International Research Journal of Business and Social Science

Volume: 11 Issue: 3
July-September, 2025
ISSN:2411-3646

International Research Journal of Business and Social Science
Volume: 11, Issue: 3, 2025

KMF Publishers http://irjbss.net/

DOI: https://doi.org/10.5281/zenodo.16920707

Research Article

KMF Publishers
http://irjbss.net/

OPEN ACCESS

Banking Law and Commercial Transactions: Legal Challenges in the Age of Digital Banking

Md. Parves Sarker*[1]; Labony Akter[1]; Md. Nayeem Haider Hamza[1]; Md. Taive Al Mamun; Sraboni Akter[1]; Kazi Abdul Mannan[1]

[1]Department of Business Administration; [1]Department of Science and Engineering
Shanto-Mariam University of Creative Technology
Uttara, Dhaka, Bangladesh

ABSTRACT

The rapid evolution of digital banking has significantly transformed commercial transactions, prompting complex legal, regulatory, and operational challenges for financial institutions and regulators. This study examines the legal implications and emerging trends associated with digital banking, focusing on cybersecurity, data protection, consumer rights, smart contracts, and cross-border financial governance. Grounded in legal institutionalism and the law and economics approach, the research draws upon comparative legal analysis, case studies, and doctrinal methodology to assess how jurisdictions are adapting to digital finance. The paper reveals that while digital banking fosters financial innovation and inclusion, it also exposes systemic gaps in existing legal frameworks, particularly in developing economies. The study highlights best practices and policy innovations from selected jurisdictions and proposes a harmonised, forward-looking legal approach that balances innovation with robust consumer and financial protections. Ultimately, the research contributes to an informed dialogue on aligning legal regimes with technological advancement in the banking sector.

ARTICLE HISTORY
Received 30 June 2025
Revised 10 July 2025
Accepted 12 July 2025

KEYWORDS
Digital banking, commercial law, cybersecurity, financial regulation, smart contracts, legal harmonisation

CONTACT Md. Parves Sarker, Email: parvessarker28@gmail.com

INTRODUCTION

The global banking sector is undergoing a profound transformation driven by digitalisation. Digital banking services, including mobile banking, internet banking, and app-based payment systems, have revolutionised how financial transactions are executed, offering unprecedented convenience and accessibility. With this advancement, traditional banking models are being challenged, and commercial transactions are increasingly conducted through automated and virtual interfaces.

Despite these benefits, the rise of digital banking introduces complex legal issues, ranging from the enforceability of electronic contracts to data privacy and consumer protection. The shift towards a digital economy requires re-examining foundational principles in banking law and commercial law. Legal systems must adapt to address the ambiguities and risks associated with virtual transactions, cross-border data flows, and technological intermediaries such as fintech platforms.

This article investigates the evolving legal challenges associated with digital banking in the context of commercial transactions. It aims to provide a comprehensive legal analysis of how existing banking and commercial laws accommodate—or fail to accommodate—the complexities of digital platforms. Key areas of inquiry include regulatory compliance, anti-money laundering (AML) obligations, electronic contract validity, data protection, cybersecurity, and dispute resolution.

LITERATURE REVIEW

The emergence of digital banking has generated a growing body of literature across legal, technological, and regulatory domains. This section explores the evolution of banking law, the transformation of commercial transactions through digitisation, the development of legal frameworks for fintech, and emerging regulatory responses to digital disruption. The review is organised thematically to reflect key scholarly debates and policy developments that shape the contemporary discourse on banking law and digital finance.

Evolution of Banking Law in the Digital Era

Historically, banking law evolved to regulate traditional institutions operating through physical branches and paper-based transactions. Foundational texts such as Cranston's Principles of Banking Law (Cranston, 2018) emphasise the reliance on contract, trust, and fiduciary principles in governing commercial banking practices. However, the rise of digital banking—defined as the delivery of banking services through electronic channels—has challenged these foundational concepts.

Scholars argue that the regulatory architecture has not kept pace with technological advancements (Zetzsche et al., 2017). The traditional focus on prudential regulation, anti-money laundering (AML), and consumer protection now needs to be expanded to include cybersecurity, data privacy, algorithmic fairness, and artificial intelligence in decision-making (Arner & Buckley, 2016). As such, legal scholars are increasingly calling for a recalibration of

banking law that integrates technology-neutral and principle-based frameworks to preserve regulatory relevance in the digital age.

Digitisation and Transformation of Commercial Transactions

The literature on digital commerce highlights how online platforms, mobile payments, blockchain, and smart contracts have disrupted conventional models of commercial transactions (Clifford & Geraint, 2020). These technologies not only reduce transaction costs and processing times but also raise new questions about enforceability, liability, and cross-border jurisdiction.

Notably, Werbach and Cornell (2017) emphasise that blockchain technology and smart contracts challenge the core assumptions of contract law, including offer, acceptance, and intent. While smart contracts are often presented as self-executing and immutable, scholars warn that they may lack the flexibility required by legal systems to accommodate ambiguity, force majeure, or public interest (Fairfield, 2014). These issues become more pronounced in cross-border transactions, where legal uncertainty can undermine trust and hinder adoption.

Further, legal scholars such as Chiu (2016) and Raskin (2017) argue that digital tokens and decentralised finance (DeFi) present uncharted territories for commercial law. These developments necessitate an interdisciplinary understanding of technology, law, and economics to assess their implications for commercial obligations and rights.

