

The adoption of digital payments in emerging economies: challenges and policy responses

Jayaprada Putrevu and Charilaos Mertzanis

Jayaprada Putrevu and Charilaos Mertzanis are both based at the College of Business Administration, Abu Dhabi University, Abu Dhabi, United Arab Emirates.

Abstract

Purpose – *This paper aims to present a comprehensive overview of the emergence and significance of digital payments, focusing on their impact on competitiveness and the need for policy interventions. In addition, it explores the design of policies that promote the adoption of digital payments, highlighting the benefits they offer to providers and users.*

Design/methodology/approach – *The paper examines the technological advances that have driven the growth of digital payment systems. It identifies key requirements for successful adoption and discusses the associated risks, along with potential strategies to mitigate these risks.*

Findings – *The findings emphasize the importance of responsible implementation and safeguarding the well-being of end users to fully realize the benefits of digital payment adoption. Understanding the inherent risks and establishing effective risk mitigation mechanisms are crucial. This necessitates the development of appropriate infrastructure to support the provision of digital payment services.*

Research limitations/implications – *More research is needed to gain deeper insights into how emerging global trends in financial technology should be analyzed and understood by policymakers, service providers and users.*

Practical implications – *The findings of this study can guide policymakers, private sector managers and consumers in comprehending the effects of emerging digitalization trends and determining their adoption responses accordingly.*

Originality/value – *This paper stands out as one of the few research contributions that provide comprehensive and actionable policy recommendations to facilitate a smooth transition to a digital payments ecosystem that benefits all stakeholders.*

Keywords *Digital payments, Digital risks, Regulation, Policy, Developing countries*

Paper type *Technical paper*

1. Introduction

The global digital payments market encompasses the exchange of money and transactions conducted electronically through digital channels and platforms. It involves a variety of payment methods, such as mobile payments, online transfers, e-wallets, digital currencies and other electronic payment systems (McKinsey, 2022). Participants in this market include financial institutions, technology companies, payment processors, intermediaries and consumers. In recent years, the global digital payments market has witnessed rapid growth due to several factors. These include increased internet and smartphone usage, the rising adoption of digital commerce, evolving consumer preferences and technological advancements (Boar and Szemere, 2020). It has become an integral part of the modern economy, offering convenience, efficiency and improved financial inclusion for individuals and businesses worldwide. As of September 2021, the global digital payments market was experiencing substantial growth and was projected to continue expanding in the future.

Received 10 June 2023
Revised 21 July 2023
Accepted 30 August 2023

This paper forms part of a special section "Multi-level socio-economic determinants of mobile money adoption in the Middle East and North Africa", guest edited by Dimitrios Reppas and Glenn Muschert.

According to a report by Statista (2022), the market's size was valued at approximately US \$4.7tn in 2020. It is worth noting that this figure encompasses various digital payment methods and includes transactions between businesses (B2B), businesses and consumers (B2C) and consumer-to-consumer transactions.

The global digital payments market, while experiencing continuous growth and development, faces various challenges and potential obstacles in the future. First, the expansion of digital payment systems brings an increased risk of cybersecurity threats and fraud (Krishna *et al.*, 2022). Cybercriminals are constantly finding new ways to exploit vulnerabilities in payment networks, leading to data breaches, identity theft and financial fraud. It is crucial to ensure robust security measures and implement effective fraud prevention strategies to maintain consumer trust. Second, the digital payments market operates within a complex regulatory landscape (Ehrentraud *et al.*, 2021). Governments and regulatory bodies continually adapt regulations to address emerging technologies, consumer protection, anti-money laundering (AML) and data privacy concerns. Keeping up with evolving regulations while fostering innovation and maintaining compliance can be challenging for digital payment providers. Third, the digital payments market consists of numerous platforms, payment providers and technologies (Kantar Public, 2022). Ensuring interoperability and standardization across different systems and networks remains a challenge. Establishing common standards and protocols can enhance efficiency, reduce friction and promote seamless transactions between various digital payment platforms. Fourth, although digital payments offer opportunities for financial inclusion, certain segments of the population still face barriers to access and adoption (BMGF, 2019). Limited internet connectivity, lack of digital literacy and restricted access to financial services in underserved regions can hinder the widespread adoption of digital payments. Bridging the digital divide and promoting inclusivity will be crucial to unlock the full potential of digital payments. Finally, digital payments rely on robust infrastructure and reliable connectivity (Universal Digital Payments Network [UDPN], 2022). However, in some areas, particularly in developing regions, inadequate infrastructure and limited internet connectivity can hinder the adoption and usage of digital payment systems. Expanding and improving infrastructure, including mobile networks and internet access, will be crucial to enable broader participation in the digital economy. Addressing these challenges will require collaboration among stakeholders, including governments, financial institutions, technology providers and regulators.

However, despite the market's rapid growth, digital payments have not yet fully replaced cash. Public demand for cash remains steady, both as a means of payment and as a store of value (The Committee on Payments and Market Infrastructure [CPMI], 2023). Although the digitalization of payments is a global trend, payment habits still differ across countries. The broad digital payment adoption challenge remains important and needs to be addressed from both a theoretical and policy perspective. Most studies analyzing digital payments primarily adopt an individual user technology adoption perspective. Their focus is on understanding the factors that influence individuals' decision-making processes, delving into psychological, sociological or behavioral aspects. These studies investigate how individuals perceive, evaluate and adopt technology within specific contexts (Jegerson and Hussain, 2022; Jagrić *et al.*, 2022; Sivathanu, 2019). Although these papers provide valuable insights, they offer limited comprehensive guidance on relevant policies. In contrast, policy studies take a broader approach, examining emerging trends in the policy landscape and the impact of policies on diverse stakeholders, including governments, industries and society. These studies prioritize the design, implementation and evaluation of policies that aim to achieve specific goals. They aspire to generate insights and recommendations that can be applied and relevant across various contexts and populations. Moreover, policy studies consider the interests and perspectives of multiple stakeholders, ensuring a comprehensive understanding of the policy implications.

The aim of this paper is to provide a comprehensive overview of the emergence and significance of digital payments in terms of enhancing competitiveness and promoting economic growth. The paper examines the technological advancements that have led to the rise and expansion of digital payment systems. It also identifies the key requirements for the successful adoption of these systems and discusses the inherent risks associated with digital payments, along with potential strategies for risk mitigation.

It is important to note that there is no universally accepted definition of digital payments (Khando *et al.*, 2023). The term “digital payments” can refer to partially digital, primarily digital or fully digital transactions. For instance, a partially digital payment involves the use of cash by both the payer and payee, facilitated through third-party agents based on digital interbank transfers. On the other hand, a primarily digital payment occurs when the payer initiates the digital transfer of funds to an agent, who then digitally transfers the cash to the payee. The characterization of digital payments varies depending on the emphasis placed on the payer–payee interface, the payment instrument or other elements. These choices become particularly important when attempting to estimate the number or proportion of digital payments under specific conditions. The characterization of digital payments determines how they are measured.

For these reasons, this paper aims to provide a comprehensive analysis of the digital payments landscape and identifies crucial considerations for implementing an efficient and inclusive digital payments system. The paper is organized in a way that highlights the key issues and aspects of the digital payments system, offering guidance for policy intervention. It uses various approaches, including conceptual analysis, historical references, quantitative data and qualitative information derived from case studies.

Section 2 of the paper explores the significance of the digital payments system (Feyen, 2021) and discusses the evolving landscape, technological advancements and essential components of the infrastructure. It emphasizes power dynamics, information technology, payment procedures and key players in the domain. Section 3 focuses on challenges in establishing a digital payments system (Sahi *et al.*, 2022). It addresses risks related to network structure, interoperability, insufficient liquidity, malfunctioning payment means, operational complexity, information dissemination and fraud vulnerabilities. In Section 4, potential strategies to mitigate risks in digital payments are examined (Ehrentraud *et al.*, 2021). It emphasizes understanding risks faced by consumers and the need for reliable, communication-driven mitigation strategies for social protection and financial inclusion. Section 5 concludes with policy insights.

2. Importance of digital payments

2.1 Digital payments landscape

The rise of financial technology and digital payment services has prompted policymakers to examine their potential benefits for financial development and stability, as well as the associated risks and the need for appropriate regulation (Risman *et al.*, 2021). Significant developments and experiments have occurred in payment services, clearing and settlements, covering several types of payments such as large-value, retail, wholesale and international transactions. The landscape of retail payment services has undergone significant changes driven by diverse motivations, including the promotion of cashless transactions, fostering competition, enhancing financial inclusion, facilitating financial integration and encouraging innovation in banking relationships (IMF, 2017). The risks to financial stability posed by digital payment services are substantial and their size relative to the overall financial system has drawn policy attention to their growth and the related regulatory and supervisory issues (The Financial Stability Board [FSB], 2019a, 2019b; IMF, 2019).

Regulation of payment systems and payment service providers is undertaken for several reasons ([Khiaonarong and Goh, 2020](#)). These reasons include maintaining the integrity of monetary transactions, safeguarding financial stability by ensuring the finality of settlement in monetary transactions and protecting financial consumers in relation to nonfiat money forms like e-money and book-money, which involve credit risks. The entry and expansion of large technology firms, commonly known as Big Tech, into the payment services market may influence the impact of digital payment services on the growth and stability of the financial system.

The evolving landscape of digital payment services suggests that, as market structures change, legal frameworks and regulatory approaches need to shift from entity-based regulation to activities-based regulation. Traditional financial regulation has focused on regulating the prudential and conduct of business behavior of financial intermediaries that provide financial services, such as payments ([He et al., 2017](#)). Prudential regimes will need to be reassessed to bring new types of service providers, including large technology firms and digital payment services, within the regulatory scope where necessary ([The Financial Stability Board \[FSB\], 2019a, 2019b](#); [BIS, 2019](#); [Restoy, 2019](#); [Frost et al., 2019](#)).

