
# Payment Resilience in Fragile and Conflict-Affected States: Lessons for Central Bank Digital Currency (CBDC)

Majid Malaika, Gabriel Soderberg, and Kateryna Zhabska

NOTE/2025/009

FINTECH NOTE

# Payment Resilience in Fragile and Conflict-Affected States: Lessons for Central Bank Digital Currency (CBDC)

Majid Malaika, Gabriel Soderberg, and Kateryna Zhabska

November 2025

**Payment Resilience in Fragile and Conflict-Affected States: Lessons for** Central Bank Digital Currency **(CBDC)**
Note 2025/009
Prepared by Majid Malaika, Gabriel Soderberg, and Kateryna Zhabska

**Cataloging-in-Publication Data**
**IMF Library**

Names: Malaika, Majid, author. | Söderberg, Gabriel, 1978-, author. | Zhabska, Kateryna, author. | International Monetary Fund, publisher.
Title: Payment resilience in fragile and conflict-afflicted states: Lessons for central bank digital currency (CBDC) / Majid Malaika, Gabriel Soderberg, and Kateryna Zhabska.
Other titles: Lessons for central bank digital currency (CBDC). | Fintech notes.
Description: Washington, DC: International Monetary Fund, 2025. | Nov. 2025. | NOTE/2025/009. | Includes bibliographical references.
Identifiers: ISBN:
9798229030977 (paper)
9798229031066 (ePub)
9798229031035 (WebPDF)
Subjects: LCSH: Digital currency. | Financial services industry—Technological innovations.
Classification: LCC HG1710.M3 2025



**RECOMMENDED CITATION:** Majid Malaika, Gabriel Soderberg, and Kateryna Zhabska 2025. "Payment Resilience in Fragile and Conflict-Affected States: Lessons for Central Bank Digital Currency **(**CBDC)" IMF Fintech Note 2025/009, International Monetary Fund, Washington, DC.

Publication orders may be placed online or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430
publications@IMF.org
IMFbookstore.org
elibrary.IMF.org

* This note was written under the supervision of Tommaso Mancini-Griffoli and Agnija Jekabsone with Kateryna Zhabska as the lead author. It has benefited from the contributions of several IMF staff members, especially Dong He who provided guidance in the early stages of the project, relevant IMF country teams, as well as from IMF Alternate Executive Director Vladyslav Rashkovan. The team is also grateful for valuable inputs from the National Bank of Ukraine (particularly Oleksii Shaban and Andriy Poddyerogin), Fares Hindi of the Palestine Monetary Authority, Hawi Bedasa of UNICEF, and Abdelnaby Ahmed Abdelaziz Faragallah of the World Bank. This note is produced with financial support from the Government of Japan.

# Content

# Acronyms

| | |
|---|---|
| ATM | Automated teller machine |
| BRH | Banque de la République d'Haïti |
| CBDC | Central Bank Digital Currency |
| CEMAC | Central African Economic and Monetary Community |
| CSIRT-NBU | Computer Security Incident Response Team of the National Bank of Ukraine |
| DLT | Distributed Ledger Technology |
| FCS | Fragile and Conflict-Affected States |
| NBU | National Bank of Ukraine |
| PMA | Palestinian Monetary Authority |
| POS | Point-of-Sale |
| PSP | Payment Service Provider |
| QR | Quick response |
| RTGS | Real-Time Gross Settlement Systems |
| SNT | Satellite Networks Technology |

# Introduction

Disruptions to making and receiving payments may have severe consequences for individuals, businesses, and national economies. Payment ecosystem resilience—the capacity to maintain payment operations during periods of stress or restore them quickly after disruption—is therefore essential to economic and social stability. Although natural disasters, cyber incidents, and technical failures have long challenged payment continuity, armed conflict or public unrest present particularly complex risks and costs. In such environments, parts of payment ecosystem may be physically damaged or inaccessible, undermining trust, institutional functioning, and essential services—with recovery further complicated by the uncertainties accompanying conflict, including the duration of violence, extent of damage, and scope for restoration.

Research and previous experience suggest that states classified as fragile are more likely to become conflict-afflicted states with potential disruptions to payments (OECD 2025a). Conversely, disruptions to payment systems can exacerbate fragility and bring about conflict. Since public trust (OECD 2025b) tends to be low in Fragile and Conflict-Affected States (FCS), it can deteriorate further as payment disruptions persist. For these reasons, payment system resilience must be treated as a core priority in fragile settings.

Well-functioning payment systems underpin economic activity, facilitate aid delivery, and contribute to broader social and financial stability. Currently, over 1 billion people live in FCS.[1] The number of FCS in the world is increasing, and by 2030, it is estimated that two-thirds of the world's extreme poor individuals will live in areas affected by fragility and conflict (World Bank Group 2020). Although payment resilience alone cannot resolve the complex drivers of fragility, it plays a critical enabling role. A resilient payment ecosystem helps central authorities meet basic obligations, allows the population to carry out everyday transactions, and ensures that both small and large businesses can continue operating.

Digitalization adds both promise and complexity to this equation. Although cash remains a crucial fallback in many contexts, its distribution can be logistically difficult and unsafe. Digital payments offer speed, efficiency, and reach, but depend on electricity, connectivity, and user trust (Khiaonarong, Leinonen, and Rizaldy 2021). New technologies, such as offline digital payments, and distributed ledger technologies (DLTs), may help mitigate these vulnerabilities, but their effective use in payments (through stablecoins or central bank digital currency [CBDC]) requires deliberate planning, designing, and targeted capacity building in both expertise and infrastructure.

The objective of this Note is to provide an overview of the policies that have helped jurisdictions ensure payment system resilience in the face of fragilities and conflict. This Note takes a comprehensive, ecosystem-wide perspective on payment resilience. Rather than focusing solely on individual systems or technologies, it examines the full set of interconnected layers—payment and connectivity infrastructure,

[1] For the definition of fragile and conflict-affected states, see World Bank Group (2024).

regulatory frameworks, institutions and payment market participants, and end users with their capacity—that together sustain payment flows under stress.

The Note is structured as follows. The **"**Payment Ecosystem Resilience**"** section introduces the concept of payment ecosystem resilience, outlines the functional layers of the ecosystem, and identifies the most acute challenges in FCS. It also highlights core practices that contribute to maintaining resilience under stress. The **"**Strategies and Lessons for Strengthening Payment Resilience**"** section presents a set of concrete strategies and lessons for strengthening payment ecosystem resilience, drawing directly from country case studies across a range of FCS settings. These cases offer practical insights into how payment systems have been adapted, or in some instances, have failed—under pressure, and what can be learned from those experiences. The **"**Applying Resilience Lessons to Central Bank Digital Currency: Opportunities and Design Considerations**"** section examines how these lessons can inform the design of emerging technologies and their use in digital payments such as CBDCs to ensure they support rather than compromise payment continuity in high-risk environments.

This Note aims to offer lessons and a framework of analysis to help countries evaluate CBDC. The Note does not intend to endorse CBDC nor reject it as a policy option. If anything, the Note is narrowly focused on the question of payment resilience, which is only one of the possible implications of CBDC. Even then, the Note does not come to universal conclusions as to whether CBDC can support or undermine payment resilience. That will depend on country circumstances. The Note is technical in nature and does not offer policy messages. It merely provides tools and conveys real-world experiences to help policymakers consider broader policy questions.

# I. Payment Ecosystem Resilience

Payment ecosystem resilience refers to the robustness of the entire payment ecosystem, and its ability to sustain operations and support payment flows during disruptions. This systemic view goes beyond the resilience of individual infrastructures to focus on the ecosystem's overall capacity to function in adverse conditions. Although individual components matter, this Note focuses on the payment ecosystem as a whole and its ability to support payments during disruptions.

In FCS, payment ecosystem resilience is critical to preserve access to payment services, maintain trust in financial institutions, support economic activity, and enable recovery. These environments often face simultaneous disruptions across both digital and physical domains, making a holistic view of the payment ecosystem essential.

Importantly, the payment ecosystem is both influenced by and a contributor to broader economic and political dynamics. Its resilience depends not only on technical design but also on proper governance, macroeconomic stability, public trust, and the political will to maintain continuity.

## Payment Ecosystem Layers

From an ecosystem perspective, payment resilience depends on the minimum viable functionality of a diverse set of interconnected elements or layers, all of which are integral to sustain smooth payment flows. In FCS, where payment ecosystems and their layers are often underdeveloped or disrupted, it becomes essential to define a minimum viable payment ecosystem that can function under crisis conditions. In this regard, payment ecosystems comprise the following interconnected layers, as summarized in Figure 1.

The user layer includes actors who initiate or receive payments: individuals, businesses, governments, and humanitarian agencies.

The payment solutions layer encompasses the instruments, tools, and applications, that individuals, businesses, and institutions use to initiate, receive, and process payments. It serves as the primary interface or instrument between users and the underlying payment infrastructure and includes both physical (cash) and digital solutions. These are typically provided by payment intermediaries but may also include instruments issued or supported by central banks or nontraditional actors. This layer comprises the following:

- Traditional digital payment solutions, such as payment cards, digital wallets (including e-money) and mobile payment apps, quick response (QR) code payment interfaces, and point-of-sale (POS) systems.
- Cash is a fundamental component of the payment ecosystem in FCS, serving as both a primary payment method and a critical fallback. Its continued availability is vital for ensuring liquidity and enabling transactions when digital channels fail because of power outages, cyberattacks, or

infrastructure damage. However, cash distribution relies on physical and digital infrastructure—bank branches, automated teller machines (ATMs), secure transport networks, and backend banking systems. When these are compromised, cash circulation is disrupted, exacerbating financial exclusion. Even physical cash systems thus depend on digital infrastructure to function reliably.

- Checks are paper-based instruments that direct a bank transfer fund from the payer to the payee. Though declining in use globally, they remain relevant in some FCS, especially for government or humanitarian payments. Their use depends on functioning clearing systems and banking infrastructure, which may be disrupted in crises.
- Potential new digital payment solutions could vary with forms of digital money. Stablecoins and crypto assets are privately issued digital assets that operate outside traditional financial networks that may be used as a payment instrument. Crypto assets such as Bitcoin or Ethereum are typically not suitable as means of payment because of their high price volatility, lack of backing, and limited regulatory oversight. By contrast, stablecoins—when properly backed by high-quality reserves and properly regulated and supervised—can provide a more stable and accessible form of value transfer.
- CBDCs are issued by central banks or monetary authorities for use as digital money.[2] CBDC may hold the potential to enhance payment ecosystem resilience, as discussed in the "Applying Resilience Lessons to Central Bank Digital Currency: Opportunities and Design Considerations" section.

The payment intermediaries layer comprises payment service providers (PSPs) that facilitate payment services: banks, fintech firms, mobile money operators, and other nonbank entities. PSPs are intermediaries between payment infrastructure and users providing front-end payment solutions. This layer typically carries out multiple functions supporting payments, such as a unified technical interface, streamlined onboarding, consolidated reporting, and services such as recurring billing and subscription management. It may also have access to consolidated account data across institutions or initiate payments directly from user accounts through third-party applications.[3]

The payment infrastructure layer forms the backbone of the ecosystem, encompassing the technical systems that process, clear, and settle payments:

- Large-Value Systems (for example, real-time gross settlement systems or RTGS): Typically operated by central banks, enabling interbank settlements.
- Retail Payment Platforms: Include automated clearinghouses, card payment networks, national switch and fast payment systems.
- Alternative Infrastructure for Digital Payments: Infrastructure such as e-money or mobile money platforms, which may operate independently or in conjunction with traditional infrastructure, including those leveraging mobile network operator systems.

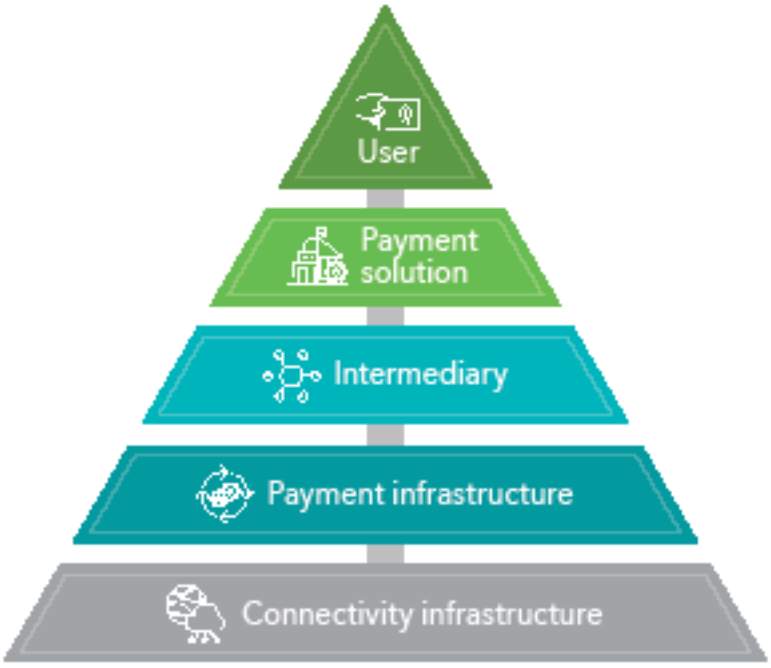
[6] Although CBDC could also be considered part of the infrastructure layer, in the context of this Note, it is primarily treated as a payment solution, unless otherwise specified.

[3] According to the European Union's Revised Payment Services Directive, payment service providers may also act as account information service providers or payment initiation service providers.