Legal Frameworks Governing Digital Banking and Fintech

A significant portion of the literature evaluates how existing legal and regulatory frameworks are adapting to the fintech revolution. Arner, Zetzsche and Veidt (2020) categorise global regulatory responses into three models: the "wait and see" approach, the "test and learn" approach via sandboxes, and proactive regulatory innovation. The United Kingdom's Financial Conduct Authority (FCA) is often cited as a pioneer in sandbox regulation, allowing fintech startups to test services under regulatory oversight (Zetzsche et al., 2017).

In the context of developing countries, the literature highlights that fragmented legal systems, weak enforcement capacity, and limited digital infrastructure hamper effective regulation (Gikay, 2018). This digital divide not only restricts access to digital banking but also increases systemic risk due to the proliferation of unregulated financial technologies. Several authors suggest that a tiered regulatory approach—where regulations are scaled based on risk and innovation—may be more effective in such jurisdictions (Fenwick & Vermeulen, 2017).

Moreover, the literature discusses how financial regulators are increasingly employing regulatory technology (RegTech) to monitor compliance in real-time, using artificial intelligence and big data

analytics (Anagnostopoulos, 2018). These innovations raise new concerns about data protection, algorithmic bias, and the rule of law in automated decision-making systems, prompting calls for "explainable AI" and algorithmic audits in financial services (Binns, 2018).

Consumer Protection in the Digital Banking Ecosystem

A recurring theme in the literature is the erosion of traditional consumer safeguards in digital banking. Several studies identify gaps in disclosure requirements, digital literacy, and grievance redress mechanisms for online financial services (OECD, 2021). For example, Marek and Pousttchi (2019) observe that consumers often accept complex terms and conditions without understanding the implications for privacy, dispute resolution, or liability.

Legal scholars advocate for a rethinking of consumer protection doctrines to include concepts such as digital vulnerability, cyber harassment, and platform responsibility. Chatzara (2020) emphasises the need for adaptive consumer laws that address the evolving nature of digital harm, including identity theft, unauthorised transactions, and fraud facilitated through phishing and social engineering.

In jurisdictions like the European Union, the General Data Protection Regulation (GDPR) has been instrumental in setting high standards for data rights, consent, and cross-border data flow. However, scholars like Kuner (2020) argue that even GDPR falls short in regulating algorithmic decisions and AI-driven credit assessments, which are becoming common in digital lending platforms.

Comparative Legal Approaches

Comparative legal scholarship has provided valuable insights into how jurisdictions are navigating the digital transformation of banking and commercial law. For instance, the U.S. has emphasised innovation and competition, with agencies like the Office of the Comptroller of the Currency (OCC) offering fintech charters to non-bank digital firms (Omarova, 2019). By contrast, the European Union has prioritised harmonisation and consumer protection through initiatives such as the Revised Payment Services Directive (PSD2) and the Markets in Crypto-Assets Regulation (MiCAR) (European Commission, 2023).

Asian jurisdictions offer varied experiences: Singapore and Japan have adopted innovation-friendly regulatory frameworks. At the same time, China has taken a centralised approach with strict data localisation rules and pilot testing of central bank digital currencies (Yao, 2021). These differences highlight the role of institutional context and legal culture in shaping the pace and direction of digital legal reform.

The comparative literature underscores the tension between legal certainty and regulatory flexibility. While rigid legal regimes risk stifling

innovation, overly lenient approaches may create regulatory arbitrage and systemic instability. Scholars suggest a middle path that emphasises risk-based, proportionate regulation and international coordination to manage cross-border digital transactions (Zetzsche et al., 2020).

Gaps in the Literature and Future Research Directions

Despite the growing scholarship, several gaps remain. First, there is limited empirical research on how legal reforms in digital banking affect marginalised populations, small businesses, and informal economies. Second, the integration of Islamic banking principles into digital banking remains underexplored, particularly in the context of Sharia-compliant smart contracts and digital financing instruments.

Additionally, much of the legal literature is siloed, lacking interdisciplinary collaboration with computer science, behavioural economics, and ethics. There is also a scarcity of longitudinal studies assessing the long-term efficacy of digital financial regulation, particularly in the Global South.

Lastly, the literature is still developing frameworks for adjudicating disputes arising from smart contracts and cross-platform financial interactions. As digital banking becomes increasingly global and decentralised, future legal scholarship must engage with transnational legal theories, network governance, and cyber-jurisdiction.

THEORETICAL FRAMEWORK

The legal challenges emerging from the proliferation of digital banking require a robust theoretical foundation to contextualise and interpret their implications. This section outlines the four key theoretical frameworks underpinning this study: Institutional Theory, Regulatory Theory, Legal Realism, and Comparative Legal Analysis. These frameworks provide essential tools for understanding how law, institutions, and policy respond to the disruptive nature of digital financial technologies.

Institutional Theory

Institutional theory focuses on how formal and informal structures evolve in response to external social, technological, and economic pressures. In the context of digital banking, institutional theory explains the interaction between legal institutions and technological innovations. According to Scott (2008), institutions comprise regulative, normative, and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life. This theory underscores the need for legal systems to adapt to the institutional transformation driven by digital banking.

Banking laws traditionally rested on the assumption of physical infrastructure, face-to-face interactions, and paper-based records. However, digital banking introduces non-traditional actors such as fintech companies and neobanks, compelling legal institutions to modify

their governance structures. This adaptation includes the formulation of new licensing regimes, oversight mechanisms, and frameworks for public-private collaboration in areas such as cybersecurity (North, 1990; DiMaggio & Powell, 1983).

