agreement (DEFA) through:

a. An interactive database of past and ongoing trade negotiations
b. Cross-ASEAN MSME business surveys
c. Regional and international business input integration

Another initiative, the **Digital Trade Development Program**, identifies challenges faced by developing nations in digital trade and helps governments implement policy reforms in **connectivity, finance, logistics, and skills development**. Additionally, the **Payments to Advance Growth for All (PAGA)** initiative promotes efficient cross-border digital payment systems.

Challenges:

a. **Uneven Digital Adoption:** Economic disparities create gaps in digital trade participation, limiting MSME access.
b. **Protectionism:** National digital policies and restrictions on data flows hinder global trade cooperation.
c. **Divergence:** Differences in national regulations complicate global standardization efforts.

To overcome these barriers, governments, corporations, and civil society must collaborate to create a more inclusive digital trade environment that benefits all stakeholders.

7. Regional Trade Agreements on Digital Payment Systems

I. United States-Mexico-Canada Agreement (USMCA)

USMCA enhances fintech integration by establishing common standards for consumer data processing, ensuring non-discriminatory treatment of foreign fintech firms, and permitting financial institutions to access payment and clearing systems across all member states. The agreement also supports regulatory **fintech sandboxes**, allowing firms to develop financial technologies in controlled environments.

Mexico's adoption of **open banking regulations** under USMCA has introduced specialized licenses for cryptocurrency exchanges, enabling them to operate as financial technology entities. However, despite these advancements, challenges remain:

a. **Divergent Regulations:** Differences in electronic authentication and transaction enforceability lead to compliance complexities.
b. **Data Localization Conflicts:** While USMCA generally prohibits data localization, exceptions exist for government data in the U.S. and Canada.
c. **Consumer Protection Disparities:** Variability in consumer rights enforcement creates inconsistencies in online transaction protections across member states.

To navigate these complexities, businesses must stay updated on evolving data regulations and implement robust compliance frameworks.

II. European Union (EU)

The **EU's Directive (EU) 2015/2366** enhances regulations for electronic payments, ensuring:

a. Secure and fraud-resistant online and mobile payments
b. Consumer data protection and authentication measures
c. Clarity on the rights and obligations of payment service users and providers

While this directive strengthens Europe's unified payment market, following challenges persist:

a. **Regulatory Variability:** Different implementations across EU member states create obstacles for cross-border payment service providers.
b. **Market Dominance of Big Tech:** Despite efforts to encourage competition, major tech firms continue to wield significant influence, as seen in the EU's antitrust investigation into Apple's payment practices.

III. Regional Comprehensive Economic Partnership Agreement (RCEP)

Given the rapid developments in e-commerce and international trade, the Regional Comprehensive Economic Partnership (RCEP) has introduced an E-Commerce Chapter as an annex to the CTE. This chapter aims to promote e-commerce adoption, expand its global reach, and strengthen cooperation among member states. It mandates parties to enhance trade administration and facilitation through electronic processes, ensuring smoother cross-border transactions. Additionally, it allows members to establish or recognize laws that support e-commerce growth while safeguarding consumer data and digital transactions.

The E-Commerce Chapter also touches upon key data-related aspects, including the location of computing facilities and cross-border data flows. However, in its current form, the dispute settlement provisions do not apply to this chapter, leaving gaps in the enforcement of e-commerce-related obligations.

Challenges in Digital Payments under RCEP

Despite these advancements, several challenges persist in standardizing digital payment systems within RCEP:

a. **Lack of Regulatory Commitments** – RCEP does not impose strict obligations on members to standardize digital payment systems, leading to fragmented regulatory frameworks across different jurisdictions.
b. **Cross-Border Enforcement Issues** – Differences in data localization and privacy laws complicate regulatory compliance. For example, ASEAN follows a more flexible approach, whereas China enforces strict data governance policies.
c. **Digital Payment Fraud and Chargebacks** – Cross-border transactions often involve fraud, chargebacks, and payment disputes. However, RCEP lacks a uniform dispute resolution mechanism to address these challenges effectively.
d. **Cybersecurity Risks** – The absence of a harmonized cybersecurity framework exposes financial institutions to increased cybercrime risks in cross-border payments.
e. **Lack of Interoperability** – RCEP members rely on different digital payment systems, making interoperability a challenge. For instance, Singapore uses PayNow, China relies on AliPay/WeChat Pay, and India has UPI, leading to incompatibility in transactions.
f. **Financial Inclusion Gaps** – Developing nations such as Cambodia and Myanmar lack the necessary infrastructure for seamless digital payments, restricting financial inclusion and cross-border financial accessibility.