Certain countries have already modernized their legal frameworks and regulatory approaches to payment services taking a risk-focused and activity-based perspective ([Committee on Payments and Market Infrastructures \[CPMI\], 2014](#)). These modernization efforts aim to foster efficiency, innovation, safety and competition. However, the emergence of new business models in the provision of payment services has obscured the lines between payment services and instruments, which may require specific authorization as both e-money issuer and e-money transfer businesses. Furthermore, if a payment instrument is not properly authorized, it will create regulatory gaps. Consequently, the modernization of regulatory oversight frameworks requires adjusting the scope of regulated activities and aligning relevant regulations to accommodate new business models in the provision of payments services. At the same time, regulatory frameworks must address the new risks associated with these new business models.

The evolution of digital payments has shifted the private businesses' focus to digital-first strategies ([Klapper, 2023](#)). The emerging business models center around the integration of technology with a company's payment system, replacing the traditional paper-based approach. As cash payments decline, customers are increasingly embracing contactless payment options and streamlined e-commerce transactions. Studies suggest that around half of the world's population may prefer digital wallets by 2024 ([McKinsey, 2022](#)). To remain competitive, it is advisable to explore how automation, payment integration and other digital solutions can optimize business processes and meet customer demands. Businesses are actively seeking ways to embrace the new digital landscape. For instance, they are adopting innovative methods to streamline operational processes. Transitioning from paper checks to digital payments has compelled financial service providers to explore innovative approaches to cater to customer needs. Payment processors are now relying on new networks, such as unique identifying tokens that use e-mail or phone numbers for secure financial transactions. Mobile remote deposit capture is another example that enables consumers to process transactions conveniently from any location and at their own pace. These digital-first shifts are likely to continue as trends like card-not-present transactions, online shopping and curbside pickup gain traction. Adapting to these changes through the introduction of mobile payment terminals, touchless payment options and efficient in-store pickup methods can enhance customer satisfaction and provide a competitive edge.

Security has become a top priority for businesses as digital transformation advances and cybercriminals become more sophisticated. The increasing threat of fraud poses significant challenges, with the US card industry projected to lose over US\$165bn to fraud in the next decade. Identity theft, accounting for over 70% of fraud cases, is particularly prevalent in

card-not-present transactions. Hence, it is crucial to proactively implement security measures that keep pace with technological advancements. Furthermore, businesses are progressively prioritizing cost-effective digital payments (Kantar Public, 2022). For example, Mastercard reports that reducing the use of checks by 10% could save the industry up to US\$1.2bn annually. Whether your business operates in the B2B or B2C sector, adopting digital payments can enhance efficiency and accelerate payment processing. To begin this transformation, review your payment processes and identify areas where automation and other digital technologies can streamline operations. Embracing a cloud-based accounting system instead of manual spreadsheet entry can provide up-to-date data and faster payment processing.

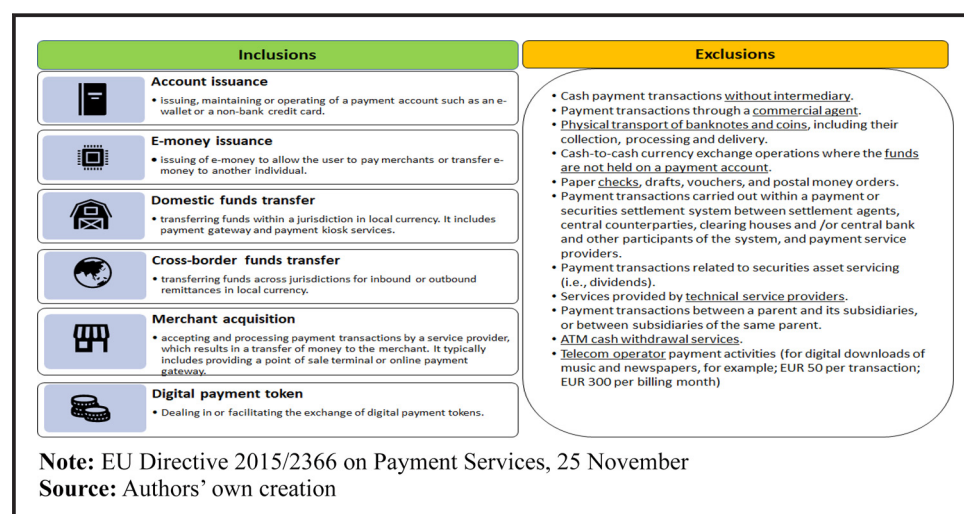
2.2 Digital payments framework

The initial step of the framework should involve determining whether an economic activity performed by an entity qualifies as a regulated payment service. Accurately identifying payment activities is crucial for establishing effective supervisory and oversight frameworks, while minimizing unnecessary regulatory duplications and overlaps. International best practices propose organizing such activities into six categories, as clearly outlined in the European Union (EU) Payment Services Directive (PSD2) (2015): e-money issuance, account issuance, digital payment token issuance, domestic funds transfer, international funds transfer and intermediary acquisition (Figure 1). These activity categories primarily relate to user payment services than the payment systems themselves.

Figure 1 presents a taxonomy of digital payment services. It is important to note that the list of payment activities may vary across countries. Some countries have implemented regulatory sandboxes, which exclude certain digital activities. In addition, there are other forms of payment services, such as tokenization, third-party initiation, payment aggregation, payment gateways and white label automatic teller machine (ATM)/point of sale (POS) provision, that are not considered core payment activities.

Clear and explicit payment service laws play a crucial role in providing clarity regarding various activities. For instance, the EU's Payment Services Directive 2 (PSD2/2015, Article 4) defines payment services by listing eight specific types of activities in the directive's annex. The EU PSD2 (Annex 1) categorizes payment services as follows:

Figure 1 Taxonomy of payment services



- services enabling cash deposits and operations related to payment accounts;
- services enabling cash withdrawals and associated operations;
- execution of payment transactions;
- execution of payment transactions with credit lines;
- money remittance;
- issuance and acquisition of payment instruments;
- payment initiation services; and
- account information services.

However, payment service laws also exclude certain payment activities from their scope. For example, the EU PSD2 (Article 3) excludes 15 types of payment activities, such as paper-based payment instruments, cash transactions and ATM cash withdrawals within the EU. The regulatory consideration of specific payment services may vary across countries, depending on factors such as the prevalence of mobile money usage.

In developing a comprehensive framework, it is essential to identify new entrants, including Big Tech companies that engage in payment services as part of their technology-related and e-commerce activities (Table 1). Some of these companies offer payment services through independent business units, leveraging their data analytics, network effects and integrated platforms for payment processing and settlement. They operate either through overlay systems (using third-party infrastructures) or proprietary systems (using their own infrastructures). Common applications include online banking, digital wallets, domestic and international fund transfers. Table 1 provides an overview of payment services offered by selected Big Tech companies.

2.3 Technological developments and digital payments growth

The evolution of payment technology in modern economies can be traced back to early banking payment systems, which still retain certain structural characteristics from their origins (Humphrey *et al.*, 1996). Initially, payments were made through the exchange of valuable items like gold coins. The emergence of goldsmith banks in the 16th century introduced ledgers to track client deposits, enabling payments to be recorded in the ledgers instead of physically exchanging assets. However, this system was limited to clients within the same bank. To facilitate interbank payments, central “clearing” banks were established, where member banks could hold accounts and simplify interbank transactions. In standard payment systems, transactions are reflected by reducing the payer’s account balance and increasing the payee’s account balance. The advancement

Table 1 Payment services provided by selected Big Techs

Type of payment service	Approximate offerings							Tencent WeChat Pay
	Google Pay	Amazon Pay	Facebook Pay	Line Pay	Apple Pay	Baidu Wallet	Alipay	
E-money issuance	N	N	N	Y	Y	Y	Y	Y
Account issuance	Y	Y	Y	Y	Y	Y	Y	Y
Domestic funds transfer	N	Y	Y	Y	Y	Y	Y	Y
International fund transfer	N	N	N	N	N	Y	Y	Y
Digital payment token	N	N	N	N	N	N	N	N
Intermediary acquisition	N	Y	N	Y	Y	Y	Y	Y

Note: Other examples include Nordic countries (Swish, Vipps, MobilePay) and Africa (M-Pesa)

Source: Authors’ own creation

of technology has played a significant role in the recording and transfer of these balances among banks.

Payment systems have been shaped by technological advancements over the past five decades in two primary ways (Boel, 2019). First, paper-based records and ledgers have transitioned to electronic formats, reducing operational risks and enhancing transaction speed. Second, the emergence of faster and cost-effective innovative technology has facilitated new payment schemes, such as digital or mobile money. Despite these technological changes, the fundamental structure of centralized payment systems has remained unchanged. A central ledger and a clearing bank, often operated by the central bank, continue to facilitate settlement. Each participant in a transaction, typically a commercial bank, maintains an account balance that is recorded both in the central bank's ledger and the participant's internal ledger. The participant bank's ledger includes balances by individual clients, smaller banks or bank branches.

Recent years have witnessed various developments in payment technologies and alternative currencies (Kantar Public, 2022). Certain innovations aim to improve service accessibility for a wider user base, such as mobile phone-based payments, while maintaining dependence on a reliable central authority. However, more recent innovations have introduced decentralized payment systems that rely on cryptography rather than a central bank. These decentralized systems represent a fundamentally different approach to traditional payment systems. New digital currencies are backed by local currencies and technically maintain a fixed exchange rate with existing currencies. Digital currencies can serve as potential forms of money or alternative payment systems. For example, although Bitcoin introduced both a new means of payment and a payment technology, the distributed ledger technology (DLT) could be used for payments without new currency creation. Thus, central banks can use a distributed ledger payment system to issue digital-only liabilities like those represented by digital currencies (Haldane and Qvigstad, 2014).

Over time, several significant innovations have played a crucial role in transforming the payments system (Bech and Hancock, 2020). The first innovation involves the provision of “wrapper” services, which aim to enhance accessibility and functionality of existing payment system designs. These services do not introduce new currencies or core payment systems but instead build upon the existing infrastructure. Their purpose can be attracted to new market entrants or encourage incumbents to improve their market share and reduce reliance on costly payment systems. Illustrations of these innovations encompass Apple Pay, Google Wallet and Paym. These platforms establish a connection between users' mobile phone numbers and their bank accounts, facilitating payments through preexisting systems.