Regulatory Theory

Regulatory theory provides a conceptual basis for evaluating how regulators respond to technological disruption and risk in financial services. The theory includes diverse models of regulation such as command-and-control, incentive-based regulation, self-regulation, and meta-regulation. Baldwin and Lodge (2012) emphasise that effective regulation requires balancing goals such as fairness, accountability, flexibility, and innovation.

In digital banking, regulation must account for both systemic risks and consumer-level harms. For example, digital lending powered by machine learning necessitates regulatory scrutiny of algorithmic bias, while open banking raises concerns about data sharing and third-party access. Regulatory theory helps assess whether current frameworks, such as the EU's PSD2 or the U.S.'s fintech charters, adequately protect the interests of stakeholders while enabling innovation (Black, 2008).

Moreover, the principle of "regulatory technology neutrality" derived from regulatory theory posits that laws should not favour or discriminate against any specific technology. This approach ensures that legal frameworks are adaptable to evolving innovations such as blockchain, artificial intelligence (AI), and decentralised finance (DeFi) (Brownsword & Goodwin, 2012).

Legal Realism

Legal realism asserts that the actual practice of law and the behaviour of legal actors often diverge from formal legal doctrines. This perspective, championed by scholars such as Jerome Frank and Karl Llewellyn, is essential in analysing how digital banking challenges traditional legal constructs. Legal realism shifts focus from abstract legal principles to how laws operate in practical, often unpredictable, settings (Frank, 1930).

For instance, while the legal enforceability of electronic contracts is theoretically established under laws such as the U.S. E-SIGN Act or the UNCITRAL Model Law on Electronic Commerce, actual enforcement may be hampered by technological failures, identity verification issues, or jurisdictional ambiguity. Legal realism encourages a nuanced understanding of these practical barriers and promotes empirical and contextual analysis in law-making (Llewellyn, 1960).

In this study, legal realism is instrumental in assessing the effectiveness of dispute resolution mechanisms in digital banking platforms, the reliability of digital evidence in commercial

litigation, and the real-world challenges consumers face in protecting their rights online.

Comparative Legal Analysis

Comparative legal analysis serves as both a methodology and a theoretical lens. It involves systematically comparing legal systems to identify best practices, legal transplants, and contextual adaptations. In the realm of digital banking, this approach is vital due to the cross-border nature of online transactions and the heterogeneity of national regulatory regimes (Zweigert & Kötz, 1998).

By examining legal systems in jurisdictions such as the United States, the European Union, the United Kingdom, Singapore, and India, this research identifies how different regulatory cultures address common challenges. For example, the EU's General Data Protection Regulation (GDPR) imposes strict data protection requirements, while Singapore's Payment Services Act encourages fintech innovation through a modular licensing framework. These comparisons provide valuable insights into how laws can be harmonised or mutually recognised to enhance legal certainty in digital commercial transactions (Michaels, 2006). Comparative analysis also reveals regulatory gaps and asymmetries. While some countries have embraced regulatory sandboxes and digital identity systems, others lag, creating barriers to cross-border interoperability. The comparative lens helps policymakers assess the transferability of legal innovations and the feasibility of regional or global regulatory coordination (Siems, 2018).

Integrating these four theoretical frameworks provides a comprehensive analytical foundation for understanding the legal challenges of digital banking. Institutional theory explains the need for legal and regulatory evolution, while regulatory theory offers models for designing effective rules. Legal realism grounds the analysis in practical realities, and comparative analysis highlights diverse regulatory experiences and opportunities for harmonisation.

These frameworks collectively support the thesis that existing legal structures must evolve to address the unique challenges posed by digital banking. They also provide the intellectual scaffolding for the subsequent analysis in this study, enabling a balanced evaluation of normative principles and empirical realities.

RESEARCH METHODOLOGY

This research adopts a qualitative legal methodology designed to explore the legal complexities of digital banking and its intersection with commercial transactions. The study integrates doctrinal, comparative, and policy-oriented methods to analyse primary and secondary legal materials. This hybrid approach is particularly suited for understanding the evolving nature of digital banking regulation and identifying key areas where legal reforms are necessary.

Doctrinal Legal Research

At the core of this study is doctrinal legal research, which involves the systematic exposition, analysis, and interpretation of legal rules, case law, statutory instruments, and regulatory policies governing digital banking and commercial transactions. This method allows for the identification of legal principles, ambiguities, inconsistencies, and gaps within the current regulatory framework. The doctrinal approach facilitates a structured analysis of various legal sources, such as the Payment Services Directive (EU), the Electronic Fund Transfer Act (USA), the General Data Protection Regulation (EU), and national banking laws in jurisdictions like the United Kingdom, Singapore, and India (Hutchinson & Duncan, 2012).

Case law from common law and civil law systems is also examined to explore judicial reasoning in matters concerning digital signatures, e-contracts, liability for cyber breaches, and enforcement of consumer rights in the digital space. By synthesising these legal sources, the doctrinal methodology helps clarify how traditional legal doctrines are evolving in response to technological innovations in banking.

Comparative Legal Research

Given the global scope of digital banking and the cross-border nature of many financial transactions, this research employs a comparative legal methodology to evaluate how different jurisdictions address similar regulatory challenges. Jurisdictions chosen for comparison include:

- United States – Regulatory developments by the Federal Reserve, Office of the Comptroller of the Currency (OCC), and Consumer Financial Protection Bureau (CFPB).
- European Union – Implementation of PSD2, GDPR, and European Banking Authority (EBA) guidelines.
- United Kingdom – Policies from the Financial Conduct Authority (FCA) and participation in regulatory sandboxes.
- Singapore – Fintech innovations regulated by the Monetary Authority of Singapore (MAS).
- India – RBI regulations on digital payments, data localisation, and fintech licensing.