The connectivity infrastructure layer provides physical and digital channels that support communication between ecosystem actors. This includes communication channels, such as the internet, mobile networks, power supply, and other enabling technologies. Reliability of the connectivity layer underpins the functionality of payment ecosystem and is a critical enabler that underpins all other layers. Outages can disrupt access to both digital payments and cash withdrawals.

All these layers are deeply interconnected, forming a complex ecosystem in which failure of one can cascade across others. For example, users rely on payment solutions to initiate transactions, but these solutions depend on intermediaries and payment infrastructure to process and settle payments. In turn, infrastructure providers are reliant on the connectivity layer that powers and links them. Understanding how these layers interact under stress is essential for assessing where vulnerabilities may arise and how resilience can be reinforced.

**Figure 1. Interconnected Layers of the Payment Ecosystem**




Source: Authors.

## Challenges for Payment Resilience

Payment ecosystems in FCS face a range of acute and persistent disruptions. The challenges outlined in this section highlight the most pressing threats to payment ecosystem resilience in such contexts.

**Cyber Threats and Digital Vulnerabilities**

Cyberattacks are deliberate, malicious attempts to breach digital systems, networks, or devices to compromise, steal, or destroy data or disrupt operations. These attacks take numerous forms, including malware infections, phishing campaigns, distributed denial-of-service attacks, and ransomware deployments often leveraging technical vulnerabilities or human psychology to gain unauthorized access. With the recent advancements in technology, cybersecurity has become increasingly complex. These threats can compromise transaction integrity, disrupt financial flows, and erode trust in digital payment solutions, exacerbating instability in fragile settings. According to the IMF, the financial impact from cyber incidents has more than quadrupled since 2017, reaching $2.5 billion as of the end of 2023, underscoring the growing scale and impact of such threats (Natalucci, Qureshi, and Suntheim 2024).

Payment infrastructure layers are especially vulnerable as they are complex, encompassing many participants, physical and digital, distinct business procedures, different software/service providers, and different platforms and architectures with many interdependencies. The payment solution layer is inherently complex, involving diverse applications and technologies that, in FCS, are often deployed without consistent security standards—further increasing exposure to cyber risks. These complexities substantially increase the attack surface, making cybersecurity and resilience challenging in contexts where institutional capacity and resources are limited. Ensuring cyber resilience is therefore key to ensuring payments resilience.

**Absence or Disruption of Fundamental Payment Infrastructure**

In regions affected by long-term instability, fundamental components of the payment infrastructure are often absent, underdeveloped, or fail to meet the minimum requirements for reliable digital payments. Core systems—such as RTGS, clearing and switching platforms, and retail payment systems—may never be established because of institutional constraints or lack of public and private investment. Where such systems do exist, they are frequently vulnerable to physical disruption during conflicts such as the destruction of central bank facilities, processing centers, or essential equipment—resulting in prolonged outages or degraded functionality.

**Access Restrictions through Disruption of Intermediary and Payment Solution Layer**

In FCS, access to payment services is frequently constrained by the limited presence and operational capacity of PSPs—including traditional banks, fintechs, and mobile money operators. In high-risk settings, these actors often lack both the commercial incentive and logistical feasibility to maintain a consistent presence. This lack of incentive and feasibility results in fragmented and unreliable service coverage, particularly in insecure areas. In some cases, mobile money or e-money platforms remain the only accessible digital payment channels. Yet these platforms often operate with significant inefficiencies and limited interoperability. In the absence of PSP engagement, even basic payment functions—such as fund transfers, salary disbursements, and merchant transactions—are severely constrained. As a result, individuals and businesses are frequently forced to rely on informal or high-risk alternatives that fall outside the scope of regulatory oversight. Over time, this undermines trust in the formal financial system, weakens financial inclusion, and heightens user vulnerability to fraud, loss, and systemic shocks.

These challenges are further exacerbated by the physical disruption of intermediary infrastructure and payment solutions. Conflict frequently damages or destroys PSP-operated facilities, agent networks, and equipment enabling payment solutions.

Cash operations are similarly affected: disruptions to distribution networks, secure transport channels, and ATM infrastructure—often managed or supported by PSPs—can drastically limit cash availability. In some cases, physical currency may even be lost or destroyed. When these cash-handling systems break down, fallback mechanisms are often unavailable.

At the user layer, personal security threats further limit access to payment services. Individuals collecting cash or visiting PSPs—especially for predictable flows such as salaries or aid—face risks of theft or extortion, discouraging use of informal channels in insecure areas.

**Cash Hoarding during Crises**

Conflict and instability often trigger a surge in cash withdrawals as individuals seek liquidity, overwhelming financial institutions and depleting available cash supplies. This creates bottlenecks in distribution and raises concerns about long-term access. In many post-conflict and fragile states, strong cash preferences can persist well beyond the immediate crisis. If not actively managed during conflict, reliance on cash may become deeply ingrained in consumer and business behavior, making transitions to digital financial systems more difficult in the long term. Furthermore, in countries experiencing prolonged conflict and fragility, the denominations of available cash often become unfit for purpose, especially in the context of sustained inflation, making everyday transactions inefficient, insecure, and difficult to scale.

**Connectivity Layer Disruptions**

Modern payment systems are dependent on stable electricity and telecommunications infrastructure. In fragile settings, these utilities are highly vulnerable—because of direct attacks on connectivity in the infrastructure layer, reliance on imported components (such as fuel and electricity) of the connectivity layer, or the inability to maintain connectivity in insecure areas. Such vulnerabilities can abruptly interrupt access to the entire payment ecosystem, posing a major challenge to payment system resilience.

**Institutional and Regulatory Strain during Conflict**

Periods of conflict place extraordinary pressure on regulatory and supervisory institutions and payment system governance. Regulatory and supervisory bodies must be robust enough to maintain public confidence in payment intermediaries. Supervisors play a critical role in managing the risk of bank runs, ensuring that responses are well coordinated and proportional to emerging threats. However, regulatory and supervisory arrangements designed for peacetime conditions may not be suited to the realities of conflict.

Institutional capacity is often strained in fragile settings. Beyond limited technical and financial resources, human capacity is frequently affected by displacement, insecurity, or loss of life. Key personnel may be killed, injured, extorted, or unable to access office facilities. In such contexts, remote work is often not

possible because of unreliable connectivity and security concerns, further hindering coordination and response.

In some cases, political fragmentation compounds these institutional weaknesses. Where dual governments or rival authorities compete for legitimacy, oversight and supervision of the payment system can become fractured. This leads to conflicting regulations, operational fragmentation, and public confusion—ultimately eroding trust in both the payment system and state institutions.

**Risks to Central Bank Reserves: Internal Misuse and External Constraints**
Central bank reserves are vital for stabilizing the payment system, enabling settlements, and managing liquidity. However, in FCS, these reserves face growing risks from both internal misuse and external geopolitical developments.

**Internal Misuse and Institutional Abuse**
In contexts of corruption and abrupt political change, public financial systems are vulnerable to misuse by those in power. Historically, this involved physical cash extractions by departing officials. In today's increasingly digital environment, this risk extends to unauthorized access or transfers through state-controlled payment infrastructures. Without strong legal safeguards and independent oversight, such actions can drain reserves and severely undermine trust in the financial system.

**External Freezes and Geopolitical Sanctions**
Reserves held abroad may be frozen because of sanctions, political regime non-recognition, or concerns over misuse. Although such measures aim to prevent abuse, they can also paralyze central bank operations—disrupting cross-border payments, foreign exchange access, and crisis response. In FCS, this adds a layer of fragility to an already strained financial system.

Together, these challenges illustrate the wide-ranging and systemic risks facing payment ecosystems in fragile and conflict-affected settings—from cyber threats and infrastructure breakdowns to institutional fragmentation and regulatory constraints. Addressing these risks requires deliberate and layered strategies that reinforce the payment ecosystem's capacity to withstand shocks.

## Practices to Maintain Resilience for the Payment Ecosystem

For the payment ecosystem to be resilient and capable of withstanding existing and emerging risks, it requires sound resilient practices to help policymakers identify and navigate choices and design options. Several key practices to maintain payment ecosystem resilience are illustrated in Figure 2.

**Figure 2. Payment Ecosystem Resilience Practices**


Source: Authors.

**Redundancy and Scalability**

This design practice focuses on ensuring uninterrupted operations by maintaining both backup options and the capacity to absorb sudden changes in demand. Redundancy refers to having multiple alternative components or pathways—such as systems, processing rails, or network links—to minimize the impact of any single point of failure. Scalability ensures that the ecosystem can flexibly handle traffic surges or shifts in usage through mechanisms such as load balancing, automated failover, and elastic infrastructure. For instance, in the connectivity and payment infrastructure layers, resilience would entail having more than one site of crucial technical equipment so if one gets disrupted, others can still function. Likewise, in the payment solution and user layer, resilience would mean that users have access and capacity to use more than one payment solution so that they are able to pay even if one solution fails. This practice applies across the entire payment ecosystem—including payment solutions, intermediaries, infrastructure providers, and connectivity layers.

**Distributed Infrastructure and Decentralization**

While redundancy provides alternatives, distribution and decentralization aim to eliminate single points of failure altogether. This design practice strengthens resilience by geographically dispersing components within the payment and connectivity infrastructure layers. Such architectural decentralization enables systems to withstand localized disruptions such as cyberattacks, natural disasters, or regional outages. It can also have implications in the intermediary layer, as individual intermediaries can choose different architectures for their IT operations.

By compartmentalizing system components across multiple sites and reducing centralized dependencies, the ecosystem enhances fault tolerance. This design practice includes two critical subcomponents to avoid single point of failures. Geographic distribution refers to the physical dispersion of infrastructure, processing, and operations across multiple locations to reduce exposure to localized

risks, and decentralization involves designing systems with decentralized control for certain functions of the system. This practice strongly focuses on the infrastructure and connectivity layers, but is also relevant to intermediary and, indirectly, solution layers.

**User-Centric Accessibility and Awareness**

This practice ensures that users retain seamless access to payment services, even during disruptions, and possess the digital literacy and awareness needed to navigate and use these financial services. The practice emphasizes offering multiple access points to various payment solutions—across different intermediaries and payments infrastructures. Other practices include the development of intuitive, inclusive user interfaces, along with effective communication channels to inform and educate users about these financial services and any status changes.

Thus, though directly centered on the user layer, this practice also implies that the payment solution layer—the closest interface to the user—is designed with accessibility in mind. A requisite for this is that all downstream layers must function reliably to make solutions accessible and usable during stressful times.

**Operational and Cybersecurity**

The operational and cybersecurity practice focuses on the capability for the payment ecosystem to withstand security threats, operational disruption, and inherent design flaws. This practice entails aligning a nation's payment ecosystem with best practices and international guidance on payment infrastructures resilience such as the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions Principles for Financial Market Infrastructures, Implementation Monitoring of PFMI: Third Update to Level 1 Assessment Report, and the Guidance on Cyber Resilience for Financial Market Infrastructures (Committee on Payments and Market Infrastructure 2012, 2016a, 2016b), as well as international standards for the banking sector's operational resilience such as the Basel Committee on Banking Supervision Principles for Operational Resilience. Finally, applying specific business continuity frameworks and best practices, like the Targeted Plan for Service Continuity (Carnegie Mellon University n.d.) by Carnegie Mellon University, can complement the international standards. Moreover, the IMF Fintech Note on Cyber Resilience of the Central Bank Digital Currency Ecosystem offers further perspective on cyber resilience.[4]

This practice covers all layers, with primary emphasis on infrastructure, intermediaries, and connectivity. However, in a robust payment ecosystem, individuals in the user layer also have a basic understanding of how to protect themselves and their devices from cyber risks.

[4] For the dedicated research, please refer to the work on Cyber Resilience of the Central Bank Digital Currency Ecosystem as a part of Bharath, Paduraru, and Gaidosch (2025).

**Regulatory and Legal Practice**

The regulatory and legal practice encompasses both foundational legal readiness and adaptive legal agility. It refers to having comprehensive and enforceable legal frameworks that support all layers of the payment ecosystem—before, during, and after a crisis. This includes not only relevant laws and regulations but also the institutional capacity to implement and enforce them effectively.

Importantly, this practice underscores the ability to rapidly adapt to regulatory and compliance requirements during times of crisis, which is referred to as regulatory agility. Together, these elements ensure the system's legal resilience and ability to respond to evolving stressors and obligations. This practice cuts across and underlies all layers, providing an enabling environment to make resilience enforceable and adaptable.

# II. Strategies and Lessons for Strengthening Payment Resilience

This section presents strategies that policymakers can consider for enhancing payment ecosystem resilience by addressing the challenges discussed in the previous section and their contributions to resilience. Each strategy draws on one or several payment ecosystem resilience practices discussed in the previous section. For simplicity, each strategy is grouped under a single primary practice, though many strategies will display aspects of multiple resilience practices. These strategies reflect practical lessons learned through challenging implementation environments, offering evidence-based pathways to build more robust payment ecosystems that can withstand various shocks while maintaining essential financial services. By examining what has and has not worked in the most challenging contexts, these strategies offer valuable insights for policymakers and practitioners seeking to strengthen payment system resilience across diverse settings.

The analysis is backed by country case studies from seven fragile and conflict-affected jurisdictions—Ukraine, West Bank and Gaza, Sudan, Yemen, Haiti, Tuvalu, and the Central African Economic and Monetary Community (Communauté Economique et Monétaire de l'Afrique Centrale or CEMAC). These cases were selected to ensure broad representation across geographic regions, levels of digitalization, and different types of fragility. Together, they provide a diverse empirical foundation for identifying context-specific strategies and common resilience challenges. The contexts and challenges of each jurisdiction differ, and any strategy to increase resilience will need to be specifically tailored to domestic circumstances. This means that a one-size-fits-all approach will not work. Nevertheless, by studying different jurisdictions, policymakers can gain information about the strategies potentially available to them.