IV. Digital Economy Partnership Agreement (DEPA)

The **Digital Economy Partnership Agreement (DEPA)** serves as a trade agreement that establishes guidelines for the digital economy while facilitating digital trade among its members. Initially signed virtually in June 2020 by Chile, New Zealand, and Singapore, DEPA functions as a "live" document, allowing for ongoing modifications and updates as digital trade evolves. Since all three founding members are part of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), DEPA acts as a complementary framework that enhances the e-commerce provisions of CPTPP. Additionally, it expands coverage to e-payments, e-invoicing, and emerging technologies such as AI and fintech.

A key aspect of DEPA is its role in establishing international digital trade standards, ensuring seamless digital transactions across borders. Article 2.7 of the agreement mandates members to support globally recognized digital payment standards and work towards payment infrastructure interoperability and market-driven payment system development. The Business and Trade Facilitation modules within DEPA further support the growth of e-payments by encouraging transparency and fair market practices. Additionally, DEPA grants member states the authority to regulate emergency situations and balance of payments challenges to maintain financial stability.

a. Challenges in Implementing DEPA

Despite its potential, digital trade agreements like DEPA face several hurdles, particularly in transnational coordination and enforcement. While the agreement promotes cooperation in artificial intelligence and digital identity systems, maintaining a balance between innovation and regulatory oversight remains a challenge, especially in areas concerning data privacy and cybersecurity.

Moreover, DEPA's member states exhibit varying levels of digital infrastructure development. Singapore, for example, has an advanced digital economy, whereas Chile is still developing its digital capabilities. This disparity necessitates a uniform implementation strategy to ensure all members can benefit equally from the agreement.

b. China's Accession and Its Challenges

China formally applied for DEPA membership on November 1, 2021, leading to the creation of an Accession Working Group by the DEPA Joint Committee on August 18, 2022. Since then, China has engaged in multiple consultative meetings with DEPA members to advance its accession process.

However, China's potential entry presents significant challenges. The agreement's provisions on data privacy, cross-border data flows, and digital taxation may conflict with China's existing regulatory framework, which emphasizes mandatory data localization and government oversight. Additionally, geopolitical tensions between China and Western nations could further complicate its participation in DEPA. Concerns over cybersecurity, intellectual property protection, and market access restrictions may lead some members to resist China's integration into the agreement

8. Successful Cross Border Fintech Collaborations

I. Unified Payments Interface (UPI) International Partnerships

Since its inception in 2016, UPI has revolutionized digital payment operations by introducing impactful new features. Developed by NPCI, UPI has seamlessly integrated into the daily banking habits of millions of Indians. [9]Paysecure's worldwide payment analysis reveals that UPI is now the most widely used digital payment system globally, boasting a processing rate of 3729.1 transactions per second in 2023. The surge in transactions reflects a 58% increase to 2,348 per second compared to the previous year.

Indians are leading the charge in global digital payments, with UPI dominating the landscape as over 40% of transactions conducted by Indians are digital via UPI. [10]Between April and July

[9]https://www.businesstoday.in/personal-finance/story/upis-partnerships-can-streamline-transaction-routes-four-users-in-foreign-lands-mohan-k-of-techfini-453805-2024-11-14

[10]https://www.businesstoday.in/personal-finance/story/upis-partnerships-can-streamline-transaction-routes-four-users-in-foreign-lands-mohan-k-of-techfini-453805-2024-11-14

2024, UPI facilitated transactions totaling ₹80.8 lakh crore ($964 billion), showcasing a year-on-year growth rate of 37% compared to transactions from April to July 2023. NIPL has entered a new agreement with Trinidad and Tobago's Ministry of Digital Transformation to create a comprehensive digital payment solution. This system aims to enable secure transactions between individuals and businesses, including merchants. This deal, made in September 2024, illustrates India's ambition to establish itself as a significant global leader in digital payments. Earlier this year, NIPL expanded its reach into Latin American and African markets by forming agreements with Peru and Namibia, where they plan to develop new payment systems leveraging UPI technology and NPCI's proven infrastructure from India.