This comparative lens enables the identification of best practices, legal innovations, and regulatory convergence or divergence trends. It provides a grounded understanding of how national legal systems respond to global financial developments (Siems, 2018).

Normative and Policy Analysis

In addition to doctrinal and comparative methods, the study integrates normative legal analysis to evaluate the efficacy of existing laws in achieving public policy goals such as consumer protection, data security, financial inclusion, and systemic risk mitigation. Policy documents from international organisations such as the Bank for

International Settlements (BIS), International Monetary Fund (IMF), Financial Action Task Force (FATF), and World Bank are critically reviewed to assess global standards and expectations.

This policy-oriented analysis also incorporates elements of legal reform and law-in-action perspectives to highlight the practical implications of regulatory gaps and inconsistencies. It evaluates the tension between innovation and regulation, proposing policy recommendations where necessary.

Sources and Data Collection

Legal sources include:

- Primary legislation and statutory instruments.
- Judicial decisions from the apex and appellate courts.
- Regulatory frameworks, guidance notes, and policy papers.
- Treaties and international conventions relevant to data protection, e-commerce, and financial services.

Secondary sources include peer-reviewed journal articles, monographs, law reform commission reports, and white papers from industry experts. Legal databases such as Westlaw, LexisNexis, HeinOnline, and official government and institutional websites are used to access these materials.

Delimitations and Limitations

The research focuses on banking law and commercial transactions related to digital banking technologies. It does not cover the broader financial ecosystem, such as insurance tech (insurtech) or capital markets. Also, this study is qualitative and does not include empirical data from financial institutions or consumers. While this limits the capacity to assess the impact of digital banking quantitatively, the legal analysis offers deep interpretative insights into the adequacy and adaptability of the legal frameworks.

Justification of Methodology

The chosen methodological framework allows for a holistic understanding of the interplay between law and digital technology in banking. Doctrinal analysis offers a firm grounding in legal rules; comparative analysis brings a global perspective; and policy-oriented approaches ensure that the findings are relevant for law reform and future regulatory strategies (Chynoweth, 2008; Salter & Mason, 2007).

Digital Banking and the Evolution of Commercial Transactions

Digital banking is fundamentally reshaping the framework of commercial transactions by digitising financial services, increasing transaction speeds, reducing overhead costs, and expanding access to financial markets. This transformation is primarily driven by innovations in financial technology (fintech), mobile platforms, blockchain systems, and regulatory

innovations such as open banking. As these technologies become integral to commerce, the legal underpinnings of commercial transactions—particularly those governing contract formation, execution, enforcement, and dispute resolution—must adapt accordingly.

Defining Digital Banking in the Commercial Context

Digital banking refers to the delivery of banking services via electronic means, including web-based platforms, mobile applications, and Application Programming Interfaces (APIs). These services include account management, fund transfers, loan applications, bill payments, and real-time financial data access. With the proliferation of fintech firms and neobanks—financial institutions operating without physical branches—the line between traditional banking and digital platforms has blurred (Zetzsche et al., 2020).

Digital banking is particularly influential in the realm of business-to-business (B2B) and business-to-consumer (B2C) commercial transactions, where electronic payments, automated invoicing, and online financing mechanisms have become standard. The use of digital banking systems reduces reliance on physical documents and manual verification processes, facilitating real-time transaction processing and global scalability (Arner, Barberis, & Buckley, 2016).

Electronic Contracts and E-Signatures

One of the most significant developments in digital commercial transactions is the widespread use of electronic contracts (e-contracts) and electronic signatures (e-signatures). These innovations challenge traditional concepts of contract law, which often presume physical presence or written documentation.

The legal recognition of e-contracts varies across jurisdictions. In the United States, the Electronic Signatures in Global and National Commerce (E-SIGN) Act and the Uniform Electronic Transactions Act (UETA) establish that electronic signatures and contracts carry the same legal weight as their handwritten counterparts. Similarly, the European Union's eIDAS Regulation provides a harmonised legal framework for electronic identification and trust services (European Commission, 2014).

Despite formal recognition, practical concerns remain about consent, authentication, and technological integrity. For example, contract enforceability may be questioned when digital signatures are produced via unverified platforms or when blockchain-based smart contracts lack interpretability within existing legal frameworks (Mik, 2017).

The Role of Smart Contracts and Blockchain Technology

Smart contracts—self-executing contracts with terms directly written into code—represent a growing innovation in digital commercial

transactions. They are typically deployed on blockchain platforms like Ethereum and execute predefined actions when specific conditions are met (Werbach & Cornell, 2017).

From a legal standpoint, smart contracts raise issues regarding contractual intention, consent, and error. Their rigid execution can produce outcomes inconsistent with the parties' intentions, and the immutability of blockchain can make errors or disputes difficult to resolve. Courts and regulators are beginning to grapple with these concerns. However, there is limited jurisprudence on how traditional doctrines—such as offer and acceptance, mistake, and frustration—apply to smart contracts (Allen & Berg, 2020).

Jurisdiction and Conflict of Laws in Cross-Border Digital Transactions

Digital banking facilitates cross-border transactions with minimal friction, raising significant jurisdictional challenges. Determining the applicable law, competent jurisdiction, and dispute resolution mechanism becomes complex when parties operate in different legal systems.