Unless otherwise indicated, the information on each jurisdiction discussed in this Note is based on interviews with representatives of monetary authorities and IMF country teams, and complemented by public sources.

**Ukraine** is a country that has achieved comparatively high levels of digitalization[5] and institutional maturity. Even amid full-scale war after the Russian invasion in 2022, Ukraine has maintained continuity of core payment services and rapidly adjusted its financial infrastructure. The country's experience underscores how prior investment in digital platforms, remote service delivery, and contingency planning can support operational resilience under extreme conditions. These efforts align with Ukraine's strategic course toward European integration; the country was granted EU candidate status in 2022, and its institutional reforms—including in the digital and financial sectors—are part of broader convergence with EU standards.

[5] As demonstrated by its ranking in the 2024 UN E-Government Survey, Ukraine ranked among the top in both the E-Participation Index and the Online Services Index (United Nations 2024).

**West Bank and Gaza** present a particularly complex case. Despite increased fragmentation of the governing authority and administration after 2007 in the World Bank Group, the Palestinian Monetary Authority (PMA) continues to implement its mandate and formulate policies for all West Bank and Gaza. This includes banking supervision and regulation as well as the oversight and regulation of the payment system, and operation of its infrastructure. The payment system infrastructure is well developed, with regulation covering nonbank PSPs, and the payment strategy focusing on promoting e-payments adoption. Recently, Gaza has experienced recurrent armed conflict, whereas the West Bank endures political and economic constraints. The example in this Note illustrates the challenges of maintaining a functioning payment system amid restrictions on the movement of goods, people, and capital, as well as external shocks.

**Sudan** is experiencing a large-scale internal conflict between rival military factions, which has resulted in the disruption of core government functions and infrastructure. With limited digitalization and constrained connectivity, Sudan exemplifies the difficulties of preserving payment system continuity in settings where both physical and digital infrastructures are under direct threat.

**Yemen** is another case of protracted internal conflict, marked by political and economic fragmentation, social instability, and humanitarian crisis. Despite limited infrastructure, fragmented financial markets, and low levels of financial inclusion, payment solutions have persisted in part through informal and hybrid systems. The Yemeni case illustrates how decentralization, diaspora remittances, and local innovation can help sustain minimal financial connectivity even in near-collapse scenarios.

**Haiti** faces extreme levels of violence driven by organized criminal groups and a breakdown in public security. The country has experienced repeated disruptions to public services, including the banking sector, and its fragility status fluctuates based on evolving levels of violence and governance capacity. Haiti provides important insights into the impact of nonstate armed actors on financial stability and service delivery.

**Tuvalu** is a microstate whose fragility stems from its geographic isolation. As a remote island nation, it faces severe infrastructure and connectivity constraints, with high dependence on external financial and communication networks. Tuvalu's case underscores the risks of isolation and highlights the importance of partnerships and targeted support in strengthening payment resilience.

**CEMAC** represents a unique case for examining both regional- and country-specific experiences. As a monetary union, it includes multiple jurisdictions with varying fragility classifications—conflict-affected states such as Cameroon and the Central African Republic, and fragile states such as Chad and the Republic of Congo. The shared central banking and currency infrastructure offers insights into how regionally coordinated systems function in highly heterogeneous environments. This dual perspective enables analysis of institutional arrangements for both the monetary union and specific counties.

To contextualize the resilience strategies discussed in this Note, Table 1 provides a snapshot of the jurisdictions covered. It includes two key indicators such as the share of the population using the internet (used here as a proxy for digitalization) and the percentage of adults with a bank account (used as a

proxy for financial inclusion). Although these indicators are not exhaustive, they offer a useful comparative reference point for understanding the starting conditions and constraints under which resilience strategies are being deployed.

**Table 1. FCS Jurisdictions Included in the Study**

| Jurisdiction | FCS List (IMF FY25) | Digitalization (%) | Financial Inclusion (%) |
|---|---|---|---|
| CEMAC | n.a.[1] | 38.9[2] | 40.6 |
| Haiti | Conflict-affected | 39.3 | 33.0 |
| Tuvalu | Fragile | 74.0 | n.a. |
| Sudan | Conflict-affected | 26.4 | n.a. |
| Ukraine | Conflict-affected | 91.8 | 84.0 |
| West Bank and Gaza | Conflict-affected | 89.0[3] | 50.1[4] |
| Yemen | Conflict-affected | 13.8 | 12.0 |

Source: Authors. Data from World Bank FCS List 2025; DataHub; and World Bank Global FinDex (see Financial Inclusion Data and Indicators n.d.).
Note: CEMAC = Central African Economic and Monetary Community; FCS = Fragile and Conflict-Affected States; n.a. = not applicable; PMA = Palestinian Monetary Authority.
[1] CEMAC comprises multiple countries several of which are FCS but not all (Gabon and Equatorial Guinea).
[2] Average.
[3] Palestinian Central Bureau of Statistics and Ministry of Communications and Information Technology. The value 89.0 percent refers to the corresponding values of 92.0 in the West Bank and 83.0 in Gaza (see PCBS 2023).
[4] The source from which this value is taken is PMA.

## Redundancy and Scalability

### Multisite Operational Architecture

A key strategy for ensuring payment system resilience is redundancy through geographic diversification of payment infrastructures. Establishing parallel multisite architecture for the payment infrastructure or backup data centers in separate locations reduces the risk of system failures because of physical disruptions. Automated failover mechanisms and regular transition training for financial institutions further strengthen resilience, ensuring that payment systems can function even if the primary infrastructure or one site of infrastructure (in the case of multisite design) is compromised. The CPSS-IOSCO Principles for Financial Market Infrastructures requires systemic payment infrastructures to have at least two sites with different risk profiles, but extreme circumstances might warrant an even greater degree of redundancy.

However, a multisite model involves challenges and costs that need to be addressed. Each site must be equipped with comparable processing capacity to maintain balanced operations and ensure seamless switching. This amounts to significant investments. Further, data synchronization between sites requires reliable communication channels between them.

**In Ukraine,** to safeguard payment operations under wartime conditions, the National Bank of Ukraine (NBU) transitioned from a three-site to a five-site parallel architecture of the systemically important payment infrastructure, RTGS. Even during the war, the NBU regularly conducts training and simulation

exercises with banks and other financial institutions to ensure that transitions between data centers can be executed smoothly and without service interruption. However, the war introduced significant risks to communication channels, which heightened the complexity of synchronizing between sites. Although major disruptions were largely avoided, the situation underscored the need for all sites to maintain equivalent capabilities—including alternative power sources and redundant communication links—to ensure independent functionality in case of isolation.

**Managing Connectivity Dependency and Single Point of Failure**

Connectivity is a critical enabler of payment system resilience. Relying on a single communication or power provider creates systemic risks, particularly in FCS—where any disruption can halt payment operations. The ability to switch between providers or technologies ensures continuity of services, reduces dependency, and gives users and institutions more control over risk management. A diversified provider landscape across the connectivity layer or independent connectivity lines of the same provider instead introduces redundancy throughout the payment ecosystem.

**In Ukraine,** after widespread attacks on the energy infrastructure, the NBU required both banks and nonbank PSPs to implement connectivity redundancy. Specifically, they were mandated to maintain access to at least two independent internet providers, using physically distinct routes. This ensured that if one provider's infrastructure was damaged, services could continue through the other. To maintain the functionality of payment terminals during blackouts, acquiring banks and large retail chains jointly established backup communication channels, typically combining cable internet with mobile networks. Many merchants also invested in power generators to ensure continuous acceptance of cashless payments.

**In Gaza,** power and connectivity infrastructure are highly centralized and heavily dependent on external sources. Both electricity and fuel required to operate generators relied on imports from Israel. During periods of conflict, these supplies were cut off, halting centralized electricity production entirely. At the same time, Gaza relied on a single telecom provider with limited redundancy, leading to prolonged and frequent network outages. Even when digital payment platforms remained technically functional, they became inaccessible to most users because of the collapse of underlying connectivity infrastructure. As a limited fallback, standalone batteries and small-scale solar-powered systems were used, but their capacity was insufficient to support wider connectivity or payment operations.

**In Haiti**, connectivity and fuel infrastructure are frequently targeted by criminal groups. Gangs have vandalized power relays and telecom towers, blocked transport routes, and seized ports—interrupting fuel supplies needed for diesel-powered generators. These conditions have prevented telecom operators from restoring damaged infrastructure. Repair crews often cannot access affected areas because of security concerns, which prolongs outages and cuts communities off from both cash and digital payment systems, as cash distribution also depends on power to operate ATMs, security systems, and cash-handling infrastructure.

## Distributed Infrastructure and Decentralization

**Distribution through Satellite Networks**

Traditional communication systems are to a large degree based on land- or sea-based cables across large distances. Cables are vulnerable to physical damage and are increasingly high-value targets for aggressors seeking to disrupt communications in a territory.

Satellite networks technology (SNT) can therefore play a vital role in enhancing the payment ecosystem resilience by providing an alternative communication channel when land- or sea-based communications are disrupted. SNT is a space-based internet system providing high-speed internet with low latency. Aside from adding redundancy in communications, satellite networks also create a network of multisite ground stations, requiring comparatively small ground-based terminals and satellite dishes to relay communication. Thus, SNT also provides decentralization, allowing access to communication at multiple locations not dependent on a centrally located site.

However, FCS settings can also expose satellite links to risks such as signal spoofing, interception, or jamming, which require strong safeguards and contingency measures, such as signal authentication protocols, fallback communication channels, and physical relocation of terminals to less obstructed areas.

**In Sudan**, where conventional telecom infrastructure has frequently been disabled amid conflict, SNT-based internet—particularly through Starlink—has emerged as a critical workaround to restore limited digital connectivity. Though not formally authorized in the country, Starlink equipment is increasingly used in areas lacking stable infrastructure. In some regions, devices are acquired from neighboring country at commercial rates and brought into Sudan, where they are rented to local users, enabling disconnected regions to access mobile banking, initiate mobile money transactions, and sync offline smart card or e-voucher data issued by humanitarian organizations.

However, access remains uneven. In some parts of the country, access to Starlink is tightly regulated and largely unavailable. Moreover, even where available, it comes with some serious risks and limitations. Access often requires physical travel to specific hotspots, exposing civilians to surveillance and violence. There have been reports of Starlink kits being seized or destroyed by armed groups. In addition, the high fees—approximately $2.50 per hour (Reuters 2024)—exacerbate unequal access.

**In Tuvalu**, connectivity has long depended on a single state-owned telecom provider and satellite links operated through foreign jurisdictions (such as Australia). In early 2025, Starlink began offering direct services to Tuvalu, introducing redundancy to its communications infrastructure. Unlike the previous arrangement, where satellite connectivity was routed through third parties, direct access helped reduce costs and improve service reliability, an important step forward to enhance the payment ecosystem resilience in remote island contexts.

**In Ukraine**, a few days after the full-scale war started, officials requested that Starlink extend services to Ukraine. Shortly thereafter, these services were provided at no cost. Although Starlink has been extensively used in military operations, it has also been a crucial backup for civilian usage in areas where land-based communication has been disrupted. It thus added redundancy to the communication layer and can enhance payment ecosystem resilience.

However, reliance on a limited number of global satellite providers has underscored the risks of vendor concentration. In politically sensitive environments, such dependencies may be affected by external pressures, and high costs for equipment and service continue to limit broader deployment. Operational constraints have also emerged in Ukraine, especially in dense urban areas where tall buildings obstruct the satellite signal's line-of-sight, affecting reliability. These settings can also expose satellite links to risks such as signal spoofing, interception, or jamming which require strong safeguards and contingency measures such as signal authentication protocols, fallback communication channels, and physical relocation of terminals to less obstructed areas.

These dynamics underscore both the promise and the complexity of satellite technologies as a resilience measure in conflict zones, where connectivity is essential but contested. However, as of now, such solutions remain expensive and not always available, limiting their widespread use.

**Decentralizing Connectivity**

One key source of resilience lies in shifting from centralized power systems—which are essential to sustaining connectivity infrastructure layer—to decentralized models that rely on local power generation. Producing electricity close to the point of use reduces vulnerability to disruptions in long-distance transmission networks and enhances the ability to maintain operations during broader grid failures. In fragile settings, where centralized responses may be delayed or unfeasible, communities and businesses often improvise localized solutions. These bottom-up adaptations play a critical role in sustaining functionality and strengthening overall system resilience.

**In Gaza**, where fuel shortages and blackouts are routine, merchants have equipped POS terminals with solar panels, enabling continued transaction processing during grid failures. Charging stations powered by solar energy have been set up in markets to allow consumers to recharge mobile devices. Some merchants have also reconfigured POS terminals to function through landline connections instead of mobile networks—ensuring functionality even when cellular networks are down.

**In Ukraine**, the NBU led the development of "Power Banking," a nationwide initiative linking over 2,400 bank branches to a resilient network spanning 60 banks out of 80. Each Power Banking location is equipped with a diesel generator, autonomous connectivity solutions (including fiber, cellular, or satellite links), and serves as a shared access point for clients of all participating banks. Functionally, the system operates as a unified ecosystem, allowing customers to access basic banking services at any participating branch regardless of which bank they normally use, as if they were being served by their own institution. As of 2025, 55 percent of bank facilities are part of this network. The initiative was

launched within a week of coordinated attacks on energy infrastructure and has since become a cornerstone of Ukraine's payment resilience strategy.