II. PayPal and MercadoLibre Collaboration

PayPal is focusing on Latin America as a key area for expanding its online payment and money transfer services. In 2020, PayPal enhanced its partnership with MercadoLibre to broaden its market presence throughout Latin America. PayPal's increasing footprint in Latin America highlights the potential for growth driven by the eCommerce boom and the needs of the underbanked population, presenting fresh business opportunities for its payment solutions.

Via LinkedIn, President and CEO Dan Schulman announced that PayPal is now available for Brasile and Mexican users of MercadoPago to make online purchases at businesses utilizing MercadoLibre's payment system. [11]Schulman stated that this integration allows PayPal's existing 300 million users to access "hundreds of thousands of new merchants" to shop with. PayPal has now joined MercadoLibre's list of payment methods for customers completing their transactions on the platform.

Through PayPal integration as a payment option on MercadoLibre's Brazilian and Mexican platform consumers are able to access international merchants and expand their purchasing opportunities while promoting international business. . The partnership enabled Xoom, the international money transfer service of PayPal to deliver remittance payments directly to MercadoPago wallets,thus serving both Mexico and Brazil. Xoom's incorporation into the platform has enabled the users to swiftly receive international money transfers. Thus, through their partnership PayPal-MercadoLibre has significantly contributed to digital payment systems in Latin America.

III. Swift and Wise Collaboration

Swift and Wise have partnered in 2023 to enhance global payment services through direct Swift transfers now fully integrated with the Wise platform for their users. The collaboration between Swift and Wise commenced at Sibos in Toronto and aimed to expand beyond the initial partnership as advancements in the financial sector demand diverse payment methods to meet consumer requests. This illustrates how collaboration among companies builds networks that ensure safety and reliability while catering to various user preferences. Our strategy aligns

[11]https://www.pymnts.com/news/ecommerce/2019/paypal-deepens-latam-reach-with-mercado-libre-integration/

perfectly with the objectives of both the G20 and the UN Sustainable Development Goals in improving cross-border payment systems.

The Wise Platform incorporates Swift's latest payment tools, including cloud connectivity and pre-validation, while maintaining Swift GPI functionalities such as real-time tracking of payments across both platforms. [12]The network operated by Wise for global payments facilitates instant transfers for 57% of transactions in under 20 seconds, and 90% of users can move funds in one hour or less. Financial institutions were able to make cross-border transactions more cost-effective for their clients by implementing Wise Platform's Correspondent Services without a complicated setup process. They can access Wise's platform via SWIFT's network to provide customers with renewed cross-border payment options without any requirement to modify their existing setups. The system is maintaining complete transparency to customers who receive detailed information about the costs along with transaction status. This partnership has established a secure connection between 11,500 financial institutions across 200 territories and 200 countries enabling the world's GDP movement approximately every three days.[13]

9. Challenges in Cross Border Digital Payments

Cross-border digital payments offer significant opportunities for global financial integration but also present unique challenges. These issues span regulatory compliance, cybersecurity threats, operational inefficiencies, financial volatility, and barriers to financial inclusion. Addressing these challenges is essential for creating a seamless and secure international payment ecosystem.

One of the biggest hurdles is regulatory compliance. Different countries have distinct Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, making it difficult for international banks to meet all legal requirements. For instance, China's Personal Data Protection Law (PIPL) imposes stricter data security mandates than many other jurisdictions, complicating cross-border transactions. Cybercriminals take advantage of regulatory inconsistencies across countries, making fraud detection harder. In many developing economies, weak cybersecurity laws expose financial institutions to financial hacks, while AI-generated identities further undermine KYC and AML enforcement.