Many jurisdictions rely on conflict-of-laws rules, such as those codified in the Rome I Regulation (EU) or the Restatement (Second) of Conflict of Laws (USA). However, these frameworks are often inadequate for addressing transactions that involve decentralised platforms or anonymised digital identities.

Further, digital banking transactions frequently rely on intermediary services, including payment processors and cloud computing platforms, which different regulatory regimes may govern. This fragmentation complicates legal accountability and remedies in the event of transactional disputes or security breaches (Lloyd, 2020).

Cybersecurity, Data Protection, and Transactional Integrity

The transition to digital banking heightens the importance of cybersecurity and data protection in commercial transactions. Breaches can compromise personal data, financial records, and intellectual property, resulting in significant financial and reputational losses.

Laws such as the General Data Protection Regulation (GDPR) in the EU and the Gramm-Leach-Bliley Act (GLBA) in the US impose strict obligations on data controllers and processors. In the commercial banking context, these obligations include ensuring secure storage, processing, and transmission of client data, as well as protocols for breach notification and consumer redress (Kuner, 2017).

In addition to statutory protections, industry standards such as ISO/IEC 27001 and the Payment Card Industry Data Security Standard (PCI DSS) guide best practices for transactional security. However, legal enforcement often lags behind technological advancements, leaving critical gaps in the protection of commercial transactions.

Financial Inclusion and Commercial Access

Digital banking also plays a pivotal role in enhancing financial inclusion, particularly for micro-entrepreneurs and small-to-medium enterprises (SMEs) in emerging markets. Mobile money platforms, such as M-Pesa in Kenya or bKash in Bangladesh, enable users to engage in formal commercial activities without traditional banking infrastructure (Demirgüç-Kunt et al., 2018).

Legal recognition of such platforms is essential for integrating them into mainstream commercial frameworks. Governments and regulators have begun to acknowledge these innovations through regulatory sandboxes and tiered licensing regimes. Nonetheless, disparities in access to digital infrastructure and digital literacy remain legal and policy challenges.

Legal Implications of Real-Time Payments and Open Banking

Real-time payment systems and open banking APIs are transforming how commercial entities interact with financial data and execute transactions. Real-time payments reduce settlement risk but require robust fraud prevention mechanisms and dispute resolution systems.

Open banking mandates, such as the EU's PSD2, compel banks to share customer data with third-party providers (TPPs) upon user consent. This regulatory shift aims to foster innovation and competition but also introduces new legal responsibilities for data custodianship, liability allocation, and consumer protection (Zetzsche, Buckley, Arner, & Barberis, 2020).

Digital banking is revolutionising commercial transactions by providing faster, more inclusive, and technologically integrated financial services. However, these benefits are accompanied by significant legal challenges. Issues surrounding contract enforceability, jurisdiction, cybersecurity, and financial access underscore the need for adaptive and forward-looking legal frameworks. As digital banking becomes a cornerstone of the global economy, legal systems must evolve to safeguard transactional integrity while enabling innovation.

COMPARATIVE LEGAL PERSPECTIVES

The regulatory responses to digital banking and the accompanying legal challenges differ significantly across jurisdictions. A comparative legal analysis highlights both the diversity and convergence of legal systems in addressing issues arising from the transformation of commercial transactions through digital banking. This section examines the regulatory approaches of the European Union, the United States, and selected Asian jurisdictions to identify best practices and legal harmonisation efforts.

The European Union Framework

The European Union (EU) has adopted a comprehensive and integrated approach to digital

banking through regulations, directives, and supervisory guidance. Key legislative instruments include the Revised Payment Services Directive (PSD2), the General Data Protection Regulation (GDPR), and the Digital Operational Resilience Act (DORA).

PSD2 introduced the concept of open banking by mandating banks to share customer data with licensed third-party providers upon the customer's consent. This provision enhances competition but introduces significant data security and liability issues (Zetzsche & Barberis, 2020). Meanwhile, GDPR reinforces customer rights over data privacy and security, compelling digital banks to implement robust consent mechanisms and data protection protocols (Voigt & Bussche, 2017).

DORA, a more recent regulation, aims to standardise IT risk management across financial entities by requiring the implementation of security protocols and incident reporting mechanisms. The EU's approach demonstrates a strong preference for harmonised legal obligations and cross-border regulatory cooperation.

The United States Approach

In contrast, the United States adopts a more fragmented and sector-based regulatory framework. A combination of federal and state-level laws and agencies governs financial services. Institutions such as the Office of the Comptroller of the Currency (OCC), the Federal Reserve, and the Consumer Financial Protection Bureau (CFPB) oversee various aspects of digital banking.

The Bank Secrecy Act (BSA) and the USA PATRIOT Act form the backbone of anti-money laundering (AML) and know-your-customer (KYC) obligations in the digital banking domain. The Gramm-Leach-Bliley Act (GLBA) regulates data sharing and privacy, while cybersecurity is addressed through guidelines issued by agencies like the Federal Financial Institutions Examination Council (FFIEC) (Crosman, 2019). Although the U.S. lacks a centralised privacy law akin to the GDPR, some states, like California, have enacted comprehensive laws, such as the California Consumer Privacy Act (CCPA), creating a patchwork legal environment. This fragmentation leads to compliance complexities for digital banks operating across multiple jurisdictions.

Asian Jurisdictions: China and Singapore

Asian jurisdictions exhibit varied levels of regulatory maturity in digital banking. China has embraced a top-down, innovation-centric regulatory approach. The People's Bank of China (PBoC) has issued guidelines on fintech development and data security, including the 2021 Personal Information Protection Law (PIPL), which mirrors aspects of the GDPR (Xia, 2022).