These decentralized solutions have proven crucial in contexts where the centralized connectivity layer is either unreliable or compromised. However, there are also costs and trade-offs with a strategy of decentralization. Modern power and communications facilities have been developed to minimize costs, favoring economies of scale in production and distribution. Creating multiple sites for small-scale power production is inevitably more expensive and less scalable.[6]

**Distribution/Scalability through Cloud Services**

Cloud services—delivered over the internet by third-party providers—allow organizations to access computing resources, storage, platforms, and software without the need to maintain their own physical infrastructure. These services are typically categorized as infrastructure as a service, platform as a service, or software as a service each offering different levels of management between the provider and the client.

For both payment infrastructures and payment intermediaries layers, cloud services can significantly enhance operational resilience. First, cloud platforms operate through multiple geographically distributed data centers, which reduces vulnerability to localized disruptions such as natural disasters, cyber incidents, or power outages. Second, cloud-based systems offer elastic scalability, enabling organizations to scale resources rapidly based on demand and helping prevent system overloads during periods of volatility while maintaining cost efficiency during normal operations. Cloud environments also offer availability and redundancy through built-in failover mechanisms, ensuring continuity even when individual components fail. Moreover, leading providers offer advanced security capabilities, including 24/7 monitoring, threat intelligence, and automated patch management—measures that would be cost-prohibitive for many institutions to implement independently.

For payment intermediaries operating in FCS, the ability to shift workloads across regions, access to real-time backups, and recover quickly from disruptions makes cloud services an increasingly vital enabler of business continuity and resilience. In such settings, migrating critical services to the cloud can also serve as a practical short-term solution when physical infrastructure is compromised or unreliable.[7]

However, cloud adoption also brings important risks and trade-offs (Board of Governors of the Federal Reserve System 2024). Moving critical infrastructure to third-party platforms can reduce direct control over operations and introduce vendor lock-in, especially when dealing with large Big Tech cloud providers. Negotiating specific contractual terms—especially for data sovereignty, operational

[6] The centralized generation was estimated to cost €25 billion less than a decentralized model at national scale according to Fraunhofer Institute 2050 scenario for Germany (see Lumbreras and others 2017).

[7] In some FCS without domestic financial market infrastructure, the World Bank has recommended and supported full deployment of core payment systems entirely on the cloud. In Somalia, for example, real-time gross settlement systems and fast payment systems were implemented under this model, with the central bank retaining oversight of business operations while an outsourced provider managing the technical and hardware components.

transparency, and service-level commitments—can be challenging, especially for FCS without a strong legal system and regulatory certainty. Furthermore, data protection and privacy concerns remain especially acute for financial market infrastructures, which are traditionally conservative in outsourcing core operations. In most stable jurisdictions, central banks and system operators still hesitate to place critical services in the cloud because of regulatory and security considerations.

**Ukraine's** experience illustrates the strategic benefits of cloud deployment under duress. The NBU operates its payment infrastructure on a corporate cloud model distributed across multiple regions, each with at least one accessibility zone—similar to availability zones in global cloud platforms—allowing dynamic rerouting during localized disruptions. This design was critical to sustaining interbank settlements and digital payments during the early phases of the full-scale war in 2022, ensuring both geographic diversification and operational continuity.

Prior to the war, most Ukrainian PSPs used cloud only for limited internal functions, as regulations prohibited storing personal client data abroad, effectively preventing use of major international providers. Facing potential physical threats to critical infrastructure, including data centers, because of nearby rocket strikes, providers implemented an urgent shift to cloud infrastructure enabled by expedited regulatory decision allowing the storage and processing of client data in trusted jurisdictions such as the EU, Great Britain, United States, and Canada. This allowed banks to move critical services such as transaction processing and data management into more secure, cloud-based environments. Global card networks such as Visa and Mastercard already operate on distributed cloud infrastructure.

The combination of resilient cloud infrastructure and rapid adaptation by domestic actors was instrumental in preserving access to financial services for households and businesses during a period of extreme instability.

**Chad, a CEMAC country,** is exploring the adoption of a hybrid cloud model to strengthen its national data infrastructure in support of broader digital development, including future enhancements to the payment ecosystem. A hybrid cloud combines public cloud services (offered by third-party providers) with private infrastructure (maintained by national authorities), enabling greater flexibility, cost efficiency, and control over sensitive data. By using this model, Chad aims to ensure secure storage and real-time access to financial and administrative data, which can underpin more resilient and interoperable payment services.

**Foreign Infrastructure for Redundancy**

In fragile and post-conflict contexts, access to foreign or jointly operated payment infrastructure can offer critical continuity when domestic systems are unavailable or unreliable. In addition, foreign infrastructure may provide more advanced technology, higher availability, and physical protection from local conflict-related damage. Hosting essential functions outside of conflict zones ensures that operational sites remain insulated from disruption, allowing core services to continue even when domestic infrastructure is compromised.

Relying on foreign systems, however, creates a trade-off. On the one hand, it adds protective redundancy. On the other hand, it can imply reliance on infrastructure that can be outside of direct influence. One way to manage such a trade-off is to ensure that domestic services are in place and that the foreign infrastructure is a layer of redundancy where feasible and that there is no direct dependency. Further, regular communication and coordination with any foreign counterpart that hosts important payments infrastructure can be beneficial to establish clear and mutually acceptable guidelines. Where feasible, a central bank with an adequate capacity could also collaborate with the overseer or supervisor of the foreign payment infrastructure to gain assurances that appropriate risk management and oversight practices are in place.

**In Sudan**, humanitarian organizations and donor-funded aid programs are increasingly relying on e-voucher platforms supported by infrastructure hosted outside the country to deliver aid in areas where local banking, mobile money, and cash distribution are unreliable or inaccessible. This shift was driven by the collapse of core domestic payment infrastructures after direct militant attacks on the Central Bank of Sudan, which destroyed the RTGS, the automated clearinghouses, and the national card switch. Although the Central Bank of Sudan successfully restored operations of domestic payment infrastructures several months later, humanitarian and donor programs continued to prefer foreign-hosted e-voucher platforms such as RedRose, AIDONIC and Last Mile Technology. These platforms combine beneficiary registration, merchant onboarding, voucher transaction processing, and most critically, settlement through bank accounts held abroad. This reliance on foreign core banking systems enables continued operations even when Sudan's domestic financial infrastructure is degraded or inaccessible.

The process is straightforward: beneficiaries receive e-vouchers through mobile apps or smart cards, which they use at approved merchants. Transactions are recorded offline and uploaded once internet access is available. Crucially, merchants are reimbursed through offshore financial institutions, allowing aid delivery to continue despite domestic financial system disruptions.

Though effective, this model limits beneficiary choice to specific merchants and raises regulatory concerns, particularly around the use of offshore settlement outside national oversight. Still, where supply chains and merchant participation can be secured, these platforms offer a scalable, resilient solution for humanitarian assistance in high-risk environments.

**In Tuvalu**, access to cross-border payment services depends heavily on correspondent banking relationships maintained by just one of the two domestic banks. This arrangement provides a vital link to the international financial system but also creates significant vulnerability because of the reliance on a single institution. Tuvalu's example illustrates how small states may depend on foreign infrastructure to sustain basic financial services, while facing heightened risk from concentrated institutional and operational dependencies.

## User-Centric Accessibility and Awareness

**Payment Solution Design for Continuity**

The ability of PSPs, operators of payment infrastructure, or other players to adapt products, expand coverage, and deliver targeted innovations plays a critical role in maintaining payment continuity when crisis conditions rapidly evolve. Adjustments may include temporarily waving fees, enhancing interoperability, or launching new tools tailored to urgent needs—such as mobile money, fast payments, and donation platforms. These innovations not only help preserve access but also build public trust by demonstrating responsiveness and reliability under stress.

**In Ukraine**, maintaining the widespread use of payment cards—still the most common digital payment method—was a priority after the full-scale war. To support the Ukrainian economy international card networks (Visa and Mastercard) eliminated merchant fees during the first two month of the war. International payment systems Visa and Mastercard temporarily reduced the interbank commission (interchange) to 0 percent for all transactions within Ukraine from March 4, 2022 and canceled transaction fees for acquiring banks and issuing banks for domestic transactions. Some digital banks in Ukraine also developed wartime-specific products to address urgent needs. One example is a donation solution designed to support military and humanitarian efforts. The coordinated efforts of payment market participants allow users to contribute easily through digital channels while providing transparency by publicly displaying the total amount collected in real time. This simplified, traceable model strengthened trust and encouraged widespread participation during a period of heightened national mobilization.

Innovative solutions can also enhance interoperability and broaden access, even amid operational constraints. **In Gaza**, the PMA launched fast payment platform in May 2024 that enabled bank-to-bank, wallet-to-wallet, wallet-to-bank, and bank-to-wallet account transfers. This allowed users with the app installed prior to internet disruptions to move funds between platforms and facilitate interoperability among PSPs. However, identity verification challenges soon emerged, including fraud attempts involving stolen credentials of deceased individuals. As a result, onboarding of new users was suspended—underscoring the importance of strong identity management as a precondition in digital payment expansion.

Digital platforms are also being leveraged to deliver humanitarian assistance. The PMA has worked with PSPs to enable aid disbursements directly into mobile wallets. Recipients are issued with QR codes that can be used to load funds into designated wallets, which can then be used for purchases or withdrawals where infrastructure permits. This system increases transparency and allows humanitarian actors to verify that funds reach the intended recipients. However, limitations in digital infrastructure remain a barrier to scale. Access to Israeli telecommunications networks is currently necessary for these systems to function, and negotiations are ongoing to facilitate broader connectivity.

**In Sudan**, the outbreak of armed conflict in April 2023 severely disrupted access to cash and banking services, leading to a sharp increase in the use of digital payment applications. Bankak, the most widely used banking app in the country, saw its activations nearly double as people turned to safer, remote

methods to transfer funds and make essential payments (Cook and others 2024). Although this shift helped maintain some continuity, usage remains limited because of internet shutdowns, low smartphone penetration, and high fees for converting digital balances into cash. Moreover, the use of the app often comes with trade-offs—users withdrawing funds through agents frequently face surcharges of up to 20 percent.

A similar example comes from **Haiti** where a debit card has launched that can be used in both the United States and Haiti, designed to function in stores and online while being fully managed through a mobile application. The product reduces reliance on cash, allowing users to manage their finances and receive funds remotely without exposing themselves to physical risk by visiting financial access points. This new debit card was quickly adopted by the population, suggesting a need among the population to diversify away from physical risks associated with cash.

**In Yemen**, a wallet-based digital payment solution is being developed to deliver humanitarian assistance more securely and efficiently. Led on the ground by UNICEF, with funding and digital design provided by the World Bank, the initiative aims to reduce reliance on cash, expand reach in remote areas, and provide beneficiaries with flexible access to aid. While still at an early stage, the solution reflects a broader effort to introduce targeted innovation that responds to operating constraints while laying the foundation for future digital inclusion.

**In Tuvalu**, where the economy remains predominantly cash-based, recent efforts focused on gradually introducing digital payment habits. The country launched its first ATM and began issuing encrypted prepaid cards which are currently used primarily for cash withdrawals. Although these cards do not yet replace cash in daily transactions, they serve as a steppingstone, familiarizing users with card-based systems and laying the groundwork for future expansion into broader digital financial services. This type of gradual strategy is supported by evidence from other countries, where phased rollouts of digital payment systems have helped build trust and drive adoption among previously cash-reliant populations (Morris 2024).

**Digital Identification for Secure Access**

Digital identity systems and government service applications play an essential enabling role in fostering payment system resilience. By providing secure, remote, and verifiable access to digital financial services and public resources, these platforms reduce reliance on physical infrastructure and in-person interactions, both of which are often disrupted in fragile and conflict-affected state settings. When properly implemented, they can serve as critical gateways to financial inclusion, benefit disbursement, and citizen–state communication during crises.

Although digital identification is vital for enabling payment access, it is typically considered just one component of a broader Digital Public Infrastructure framework that also includes digital payments and trusted data exchange systems. In practice, digital ID is often the foundational layer from which other Digital Public Infrastructure elements develop. When these components are designed to work together, they can enable a wide range of digital public and private services such as remote education, government transfers, healthcare delivery, and support for small business ecosystems. A robust digital

ecosystem, underpinned by interoperable Digital Public Infrastructure, enhances the reach and utility of digital financial tools and reinforces the resilience of the payment ecosystem itself.

**In Ukraine**, NBU BankID System—a secure digital identification system developed before the war by the NBU—enables individuals to remotely onboard and access a wide range of public, financial, and other commercial services through participating banks. Originally designed to promote digital inclusion, BankID System proved especially critical during wartime, allowing displaced individuals to maintain access to essential financial services despite disruptions. In addition, the Ukrainian government launched in 2020 the "Diia" app as a central digital platform for accessing public services, enabling citizens to retrieve digital versions of official documents, access administrative services, and receive emergency notifications. NBU BankID System is one of the authentication methods in "Diia" app.

The experience **in Gaza** highlights the risks to digital identity systems when critical infrastructure—such as power and telecommunications—is disrupted or unavailable. During outages, access to digital ID services was limited to users who had previously downloaded the app, while new users were unable to onboard, and identity verification became a growing concern. Instances of attempted fraud using stolen credentials prompted the PMA to suspend digital onboarding. However, where the necessary infrastructure exists, wallet providers could conduct physical know-your-customer and due diligence processes and open a wallet for end users who successfully provided sufficient proof of identity.

**In CEMAC**, the Cameroonian government launched a new biometric national ID system in February 2025, capable of issuing secure ID cards within 48 hours. This system integrates online pre-enrollment and biometric verification, significantly reducing processing times and improving accessibility. Although the new system holds strong potential, it is important to note that wait times after enrollment can still be substantial, and a large number of applicants remain in the queue, reflecting a legacy of delays and system backlogs. As implementation advances, the full benefits of the initiative are expected to materialize progressively. In addition, the issuance of biometric ID cards to refugees from other CEMAC countries such as the Central African Republic has begun.