The second innovation is the development of e-money systems, which represent new digital payment schemes, in which fiat money is stored as digital credit on a smart card or in a system provider's ledger but still uses local currency (Humphrey *et al.*, 1996). E-money is a debt-like instrument issued by entities to facilitate payment transactions. It can be viewed from different perspectives (Adrian and Griffoli, 2019). From a balance sheet standpoint, it represents a fixed value claim and liability for the issuer, typically redeemable in fiat currency at face value upon demand. The issuer must hold enough liquid assets to always meet redemption requests. However, the value of these assets is subject to certain risks depending on how they are invested. From a user perspective, e-money offers convenience as a digital alternative to cash, allowing easy payments for goods and services and transfers to others. Users perceive it as functionally equivalent to fiat currency as they can redeem it at face value at any time. Technically, e-money can be stored on hardware-based devices (e.g. chip cards) or software-based products (e.g. e-wallets) that may or may not require real-time network connectivity. In addition, DLT applications serve as a basis for digital representations of value that can be used for payments. Due to the guarantee of redemption, e-money is exposed to run risk like constant net asset value funds but with the

distinction that the issuer may default if unable to redeem all outstanding e-money fully, unlike money market funds. One successful e-money example is Kenya's M-Pesa mobile money service, which provides user access to payment and other financial services through the users' mobile phones. In regions with limited access to traditional banking facilities, the development and adoption of new payment systems fulfils unmet demand for payment services. Conversely, in more advanced economies, the adoption of new payment systems is motivated by the substantial user costs and usability features associated with existing systems.

The third innovation is the introduction of "credit in local currency" schemes, where users place trust in a new currency as a unit of account and a medium of exchange ([Naqvi and Southgate, 2013](#)). These schemes involve private companies accepting money in exchange for the provision of an alternative means of payment that can operate within a specific platform. However, these new payment schemes rely on existing payment systems for money transfers. Local currencies function in a comparable manner, where individuals exchange them for a localized equivalent that can be used within a specific geographical area. The Bristol Pound in the UK, for instance, frequently maintains a fixed exchange rate with the pound sterling and seeks to encourage local spending and regional economic sustainability.

The fourth innovation encompasses the development of "digital currency" schemes ([Brainard, 2019](#)). These schemes introduce both a new currency and a new decentralized payment system. One defining feature of digital currency schemes is the publicly visible ledger shared among a network of computing participants. Most digital currencies fall under the category of "cryptocurrencies" as they achieve consensus through cryptographic techniques instead of central bank backing. Digital currencies can also function within centralized ledgers and could seek consensus through alternative noncryptographic means (i.e. the Ripple).

The fifth innovation pertains to the development of DLT, also known as blockchain ([Hacker et al., 2019](#)). This technological advancement plays a fundamental role in the emergence of digital currencies by addressing the "double spending" problem within a decentralized payment system. The concept of distributed ledger originated from various earlier innovations, including the internet, and draws upon principles from cryptography, peer-to-peer networking and game theory. Electronic payment systems often face the challenge of ensuring that money cannot be spent twice. In a physical payment system, the act of transferring currency prevents the payer from duplicating the payment. However, in a digital payments system, mechanisms must exist to prevent double spending, as it is easy to modify or copy digital transaction records. [Table 2](#) presents a table of the key innovations and associated examples that have transformed the payment system.

The success of these innovations rests crucially on having established and maintained user trust in the payments system under evolving market conditions. Trust is a fundamental element in monetary exchange. For money users, it is essential to trust the money issuers not to default, whereas the issuers must trust users to meet financial integrity requirements. Payments can be properly made only when trust is present. The concept of interoperability between different forms of money can be likened to a network of trusted links necessary for transactions. Such networks are easily established within countries where a unitary legal system and the central bank's role in providing a trusted settlement asset simplify the process. Trust is a key issue in cross-border payments too ([Adrian et al., 2023](#)). Trust links must also be established on a bilateral basis among correspondent banks. In these cases, the fixed costs needed to establish trust result in an expensive and concentrated payments system. Furthermore, correspondent banking relationships are dwindling, especially for lower-income countries, leading to exclusion from international payment networks. Although some central banks in certain countries facilitate cross-border payments, many lack the

Table 2 Innovations that have transformed the payment system

<i>Types of payment innovation</i>	<i>Examples of payments innovation</i>
The first innovation involves “wrapper” services that enhance accessibility and functionality without introducing new currencies or core payment systems	■ Examples include Apple Pay, Google Wallet and Paym ■ These platforms connect users’ mobile phone numbers with their bank accounts, facilitating payments through existing systems
The second innovation is “mobile money” systems, representing new digital payment schemes using local currency	■ Kenya’s M-Pesa is an example, providing financial services through mobile phones in areas with limited access to traditional banking ■ In advanced economies, new payment systems are adopted due to user costs and usability features
The third innovation is “credit in local currency” schemes, where users trust a new currency for payment within a specific platform	■ These schemes often rely on existing payment systems for money transfers ■ Local currencies like the Bristol Pound encourage local spending and regional economic sustainability
The fourth innovation involves “digital currency” schemes introducing new decentralized payment systems (e.g. cryptos)	■ Digital currencies use publicly visible ledgers and consensus through cryptographic techniques ■ Some digital currencies operate within centralized ledgers with alternative consensus methods like Ripple
The fifth innovation is distributed ledger technology or blockchain, addressing the “double spending” problem in decentralized payment systems	■ Distributed ledger draws on principles from cryptography, peer-to-peer networking and game theory ■ It prevents double spending in digital payments, where copying or modifying digital records is possible
Source: Authors’ own creation	

trust necessary to do so with each other. Consequently, links between central banks exist among countries that share geopolitical proximity or historical connections.

In the traditional banking system, which currently uses computerized versions of paper-based records, the double spend problem is mitigated by specialized entities, typically banks, that maintain master ledgers serving as the authoritative records of individuals’ money holdings. These entities hold accounts recorded in a centralized ledger maintained by a central authority, such as a central bank. Those with access to the ledger can prevent any transaction they deem invalid. To participate in the digital payment system, users must have trust that these centralized ledgers are honestly and reliably maintained. The “double spend” problem can be alternatively addressed by establishing a fully decentralized payments system, which shares the ledger structure among all system participants and uses a consensus mechanism to determine valid changes to the ledger (i.e. recorded transactions). In this case, the participants or a central authority does not need to rely on the integrity of a single transacting entity. The distributed payment system’s key feature lies in how consensus is achieved regarding proposed ledger changes or transactions.

However, reaching the required consensus presents significant challenges to the system’s integrity (Zachariadis *et al.*, 2019). Achieving consensus among network participants at the absence of complete user trust has long been recognized as a game theory problem. Merely accepting all statements is insufficient, as it incentivizes dishonesty for personal gain. Similarly, relying on user voting to determine ledger changes is prone to manipulation, as a single actor can create multiple nodes on the network to distort the voting process. Digital currencies address these challenges by incorporating game theory principles, recognizing that a proposed change to the ledger, on its own, carries little weight as it can

be easily issued at no cost. To gain acceptance as a true change, those proposing modifications (“miners” who verify transactions) must demonstrate a clear cost-based rationale. Therefore, the effective functionality of digital currencies within a decentralized payment system requires users participating in the transaction verification process (miners) to provide cryptographic “proof of work” to demonstrate they have expended computational resources before their modifications are implemented. As part of the transaction process, certain digital currencies incur costs by destroying a small portion of the currency involved.

2.4 Digital payments infrastructure

To enable innovative digital payment mechanisms that are user-friendly, secure and cost-effective, the development of reliable and efficient infrastructures is essential. These infrastructures have the potential to enhance financial access, promote financial inclusion and support the digital payments system. The establishment of a functional digital payments system relies on four foundational infrastructures ([Khiaonarong et al., 2021](#)). First, the electricity supply needs to be reliable. Digital payments depend on a constant supply of adequate power, which is often not secured in urban and rural settings. Second, the information and communications technology (ICT) infrastructure must be robust. Third, the basic payment structure (i.e. automated clearing houses, payment switches and system interoperability) must be in place. Fourth, identification infrastructure (i.e. digital identification ID) is required for digital payment service providers to carry out their due diligence and enable digital access. These infrastructures are described below, emphasizing their significance:

First, a dependable and uninterrupted supply of electricity plays a crucial role in facilitating digital payments, as highlighted by [Agur et al. \(2022\)](#). Interruptions in power supply have adverse effects on users, suppliers and access points of payment services. One significant consequence is the limited deployment of ATMs, particularly in rural areas, due to the lack of reliable power. In fact, payment service providers often cite this as a primary reason for the restricted availability of ATMs. It is worth noting that regions with the highest concentration of financially underserved individuals typically coincide with areas lacking reliable access to electricity. To address this challenge, it is important to incentivize private vendors to offer solutions that mitigate the adverse effect of power outages on ATM transactions and therefore on the efficiency of payment services.

Second, the quality and affordability of ICT infrastructure have a direct impact on users, providers and access points of digital payment services. The significant increase in global mobile phone subscriptions ([GSMA, 2019](#)) holds the potential for enabling digital payments, provided that sufficient network coverage is secured. In 2018, approximately 12.7% of the world's population resided in areas with inadequate mobile coverage, especially rural areas with low population density and literacy rate as well as inadequate infrastructure and access to electricity grids (World Bank, 2014). Consequently, mobile network operators (MNOs) often find little economic incentive to expand their services into these areas ([Biscaye et al., 2015](#)). A feasible solution involves granting operator authorizations to MNOs, contingent upon fulfilling certain criteria such as providing minimum telecommunication network coverage and internet access in designated areas, along with offering payment services. The absence of reliable or nonexistent mobile network and internet coverage presents a substantial barrier to the widespread adoption of digital payment services. MNOs play a crucial role in ensuring sufficient connectivity and reliability of GSM networks to instill trust in mobile money among B2C, particularly those in low-income groups who heavily rely on mobile money wallets for conducting digital payments ([Gilman et al., 2013](#)).