China's digital banking sector is dominated by tech giants such as Ant Group and Tencent,

prompting the government to introduce sector-specific rules to curb monopolistic practices and ensure financial stability. The Digital Yuan (e-CNY) further exemplifies China's proactive stance in integrating central bank digital currencies (CBDCs) with commercial banking activities (Arner, Barberis, & Buckley, 2021).

Singapore, meanwhile, offers a well-balanced regulatory framework grounded in principles of innovation and risk management. The Monetary Authority of Singapore (MAS) has issued the Payment Services Act (PSA), which consolidates licensing and regulatory requirements for digital payment services. MAS also supports a regulatory sandbox to allow fintech experimentation under controlled conditions (MAS, 2020).

Singapore's approach is often cited as a model of proactive regulation, offering clarity and predictability while encouraging innovation. Its commitment to cybersecurity is reinforced through the Cybersecurity Act 2018, which mandates critical information infrastructure protection.

Legal Harmonisation and Divergence

A significant challenge in comparative digital banking regulation is the divergence in legal traditions and regulatory philosophies. While the EU leans toward centralised regulation with a consumer-rights orientation, the U.S. favours a market-driven, sectoral approach. Asian jurisdictions, especially Singapore, have adopted hybrid models emphasising agility, innovation, and oversight.

Harmonisation efforts are gradually emerging through international standards set by bodies such as the Basel Committee on Banking Supervision, the Financial Stability Board, and the International Organisation for Standardisation (ISO). These organisations promote principles of interoperability, digital identity management, and cross-border data flows (Bains, 2021).

Nevertheless, achieving substantive harmonisation is constrained by jurisdictional sovereignty, differing legal cultures, and geopolitical interests. Digital banking's inherently borderless nature amplifies these complexities, requiring ongoing dialogue between regulators and stakeholders at both bilateral and multilateral levels.

Lessons and Best Practices

Comparative analysis reveals several best practices that can guide national policy-making: Integrated legal frameworks such as those in the EU and Singapore offer greater predictability and consistency.

- Strong data protection laws and cybersecurity protocols are essential to maintain user trust and regulatory compliance.
- Regulatory sandboxes allow for innovation without compromising consumer safety. Cross-border regulatory cooperation is necessary to

address global risks such as cybercrime and money laundering.

The comparative legal landscape shows that while no one-size-fits-all solution exists, converging trends toward data protection, operational resilience, and innovation support are shaping the future of digital banking law.

FUTURE OF BANKING LAW AND COMMERCIAL TRANSACTIONS

As digital transformation continues to reshape financial services, the future of banking law and commercial transactions is poised for unprecedented change. The increasing integration of digital platforms, artificial intelligence (AI), decentralised finance (DeFi), and blockchain technologies is reshaping not only the operational dynamics of financial institutions but also the legal frameworks governing these interactions. This section examines the anticipated trajectory of banking law, emerging regulatory trends, and the implications for commercial transactions in the digital economy.

Anticipated Evolution in Banking Law

Banking law must evolve to accommodate technological innovations that redefine traditional financial relationships. One of the most significant transformations involves the move from centralised to decentralised systems. Decentralised finance, powered by blockchain and smart contracts, bypasses traditional intermediaries, raising questions about the applicability of existing laws that presume centralised oversight (Zetzsche, Buckley, Arner, & Barberis, 2020).

As financial services become increasingly algorithmic, AI systems in credit scoring, fraud detection, and automated customer interactions introduce novel legal concerns. Questions of liability, fairness, transparency, and algorithmic bias must be addressed, potentially requiring amendments or new legislation such as AI-specific regulatory frameworks (Baker & Dellaert, 2019).

Another development relates to the definition and oversight of digital assets. The emergence of cryptocurrencies and stablecoins has forced regulators to reassess what constitutes a "currency," "security," or "commodity," creating new obligations for legal classification and financial reporting (Gomber, & Weber, 2018).

Regulatory Innovation and Digital Sandboxes

To keep pace with innovation, regulatory authorities are adopting agile governance models such as digital regulatory sandboxes. These controlled environments allow fintech firms to test innovative solutions under regulator supervision, fostering innovation while maintaining compliance (Arner, Barberis, & Buckley, 2017). The United Kingdom's Financial Conduct Authority (FCA) and Singapore's Monetary Authority (MAS) are leading examples of this approach.

Such sandboxes highlight a shift from command-and-control regulation to more adaptive, outcome-based models. This change emphasises collaboration between regulators and industry actors and represents a fundamental rethinking of how financial law is formulated and enforced in the digital age.

Global Harmonisation and Cross-Border Challenges

The borderless nature of digital financial services necessitates greater harmonisation of banking laws across jurisdictions. Cross-border data transfers, digital identity verification, and interoperable payment systems demand consistency in legal standards for consumer protection, cybersecurity, and anti-money laundering (AML) compliance (Schillig, 2021).

The Basel Committee on Banking Supervision and the Financial Action Task Force (FATF) are playing important roles in coordinating global standards. However, challenges persist, especially in the face of nationalistic data policies and geopolitical fragmentation. As digital finance expands, international legal frameworks—such as model laws or treaties—may become crucial to address jurisdictional conflicts and facilitate secure, seamless global transactions (FATF, 2020).