**In Haiti**, the Banque de la République d'Haïti (BRH) has initiated efforts to explore the use of digital signatures to enhance the security of digital payments and, more importantly, to bolster public trust in these digital financial instruments. This initiative aligns with BRH's broader strategy to modernize the national payment system, reduce reliance on cash transactions, and promote financial inclusion through payment resilience.

**Promoting Digital Literacy**

A digitally literate population significantly enhances national payment ecosystems resilience in times of crisis. When users are familiar with a range of digital payment methods and platforms, they can more easily adapt when one service becomes unavailable, shifting quickly to alternatives such as mobile wallets, fintech solutions, and peer-to-peer transfers. This flexibility helps distribute transactional pressure across multiple channels, reducing the risk of overloading any single system and supporting continuity of essential payments.

In addition, digitally literate users are better equipped to avoid crisis-related fraud. They are more likely to implement strong security practices, such as using unique passwords, enabling two-factor authentication, and verifying transaction sources. This contributes to the overall cybersecurity of the payment ecosystem (see the following section Operational and Cybersecurity).

Digital literacy also plays a crucial role in protecting users from scams. Unlike fraud, which often involves unauthorized access, scams typically involve authorized transactions where users are tricked into transferring money voluntarily. These plans often originate outside the financial sector. In FCS, populations with low financial literacy—such as displaced persons or first-time digital users—are especially vulnerable, particularly when informal remittance channels or unfamiliar digital payment solutions are involved.

Developing digital literacy together with targeted outreach and inclusive policies can ensure that more citizens are empowered to engage with, and benefit from, resilient digital payment systems when crises arise.

**In Yemen**, resistance to digital payments is linked to widespread distrust in formal financial sector given Yemen's economic fragmentation and inconsistent regulation between the northern part of the country and Yemen's south which is under the control of its internationally recognized government. This distrust cuts across education and income levels. These examples underscore the need not only for improved digital literacy but also for broader trust-building measures and incentives to promote digital financial adoption.

**In the CEMAC region**, micro, small, and medium enterprises play a central role in the economy but are particularly vulnerable during crises because of limited access to formal financial services and a heavy reliance on cash. Recognizing this, the regional central bank has begun working directly with micro, small, and medium enterprises to promote financial resilience. This includes supporting tailored innovations, expanding access to digital tools, and advancing public awareness initiatives focused on digital payments and financial inclusion. These efforts are designed to increase the resilience of the enterprises but also the broader payment ecosystem.

**The Sudan** experience, however, shows that financial literacy is not the primary barrier to adopting new payment modalities. The rapid uptake of apps like Bankak during liquidity crises demonstrates that individuals can quickly adapt when the need arises. According to the Bank of Khartoum, Bankak saw an 85 percent increase of users, reaching approximately 7 million (The New Humanitarian 2024). Instead, the more pressing challenges are access to mobile phones, the internet, and reliable electricity for recharging devices. In Sudan, for example, many households—particularly among displaced populations—lack access to power at home.

**In Haiti**, as the adoption of digital services becomes increasingly important particularly in the context of the ongoing crisis, digital literacy has also become essential for consumer protection. In this regard, the BRH, in accordance with the National Financial Education Plan (PNEF 2020), has developed a series of

informational videos and publications to promote the use of digital financial products, while raising awareness about the risks associated with their use.

**Role of Cash for Continuity**

Payment resilience in crisis settings often requires both cash and digital payments to function, and be trusted and accessible by users. Cash retains strong advantages in terms of familiarity and resilience for person-to-person use. Yet it becomes risky or inaccessible when infrastructure breaks down or movement is dangerous. Conversely, digital payments can offer secure, remote alternatives, but rely on connectivity, device access, and public confidence. Maintaining this balance requires public trust in financial institutions, as crises can trigger destabilizing behaviors such as panic withdrawals or disengagement from formal systems. Proactive communication and financial education are essential tools for reinforcing confidence and stabilizing payment behavior during periods of uncertainty.

**In Ukraine**, the NBU implemented coordinated outreach campaigns during the early stages of the full-scale war, delivering consistent messaging across television, radio, and digital channels. These campaigns advised the population to hold only a week's worth of cash and reassured businesses about the continuity of digital payment operations. Public announcements by the NBU helped to prevent panic, reduce pressure on cash supply chains, and stabilize the ratio of cash to digital transactions. Other proactive measures also helped restore confidence in digital banking, reducing pressure on cash reserves. The NBU ensured banks maintained sufficient cash reserves, stabilized supply chains, and launched informational campaigns to prevent panic. In addition, cash withdrawals through cashiers at gas stations, in cooperation with card plans, provided an additional means of accessing cash when traditional banking infrastructure was under strain. Such measures helped mitigate supply bottlenecks and ensure continued cash circulation in high-risk areas.

**In Yemen,** humanitarian actors ensured continuity of cash transfers through close coordination with banks and flexible fund movement strategies. UNICEF provided advance warnings to banking partners about monthly cash needs, and organizations used a combination of formal financial channels, money transfer operators, and direct cash distributions. In addition, UNICEF is now developing wallet-based digital payment alternatives to expand coverage and reduce reliance on physical cash transfers—an approach discussed further in this section.

**In Gaza,** the PMA announced plans to transition the territory to a fully cashless system, as cash is increasingly difficult to circulate because of logistical and political constraints. The move aims to ensure more secure and targeted delivery of humanitarian aid. However, the transition is challenged by unreliable electricity, frequent internet disruptions, and lack of knowledge about, and trust in, digital financial tools. This highlights that digital-only solutions cannot succeed without foundational infrastructure and public engagement.

**In Haiti,** frequent disruptions in access to ATMs and bank branches during unrest and natural disasters recurrently disrupt payments in cash. As a result, the BRH supports expanding digital payments to preserve continuity when traditional cash-based channels are inaccessible.

These experiences show that resilience does not depend on a single modality, but on a payment ecosystem that can flexibly shift between cash and digital options based on context. Ensuring this requires not only infrastructure, but also public trust, redundancy in distribution channels, and proactive communication to prevent panic and maintain use of formal payment mechanisms.

**Digital Money for Resilience**

Stablecoins are digitally native assets that aim to maintain stable value by being backed by safe and liquid assets such as currency (like the dollar or euro), a commodity (such as gold), or a basket of currencies. Stablecoins are emerging as a payment solution and can potentially enhance payment resilience in FCS. Their ability to operate across borders, settle near-instantly, and function with limited infrastructure makes them potentially useful for humanitarian operations where traditional banking systems are disrupted or inaccessible.

Although stablecoins can offer advantages—such as reducing reliance on intermediaries, enhancing transparency through blockchain, and helping preserve value in volatile economic environments—many of these benefits have yet to materialize on scale. Merchant acceptance remains limited, constraining real-world usability, and in many jurisdictions the lack of clear regulatory frameworks raises concerns about oversight, consumer protection, and long-term sustainability. US dollar–backed stablecoins also pose risks of dollarization, which could erode monetary sovereignty and bring broader financial stability risks. These limitations underscore the gap between the promise of stablecoins and their practical implementation, particularly in FCS.

**In Sudan,** stablecoins are being used to deliver humanitarian aid in regions with limited cash access and severely degraded financial infrastructure. Because stablecoins are not legally classified as currency under Sudanese law, inbound transfers are not considered foreign exchange operations, enabling aid flows to bypass restrictions typically applied to cross-border cash movements through unlicensed channels. Aid is distributed through crypto wallets managed by providers such as COALA Pay, a blockchain-based payments platform that facilitates payments, including humanitarian transfers, while maintaining compliance with international sanctions and avoid blacklisted entities. Inside Sudan, a growing network of local agents redeems stablecoins for cash or goods. The model supports both group cash transfers, where one member receives and redistributes funds, and individual aid, where beneficiaries are issued QR codes linked to wallets. Agents scan the code, receive stablecoins, and disburse local currency. The system is fast, discreet, and more stable than the local currency, especially for displaced populations. However, the lack of a domestic regulatory framework raises risks, particularly around anti–money laundering and potential circumvention of capital flow management measures. Although providers comply with international standards, the absence of local supervision leaves vulnerabilities in monitoring inflows and enforcing currency controls.

**In Ukraine,** the United Nations High Commissioner for Refugees and Stellar Development Foundation piloted a stablecoin-based aid system using the USDC, U.S. dollar–denominated stablecoin issued by Circle, on the Stellar blockchain to support refugees. Funds were delivered to recipients' digital wallets and could be cashed out at over 4,500 MoneyGram locations, offering secure and transparent access

without the need for a bank account. This was especially valuable for people abroad facing administrative hurdles or language barriers when opening accounts (Circle Internet Financial 2024). Since most merchants do not accept stablecoins directly, Stellar partnered with MoneyGram to enable easy conversion to local currency, allowing refugees to meet essential needs without relying on foreign banking systems.

Unbacked crypto assets such as Bitcoin and Ethereum are less suitable for everyday payment use. Their extreme price volatility, high transaction costs, and slow processing times make them impractical for most real-world transactions. Nonetheless, in exceptional cases—such as during the early stages of the Ukraine conflict—they were leveraged for rapid fundraising and cross-border donations, demonstrating limited utility in crisis-driven scenarios (see Box 1 on the Use of Crypto Assets in Wartime Ukraine).

**Box 1. Use of Crypto Assets in Wartime Ukraine**

At the beginning of the full-scale war, crypto assets were widely used in Ukraine as a tool for collecting donations. Opening traditional bank accounts for public authorities to collect donations in foreign currency took some time, so the Ministry of Digital Transformation quickly launched official wallets to receive donations in Bitcoin and Ethereum. These wallets provided an alternative way to support Ukraine's military and humanitarian needs through cross-border transactions.

Since the beginning of the full-scale war, the use of crypto assets to circumvent capital controls has expanded. In the absence of an adequate regulatory framework and unclear mandates and responsibilities among the authorities tasked with regulation and supervision, it became difficult to monitor such activity. In response, the National Bank of Ukraine introduced restrictions on the purchase of crypto assets using traditional digital payment methods through Ukrainian banks. However, some users continued to buy crypto using cards issued by crypto-friendly foreign banks, often with relaxed KYC requirements, or through cash-based transactions at crypto kiosks.

This experience highlights both the practical role that crypto assets can play in crisis settings and problems that may arise in the absence of a legal and regulatory frameworks and clear supervisory action.

## Operational and Cybersecurity

### Contingency Planning

To ensure the resilience of payment systems during crises, countries must develop comprehensive contingency plans that account for various risks. These plans should include pre-established crisis protocols, regulatory adaptations, alternative operational arrangements, and comprehensive training for all staff involved in various layers of the payment ecosystem and participants. A strong contingency framework ensures that financial institutions can adapt quickly, sustain services, and minimize disruptions during conflict or disaster.

**Ukraine's** contingency planning was first developed after the beginning of the war in 2014 and later

activated in 2022 when the full-scale war began (European Payments Council 2023). The plans put in place after 2014 included relocating key financial institutions, safeguarding payment infrastructure, and ensuring liquidity measures were in place. This preparation made a significant difference in the ability to uphold operations after the beginning of the war.

**In Haiti,** BRH had contingency plans in place prior to the resurgence of violence and activated them as instability worsened. The BRH established a backup facility, including servers, services, and a data center essential for the resilience of their payment ecosystem. Staff, servers, and financial infrastructure were relocated to buildings outside Port-au-Prince to ensure continued payment operations. However, there have been delays in moving infrastructure out of unsafe areas because of concerns over the physical security of the staff operating them, underscoring the challenges of safeguarding financial systems in prolonged conflict situations. In part, this led to the 2023 cybersecurity incident that disrupted BRH operations.

**Coordinated Incident Response**

Cyberattacks have become a key element of modern warfare, targeting financial systems to disrupt stability, and erode trust. Building an effective response to cyber and digital threats requires timely, coordinated, and sector-wide action. In FCS contexts, where the impact of cyber incidents can be amplified by physical disruptions and institutional strain, a structured and collaborative response is critical to maintaining payment system continuity. This includes close cooperation between regulatory and supervisory bodies, national cybersecurity agencies, and payment intermediaries and operators of payment infrastructure able to detect threats, contain damage, and restore operations rapidly.

In addition to cyberattacks, scams—including phishing, impersonation, and social engineering—are increasingly recognized as systemic risks in FCS. Although long-term efforts to build financial literacy are essential (as discussed in the “Promoting Digital Literacy” subsection), these threats also require structured and coordinated incident response, like frameworks used for fraud and cyber threats. A proactive, centralized, and publicly available institutional response—potentially through a dedicated public-private body—could help develop practical tools such as scam intelligence-sharing platforms, blacklists of malicious websites, user alerts, and coordinated takedown mechanisms. These measures complement educational efforts and enable faster detection, containment, and prevention of scam-related harm within the payment ecosystem.

**In CEMAC**, the Central Bank of Central African States has identified cybersecurity, frauds, and scams as the most significant threats to payment resilience and reputation within the CEMAC region. To address these risks, Central Bank of Central African States has implemented procedures requiring PSPs to establish robust IT security measures and comply with anti–money laundering and countering the financing of terrorism regulations.

**In Gaza,** to respond to heightened cyberattacks during periods of conflict, the PMA has implemented measures to compartmentalize financial institution networks through the establishment of firewalls and network segregation techniques. These cybersecurity designs and strategies proved essential for

safeguarding the financial network between financial institutions and the central bank. If one of the participants was breached, the impact could be contained, enabling focused incident response efforts to mitigate the damage effectively.