Third, to establish effective financial services that encompass transaction accounts and digital payment mechanisms, it is essential to have appropriate financial infrastructure in place ([Demirgüç-Kunt et al., 2021](#)). This infrastructure encompasses payment exchanges,

large-value clearing and settlement systems, data-sharing and data-hosting facilities, as well as information systems like credit registry and collateral value databases. Furthermore, intermediary-level arrangements, such as centralized client account management systems, play a crucial role in enhancing the commercial feasibility of providing affordable payments and financial services to lower-income groups.

Efficient and cost-effective electronic fund transfers are facilitated by centralized and interoperable clearing and settlement systems. Interbank systems specifically designed for retail payments, along with the availability of payment switches for card and mobile transactions, contribute to the swift, secure and economical processing of payment transactions. This, in turn, leads to increased quantity and efficiency of transactions while expanding the network of access points (such as ATMs, agents, POS terminals or branches) accessible to individuals with limited access. Although restrictions on infrastructure access may exist, they should adhere to the principles of proportionality, transparency and nondiscrimination. However, the challenges related to technological and commercial viability are often compounded by limitations in human resources availability and competence, which also need to be addressed.

Infrastructure challenges can be further compounded by legal, regulatory and governance factors (Ehrentraud *et al.*, 2021). For instance, certain service providers like credit cooperatives, nonbank mobile financial service (MFS) providers, savings associations and microfinance institutions may face difficulties in meeting the risk management and operational requirements necessary to participate in payment system operations. Specialized MFS providers require a robust payments system that accommodates both traditional and mobile transactions by clients and tied agents, while also interacting with other payment infrastructures, such as payment switches, to manage high transaction volumes (McGrath and Susie, 2013). Furthermore, inefficient governance infrastructure can thwart business operations and erode confidence in MFSs. Excessive costs of direct participation in payment infrastructures often hinder smaller authorized payment service providers from offering efficient payment services. Finally, regulatory and operational rules governing payment infrastructure systems may prevent certain providers from participating directly, even if they have the necessary infrastructure investments and can afford participation costs. In such cases, technical service providers can collaborate with commercial banks to offer authorized and/or regulated nonbank payment services (depending on the country, this could involve MNOs or their subsidiaries) using the country's existing payments system infrastructure, which these providers would otherwise be legally prohibited from accessing (Almazán and Frydrych, 2015; Navajas, 2015). Banks and MNOs (Big Tech entities) can interact on designated platforms, facilitating the efficient conversion of mobile payment transactions into card transactions, thereby effectively processing them in the clearing and settlement system (Fargallah *et al.*, 2015).

2.5 Digital identification infrastructure

The availability of a dependable client and transaction identification infrastructure, accessible to financial service providers, plays a crucial role in supporting financial access (Alonso, 2020). Difficulties in obtaining proof of identity and associated credentials for transaction parties can create significant barriers to access, particularly in the context of digital payments. Efficient and error-free validation of IDs is essential from a Know Your Customer (KYC) perspective. From a financial inclusion standpoint, the identification infrastructure needs to be robust enough to meet KYC requirements and facilitate efficient verification of individuals' identities (Dahan and Gelb, 2015). Insufficient or inaccurate identification records hinder client access to various financial services and impede effective system oversight and regulatory enforcement. The establishment of digital identification (ID) can address the needs of underprivileged and isolated populations. Modern electronic and biometric technologies can be used in the ID infrastructure to confirm user identities and enhance access to financial services. Moreover, governments can share the costs of such

systems through the formation of public–private partnerships, ensuring sustainability, scalability, fostering innovation and generating revenue streams (World Bank, 2014).

3. Global trends and key players in digital payments

The process of digital transformation that has facilitated the emergence and growth of digital payments has experienced significant momentum worldwide, but in 2020, the global markets were disrupted by the COVID-19 pandemic (Figure 2). Initially, the commerce and finance sectors exhibited the strongest growth in digital transformation, whereas the manufacturing and infrastructure sectors witnessed comparatively lower growth. The digital transformation in the public sector occupied a middle position. However, it is projected to undergo substantial growth in the post-COVID-19 era.

Considerable progress has been witnessed in the global digital payments market, primarily driven by consumer transactions involving online payments for instruments and services, mobile payments at POS through smartphone applications and international money transfers via the internet (digital remittances). Table 3 presents a cross-country breakdown of digital payment transactions, including online processed payments, mobile POS payments using smart devices at the POS, digital consumer commerce transactions (e.g. credit card, online payment providers), online international payments and remittances and money transfers facilitated by online-pure players (e.g. TransferWise). The transaction value represents money transfers out of the selected region and does not encompass B2B payments or card reader transactions at the POS. The digital payments segment recorded a global transaction value of US\$5,204bn in 2020, making it the largest segment. Prior to the pandemic, China held the top position in the global digital payments market, with a transaction value of US \$2,568bn, followed by the USA (US\$1,252bn) and the UK (US\$269bn). In the Middle-East and North Africa (MENA) region, Saudi Arabia emerged as the largest market for digital payments in the same year, with a transaction value of US\$19.76bn, followed by the United Arab Emirates (UAE) (US\$13.71bn), Iran (US\$11.93bn) and Israel (US\$9.45bn). These trends persisted during the pandemic and are expected to continue in the coming years.

Figure 2 Digital transformation spending growth globally by sector, pre- and post-COVID-19

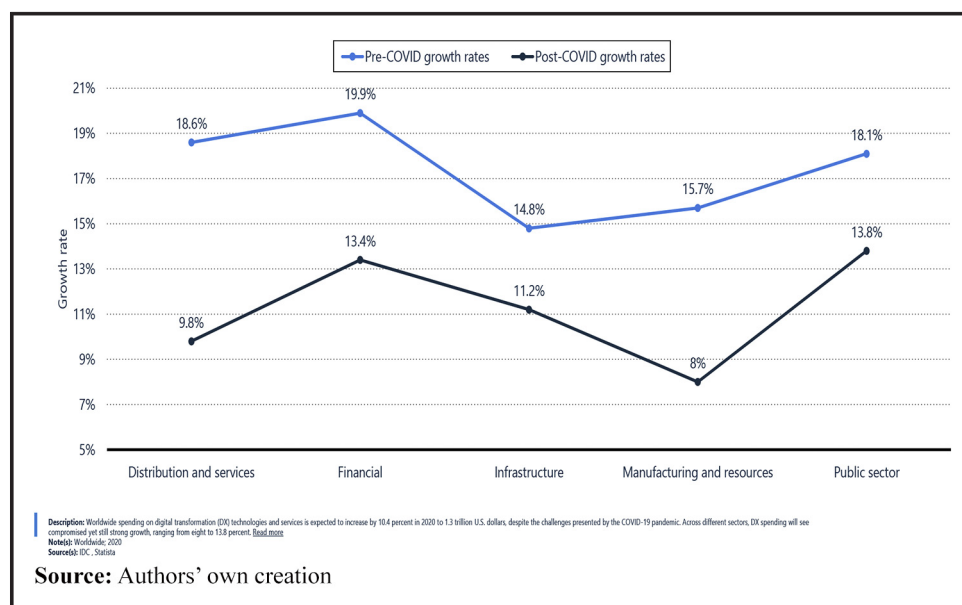


Table 3 Value of digital payments, realized and projected, in selected countries (USD bn)

	2017	2018	2019	2020	2021	2022*	2023*	2024*	2025*	2026*
<i>Panel A. Middle East and North Africa</i>										
Algeria	1.326	1.744	2.413	2.844	3.666	4.272	4.847	5.332	5.788	6.292
Bahrain	0.861	0.942	1.048	1.253	1.463	1.727	1.938	2.167	2.401	2.596
Egypt	4.311	4.574	5.948	8.064	11.64	14.07	16.14	18.09	20.1	22.45
Iran	5.326	6.929	8.826	11.93	17.81	21.54	26.38	32.95	41.17	51.7
Iraq	2.181	3.173	4.23	5.209	6.348	7.643	9.119	10.65	12.32	14.17
Israel	5.266	6.275	7.713	9.451	14.64	19.4	24.77	31.04	37.68	43.77
Jordan	1.332	1.854	2.518	3.887	5.117	6.238	7.377	8.524	9.753	11.12
Kuwait	3.262	3.909	4.761	6.129	8.024	10.08	12.43	14.81	17.42	20.28
Lebanon	1.894	2.079	2.300	2.785	3.463	4.203	4.858	5.538	6.238	6.982
Morocco	2.102	2.500	2.832	2.965	3.93	4.874	5.814	6.771	7.743	8.744
Oman	1.512	1.871	2.444	3.698	5.124	6.514	7.932	9.445	11.07	12.85
Qatar	2.746	3.113	3.424	3.79	4.534	5.457	6.425	7.334	8.294	9.285
Saudi Arabia	8.898	12.12	15.85	19.76	24.98	30.66	36.28	42.06	48.04	54.46
UAE	7.269	8.858	10.65	13.71	18.12	20.15	22	23.95	26.05	28.41
<i>Panel B. Other countries</i>										
Singapore	4.038	5.196	6.748	8.614	13.43	17.18	21.68	26.7	32.3	38.37
Malaysia	4.843	6.704	8.424	9.664	14.38	18.22	22.34	27.04	32.2	37.9
India	42.16	51.3	66.79	88.52	116.9	137.4	158.8	181.1	205.7	233.7
Indonesia	13.63	19.26	28.5	40.01	62.92	71.41	80.15	89.71	100.5	113
China	1,360	1,754	1,989	2,568	2,997	3,318	3,645	3,952	4,292	4,666
UK	172.9	198.2	214	269.3	352.5	436.4	514.2	596.2	685.6	782.1
USA	740.1	867.5	1,019	1,252	1,527	1,801	2,090	2,417	2,787	3,200

Notes: Digital payments report, 2021. Statista. The star (*) indicates estimated values

Source: Authors' own creation

4. Risks and challenges in adopting digital payments

The limited adoption of digital payment technologies can be attributed to a range of factors. Among low-income users, who often face greater vulnerability, lower literacy levels and less familiarity with innovative technologies, the experiences and perceptions of risks associated with digital payment services have a significant impact on client trust and confidence (McKee *et al.*, 2015). This unique segment of users faces distinct consumer risks, which are particularly pronounced or experienced in specific ways. These risks include:

- network or service unreliability leading to the inability to conduct transactions;
- insufficient ATM liquidity or agent availability;
- complex user interfaces and payment processes that hinder ease of use;
- inadequate or nonexistent recourse mechanisms for dispute resolution; and
- user-targeted fraud, which poses a threat to the security of digital payment transactions.