Ethical and Human Rights Dimensions

Future banking laws must address not only technical and financial aspects but also ethical and human rights concerns. Financial inclusion, data justice, and protection from digital surveillance are increasingly central to discussions about the role of banking in a digitised society (UNCTAD, 2020).

AI-based financial tools can potentially exclude marginalised groups due to algorithmic bias or data poverty, while surveillance-driven fintech models can compromise individual privacy and autonomy. Legal reforms will need to incorporate rights-based approaches, ensuring that innovation does not come at the expense of fairness and justice (Rahwan, 2018).

Smart Contracts and Automation of Transactions

The future of commercial transactions is inextricably linked with smart contracts—self-executing code on blockchain platforms that automatically enforce contractual obligations. These tools reduce transaction costs and increase efficiency but present novel legal issues around contract formation, enforceability, and remedies in cases of breach or malfunction (Werbach & Cornell, 2017).

Legal systems must determine whether smart contracts satisfy the elements of traditional contract law—offer, acceptance, and consideration—and how courts should interpret code as contractual language. Jurisdictions like the U.S. state of Arizona and the U.K. Law Commission are already exploring legislative recognition of smart contracts, which will likely proliferate globally.

Role of Central Bank Digital Currencies (CBDCs)

Another transformative development in digital banking is the introduction of Central Bank Digital Currencies. CBDCs, unlike cryptocurrencies, are state-backed digital forms of fiat currency and promise to modernise payment systems, enhance monetary policy transmission, and reduce reliance on private intermediaries (Auer & Böhme, 2020).

The implementation of CBDCs will require foundational changes in banking law, including legal tender status, liability frameworks for digital wallets, and privacy safeguards. Countries like China, Sweden, and the Bahamas are at the forefront of CBDC development, offering blueprints for future regulatory reforms.

Preparing Legal Education and Practice for Digital Banking

To meet the challenges of the evolving financial ecosystem, legal education and professional training must adapt. Law schools and bar associations should integrate fintech law, data privacy, cybersecurity, and AI ethics into their curricula. Legal practitioners must also develop interdisciplinary expertise, combining legal reasoning with technological fluency (Schwarcz, 2021).

Emerging certifications in fintech law, joint degree programs, and continuing legal education on digital regulatory compliance will be essential in preparing the next generation of banking lawyers.

The confluence of technology, regulatory innovation, and global coordination will shape the future of banking law and commercial transactions. The legal system must remain responsive, adaptive, and inclusive, capable of fostering innovation while safeguarding rights and ensuring financial stability. As the digital financial ecosystem matures, the law will play an indispensable role in framing this transformation, ensuring that the benefits of digital banking are broadly shared and legally sustainable.

CONCLUSION AND POLICY RECOMMENDATIONS

The advent of digital banking has fundamentally reshaped the landscape of commercial transactions, offering new opportunities for financial inclusion, efficiency, and innovation. However, these transformations have simultaneously exposed substantial legal and regulatory challenges that traditional banking laws and commercial frameworks were not designed to address. This research has shown that key concerns include regulatory fragmentation, cybersecurity vulnerabilities, inadequacies in consumer protection, and ambiguities surrounding smart contracts and cross-border digital financial services.

Through a theoretical lens combining legal institutionalism and the law and economics

approach, and using doctrinal and comparative legal methods, the paper has examined how various jurisdictions—such as the European Union, the United States, and emerging economies in Asia—are adapting to the challenges of digital finance. It has become evident that while developed countries have made notable progress in regulatory modernisation and digital infrastructure, developing nations often struggle with institutional capacity, legal inertia, and digital divides.

In light of these findings, several policy recommendations are proposed to ensure the future resilience and inclusiveness of banking law in the digital age:

- Legal Harmonisation and Cross-Border Cooperation: There is an urgent need for international and regional legal harmonisation to facilitate interoperability of financial regulations. Multilateral institutions, such as the Financial Action Task Force (FATF) and the Bank for International Settlements (BIS), should work closely with national regulators to establish common standards for data privacy, consumer rights, and cybersecurity.
- Dynamic Regulatory Sandboxes: Jurisdictions should implement flexible, innovation-driven regulatory sandboxes that allow fintech startups to experiment under supervision. These frameworks should be iterative and tailored to national legal capacities but informed by global best practices.
- Strengthening Consumer Protection: Legal frameworks must evolve to address digital fraud, algorithmic discrimination, and unfair contractual terms in online banking. Enhanced disclosure obligations, algorithmic audits, and mandatory grievance redress mechanisms should be adopted.
- Investment in Digital Legal Infrastructure: Governments and financial regulators should invest in digital registries, AI-powered regulatory monitoring systems (RegTech), and innovative contract validation platforms to keep pace with the digitisation of commerce.
- Inclusive Legal Reforms: Special attention must be given to ensuring that reforms accommodate the interests of marginalised communities, small and medium enterprises (SMEs), and digitally underserved regions, thereby ensuring equitable access to digital banking.

In conclusion, the future of banking law and commercial transactions rests on the legal system's ability to remain adaptive, inclusive, and proactive. Legal scholars, policymakers, and financial institutions must collaborate to create a balanced ecosystem that fosters trust, innovation, and resilience in the digital age. Without such a concerted effort, the promise of digital banking

may remain unrealised or, worse, deepen existing legal and financial inequalities.

REFERENCES

Allen, D. W., & Berg, C. (2020). Smart contracts: The essential guide to blockchain applications in the real world. Journal of Institutional Economics, 16(1), 1–20.

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business, 100, 7–25.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? Georgetown Journal of International Law, 47(4), 1271–1319.