Cybersecurity threats pose another significant risk to cross-border digital payments. Cybercriminals exploit user trust through phishing attacks, tricking individuals into revealing sensitive financial data. Additionally, malware infiltration compromises payment security, leading to financial losses and data breaches. As digital transactions grow, financial institutions become more attractive targets for cyber threats, increasing the urgency for enhanced security measures.

Beyond security concerns, currency volatility and taxation differences create financial challenges. Exchange rate fluctuations during payment processing can lead to unexpected deficits or surpluses, affecting transaction profitability. Moreover, differing tax regulations across countries require careful

[12]https://www.swift.com/news-events/press-releases/swift-and-wise-join-forces-expand-cross-border-payment-options-globally

[13]https://www.crowdfundinsider.com/2024/09/230357-global-fintech-wise-and-swift-to-expand-cross-border-payments-options

evaluation by both buyers and sellers, as tax implications can significantly impact the fairness and viability of agreements.

Operational challenges further complicate international digital payments. Financial institutions must comply with international sanctions (such as US restrictions on Russia), which can limit payment accessibility in certain regions. Time zone differences and traditional banking hours also cause delays in transaction processing. Many banks still rely on legacy systems like SWIFT, slowing down cross-border payments despite the availability of faster digital solutions. While blockchain technology has the potential to enhance security and speed, widespread adoption remains slow due to regulatory uncertainties. Similarly, IoT-based payment automation faces difficulties in integrating with existing financial infrastructures.

In many developing regions, infrastructure limitations hinder digital payment adoption. Unreliable internet connectivity prevents seamless digital transactions, making modern payment systems impractical. Businesses also remain hesitant to embrace cryptocurrency and blockchain technology due to unclear regulations and security concerns. Without significant improvements in payment network infrastructure, these regions will continue to struggle with financial inclusion.

Finally, high remittance costs and lack of banking access create financial exclusion for millions. The high cost of sending money abroad, especially in South Asia and Africa, prevents many individuals from fully participating in the digital economy. Over 1.4 billion people worldwide remain unbanked, lacking access to secure digital payment options. Additionally, inadequate identity verification and credit history make it difficult for individuals to save, invest, or obtain credit. This lack of financial inclusion limits economic growth and exacerbates income inequality in underdeveloped regions.

10. Policy Recommendations for India's Domestic and Global Digital Payment Ecosystem

I. Recommendations for India

a. Digital Identity & KYC Repository

i. Establish a national digital identity framework integrating Aadhaar, DigiLocker, CKYC, and fintech players.

ii. Expand CKYC to non-financial sectors, fintech startups, and digital service providers.

b. IoT-Powered Security in AML

i. Mandate IoT-based authentication for high-value and cross-border transactions.

ii. Promote fintech innovation grants for AI and IoT-driven security in payments.

c. Blockchain for Domestic Payments & Compliance

i. Pilot blockchain-based verification for domestic digital transactions.

ii. Launch blockchain-powered smart contracts for regulatory compliance and fraud detection.

d. Cybersecurity & Data Protection Framework

i. Set up a real-time digital fraud monitoring system through NPCI, RBI, and CERT-In.

e. Tax Incentives for Compliance

i. Provide tax relief for fintech firms investing in secure, compliant payment solutions.
ii. Incentivize adoption of AML-compliant digital wallets and banking tools.

f. Green & Sustainable Digital Payments

i. Encourage energy-efficient blockchain for UPI & CBDC transactions.
ii. Promote carbon-neutral fintech innovations in the Indian digital economy.

g. Legal Recognition of Digital Currencies

i. Finalize CBDC (Digital Rupee) legal framework under the RBI.
ii. Engage in bilateral agreements for crypto taxation and regulation.

h. FIU Data Sharing & AML Collaboration

i. Strengthen Financial Intelligence Unit (FIU-IND) with AI-driven fraud tracking.
ii. Initiate bilateral AML data-sharing agreements (e.g., with UAE, Singapore, EU).

i. Cross-Border Dispute Resolution Mechanism

i. Develop cross-border payment arbitration laws in Indian courts.
ii. Push for regional dispute resolution frameworks with SAARC, ASEAN, and BRICS nations.

j. Inclusive Financial Access & Digital Literacy

i. Expand UPI Lite & offline payments in rural India.
ii. Strengthen digital literacy campaigns in regional languages.

k. Public-Private Collaboration for Innovation

i. Establish RBI + fintech task forces for digital payment best practices.