These risks contribute to the limited active use of digital payment technologies, as they undermine the confidence and trust of users, especially those from low-income backgrounds. These risks assume various specific forms (Table 4) and their implications are briefly analyzed below.

4.1 Transactions constraints due to network unreliability

In poor and remote areas targeted by many digital service provider (DSP) programs, weak mobile network coverage poses significant challenges. Users often face frequent network connectivity issues, impacting the functionality of mobile phones and POS devices. This

Table 4 Risks in digital payment transactions

<i>Risk type</i>	<i>Risk form</i>
Network or service unreliability	Distributed denial of service (DDOS) attacks; internet outages; server downtime; cloud service interruptions; data packet loss and latency; power failures; software failures; data breaches and cybersecurity incidents; bandwidth limitations in cases of heavy network congestion; domain name system (DNS) errors in accessing websites; mobile network coverage issues; incompatibility and interoperability problems
Insufficient automatic teller machine (ATM) liquidity or support	Cash shortage in ATMs; ATM cash replenishment delay; out-of-network ATM; low access in rural or remote areas; network connectivity issues; banking agent unavailability; banking system errors and technical glitches; insufficient cash planning
Complex user interfaces and payment processes that hinder ease of use	Overly complicated checkout processes; intricate multi-factor authentication (MFA) processes; complex card verification for online payments; unintuitive payment gateways; cryptocurrency transactions for unfamiliar users; numerous payment options and add-ons; mobile payment apps with excessive permissions; inconsistent user interface elements; poor error handling; slow or unresponsive interfaces
Inadequate or nonexistent recourse mechanisms for dispute resolution	Unauthorized transactions; disputed service charges; nondelivery of services; misleading service product descriptions; fraudulent sellers; double charging or overcharging; tech glitches and errors; subscription cancellations; delayed refunds; lack of customer support
User-targeted fraud and integrity of digital payment transactions	Phishing scams; social engineering; malware and spyware; sim swapping; card skimming; card not present (CNP) fraud; man-in-the-middle (MITM) attacks; fake payment requests; ransomware on decrypting data

Source: Authors' own creation

unreliability severely affects DSP users' access to their periodic payments, leading to various negative consequences. For instance, in the World Food Program's (WFP) digital cash and voucher programs in Africa and the Middle East, inadequate connectivity and pervasive network failures exposed users to financial losses. Transactions were frequently interrupted, leaving payments in a state of uncertainty. In such situations, users often tend to leave their access cards and personal identification numbers (PINs) with their intermediaries, asking them to complete the transaction whenever possible. Unfortunately, this practice resulted in fraudulent or inappropriate agent behavior (El-Huni, 2014; The World Food Program [WFP], 2016). Network or infrastructure failures are common, leading to difficulties for users in accessing their funds and therefore maintain confident in the digital payments system (Islam and Woodard, 2014; InterMedia Africa, 2015; Adewole, 2015). In addition to network connectivity problems, users often face unreliable and inconsistent service schedules by DSPs. Network outages and unattended agent shops further prolonged the waiting time for cashing out and using the transfers (Zimmerman and Bohling, 2015; Islam and Woodard, 2014b). In summary, DSP users in underserved areas encounter frequent network connectivity issues, leading to challenges in accessing their payments and exposing them to various risks and potential fraud.

4.2 Insufficient automatic teller machine liquidity and agent availability

DSP services are commonly distributed in massive quantities and users often withdraw the entire amount in a single day. This puts considerable strain on payment access points, particularly in remote and less secure areas, to fulfill the users' liquidity needs. As a result, users often face extended queues and wait for several hours to collect their payments. In certain instances, they may be advised to return home and repeat the process on another day. This creates a cycle where the scarcity of liquidity undermines users' trust and confidence in the system, prompting them to urgently withdraw all funds at once, further exacerbating liquidity challenges at cash-out points. As an example, during a covert shopping evaluation conducted in WFP Kenya's Cash for Assets (CfA) program, it was found that 21% of users faced difficulties in cashing out their transfers due to insufficient availability of agents, as reported by the WFP (2016). In another mobile cash transfers case

under the WFP Kenya CfA program, users identified liquidity limitations as a major hurdle, considering the long distances they had to travel and the limited presence of M-Pesa agents. In addition, in a mobile cash transfers program implemented in the Philippines, DSPs often could not provide exact withdrawal amounts, leading to payments being distributed to randomly assigned groups. Consequently, users had to find ways to split the payments themselves or accept alternative forms of payment to compensate for the difference (Zimmerman and Bohling, 2015). The practice of bulk transfers in DSPs puts immense pressure on access points to meet liquidity demands, especially in remote areas. This leads to long waiting times for users and perpetuates a cycle where liquidity constraints erode trust in the system, prompting immediate and full withdrawal of funds, further exacerbating liquidity challenges at cash-out points.

4.3 Complex payment processes

The complexity of user interfaces and intricate payment procedures heightens the risk of recurring timeouts due to limited transaction times or of errors and losses due to incorrect transactions. This not only poses risks but also leads to a subpar user experience for all categories of DPS users. However, these risks are particularly pronounced for the least literate and most vulnerable consumer segments, who are initially uncomfortable with or new to digital payment systems. Navigating the digital technology and the various intricate steps required to access payment services presents challenges for these users (WFP, 2016). Furthermore, apart from the inconvenience caused by frequent transaction failures, complex payment processes and user interfaces increase the likelihood of users incurring additional fees charged by DSPs or falling prey to fraud as they seek assistance from others. These issues severely undermine trust in the digital payment system and create a perception of an unwelcoming system, subsequently reducing the likelihood of users embracing and using formal (digital) financial services. In many cases, users of digital payments demonstrate a limited understanding of how the payment schemes, especially the digital payment aspect, function (Zimmerman *et al.*, 2014).

4.4 Weak resource mechanisms

DSP programs frequently exhibit inadequate recourse mechanisms, including avenues for complaints, queries and dispute resolution, which leaves users vulnerable (Zimmerman *et al.*, 2014). Users often lack knowledge or feel confused about the available options for addressing service-related issues, making it difficult for them to resolve payment problems or obtain answers to payment-related inquiries. In several programs, users expressed concerns that lodging complaints could result in the loss of their transfers, leading to a reluctance to report problems. Even when client support or grievance services are available, users may be unaware of them or have had negative experiences, such as being stuck in lengthy automated waiting lines or experiencing call disconnections before speaking to a representative. These situations often lead to frustration in using services, along with potential financial losses from costly phone calls (Islam and Woodard, 2014). Influenced by cultural and personal biases, users often prefer face-to-face problem-solving and frequently seek assistance from intermediaries. However, these intermediaries are not always adequately equipped to address problems, as they may lack the necessary expertise, access to faster support channels and sufficient incentives to allocate time to assist clients (McKee *et al.*, 2015).

4.5 Fraud

DSP users face heightened vulnerability to various forms of fraud, such as unauthorized fees, price inflation at obtaining service and payment skimming. For instance, in the implementation of WFP Kenya's Cash Lite Program, 72% of users who used their bank

cards to pay for commercial transactions experienced higher prices or additional charges (WFP, 2016). Users of digital government-to-person (G2P) programs have also reported incurring extra costs during payment withdrawals (Zimmerman *et al.*, 2014). In India, a survey revealed that 13% of G2P users admitted to paying bribes to intermediaries to access their payments properly (InterMedia India, 2014). Users often lack awareness of the actual charges and fees associated with their payment arrangements, both formally and informally, as well as the precise amount and frequency of their benefits. This leaves them vulnerable to unfair treatment and fraudulent risks. Another prevalent challenge in DSP programs is the protection of PINs. Many users tend to share their PINs with agents or third parties instead of personally entering them into mobile phones or POS devices. It appears that both users and agents often compromise data protection protocols in favor of payment efficiency, particularly when dealing with a large number of users on payday, requiring agents to serve numerous clients quickly (Leonard, 2020).

5. Mitigation of digital payment adoption risks

Evaluating and managing risks associated with digital payments is crucial for the growth of the market (Akanfe *et al.*, 2020; Khiaonarong and Goh, 2020). To comprehensively understand the nature, occurrence and impacts of consumer risks in digital payment systems, it is essential to prioritize reliability, communication and monitoring. These key principles form the foundation of an effective risk mitigation policy, enabling financial inclusion in DSPs. Although these principles are fundamental requirements for providing trustworthy digital payment services, their proper implementation within DSPs ensures that these programs effectively meet their goals of users' financial inclusion. They play a vital role in mitigating consumer risks across various digital payment services. The following policies are significant measures for mitigating these risks:

5.1 Ensure reliability in the payments experience

DSPs use intricate systems involving agents, intermediaries, mobile phones, ATMs and POS devices to reach users. The seamless processing of real-time digital payments within this value chain and payments system heavily relies on robust network connectivity. Conducting thorough risk assessments and implementing contingency plans during the design phase can help mitigate certain risks. This includes measures such as ensuring high-quality intermediary services, adequate training and effective float and liquidity management; enhancing user-friendliness of client interface; and defining clear roles and responsibilities of all actors involved in risk mitigation (Zimmerman and Bohling, 2015).