**In Ukraine**, a wave of powerful distributed denial-of-service attacks targeted major banks ahead of the full-scale war in early 2022. The two largest banks repelled the attacks without disruption, but smaller institutions faced temporary outages, though core services were restored within 24 hours.

This resilience was enabled by the Computer Security Incident Response Team of the National Bank of Ukraine (CSIRT-NBU), established by the NBU after earlier cyber incidents. Its role includes protecting internal systems, analyzing cyber incidents, coordinating with cybersecurity entities, and supporting PSPs. This structure enabled real-time monitoring, cross-sector coordination, and incident response. To counter rising threats such as phishing and malware, CSIRT-NBU took part in a project of developing a countrywide threat-monitoring system that blocks malicious websites and alerts users at the browser level.

To mitigate a broader range of digital threats—including scams such as phishing and impersonation fraud—a dedicated public-private partnership was also established. On the central bank side, the NBU launched the Malware Information Sharing Platform, which facilitates collaboration and allows for the real-time exchange of threat intelligence, enabling rapid identification and neutralization of malicious websites and applications. A threat-monitoring system was deployed in cooperation with payment intermediaries and industry associations to block scam infrastructure and alert users at the browser level. When users attempt to access known malicious websites, a pop-up warns them that the page is associated with fraudulent activity, serving as a real-time preventive measure. These measures curtailed phishing targeting vulnerable groups, underscoring the role of coordinated action in enhancing system and user resilience.

## Regulatory and Legal Resilience

**Pre-crisis Financial Stability for Payment Resilience**

A country's ability to maintain payment system functionality during a crisis is significantly influenced by the pre-crisis stability of its financial sector. A well-regulated banking system, sound monetary policy, and established payment market infrastructure provide the necessary foundation for resilience. Robust financial oversight, strong liquidity management, and adherence to international supervision standards ensure that disruptions can be managed effectively, allowing digital payments to continue functioning even in times of crisis. This preexisting foundation largely determines how a country enters crisis. Those already facing prolonged fragility, institutional weakness, or economic instability are especially vulnerable, as they lack the structural capacity to respond quickly or maintain public trust in formal payment ecosystems.

Where institutional foundations are weak, another critical risk emerges: the potential misuse of public financial systems by those in power. In FCS, abrupt political transitions or entrenched elite interests may lead to unauthorized extraction or diversion of public resources, including through the payment

ecosystem itself. As government operations and disbursements become increasingly digitized, these risks evolve to include manipulation of funds through state-controlled digital platforms. Without clear legal constraints, transparency mechanisms, embedded operational safeguards, and independent oversight, such actions can severely erode public trust and undermine the very infrastructure needed to maintain payment continuity during crises.

**Yemen** illustrates the consequences of entering into conflict without a stable financial base. Years of political and institutional division have led to a profound lack of trust in the banking system. This distrust cuts across social and educational lines and fuels a strong cultural preference for cash and informal payment systems (such as the Hawala system operating mostly through money exchangers). As a result, the bank-based digital payment usage remains extremely limited, and many customers routinely withdraw balances in full.

The banking sector suffers from liquidity shortages that have at times prevented the completion of settlement of donor-funded disbursements, further undermining confidence. Arbitrary restrictions imposed by de facto authorities in both the northern and southern regions have worsened the situation. Banks face region-specific sanctions and limited interoperability, leading to sudden disruptions in closed-loop systems and loss of access to funds for ordinary users. These conditions make any scaled deployment of digital payments highly challenging (Sana'a Center for Strategic Studies n.d.).

By contrast, **Ukraine** entered the 2022 full-scale war with a much stronger financial foundation. After the 2014 war and subsequent economic challenges, Ukraine implemented major banking reforms. These included adopting international supervision and financial monitoring standards, resolving nonperforming loans, closing insolvent banks, and nationalizing systemically important ones. As a result, trust in the banking system steadily improved.

This institutional strength helped contain panic in the early days of the full-scale war. The ability of the authorities to reassure the public and ensure uninterrupted access to funds and digital services helped prevent cash hoarding and bank runs. Confidence in the payment ecosystem—built on a reformed and credible financial sector—proved essential to sustaining resilience under pressure.

**West Bank and Gaza** also entered the current conflict in Gaza and Israel with a sound banking sector characterized by significant capital and liquidity buffers. Since 2008, the PMA has strengthened the financial stability toolkit including the supervisory and regulation framework, macroprudential tools, crisis management arrangements, and payment infrastructure. Trust in the banking system has contributed to the stability of the depositor base during the conflict.

Throughout periods of instability in West Bank and Gaza, the PMA successfully contributed to the financial stability of the banking system through the implementation of its regulatory and supervisory framework, which is strictly adhered to by banks under PMA oversight. The PMA accomplishes this through off-site supervision, on-site inspections of banks, licensing of banks, the approval of mergers and acquisitions, the issuance of laws and regulations, the maintenance of a credit registry, and

implementation and analysis of its macroprudential tools. Furthermore, the PMA has made substantial progress in its implementation of Basel III, IFRS9, and risk-based supervision.

**Tuvalu** does not have a central bank. Its two domestic banks operate without effective prudential regulation and oversight. There is, however, a positive development around financial integrity. Tuvalu is a member of the Asia/Pacific Group on Money Laundering, the FATF-style regional body. These institutional gaps undermine the country's ability to support and oversee the payment ecosystem.

**Adaptability of Regulatory and Institutional Responses**

In fragile and conflict-affected state settings, maintaining payment system functionality requires not only strong institutions but also the flexibility to adapt quickly. Agile regulatory responses and informal coordination mechanisms can be critical when formal processes are strained, or institutional capacity is limited.

**Ukraine** offers a clear example of adaptive crisis management. After the full-scale war, martial law enabled the NBU to swiftly implement and revise emergency regulations across relevant sectors of Ukrainian society. These included fixing the exchange rate, adjusting capital controls, and limiting cash withdrawals. Temporary measures also eased reporting burdens on banks, introduced new transaction data requirements for card networks, and allowed cloud-based data storage outside the country to address infrastructure vulnerabilities.

Additional government measures complemented these regulatory efforts, including relocation grants for businesses, low-interest rate loans under the "5-7-9" program,"[8] and state-backed financing for housing and infrastructure reconstruction. At the same time, institutional capacity challenges, especially in IT and cybersecurity, intensified because of conscription, displacement, and emigration.

To address operational constraints and broader challenges, the NBU launched weekly coordination calls with bank chief operating officers. This informal platform enabled real-time problem solving, peer exchange, and alignment across the sector, helping sustain trust and operational coherence within the intermediary layer of the payment ecosystem under rapidly evolving conditions. These meetings were crucial not only for strategic coordination but also for practical, day-to-day problem solving. Participants openly discussed even the smallest logistical details, such as using the scheduled routes of armored cash deliveries to transport meals to essential staff or selecting diesel over gasoline generators for greater safety.

**Licensing and Oversight Response**

Closely linked to regulatory functions, wartime and fragile contexts expose payment ecosystems to unique operational and security risks that may require exceptional oversight measures. In such environments, some types of market participants may pose elevated risks that cannot be adequately

[8] The "Affordable Loans 5-7-9%" program is a Ukrainian government initiative launched to provide subsidized loans to micro, small, and medium-sized enterprises.

addressed through standard oversight procedures and best practices, particularly when institutional capacity is strained, or real-time supervision is not feasible. In these cases, regulatory authorities may need to adopt temporary bans or impose exceptional restrictions to mitigate systemic vulnerabilities.

**Ukraine's** wartime experience illustrates this dynamic. For example, a temporary ban on e-money issuance was introduced in response to concerns about its potential misuse for terrorist financing. This measure, though extreme under normal conditions, was deemed necessary in the evolving security context. The episode highlights the importance of maintaining flexibility in supervisory frameworks and the ability to recalibrate oversight tools as risks evolve.

In parallel, the regulatory framework was revised to require that important payment infrastructures maintain at least two independent communication channels, with an added specification that these channels must follow geographically distinct routes. This case demonstrates the need for context-specific oversight measures that go beyond standard global practices when operating in fragile or high-risk environments.

**Foreign Currencies for Short-Term Support**

In the FCS context, foreign currencies can offer temporary relief for a domestic system that is in crisis by serving as a reliable store of value and medium of exchange when domestic currencies are volatile or inaccessible. However, although such arrangements may ease immediate pressures, they often carry long-term trade-offs such as diminished monetary sovereignty, limited policy space, and increased external dependency.

**West Bank and Gaza** is a dollarized economy with no domestic currency.[9] The Israeli shekel is the main currency for most transactions, including official transactions, retail payments, and foreign trade. Retail payments are mostly conducted in cash and by checks. The reliance on the shekel has introduced recurring challenges related to cash shortages and supply bottlenecks—particularly for small-denomination notes in Gaza—while buildups of New Israeli Shekel excess cash holdings in Palestinian Banks are difficult to repatriate (Coulibaly 2022, pp. 2–10). As a result, the currency arrangement, while offering some transactional stability, has limited monetary flexibility and introduced additional constraints to building long-term economic resilience.

**Yemen** presents a more complex case, marked by monetary fragmentation and dual currency regimes. The instability of the Yemeni rial, coupled with regional political divisions, has led to widespread use of the Jordanian dinar, Saudi riyal, and US dollar—particularly for savings and larger transactions. This informal substitution reflects a practical response to hyperinflation and currency depreciation but complicates monetary governance and financial sector cohesion.

[9] The Paris protocol, subscribed in September 1995, established the procedures and regulations governing economic relations between Palestine and Israel for the interim period. The currency arrangement (Article IV on Monetary and Financial Issues) allows the shekel to serve as means of payments alongside with other currencies. Payments are conducted also in Jordanian dinar, US dollar, and euro currencies. The protocol also provides the possibility of introducing a mutually agreed Palestinian currency or temporary alternative currency arrangements for the Palestinian Authority.

**Sudan** exhibits a high degree of de facto dollarization. Amid chronic economic instability, hyperinflation, and eroding trust in the Sudanese pound, foreign currencies—especially the US dollar—are widely used in trade, remittances, and informal savings. Although this allows limited continuity of commerce and value storage, it further undermines the role of the domestic currency and poses additional challenges for future monetary stabilization efforts.

**Tuvalu** is also characterized by the absence of a national currency and central bank, using the Australian dollar as its official currency. This arrangement provides monetary stability and facilitates transactions—especially for trade and aid—but limits policy autonomy and deepens reliance on external financial systems. Although the use of a stable foreign currency helps ensure basic financial continuity, it reinforces dependence on offshore infrastructure and leaves the payment system vulnerable to external shocks and liquidity constraints.

# III. Applying Resilience Lessons to CBDC: Opportunities and Design Considerations

Several central banks explore CBDCs as a potential tool to enhance payment system resilience as one policy goal, particularly in environments exposed to conflict, economic instability, or operational disruption. Although most CBDC initiatives with a few exceptions remain at the pilot or exploratory stage, the strategic interest in their role during crisis scenarios is growing. A number of FCS are considering CBDC options (see Annex 1 which presents available data and information on the status of CBDC initiatives in fragile states, including whether efforts are at the research, pilot, or implementation phase). This suggests that authorities view CBDCs as a possible path forward. The experience of Nigeria, one of the few states to launch a retail CBDC, demonstrates both the opportunity and the complexity involved. Although the e-Naira was introduced with the aim of promoting inclusion and supporting unbanked populations, adoption has been slow (Cornell SC Johnson College of Business 2023),[10] and pilot phases targeting conflict-affected areas were deferred to a later stage, which is currently on hold.

CBDC presents numerous opportunities for central banks to enhance the resilience of their payment ecosystems, particularly for FCS. By introducing a new layer to the payment ecosystem, CBDC could provide a redundant digital payment infrastructure with the flexibility to adapt to regulatory changes. Moreover, CBDC can offer robust and flexible offline functionality, as well as programmable disbursements during emergencies.

Building on the resilience strategies outlined in the previous section, this section explores how similar principles can inform the design and implementation of CBDCs. The insights gained from ensuring redundancy and scalability, and enabling user-centric access, operational continuity, and regulatory adaptability offer a valuable foundation for developing CBDCs that can contribute to payment resilience in FCS. Although CBDC remains nascent and largely experimental, with few solid and successful real-world deployments, it could still serve as an additional instrument to reinforce resilience if designed with resilience in mind. Therefore, building a safe and secure CBDC will require substantial planning, robust design, national and international collaboration, and specialized technical expertise.

CBDC is not a universal solution, and its potential to strengthen resilience must be weighed carefully against a range of challenges. Such key challenges include balancing decentralization and operational efficiency, ensuring cybersecurity, and mitigating operational risks and risks of illicit finance when enabling offline or anonymous functionality (Soderberg and others 2023; Tourpe, Lannquist, and Soderberg 2023; Bharath, Paduraru, and Gaidosch 2024). Many of the underlying technologies are still evolving and may introduce new vulnerabilities. Further, the specific challenges of FCS are themselves formidable obstacles for ensuring a successfully implemented a CBDC project. For instance, ensuring a

[10] Design and technical issues have been identified as key factors in the slow adoption of the eNaira. Challenges included privacy-related features such as anti–money laundering and KYC requirements, a difficult user experience, and infrastructure gaps, all of which contributed to slow adoption of the eNaira CBDC.

sound regulatory environment is particularly difficult in a situation in which there is low trust in governance or continual conflict regularly disrupts payments services.
Although these limitations are important to recognize, this section focuses specifically on how CBDC design and implementation strategies could draw from the payment resilience lessons observed in FCS.