II. General Global recommendations

a. Adopt a globally recognized digital identity framework to streamline Know Your Customer (KYC) and customer due diligence (CDD) processes while maintaining stringent financial integrity standards. Also, Develop an international KYC repository for secure, real-time information sharing while ensuring strict data privacy protections.

b. IoT-Powered Security – Integrate IoT-based authentication in AML frameworks to strengthen anti-theft measures in digital transactions.

c. Global FIU Data Sharing – Establish real-time international data-sharing networks among Financial Intelligence Units (FIUs) to detect and prevent financial crimes.

d. Blockchain-Based Payment Networks – Develop a global framework for blockchain-based payment validation, reducing costs and eliminating third-party intermediaries. Promote AI-driven transaction monitoring and blockchain-based smart contracts to enhance transparency, fraud detection, and AML enforcement in global digital payments. Standardize blockchain-based transaction verification to enhance transparency, reduce fraud, and improve cross-border payment traceability.

e. Cybersecurity Framework – Implement global cybersecurity protocols with real-time threat detection and response mechanisms to protect digital payment networks.

f. **Standardized Regulatory Framework** – Establish a global digital payment regulatory framework under international financial bodies like the IMF, BIS, and FATF to ensure uniform compliance, risk management, and anti-money laundering (AML) standards.
g. **Interoperability Mandates** – Develop cross-border payment systems that ensure seamless interoperability between national and regional payment infrastructures, enabling real-time transactions across different currencies and platforms.
h. **Legal Recognition of Digital Currencies** – Encourage international consensus on the classification, taxation, and regulation of cryptocurrencies and central bank digital currencies (CBDCs) to foster transparency and reduce regulatory arbitrage.
i. **Cross-Border Dispute Resolution Mechanism** – Establish an international arbitration mechanism for resolving cross-border payment disputes efficiently, ensuring legal clarity and consumer protection.
j. **Public-Private Collaboration** – Strengthen partnerships between regulatory authorities, financial institutions, and fintech players to develop best practices, innovation-friendly regulations, and continuous compliance monitoring.
k. **Green Digital Payments** – Introduce sustainability guidelines for digital payment systems, encouraging energy-efficient blockchain technologies and environmentally responsible fintech innovations.

11. Conclusion

The advancement of digital payment systems is poised to modernize global trade by expediting transactions while ensuring robust security measures. However, realizing their full potential requires a parallel evolution of international trade regulations that accommodate these technological advancements. A harmonized regulatory framework across jurisdictions is essential to address discrepancies in payment rules, enhance security standards, and rectify systemic inefficiencies within financial networks.

To achieve this, public authorities must collaborate with financial institutions, technology providers, and businesses to develop comprehensive cross-border payment solutions that align with emerging fintech innovations. Regulatory consistency, coupled with strong public-private partnerships, will facilitate the seamless integration of digital payment systems into the global financial ecosystem.

As digital financial frameworks continue to evolve, their role in international trade will become increasingly significant. By streamlining cross-border transactions, improving financial inclusion, reducing costs, strengthening security, and providing valuable economic insights, digital payments contribute to a more efficient and resilient global economy. Moving forward, the integration of these systems into international trade policies will be crucial for fostering economic stability, ensuring equitable trade practices, and supporting sustainable financial growth.