5.2 Ensure efficient monitoring of automatic teller machine liquidity and user support

To mitigate the risk of inadequate ATM liquidity and limited agent availability and ensure a seamless user experience, a range of strategic measures can be used. For instance, advanced monitoring systems can be implemented to track real-time ATM liquidity levels and agent availability (Cabello, 2013). These systems can promptly alert relevant personnel when liquidity drops below a specified threshold or agent availability becomes constrained. In addition, leveraging historical transaction data enables accurate cash demand forecasting on a per-jurisdiction or regional basis. Data analytics can identify peak usage periods, facilitating better preparation for increased demand. Efficient cash management strategies can be adopted to ensure optimal cash levels at each ATM location. The introduction of cash recycling ATMs, which accept, validate and store deposited cash for future dispensing, aids in enhancing ATM liquidity and reducing cash replenishment frequency. Moreover, implementing dynamic ATM networks equipped with intelligent algorithms allows for redirecting users to nearby ATMs with sufficient liquidity. Collaborative initiatives, such as

ATM sharing agreements between financial institutions, contribute to expanded ATM access and agent network coverage. Remote ATM monitoring and troubleshooting tools can minimize downtime by enabling prompt identification and resolution of issues without physical intervention. Through a combination of these measures, financial institutions can mitigate the risk of insufficient ATM liquidity and agent availability, leading to improved support and services for their users.

5.3 Improve communication between providers and users

Proper training and effective communication are essential for consumers of digital payment services, both during the initial introduction of a new system and continuously after its implementation. Users need comprehensive information about their payment amounts, frequencies and the functioning of the payment mechanism. They also require clear guidance on where to seek assistance in case of any issues. It is crucial to establish well-defined responsibilities among the stakeholders involved in the payment value chain to ensure user confidence and self-control. In addition, implementing a well-structured grievance and complaints mechanism can contribute to program improvement through user feedback ([Abbey et al., 2014](#)). Many initiatives are now focusing on establishing dedicated communication channels and toll-free service facilities specifically catered to DSP users (Zimmerman and Bohling, 2014; [Almazan, 2013](#)).

5.4 Institutionalize monitoring and customize implementation

The integration of digital payment mechanisms has a significant impact on the behaviors and incentives of both users and providers. To ensure the successful implementation of DSP programs, effective monitoring and evaluation of user experiences, preferences and behaviors are crucial. This process helps identify necessary adjustments, whether they are minor modifications or more substantial process changes, to promptly address any issues that may arise. For example, in the fight against fraud, partner banks have collaborated to closely monitor transactions of participating intermediaries in real time and act if transactions exceed specific thresholds, such as freezing a POS device used by an intermediary ([El-Huni, 2014](#)). Likewise, publicly displayed posters have been created to illustrate payment procedures and provide self-protection guidelines, addressing the issue of unauthorized fees and unfair treatment by intermediaries ([WFP, 2016](#)). Furthermore, some intermediaries have been required to modify their fee structures after discovering that agents were passing on POS transaction fees to users or imposing minimum purchase requirements, aiming to reduce costs for agents when serving users ([Leonard, 2020](#)). Successfully transitioning to a digital payments system necessitates adherence to fundamental principles in delivering DSP services. Both the supply side (providers of digital payment services) and the demand side (users of these services) must address the challenges. However, to improve access to DSP services, policies need to go beyond basic principles and implement interventions that foster generalized trust in the digital payment system and ensure that it enhances the value of users' lives. Meeting these challenges requires DSPs to provide reliable, convenient and cost-effective digital payment services. This will involve trade-offs and require the allocation of time and resources by all stakeholders involved.

5.5 Explore innovative technologies: the case of blockchain

As technology advances, the rapid growth of cybersecurity vulnerabilities is becoming a pressing concern. The complexity and risks associated with digital payment systems require immediate action to ensure comprehensive protection. Cyberattacks have become increasingly sophisticated, with advanced ransomware and the rise of professional cyber organizations posing significant threats. In response to these challenges, there is a growing

interest in blockchain-based solutions ([Zachariadis et al., 2019](#); [Zheng et al., 2022](#)). Blockchain, a decentralized distributed ledger operating without a central authority, offers potential in enhancing cyber defense and preventing fraudulent activities due to its decentralized, immutable and transparent nature.

Exploring the role of blockchain technology in mitigating cyber risks reveals several areas of concern and the need for policy interventions. First, authentication and authorization control are crucial. While public blockchains allow unrestricted network access, private blockchains require robust security controls to prevent unauthorized users from accessing the network. Technological advancements enable encryption-driven authorization, safeguarding data access and confidentiality. Proper utilization of cryptographic algorithms ensures data security, particularly against cyberattacks seeking unauthorized access.

Second, leveraging threat intelligence is essential. Gathering valuable insights about emerging or existing cyber threats is a high-level process, but duplication of efforts and missed threats can be significant obstacles. Blockchain's decentralized and peer-to-peer architecture facilitates synchronization between different parties, transforming the threat intelligence process. In addition, the blockchain's anti-tampering structure detects real-time changes, making it difficult for attackers to erase their presence.

Third, maintaining data consistency and integrity is vital for organizations. Blockchain's immutability and transparency ensure data integrity by using sequential hashing and cryptography, making data tampering impossible. Each transactional record is digitally signed and time-stamped, allowing traceability and accountability. Nonrepudiation guarantees that transaction details cannot be denied, enhancing the reliability of the data system.

Fourth, blockchain technology contributes to the accuracy and quality of information. Although it cannot enhance data quality directly, blockchain ensures the accuracy and durability of information once it is entered into the system. Real-time capabilities enable DSPs to validate transactional data quickly and take initiative-taking measures, assuming the initial data input is reliable.

Finally, blockchain can address the risk of distributed denial-of-service (DDoS) attacks that aim to disrupt internet service availability. Although blockchain technology has experienced DDoS attacks in the past, they have become less frequent due to their excessive cost and the challenge of overwhelming an entire blockchain network composed of numerous small transactions.

6. Digital payment adoption strategy

Encouraging the adoption of digital payments can bring numerous benefits to economies and individuals, including increased transparency, efficiency and financial inclusion. Policies that governments and institutions can implement to promote the use of digital payments may include the following (World Bank, 2021):

First, to promote the adoption of digital payments, substantial investments are needed to develop strong digital infrastructure, such as high-speed internet and mobile networks, ensuring accessibility for all citizens, even in remote areas ([Khando et al., 2023](#)). These investments must prioritize the establishment of a secure payment infrastructure, incorporating robust cybersecurity measures to safeguard against fraud and data breaches, thereby instilling trust in digital payment methods. In addition, government payments should be digitalized, with authorities leading by example by transitioning social benefits, tax refunds and government salaries to digital platforms, encouraging citizens to embrace digital payment solutions. Another crucial aspect of these investments is to promote financial inclusion, particularly among underserved populations, enabling their access to digital payment methods and integration into the formal financial system.

Second, as part of their broader monetary policy objectives, governments should consider intervening to reduce cash circulation by progressively phasing out higher denomination banknotes or imposing restrictions on cash transactions (Berentsen, 1998). This strategic approach aims to dissuade reliance on physical currency and encourage the adoption of digital payment alternatives. Simultaneously, the government should assess the feasibility of introducing a government-backed digital currency, which has the potential to further bolster the prevalence of digital payments across the nation.

Third, governments must foster a regulatory environment that supports digital payments, ensuring clarity in the legal framework while accommodating various digital payment providers (Allen *et al.*, 2022). Simultaneously, consumer rights and data privacy must be safeguarded. To encourage standardization and interoperability, common standards and protocols should be established for digital payment systems, facilitating seamless transactions across different platforms. Moreover, the regulatory landscape should offer substantial financial and nonfinancial incentives and subsidies to potential adopters, such as businesses, to expedite the shift away from cash transactions. Collaborative efforts between the government and private entities, including fintech startups and established financial institutions, are vital in cultivating innovative digital payment solutions and enhancing their accessibility.

Fourth, governments should enhance the population's proficiency in understanding and using digital technologies (Prete, 2022). To achieve this, the focus should be on implementing financial literacy programs, which involve launching educational campaigns and workshops to enhance financial literacy and create awareness regarding the advantages of digital payments. This effort will dispel myths and misconceptions, instilling greater confidence in adopting digital payment methods. In addition, special attention must be given to developing secure and user-friendly digital payment platforms that offer consumers a smooth and seamless experience, thus promoting wider adoption. Ensuring adequate customer support and efficient dispute resolution mechanisms for digital payment users will further contribute to building trust and confidence in the system. Finally, conducting awareness campaigns is vital to address security concerns, misconceptions and doubts surrounding digital payments. These campaigns will emphasize the convenience and benefits of using digital payment methods, encouraging more individuals to embrace this mode of financial transactions. Overall, the successful implementation of these policies requires coordination among various stakeholders, including governments, financial institutions, technology providers and consumer advocacy groups.

7. Conclusions and way forward

The rise of financial technology and digital payment services has led policymakers to examine their potential benefits, risks and the need for effective regulation. Activities related to payments, clearing and settlements have witnessed rapid developments and experimentation in payment services. The adoption of digital payments offers various advantages for individuals, companies, governments and international development organizations. These benefits include cost savings because digital payments enable faster and more efficient transactions, leading to reduced costs. They also include higher transparency and security, because by enhancing traceability and accountability, digital payments improve transparency and security, reducing instances of corruption and theft. Furthermore, they improve financial inclusion, as access to a range of financial services, such as savings, credit and insurance, is expanded through digital payments, promoting financial inclusion. Moreover, they improve women's economic participation because digital payments empower women by providing them with greater control over their financial lives and increasing economic opportunities. Finally, they promote inclusive economic growth and poverty reduction. The cumulative effect of the benefits helps unlock economic opportunities and facilitates a more efficient flow of resources in the economy. To realize the

benefits of digital payments, responsible implementation and the protection of end users' well-being are crucial. It is essential to understand the inherent risks associated with digital payments and establish effective risk mitigation mechanisms. This requires the development of proper infrastructure to support the provision of necessary services for digital payments.