**CBDC as a Tool for Building Trust**

As a direct liability of the central bank, CBDC can strengthen payment system resilience by offering a credible and secure alternative for transactions—particularly where confidence in the monetary authority remains intact. In such settings, it can help reinforce the state's presence, support financial continuity, and serve as a trusted anchor in times of disruption. However, in FCS, trust in domestic institutions, including central banks, can erode rapidly, posing a fundamental challenge to CBDC adoption. Since public confidence in the issuing authority is critical for uptake, it is essential to assess how trust in the central bank compares to that in private providers, foreign platforms, and informal channels. If designed and communicated effectively, CBDC may still enhance resilience by presenting a more reliable alternative. However, where institutional legitimacy is weak, complementary communication efforts and strategic partnerships may be necessary to build and sustain user trust.

**CBDC as a Complementary Form of Money**

As noted in previous sections, maintaining a balance between cash and digital payments has been a cornerstone of resilience in fragile contexts. Introducing retail CBDC as a third form of money—alongside cash and private digital money—can help strengthen that balance. In periods of conflict or instability, one form of money may become temporarily inaccessible because of supply chain disruptions, cash shortages, or digital outages. By diversifying the available means of payment, CBDC can help reduce dependence on any single instrument and offer fallback options during crises. Importantly, authorities must ensure that CBDC introduction does not displace cash or undermine trust in existing payment systems, but instead complements them in pursuit of greater overall system resilience.

**CBDC as a Redundancy Layer in Digital Payments**

In many developed economies, redundancy in digital payment systems is achieved through multiple layers of infrastructure—including financial market infrastructures, PSPs, and communication networks. In fragile settings, however, options are often limited, and failure at one layer can result in system-wide disruptions. CBDC can introduce a new digital rail with distinct operational and technical features, offering additional redundancy even where traditional digital services are underdeveloped or compromised. This is especially relevant in low-inclusion environments, where CBDC can provide new digital entry points for unbanked populations while improving societal stability for countries with partial or fragile payment infrastructure.

**CBDC as Infrastructure Where None Exists**

In extreme scenarios where private-sector payment infrastructure has collapsed or failed to develop—because of insecurity, market exit, or technical constraints—CBDC offers a unique opportunity to establish foundational infrastructure directly through the central bank. Retail CBDC could provide secure, basic payment functionality to end users, whereas wholesale CBDC could serve as a building block for

re-establishing core interbank settlement systems, including RTGS and automated clearinghouses functions. This option may be relevant in jurisdictions where e-money networks or fiat-backed stablecoins have become the de facto dominant payment instrument but without proper regulatory framework.

**CBDC as a Direct Public Access Channel**

In extreme FCS where PSPs are scarce and correspondent banking relationships are limited or non-existent, a direct CBDC model—where the central bank provides wallets or accounts directly to end users—can offer a practical, though exceptional, solution for maintaining payment continuity. This approach circumvents the need for intermediary institutions, which may be unavailable because of underdeveloped financial markets, insecurity, or institutional collapse. By enabling the central bank to deliver payment services directly, it helps preserve basic monetary functions and facilitate state transfers when no viable private infrastructure exists. However, this model is likely feasible only in extreme cases, as it places significant operational and technical demands on the central bank. Where possible, such arrangements should be considered a last-resort contingency, to be deployed when conventional distribution channels are entirely absent or nonfunctional.

**Secure Central Bank Digital Currency Design and National Incident Response**

The CBDC design should incorporate defense-in-depth and compartmentalization strategies to enhance resilience. These strategies include segmentation of system components, isolation of sensitive information and the enforcement of the need-to-know and least privilege principles. Furthermore, the CBDC should be regarded as a national critical infrastructure and should integrate with the national coordinated incident response network.

**Incentivizing Resilience by Bolstering Competition**

CBDC can also improve market dynamics in FCS by providing a level playing field for new PSPs. Offering CBDC as a platform for interoperability could lower barriers to entry, encouraging competition and improving the quality of services. This diversification not only expands access but also increases redundancy in payment channels. With more providers in the system, users have alternatives if one platform fails—improving both resilience and accountability.

**Designing for Connectivity and Power Constraints**

Connectivity and power disruptions are among the most pervasive challenges for digital payments in FCS. CBDC systems should be designed to function under low-connectivity conditions, including support for unstructured supplementary service data–based payments that operate on basic mobile networks without requiring internet access (Tourpe and others 2025). In areas with limited power, compatibility with battery-powered or solar-charged devices is essential. Designing CBDC systems that can operate with minimal technological dependencies is critical for ensuring reach and reliability under stress.

**Central Bank Digital Currency with Offline Capabilities**

Many of the ongoing CBDC research and developments are investigating the offline functionality for retail CBDC (Bank for International Settlement 2024). This stems from the desire to mimic cash and for

inclusiveness, especially with limited connectivity areas. Furthermore, offline functionality is particularly valuable in environments where electricity or internet access may be unavailable for prolonged periods. Although other digital solutions—such as offline-enabled cards or mobile wallets—already support resilience under such conditions, CBDCs can expand these capabilities by integrating offline use into a broader, centrally issued and managed platform. CBDC systems that allow users to transact securely offline—using preloaded hardware tokens, smart cards, or software-based wallets that synchronizes later—can provide a reliable fallback. Combined with programmability, identity integration, and broad central bank support, offline-enabled CBDC could offer a uniquely comprehensive solution for crisis scenarios, especially where existing tools are fragmented or not widely accessible.

CBDC offline functionality expands financial and security risks, especially with longer offline durations or consecutive offline transactions (International Monetary Fund 2025). Designing agility within the regulatory and legal frameworks can enhance payment system resilience while mitigating this risk. During normal periods, authorities should enforce low numbers of consecutive offline transactions with frequent reconciliations. In disaster periods or blackouts, authorities can temporarily relax restrictions to allow more offline transactions and extended reconciliation periods. This flexibility helps balance resilience and risk management at a national level for the payment's ecosystem.

**Flexible Front-End Solutions**

CBDCs should support a range of front-end interfaces to accommodate diverse user needs and contexts. Physical tokens, QR-code payment systems, and digital wallets can serve users with varying levels of digital literacy and connectivity. In crisis settings, such redundancy ensures that users can continue accessing their funds through at least one viable channel, even when others are compromised.

**Programmability for Crisis Response**

CBDCs with programmable features—such as smart contracts—can facilitate targeted payments during emergencies. For example, authorities could disburse emergency aid or subsidies directly to verified recipients with pre-defined conditions such as usage restrictions or expiration dates. These tools can enhance the transparency, speed, and control of financial relief mechanisms in fragile contexts. Programmability can also support remote identity verification or limit fraud in environments where physical documentation is unavailable or compromised.

**Regulatory Agility to Support CBDC Operations**

CBDC implementation in fragile settings requires legal frameworks that are both robust and adaptable. Conflicts and economic shocks often demand rapid changes to capital controls, anti–money laundering rules, financial sector governance, and financial sector supervision. Regulatory agility—supported by tools such as sandboxes, emergency protocols, and real-time monitoring—can help authorities adjust CBDC operations quickly while maintaining stability and compliance. Predefining such flexibility in the legal design of CBDC frameworks may reduce delays in crisis response.

**Cross-Border Functionality and Migration Support**

Fragile states often experience large-scale displacement and remittance dependency. CBDCs with cross-border functionality could support payment continuity for migrants and refugees, easing access to funds across jurisdictions. Collaboration between central banks on interoperability, particularly across major migration corridors, could enable secure, low-cost transfers while preserving regulatory safeguards. At the same time, coordination is needed to prevent financial instability or regulatory arbitrage.

**Role of Foreign CBDC Adoption**

In some FCS, public trust in foreign currencies may exceed that of the domestic currency. In such cases, foreign CBDCs could offer temporary stability, though potentially at the expense of monetary sovereignty. Overreliance on foreign digital currencies, especially in a crisis, may weaken local financial institutions and increase exposure to geopolitical risks. Central banks should monitor developments in foreign CBDCs and assess how they may affect domestic resilience and financial integrity. However, most central banks—including those exploring cross-border use cases—currently aim to limit or prevent CBDC circulation beyond their national jurisdictions.

## Box 2. CBDC Resilience through Enabling Technologies—Cloud and Distributed Ledger Technology

**Cloud Infrastructure for Resilience**

Cloud computing can offer key operational benefits for central bank digital currency (CBDC) systems, particularly in FCS. Multiregion or multizone deployment enables geographic redundancy and high availability, helping CBDC infrastructure remain functional during localized disruptions such as cyberattacks, power outages, or physical infrastructure damage. As with broader payment infrastructures, cloud adoption for CBDC must also address the human capital gap. Managing cloud-based CBDC platforms requires specialized technical skills as misconfigurations and insufficient security awareness could introduce legal and jurisdiction issues for sensitive data. Investment in cloud-specific training—tailored to central bank needs—is essential to mitigate these risks as well as flexibility of supervisors to relax cloud usage-related restrictions should it become necessary in times of conflict or natural disasters.

**Distributed Ledger Technology as a Resilience-Enabling Architecture**

If CBDC systems are designed using distributed ledger technology (DLT), certain resilience features may be built-in—such as eliminating single points of failure and enabling data replication across nodes. Depending on the governance and implementation model, DLT could support greater redundancy and fault tolerance, allowing the system to continue operating even when some nodes are offline. However, the resilience benefits of DLT are highly dependent on design. Network centralization, consensus mechanisms, and infrastructure hosting arrangements can all affect how well the system performs under stress. DLT may complement—but not replace—other resilience measures and should be evaluated in relation to broader operational and institutional factors.

# IV. Conclusion

This Note presents a structured overview of the payment ecosystem and its key functional layers, identifying the principal challenges faced in FCS and outlining practical strategies to strengthen resilience. The Note introduced a functional decomposition of the payment ecosystem into five layers—payment infrastructure, PSPs, payment solutions, users, and connectivity infrastructure—each of which must operate under significant constraints in FCS environments.

Furthermore, this Note represents an initial step toward a more systematic approach to strengthening payment resilience in FCS. However, FCS contexts are highly heterogeneous—differing in the level of disruption, institutional fragility, and the duration of crisis exposure. As a result, not all strategies presented here will be equally applicable or useful across all settings. Many of the strategies discussed in this Note can be expected to have a medium- or long-term effect. FCS jurisdictions, as well as supporting international organizations, will need to ensure that essential first steps are taken before embarking on more ambitious strategies, or ensure that they are carried out gradually alongside fundamental actions to address acute challenges. Several of these strategies are also costly to implement, so careful prioritization is warranted. Addressing payments resilience in FCS thus relies on tailored sequencing of reforms and strategies as well as prioritization of policy objectives. There is no universal formula to get this right. In this regard, capacity development is a critical tool for operationalizing resilience strategies in ways that reflect each country's unique context and constraints.

The IMF, consistent with its macrofinancial mandate, supports payment resilience through bilateral and multilateral capacity development and ongoing policy advice. IMF capacity development engagements can help advance the application of resilience strategies by building local capacity and strengthening the enabling environment for reform.

The IMF's work in this area complements that of other international institutions such as UN agencies including UNICEF, UNCDF, and UNDP, and the World Bank. Together, these efforts contribute to a more coordinated global response to strengthening payment systems in fragile environments.

Table 2 offers a summary of the strategies discussed in the "Strategies and Lessons for Strengthening Payment Resilience" section in the form of a matrix. The first dimension reflects the functional layers of the payment ecosystem, whereas the second captures five crosscutting resilience practices—redundancy and scalability, distributed infrastructure and decentralization, user-centric accessibility and awareness, operational and cyber resilience, and regulatory and legal Resilience. Each cell in the matrix represents a concrete point of action where resilience can be assessed, strengthened, or maintained by applying one or more strategies discussed in the Note. Notably, many strategies span over multiple cells, highlighting their relevance across different areas of the payment ecosystem.

**Table 2. Matrix of Payments Ecosystem Resilience Strategies[1]**

| | Users | Payment Solutions | Intermediaries | Payment Infrastructure | Connectivity Infrastructure |
|---|---|---|---|---|---|
| **Redundancy and scalability** | • Promotion of digital literacy | • Role of cash for continuity<br>• Digital money for resilience<br>• Foreign currency for (short-term) resilience | • Multisite operational architecture<br>• Managing connectivity dependency and single point of failure | • Multisite operational architecture<br>• Managing connectivity dependency and single point of failure<br>• Foreign infrastructure for redundancy | • Multisite operational architecture<br>• Managing connectivity dependency and single point of failure |
| **Distributed infrastructure and decentralization** | | | | • Distribution/scalability through cloud services<br>• Multisite operational architecture | • Distribution through satellite networks<br>• Decentralized connectivity<br>• Distribution/scalability through cloud computing |
| **User-centric accessibility and awareness** | • Digital ID for secure access<br>• Promotion of digital literacy | • Payment solution design for continuity | | | |
| **Operational and cybersecurity** | • Promotion of digital literacy | | • Contingency planning<br>• Coordinated incident response | • Contingency planning<br>• Coordinated incident response | • Contingency planning<br>• Coordinated incident response |
| **Regulatory and legal resilience** | • Pre-crises financial stability<br>• Regulatory adaptability | | • Pre-crises financial stability<br>• Regulatory adaptability | • Regulatory adaptability | • Regulatory adaptability |

Source: World Bank 2022.
[1] For details on the strategies, see the "Strategies and Lessons for Strengthening Payment Resilience" section.

Building on this foundation, the same matrix-based approach is applied to CBDCs as a potential resilience-enhancing instrument. CBDCs may serve multiple roles in the ecosystem—acting simultaneously as a form of sovereign money, payment infrastructure, and payment solution—while also introducing new design considerations for intermediaries and connectivity. As such, CBDCs inherently touches every layer of the payment ecosystem: payment infrastructure, intermediaries, payment solutions, users, and connectivity infrastructure. Table 3 presents this mapping, linking resilience practices to specific CBDC design features.