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). Fintech and regtech: Impact on regulators and banks. Journal of Banking Regulation, 19(4), 1–14.

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Veidt, R. (2020). Sustainability, fintech and financial inclusion. European Business Organisation Law Review, 21(1), 7–35.

Arner, D. W., Barberis, J., & Buckley, R. P. (2021). The evolution of central bank digital currencies. Journal of International Economic Law, 24(3), 585–603.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: Theory, strategy, and practice (2nd ed.). Oxford University Press.

Bains, P. (2021). Cross-border payments: A vision for the future. Financial Stability Board. https://www.fsb.org

Baker, T., & Dellaert, B. G. C. (2019). Regulating robo advice across the financial services industry. Iowa Law Review, 103(3), 713–740.

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & Governance, 2(2), 137–164.

Binns, R. (2018). Algorithmic accountability and transparency in the GDPR. Philosophy & Technology, 31(4), 543–563.

Brownsword, R., & Goodwin, M. (2012). Law and the technologies of the twenty-first century: Text and materials. Cambridge University Press.

Chatzara, V. (2020). Digital finance and consumer protection: Challenges and opportunities. European Journal of Risk Regulation, 11(4), 681–696.

Chiu, I. H. (2016). A new era in fintech regulation: Market-enabling or market-harnessing? Law and Financial Markets Review, 10(4), 226–236.

Chynoweth, P. (2008). Legal research. In A. Knight & L. Ruddock (Eds.), Advanced research methods in the built environment (pp. 28–38). Wiley-Blackwell.

Cranston, R. (2018). Principles of Banking Law (3rd ed.). Oxford University Press.

Crosman, P. (2019). U.S. bank regulators issue new cybersecurity guidance. American Banker. https://www.americanbanker.com

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution. World Bank Group.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields. American Sociological Review, 48(2), 147–160.

European Commission. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services. Retrieved from https://eur-lex.europa.eu/

FATF. (2020). FATF report to the G20 finance ministers and central bank governors on so-called stablecoins. Financial Action Task Force.

Fairfield, J. (2014). Smart contracts, Bitcoin bots, and consumer protection. Washington and Lee Law Review, 71(2), 535–568.

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2017). Regulation tomorrow: What happens when technology is faster than the law? American University Business Law Review, 6(3), 561–594.

Frank, J. (1930). Law and the modern mind. Brentano's.

Gikay, A. A. (2018). Financial consumer protection in the fintech age. Journal of Consumer Policy, 41(4), 463–487.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220–265.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83–119.

Kim, N. S. (2013). Wrap contracts: Foundations and ramifications. Oxford University Press.

Kuner, C. (2017). Transborder data flows and data privacy law. Oxford University Press.

Kuner, C. (2020). Transborder data flows and data privacy law. Oxford Handbook of International Economic Law.

Llewellyn, K. N. (1960). The common law tradition: Deciding appeals. Little, Brown and Company.

Lloyd, I. J. (2020). Information technology law (9th ed.). Oxford University Press.

Marek, R., & Pousttchi, K. (2019). Impact of digitalisation on the legal framework for banking. Electronic Markets, 29(3), 453–470.

Michaels, R. (2006). The functional method of comparative law. In M. Reimann & R. Zimmermann (Eds.), The Oxford

Handbook of Comparative Law (pp. 339–382). Oxford University Press.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real-world complexity. Law, Innovation and Technology, 9(2), 269–300.

Monetary Authority of Singapore (MAS). (2020). Payment Services Act Guide. https://www.mas.gov.sg

North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press.

OECD. (2021). Digital transformation and financial consumer protection. OECD Publishing.

Omarova, S. T. (2019). New tech v. new deal: Fintech as a system threat. Yale Journal on Regulation, 36(2), 735–793.

Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. Ethics and Information Technology, 20(1), 5–14.

Raskin, M. (2017). The law and legality of smart contracts. Georgetown Law Technology Review, 1(2), 305–341.

Salter, M., & Mason, J. (2007). Writing law dissertations: An introduction and guide to the conduct of legal research. Pearson Education.

Schillig, M. (2021). Regulating digital finance: Between innovation and financial stability. Law and Financial Markets Review, 15(1), 1–18.

Scholten, M. (2021). Blockchain and the law: Redesigning code-based governance. Harvard Journal of Law & Technology, 34(2), 345–386.

Schwarcz, S. L. (2021). Artificial intelligence, legal change, and separation of powers. Northwestern University Law Review, 115(4), 1161–1194.

Scott, W. R. (2008). Institutions and organisations: Ideas and interests (3rd ed.). Sage Publications.

Siems, M. M. (2018). Comparative law (2nd ed.). Cambridge University Press.

Srinivasan, S. (2020). India's data protection framework: A review of the Personal Data Protection Bill. Indian Journal of Law and Technology, 16(1), 1–30.

UNCTAD. (2020). Digital Economy Report 2020: Cross-border data flows and development. United Nations Conference on Trade and Development.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.

Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313–382.

Xia, M. (2022). China's Personal Information Protection Law: Toward a new era of digital regulation. Asian Journal of Law and Society, 9(1), 15–32.

Yao, Q. (2021). A systematic framework for the development of central bank digital currency. Springer.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of

data-driven finance. New York University Journal of Law and Business, 14(2), 393–446.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). Decentralised finance (DeFi). Journal of Financial Regulation, 6(2), 172–203.

Zweigert, K., & Kötz, H. (1998). Introduction to comparative law (T. Weir, Trans., 3rd ed.). Oxford University Press.