12. References

I. Cross-border payment modernization | J.P. Morgan. (n.d.). https://www.jpmorgan.com/payments/payments-unbound/volume-3/cross-border-payment-modernization

II. IoT Business News. (2024, December 31). The future of payment processing for eCommerce. https://iotbusinessnews.com/2024/12/31/30322-the-future-of-payment-processing-for-ecommerce/

III. Banco Santander & ECB Operations Managers Group. (2022). The impact of New Technologies on the KYC and AML processes. https://www.ecb.europa.eu/paym/groups/pdf/omg/2022/220922/item_4_The_impact_of_New_Technologies-on_the_KYC-and-AML-processes.en.pdf

IV. PricewaterhouseCoopers. (n.d.). Nearly 50% EMEA firms believe AML regulations need more clarity to be more effective. PwC. https://www.pwc.lu/en/press/press-releases-2024/aml-survey-2024.html

V. Kumar, A. (2024, June 6). RBI penalties surge 88% in last 3 years, KYC and AML top violations list. www.business-standard.com. https://www.business-standard.com/finance/news/rbi-penalties-surge-88-in-last-3-years-kyc-and-aml-top-violations-list-124060600486_1.html

VI. Sidhartha. (2024, February 2). Alleged KYC violations, laundering fears led to Paytm Payments Bank curbs. The Times of India. https://timesofindia.indiatimes.com/business/india-business/alleged-kyc-violations-laundering-fears-led-to-paytm-payments-bank-curbs/articleshow/107373489.cms

VII. What developing countries should know about negotiations for a new global agreement on E-Commerce. (n.d.). International Institute for Sustainable Development. https://www.iisd.org/articles/explainer/what-developing-countries-should-know-about-negotiations-new-global-agreement-e

VIII. WITA. (2024, October 17). A vision for the WTO's Global Digital Trade Rules - WITA. https://www.wita.org/blogs/wto-digital-trade-rules/

IX. Binder, E., Reicheneder, L., & European Parliamentary Research Service. (2023). Implementation Appraisal. In EPRS (PE 747.447). https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747447/EPRS_BRI(2023)747447_EN.pdf

X. Nah, Y. & Global Research Institute of International Trade. (2020). Leveraging the USMCA: How to Maximize Profits from Digital Trade in North America [Report]. https://griit.org/wp-content/uploads/2023/03/Leveraging-the-USMCA_and_Digital_Trade_Part-I_Final.pdf

XI. A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) VVA: Ivan Bosch Chen, Davide Fina, Pierre Hausemer, Andrej Henžel, Christian Neumann, Nelly Patroclou, Charu Wilkinson. CEPS: Willem Pieter De Groen, Tamás Kiss-Galfalvi, Jelmer Nagtegaal, Inna Oliinyk, Meryen Gökten, Fredrik Andersson, Beatriz Pozo, Agustina Korenblit, Tobias Lannoo.

XII. SUMMARY OF THE REGIONAL COMPREHENSIVE ECONOMIC PARTNERSHIP AGREEMENT https://asean.org/wp-content/uploads/2020/11/Summary-of-the-RCEP-Agreement.pdf

XIII. Fang, Y. (2024, December 4). Between the Chinese approach to digital trade and the DEPA regulatory framework: convergence, conflicts and beyond. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5055314#:~:text=However%2C%20China's%20accession%20to%20the,trade%2C%20both%20regionally%20and%20globally.

XIV. New Zealand Ministry of Foreign Affairs and Trade. (n.d.). New Zealand Ministry of Foreign Affairs and Trade. https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-modules

XV. Taheri, R., Adams, O., & Adams, O. (2021, October 7). DEPA: the world's first Digital-Only Trade Agreement. Asia Pacific Foundation of Canada. https://www.asiapacific.ca/publication/depa-worlds-first-digital-only-trade-agreement

XVI. Business Today Desk. (2024, November 14). 'UPI's partnerships can streamline transaction routes for users in foreign lands': Mohan K of TechFini. Business Today. https://www.businesstoday.in/personal-finance/story/upis-partnerships-can-streamline-transaction-routes-four-users-in-foreign-lands-mohan-k-of-techfini-453805-2024-11-14

XVII. PayPal makes strategic investment in MercadoLibre. (n.d.-b). PayPal Newsroom. https://newsroom.paypal-corp.com/paypal-makes-strategic-investment-in-mercadolibre