A comprehensive digital payment regulatory framework should establish a safe, secure and efficient environment for conducting digital transactions while protecting the interests of consumers, businesses and the overall economy. The specific components of such a framework may vary from one jurisdiction to another, but they should include the following are some essential elements. First, a clear definition of the digital payments and the requirements and criteria for authorization of digital payment service providers. This ensures that only qualified and reputable entities can offer payment services. Second, the implementation of regulations that safeguard consumers against fraud, unauthorized transactions and other potential risks associated with digital payments. This may also include provisions for dispute resolution, liability limits and transparency in fee disclosures. Third, the establishment of stringent data protection and security standards to safeguard sensitive customer information and prevent data breaches. Companies handling payment data should adhere to strict protocols to ensure data confidentiality and integrity. Fourth, the integration of measures to combat money laundering and the financing of terrorism. Digital payment providers should comply with AML and counter-terrorism financing (CTF) regulations to prevent their platforms from being misused for illegal activities. Fifth, the encouragement of interoperability between different payment systems and the promotion of open application programming interfaces to foster competition and innovation in the digital payment space. Sixth, the establishment of transaction limits and reporting requirements for digital payments to prevent misuse and monitor potentially suspicious activities. Seventh, the requirement on payment providers to have robust risk management practices in place, along with contingency plans for handling disruptions, cyberattacks and other emergencies. Eighth, the establishment of mechanisms for monitoring and enforcement of compliance with the regulatory framework, including penalties for noncompliance, as well as international cooperation and coordination to address cross-border payment challenges and promote global interoperability. From a broader economic perspective, the regulatory framework should promote fair competition in the digital payment industry by preventing anticompetitive practices and ensuring a level playing field for all participants, encourage innovation in digital payments by providing a conducive regulatory environment that allows new technologies and business models to flourish and ensure that the promotion of financial inclusion, making digital payment services accessible to all segments of society, including underserved and unbanked populations.

Empowering users of digital payment services is also important. This can be achieved by raising awareness, facilitating user education and implementing efficient risk mitigation policies that prioritize communication, protection and system reliability. Emphasizing the importance of innovative technologies, particularly blockchain, is paramount. Blockchain's decentralized, immutable and transparent nature can enhance cybersecurity defenses and prevent fraudulent activities.

It is important to note that the digital payment landscape is continuously evolving and regulatory frameworks need to be adaptable to keep pace with technological advancements and emerging risks. Moreover, as we move toward a more digitized and interconnected world, the future of digital payment adoption presents several challenges that need to be addressed to ensure a smooth transition and widespread acceptance.

For example, the increase of digital payment transactions will raise considerable security and fraud concerns. Ensuring robust cybersecurity measures and developing secure encryption protocols are essential to build trust among users. Furthermore, especially in developing countries, there is inadequate digital infrastructure to support widespread

digital payment adoption. Access to reliable internet connections and smartphones or other digital devices is crucial for enabling seamless transactions. Moreover, although digital payment methods offer convenience, there are still segments of the population, such as the elderly, those in remote areas and poor individuals, who may struggle to adopt these technologies. Bridging the digital divide and promoting financial literacy are necessary to ensure inclusivity. Furthermore, the digital payment ecosystem is fragmented with numerous payment platforms, wallets and services, making it challenging for users to transfer money across different systems seamlessly. Achieving future interoperability between various digital payment providers will be crucial for a more user-friendly experience. Further yet, many individuals still perceive cash transactions as more secure and tangible compared to digital payments as well as less costly. Building trust among users and addressing concerns about privacy, data sharing and potential system failures is vital to encourage broader adoption. Reducing transaction costs and promoting cost-effective digital payment solutions will drive wider acceptance. Finally, facilitating secure and efficient cross-border digital payments involves overcoming regulatory hurdles, currency conversion challenges and compliance with international standards.

Addressing these challenges will require collaboration between governments, financial institutions, technology providers, consumers and other stakeholders to strike the right balance between innovation and consumer protection. By proactively addressing these issues, we can accelerate the adoption of digital payments, making transactions more efficient, accessible and secure for everyone involved.

References

- Abbey, C.O., Odonkor, E. and Boateng, D. (2014), *A Beneficiary Assessment of Ghana's Cash Transfer Program (LEAP)*, African Development Program Ghana, Accra.
- Adewole, A. (2015), "Consumer payment system and the challenge of confidence in national payment system of developing countries: a case study of Nigeria", *Mediterranean Journal of Social Sciences*, Vol. 6 No. 2.
- Adrian, T., Garratt, R., He, D. and Mancini-Griffoli, T. (2023), "Trust bridges and money flows - a digital marketplace to improve cross-border payments", *FinTech Note 2023/001*, International Monetary Fund, Washington, DC.
- Adrian, T. and Griffoli, T.M. (2019), "The rise of digital money", *FinTech Note No. 2019/001*, International Monetary Fund, Washington, DC.
- Agur, I., Deodoro, J., Lavayssière, X., Martinez Peria, S., Sandri, D., Tourpe, H. and Villegas Bauer, G. (2022), "Digital currencies and energy consumption", *FinTech Notes*, Vol. 2022 No. 6, p. A001.
- Akanfe, O., Valecha, R. and Rao, H.R. (2020), "Assessing country-level privacy risk for digital payment systems", *Computers & Security*, Vol. 99 No. 2, p. 102065.
- Allen, J., Carbo-Valverde, S., Chakravorti, S., Rodriguez-Fernandez, F. and Pinar Ardic, O. (2022), "Assessing incentives to increase digital payment acceptance and usage: a machine learning approach", *Plos One*, Vol. 17 No. 11, p. e0276203.
- Almazan, M. (2013), *G2P Payments and Mobile Money: Opportunity or Red Herring? Blog*, GSMA, London.
- Almazán, M. and Frydrych, J. (2015), "Mobile financial services in Latin America and the Caribbean: state of play, commercial models, and regulatory approaches", GSMA, available at: www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/05/2015_GSMA_Mobilefinancial-services-in-Latin-America-the-Caribbean.pdf
- Alonso, L.B. (2020), "European digital identity framework", European Central Bank, available at: file:///C:/Users/charilaos.mertzanis/Downloads/Digital_identity_update.pdf
- Bech, M. and Hancock, J. (2020), "Innovations in payments", *BIS Quarterly Review*, pp. 21-36.
- Berentsen, A. (1998), "Monetary policy implications of digital money", *Kyklos*, Vol. 51 No. 1, pp. 89-118.

- Bill and Melinda Gates Foundation (BMGF) (2019), "Inclusive digital financial services: a reference guide for regulators", July.
- Biscaye, P. *et al.* (2015), "Review of mobile coverage", EPAR Brief No. 261. University of Washington, available at: http://evans.uw.edu/sites/default/files/public/EPAR_UW_261_Mobile%20Coverage%20Estimates_2.26.15.pdf
- Boar, C. and Szemere, R. (2020), "Payments go (even more) digital [commentary to 2019 red book statistics]", available at: www.bis.org/statistics/payment_stats/commentary2011.htm
- Boel, P. (2019), "Payment systems: history and challenges", *Sveriges Riksbank Economic Review*, pp. 51-66.
- Brainard, L. (2019), "Digital currencies, stablecoins, and the evolving payments landscape", *Remarks at the Future of Money in the Digital Age*, Washington, DC.
- Cabello, G.J. (2013), "Efficient liquidity management for ATMs", *AESTIMATIO: The IEB International Journal of Finance*, Vol. 6, pp. 50-75.
- Committee on Payments and Market Infrastructures (CPMI) (2014), "Principles for financial market infrastructures: assessment methodology for the oversight expectations applicable to critical service providers", Bank for International Settlements, December.
- Dahan, M. and Gelb, A. (2015), "The role of identification in the post-2015 development agenda", World Bank Working Paper, available at: <https://openknowledge.worldbank.org/handle/10986/22513License:CCBY3.0IGO>
- Demirgüç-Kunt, A., Klapper, L., Singer, D. and Ansar, S. (2021), *The Global Findex Database*, World Bank, Washington, DC.
- Ehrentraud, J., Prenio, J., Boar, C., Janfils, M. and Lawson, A. (2021), "Fintech and payments: regulating digital payment services and e-money", FSI Insights on policy implementation No 33, BIS.
- El-Huni, E.M. (2014), *WFP e-Voucher Program in Lebanon*, Field Exchange 48 Emergency Nutrition Network, Oxford.
- Faragallah, A. *et al.* (2015), *Innovative Digital Payment Mechanisms*, World Bank Group's Payment System Development Group, World Bank.
- Feyen, E., Frost, J., Natarajan, H. and Rice, T. (2021), "What does digital money mean for emerging market and developing economies? BIS working papers", no 973, October.
- Frost, J., Gambacorta, L., Huang, Y., Shin, H.S. and Zbinden, P. (2019), "BigTech and the changing structure of financial intermediation", BIS Working Papers No. 779, April.
- Gilman, L. *et al.* (2013), "Mobile money in the democratic republic of Congo: market insights on consumer needs and opportunities in payments and financial services", GSMA, available at: www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/07/Mobile-Money-in-the-DRC_July-2013.pdf
- GSMA (2019), "The impact of mobile money on monetary and financial stability in Sub-Saharan Africa", March.
- Hacker, P., Lianos, I., Dimitropoulos, G. and Eich, S. (Eds). (2019), *Regulating Blockchain: Techno-Social and Legal Challenges*, Oxford Academic.
- Haldane, A. and Qvigstad, J. (2014), "The evolution of central banks: a practitioner's perspective", available at: www.norges-bank.no/pages/100044/14_2_Haldane_and_Qvigstad_28_June_2014.pdf
- He, D., Leckow, R., Haksar, V., Mancini-Griffoli, T., Jenkinson, N., Kashima, M., Khiaonarong, T., Rochon, C. and Tourpe, H. (2017), "Fintech and financial services: initial considerations", *IMF Staff Discussion Note 17/05, June*, International Monetary Fund, Washington, DC.
- Humphrey, D.B., Sato, S., Tsurumi, M. and Vesala, J.M. (1996), "The evolution of payments in Europe, Japan, and the United States", Policy Research Working Paper 1676, World Bank, Washington DC.
- InterMedia India (2014), *Financial Services Use and Emerging Digital Pathways. Highlights from the FII Tracker Survey and the Digitized Government Payments Qualitative Study*, October 2013-January 2014 InterMedia, Washington, DC.
- Islam, A. and Woodard, J. (2014), "Mobile money snapshot: English in action", Doha/Washington, D.C.: USAID's Mobile Solutions Technical Assistance and Research (mSTAR) Bangladesh, February.