**Table 3. Overview of Resilience Lessons to CBDC**

| | CBDC Design |
|---|---|
| **Redundancy and scalability** | • Complementary form of money<br>• Redundant layer in digital payments |
| **Distributed infrastructure and decentralization** | • Resilience through enabling technologies—cloud and DLT<br>• Infrastructure where none exists |
| **User-centric accessibility and awareness** | • Incentivizing resilience by bolstering Competition<br>• Designing for connectivity and power constraints<br>• Offline capabilities<br>• Flexible front-end solutions<br>• Programmability for crisis response |
| **Operational and cybersecurity** | • Secure design with compartmentalization strategies<br>• Critical infrastructure consideration with national coordinated incident response |
| **Regulatory and legal resilience** | • Tool for building trust<br>• Regulatory agility to support CBDC operations<br>• Role of foreign CBDC adoption<br>• Cross-border functionality and migration support |

Note: CBDC = central bank digital currency; DLT = distributed ledger technology.

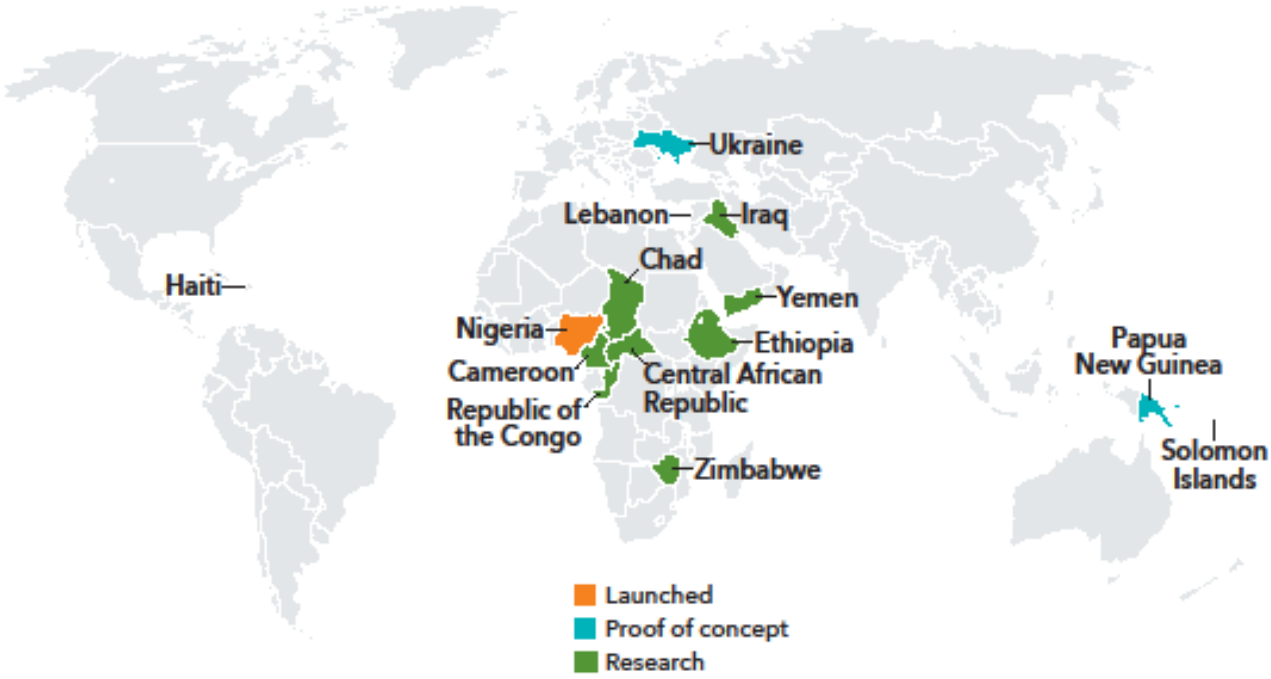
As illustrated, CBDCs offer considerable potential to enhance redundancy and scalability by serving as a complementary form of money and introducing an additional layer of digital payments infrastructure. CBDCs can also support decentralization through enabling technologies such as cloud computing or DLT, particularly in contexts where conventional infrastructure is weak or absent. However, their most significant resilience potential lies in user-centric design features, including offline functionality, flexible front-end solutions, and programmability for crisis response—which can expand access and ensure continuity in adverse conditions.

By contrast, the role of CBDCs in enhancing operational and cybersecurity resilience is less evident, and similar to other payment infrastructures. Similarly, although they can support regulatory agility and serve as a tool for building trust, careful legal and institutional design is needed to ensure they truly enhance resilience rather than introduce new risks.

Ultimately, enhancing payment resilience in FCS requires more than technical fixes—it demands a comprehensive and layered approach that reflects the realities on the ground, as well as a clear understanding of costs and associated risks. The strategies outlined in this Note demonstrate that even under extreme conditions, targeted interventions across ecosystem layers can sustain continuity, reinforce trust, and enable recovery. As countries explore new technologies such as CBDCs, these tools must be seen not as standalone innovations, but as integrated components of a broader payment resilience agenda.

With thoughtful design grounded in the resilience practices identified here, CBDCs can serve as a catalyst for more robust, inclusive, and adaptive payment systems capable of withstanding shocks and supporting essential economic functions when they are needed most. Their success, however, will rely not only on the technological leapfrogging but also on the ability of the central bank and all CBDC stakeholders to invest in specialized resources, infrastructure, and sustained national and international collaboration. Moreover, the costs and risks of implementing CBDCs must be considered (see detailed discussions at https://www.imf.org/en/Topics/digital-payments-and-finance/central-bank-digital-currency/virtual-handbook). In environments of pervasive corruption and weak rule of law, common across many FCS, CBDCs face considerable hurdles to become a trusted means of payment. Mitigating these challenges requires reforms to address corruption and strengthen judicial and regulatory independence and capacity, and where such reforms are unlikely, CBDC adoption should be approached with careful consideration.

# Annex: CBDC Status in Fragile and Conflict-Affected States




Source: Developed by authors, based on CBDC Tracker and World Bank Group 2024.

Note: The boundaries, colors, denominations, and any other information shown on the maps do not imply, on the part of the International Monetary Fund, any judgment on the legal status of any territory or any endorsement or acceptance of such boundaries.

# References


Bharath, Arvinder, Anca Paduraru, and Tamas Gaidosch. 2025. “Cyber Resilience of the Central Bank Digital Currency Ecosystem. In Central Bank Digital Currency (CBDC)—Virtual Handbook.” International Monetary Fund.

Board of Governors of the Federal Reserve System. 2024. “Cybersecurity: A Growing Threat to Financial Stability.” July. https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf

Carnegie Mellon University. n.d. “A Targeted Improvement Plan for Service Continuity.” Software Engineering Institute. https://insights.sei.cmu.edu/documents/2311/2019_004_001_543741.pdf

Central Bank Digital Currency (CBDC) Tracker and World Bank Group. 2024. “FY25 List of Fragile and Conflict-Affected Situations.” June 28. https://cbdctracker.org/ and https://thedocs.worldbank.org/en/doc/b3c737c4687db176ec98f5c434d0de91-0090082024/original/FCSListFY25.pdf

Circle Internet Financial. 2024. “Enhancing Global Impact with Digital Dollars.” Circle Impact Report. https://www.circle.com/circle-impact-report

Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions. 2016a. “Implementation Monitoring of PFMI: Third Update to Level 1 Assessment Report.” Bank for International Settlements. https://www.bis.org/cpmi/publ/d145.pdf

Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions. 2012. “Principles for Financial Market Infrastructures.” Bank for International Settlements. https://www.bis.org/cpmi/publ/d101a.pdf

Committee on Payments and Market Infrastructures & International Organization of Securities Commissions. 2016. “Guidance on Cyber Resilience for Financial Market Infrastructures.” Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

Cook, William, Dylan Lennox, Sara Murray, and Souraya Sbeih. 2024. “From Crisis to Resilience: The Role of Inclusive Finance in Fragile Countries.” Working Paper. Washington, DC: Consultative Group to Assist the Poor (CGAP). https://www.cgap.org/research/crisis-to-resilience-role-of-inclusive-finance-in-fragile-countries

Cornell SC Johnson College of Business. 2023. “Nigeria’s eNaira CBDC: What Went Wrong?” Cornell Business Hub. April 28. https://business.cornell.edu/hub/2023/04/28/nigerias-enaira-cbdc-what-went-wrong/

European Payments Council. 2023. “Payments in Wartime: The Story of the National Bank of Ukraine.” July 28. https://www.europeanpaymentscouncil.eu/news-insights/insight/payments-wartime-story-national-bank-ukraine

Financial Inclusion Data and Indicators. n.d. https://www.pma.ps/en/Financial-Inclusion/Financial-Inclusion-Data-and-Indicators and

https://www.pma.ps/Portals/0/Users/002/02/2/Publications/Financial%20Inclusion%20publication/Summary%20of%20FI%20Study.pdf

Khiaonarong, Tanai, Harry Leinonen, and Ryan Rizaldy. 2021. “Operational Resilience in Digital Payments: Experiences and Issues.” IMF Working Paper 2021/288, International Monetary Fund.

Lumbreras, Sara, Luis Olmos, Andrés Ramos, Quentin Ploussard, Frank Sensfuss, Gerda Deac, and Christiane Bernath. 2017. “Issue Paper on Case study 6.2: Centralized vs. Decentralized Development of the Electricity Sector. Impact on infrastructure.” https://publica-rest.fraunhofer.de/server/api/core/bitstreams/907963b1-e2a1-4082-930d-eb92028a5736/content.

Morris, Julian. 2024. “Digital Payments and Financial Inclusion.” International Center for Law & Economics. https://laweconcenter.org/resources/digital-payments-and-financial-inclusion/?utm_source=chatgpt.com

Natalucci, Fabio, Mahvash S. Qureshi, and Felix Suntheim. 2024. “Rising Cyber Threats Pose Serious Concerns for Financial Stability.” International Monetary Fund, April 9. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

OECD. 2025a. “Lack of Trust in Institutions and Political Engagement.” OECD. https://www.oecd.org/en/publications/lack-of-trust-in-institutions-and-political-engagement_83351a47-en.html#:~:text=This%20paper%20provides%20an%20analysis%20on%20the%20socioeconomic,identifying%20governments%E2%80%99%20actions%20to%20engage%20citizens%20in%20policymaking.

OECD. 2025b. “States of Fragility 2025.” OECD Publishing. https://doi.org/10.1787/81982370-en

PCBS. 2023. “PCBS & The Ministry of Communications and Information Technology: The World Telecommunication and Information Society Day.” https://www.pcbs.gov.ps/post.aspx?lang=en&ItemID=4510#:~:text=The%20majority%20of%20Palestinian%20households,Million%20active%20cellular%20phone%20subscriptions

Reuters. 2024. “Sudanese Seek Connections through Starlink after Weeks of Blackouts.” March 13. https://www.reuters.com/world/africa/sudanese-seek-connections-through-starlink-after-weeks-blackouts-2024-03-13/#:~:text=OMDURMAN%2C%20Sudan%2C%20March%2013%20(,other%20parts%20of%20the%20country

Sana’a Center for Strategic Studies. n.d. “Rethinking Yemen’s Economy: No. 10.” https://sanaacenter.org/files/Rethinking_Yemens_Economy_No10_En.pdf

Soderberg, Gabriel, John Kiff, Hervé Tourpe, Marianne Bechara, Stephanie Forte, Kathleen Kao, Ashley Lannquist, Tao Sun, and Akihiro Yoshinaga. 2023. “How Should Central Banks Explore Central Bank Digital Currency?” Fintech Notes No. 2023/004, International Monetary Fund, September 8. https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504

The New Humanitarian. 2024. “Digital Money Apps Become a Lifeline for War-Affected Sudanese.” February 7. https://www.thenewhumanitarian.org/news-feature/2024/02/07/sudan-war-digital-money-online-banking-apps

Tourpe, Hervé, Ashley Lannquist, and Gabriel Soderberg. 2023. “A Guide to Central Bank Digital Currency Product Development.” Fintech Notes No. 2023/003, International Monetary Fund, September 8. https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/A-Guide-to-Central-Bank-Digital-Currency-Product-Development-538496

Tourpe, Hervé, John Kiff, Majid Malaika, and Chris Ostrowski. 2025. “CBDC Solutions in Connectivity-Challenged Environments.” Fintech Notes No. 2025/005, International Monetary Fund, August 7. https://www.imf.org/en/Publications/fintech-notes/Issues/2025/08/07/Technology-Solutions-to-Support-Central-Bank-Digital-Currency-with-Limited-Connectivity-A-569259

United Nations. 2024. “UN E-Government Survey 2024.” United Nations Department of Economic and Social Affairs. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

World Bank. 2022. “The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19.” World Bank https://www.worldbank.org/en/publication/globalfindex/Data

World Bank Group. 2020. “World Bank Group Strategy for Fragility, Conflict, and Violence 2020–2025.” World Bank. https://documents1.worldbank.org/curated/en/844591582815510521/pdf/World-Bank-Group-Strategy-for-Fragility-Conflict-and-Violence-2020-2025.pdf

World Bank Group. 2024. “FY25 List of Fragile and Conflict-Affected Situations.” June 28. https://thedocs.worldbank.org/en/doc/b3c737c4687db176ec98f5c434d0de91-0090082024/original/FCSListFY25.pdf

PUBLICATIONS

**Payment Resilience in Fragile and Conflict-Affected States: Lessons for Central Bank Digital Currency (CBDC)**

NOTE/2025/009