- Jagrič, T., Fister, D., Amon, A., Jagrič, V. and Beloglavec, S.T. (2022), "The banking industry in the ecosystem of digital currencies and digital central bank currencies", in Grima, S., Özen, E. and Boz, H. (Eds), *The New Digital Era: Digitalisation, Emerging Risks and Opportunities (Contemporary Studies in Economic and Financial Analysis*, Vol. 109A, Emerald Publishing Limited, Bingley, pp. 89-115.
- Jegerson, D. and Hussain, M. (2022), "A framework for measuring the adoption factors in digital mobile payments in the covid-19 era", *International Journal of Pervasive Computing and Communications*, doi: [10.1108/IJPCC-12-2021-0307](https://doi.org/10.1108/IJPCC-12-2021-0307).
- Kantar Public (2022), *Study on New Digital Payment Methods*, European Central Bank.
- Khando, K., Islam, M.S. and Gao, S. (2023), "The emerging technologies of digital payments and associated challenges: a systematic literature review", *Future Internet*, Vol. 15 No. 1, p. 21, doi: [10.3390/fi15010021](https://doi.org/10.3390/fi15010021).
- Khiaonarong, T., Leinonen, H. and Rizaldy, R. (2021), "Operational resilience in digital payments: experiences and issues", Issue 288, International Monetary Fund.
- Khiaonarong, T. and Goh, T. (2020), "Fintech and payments regulation: analytical framework", IMF, Paper No 075, ISBN: 9781513531496, International Monetary Fund.
- Klapper, L. (2023), "How digital payments can benefit entrepreneurs", *IZA World of Labor*, doi: [10.15185/izawol.396.v2|T](https://doi.org/10.15185/izawol.396.v2|T).
- Krishna, B., Krishnan, S. and Sebastian, M.P. (2022), "Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective", *Information Systems Frontiers*, pp. 1-17, doi: [10.1007/s10796-022-10280-7](https://doi.org/10.1007/s10796-022-10280-7).
- Leonard, P. (2020), "Data privacy in a data and algorithm-enabled world", Australian Society for Computers and Law. July, available at: <http://138.25.65.17/au/journals/ANZCompuLawJI/2021/7.pdf>
- McGrath, F. and Susie, L. (2013), "Platforms for successful mobile money services", GSMA, available at: www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/06/2013_MMU_Platformsfor-Successful-Mobile-Money-Services.pdf
- McKee, K., Kaffenberger, M. and Zimmerman, J.M. (2015), "Doing digital finance right: the case for stronger mitigation on client risks", *Focus Note 103*, CGAP, Washington, DC.
- McKinsey (2022), "Global payments report", October, available at: www.mckinsey.com/industries/financial-services/our-insights/the-2022-mckinsey-global-payments-report
- Naqvi, M. and Southgate, J. (2013), "Banknotes, local currencies, and central bank objectives", *Bank of England Quarterly Bulletin*, Vol. 53 No. 4, pp. 317-325.
- Navajas, S. (2015), "Financial inclusion just a click away: e-wallets and payment platforms", FOMIN, available at: www.fomin.org/enus/Home/FOMINblog/Blogs/DetailsBlog/ArtMID/13858/ArticleID/3090/Financial-inclusion-just-a-clickaway-E-wallets-and-payment-platforms.aspx
- Prete, A.L. (2022), "Digital and financial literacy as determinants of digital payments and personal finance", *Economics Letters*, Vol. 213, p. 110378.
- Restoy, F. (2019), "Regulating Fintech: what is going on, and where are the challenges? ASBA-BID-FELABAN XVI banking public-private sector regional policy dialogue", Challenges and Opportunities in the New Financial Ecosystem. Washington DC, 16 October.
- Risman, A., Mulyana, B., Silvatika, B. and Sulaeman, A. (2021), "The effect of digital finance on financial stability", *Management Science Letters*, Vol. 11 No. 7, pp. 1979-1984.
- Sahi, A.M., Khalid, H., Abbas, A.F., Zedan, K., Khatib, S.F.A. and Al Amosh, H. (2022), "The research trend of security and privacy in digital payment", *Informatics*, Vol. 9 No. 2, p. 32, doi: [10.3390/informatics9020032](https://doi.org/10.3390/informatics9020032).
- Sivathanu, B. (2019), "Adoption of digital payment systems in the era of demonetization in India: an empirical study", *Journal of Science and Technology Policy Management*, Vol. 10 No. 1, pp. 143-171.
- The Bank for International Settlements (BIS) (2019), "Big tech in finance: opportunities and risks", BIS Annual Economic Report 2019, June 23.
- The Committee on Payments and Market Infrastructure (CPMI) (2023), "Digital payments make gains but cash remains", CPMI Brief No 1. Committee on Payments and Market Infrastructure, Basel.
- The Financial Stability Board (FSB) (2019a), "FinTech and market structure in financial services: market developments and potential financial stability implications", February 14.

The Financial Stability Board (FSB) (2019b), "Crypto-assets: work underway, regulatory approaches and potential gaps, may 31".

The International Monetary Fund (IMF) (2019), *Singapore Technical Note-Fintech: Implications for the Regulation and Supervision of the Financial Sector*, International Monetary Fund, Washington, DC.

The World Food Program (WFP) (2016), *TOOLKIT. Behavioral Program Monitoring in Cash Transfer Programs*, WFP Kenya, Nairobi.

Universal Digital Payments Network (UDPN) (2022), "Interoperable payment infrastructure for the digital currencies of tomorrow", available at: www.udpn.io

Zachariadis, M., Hileman, G. and Scott, S.V. (2019), "Governance and control in distributed ledgers: understanding the challenges facing blockchain technology in financial services", *Information and Organization*, Vol. 29 No. 2, pp. 105-117.

Zheng, S., Hu, Y., Chong, A.Y.L. and Tan, C.-W. (2022), "Leveraging blockchain technology to control contextualized digital business risks: evidence from China", *Information & Management*, Vol. 59 No. 7, doi: [10.1016/j.im.2022.103628](https://doi.org/10.1016/j.im.2022.103628).

Zimmerman, J.M. and Bohling, K. (2015), *Partnering with Existing National Safety Nets for Emergency Payments: WFP's Collaboration with the Pantawid Pamilyang Pilipino Program in the Typhoon Haiyan Response*, Bankable Frontier Associates, Somerville, Mass.

Zimmerman, J.M., Bohling, K. and Parker, S.R. (2014), *Electronic G2P Payments: Evidence from Four Lower-Income Countries. Focus Note 93*, CGAP, Washington, DC.

Further reading

eCommerceDB (2021), "Ecommerce in the United Arab Emirates, Country Report", November.

El Qorchi, M., Maimbo, S.M. and Wilson, J.F. (2003), *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, Occasional Paper 222 International Monetary Fund, Washington, DC.

He, D. (2018), "Monetary policy in the digital age", *Finance and Development*, Vol. 55 No. 2, pp. 13-16.

The International Monetary Fund (IMF) and the World Bank (WB) (2019), *Fintech: The Experience so Far*, IMF Policy Paper, June, International Monetary Fund, Washington, DC.

Klapper, L. (2014), "The opportunities of digitizing payments", World Bank, available at: <http://documents.worldbank.org/curated/en/2014/08/20326428/opportunities-digitizing-payments>

Kuo Siong Tan, G. (2022), "Buy what you want, today! Platform ecologies of 'buy now, pay later' services in Singapore", *Transactions of the Institute of British Geographers*, Vol. 1, pp. 1-15.

Liu, C. (2015), "Consumer protection in mobile payments in China: a critical analysis of Alipay's service agreement", *Computer Law & Security Review*, Vol. 31 No. 5, pp. 679-688.

McKinsey (2014), "Offline and falling behind: barriers to internet adoption", available at: www.mckinsey.com/insights/high_tech_telecoms_internet/offline_and_falling_behind_barriers_to_internet_adoption

Mahesh, A. and Bhat, G. (2021), "Digital payment service in India - a case study of unified payment interface", *International Journal of Case Studies in Business, IT, and Education*, Vol. 5 No. 1, pp. 256-265.

Norman, B., Shaw, R. and Speight, G. (2011), "The history of interbank settlement arrangements: exploring Central banks' role in the payment system. Bank of England working paper no. 412", available at: www.bankofengland.co.uk/research/Documents/workingpapers/2011/wp412.pdf

Pickens, M., Porteous, D. and Rotman, S. (2009), "Banking the poor via G2P payments", *Focus Note 58*, CGAP, Washington, DC.

Riecke, J. (2014), *Global Progress in Electronic Payment Systems*, Center for Financial Inclusion, Washington, DC.

Riju, D. (2016), "Here are the advantages of cashless payments and the pitfalls of which you should beware", *The Economic Times*, December 12th.

Swinehart, M.W. (2018), "Modeling payments regulation and financial change", *Kansas Law Review*, Vol. 67 No. 1, pp. 83-147.

The Consultative Group to Assist the Poor (CGAP) (2014), *Going Mobile with Conditional Cash Transfers. Insights and Lessons from the Payment of Familias en Accion through DaviPlata Wallets in Colombia*, Working Paper CGAP, Washington, DC.

The International Monetary Fund (IMF) and the World Bank (WB) (2018), *The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities*, IMF Policy Paper, October, International Monetary Fund, Washington, DC.

The World Bank (2012), "From remittances to m-payments", Understanding "Alternative" Means of Payment within the Common Framework of Retail Payments System, available at: http://siteresources.worldbank.org/EXTPAYMENTREMITTANCE/Resources/WB2012_Mobile_Payments.pdf

The World Bank (2015), "The global index database", available at: <http://datatopics.worldbank.org/financialinclusion/>

The World Bank Group (WBG) (2016), *Retail Payments: A Practical Guide to Measuring Retail Payment Costs*, World Bank, Washington, DC.

The World Bank Group (WBG) (2021), *Electronic Payments Acceptance Toolkit: examples of Incentive Implementations*, World Bank, Washington, DC.

Corresponding author

Charilaos Mertzanis can be contacted at: charilaos.mertzanis@adu.ac.ac

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com