NRC NORWEGIAN REFUGEE COUNCIL

REPORT

EXPLORING BLOCKCHAIN OPTIONS FOR HUMANITARIAN TRANSACTIONS INTO SYRIA

January 2026

Funded by
the European Union

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

NRC NORWEGIAN REFUGEE COUNCIL

ACKNOWLEDGEMENTS

The Norwegian Refugee Council (NRC) is an independent, international, humanitarian non-governmental organisation (NGO) that provides assistance and protection and contributes to durable solutions for refugees and internally displaced people worldwide.

NRC produced this report with financial assistance from the EU's Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) and the Swiss Federal Department of Foreign Affairs (FDFA).

The report was researched and written by Cherise Chadwick and Sandra Uwantege Hart, Technology Strategist at the PoliSync Centre for International Policy Engagement, with additional contributions from Beatriz Ferreira de Carvalho. It benefits from the contributions of key informant interviewees from various NGOs, FinTech providers, international organisations, banks, money service providers and donor governments. NRC would like to thank those who contributed their time and expertise to this work.

For further information, please contact nrcgeneva.policy@nrc.no.

Layout & Design: BakOS DESIGN

TABLE OF CONTENTS

ACRONYMS

AML Anti-money laundering

BIS Bank for International Settlements

CASP Crypto-asset service provider

CBDC Central bank digital currency

CBT Cash-based transfer

CFT Countering the financing of terrorism

CT Counterterrorism

CVA Cash and voucher assistance

CWG Cash working group

DeFi Decentralised finance

DLT Distributed ledger technology

ECHO Directorate-General for European Civil Protection and Humanitarian Aid Operations

FATF Financial Action Task Force

FCDO Foreign, Commonwealth and Development Office

HMRC His Majesty's Revenue & Customs

IDP Internally displaced person

IHL International humanitarian law

KYB Know your business

KYC Know your customer

KYS Know your supplier

MiCA Markets in crypto-assets

ML Money laundering

MPCA Multi-purpose cash approach

MSB Money service business

MSP Money service provider

MVTS Money or value transfer service

NFT Non-fungible token

NGO Non-governmental organisation

OCHA UN Office for the Coordination of Humanitarian Affairs

OFAC US Office of Foreign Assets Control

OFSI Office of Financial Sanctions Implementation

SOP Standard operating procedure

SWIFT Society for Worldwide Interbank Financial Telecommunication

TradFi Traditional Finance

TF Terrorist financing

UNSC United Nations Security Council

US United States of America

USAID United States Agency for International Development

USDC US dollar coin

USDT Tether

USSD Unstructured Supplementary Service Data

VASP Virtual asset service provider

WFP World Food Programme

TERMS AND DEFINITIONS

Aid diversion

Any event, including fraud, corruption, bribery, theft, money laundering and other misuse of funds that prevents them being directed to their intended recipients.[1]

Bitcoin

The first and most well-known cryptocurrency, designed as a decentralised digital currency without a central authority.

Blockchain

A type of digital ledger that records transactions in a secure and transparent way that is distributed across a network of participants who maintain, update and validate it together.

Counterterrorism (CT) measures

International, regional and national laws and policies or donor provisions, including sanctions adopted for CT purposes and criminal laws.

Crypto-asset service provider (CASP)

A specialised and licensed financial service provider that helps clients to buy, hold, exchange and send crypto assets such as stablecoins.

Cryptocurrency

A digital or virtual currency secured by cryptography and typically operating on decentralised networks such as blockchains.

Decentralised finance (DeFi)

A financial ecosystem built on blockchain technology that offers services such as lending, borrowing and trading without recourse to traditional banks.

Derisking

When the private sector or financial institutions terminate or restrict financial services to avoid rather than manage risk. Bank derisking is driven by risk aversion, concerns about reputation and profitability, and requirements to comply with sanctions and anti-money laundering (AML) and countering the financing of terrorism (CFT) obligations.

Digital asset

a digital representation of value, such as a cryptocurrency or non-fungible token (NFT), that is recorded on a distributed ledger or blockchain, and which can be used for payment or investment purposes, or to access a good or service. This definition includes various forms, including those backed by central bank money, commercial bank money or other safe assets. Regulatory and supervisory bodies, such as the Bank for International Settlements (BIS), also differentiate between tokenised traditional assets and other crypto-assets.

Digital wallet/crypto-wallet

A software application or a hardware device that allows individuals to send, store and receive cryptocurrencies, including stablecoins. Rather than directly storing digital assets, the wallet securely retains the private keys necessary to authorise transactions on the respective blockchain network. It functions as a digital repository for the credentials required to access and transact with one's cryptocurrency. Many crypto-wallets, such as Metamask and Trust Wallet, are available for free download.

[1] This is NRC's internal definition of aid diversion. Other definitions exist in the humanitarian sector, including those that distinguish between fraud and diversion. ECHO, for instance, defines aid diversion as an event that *"occurs when, due to the action or inaction of actor/s external to DG ECHO's partner, its staff or its implementing partner(s), aid is prevented from reaching the action's intended beneficiaries or activities"*.

Due diligence

The application of organisational policies, controls and processes designed to identify and assess the impact of activities and relationships on humanitarian work throughout the project cycle.

Fiat currency

Government-issued money, such as the US dollars or euro, that is not backed by a physical commodity but by trust in the issuing authority.

Hawala

A non-bank financial service characterised by the settlement of imbalances through trade, cash and/or long-term net settlement rather than a simultaneous wire transfer.

Humanitarian safeguard or carve-out

Non-legal terms that refer to approaches taken to exempt organisations or activities from restrictions that legal provisions impose to protect principled humanitarian action. As far as sanctions are concerned, there are two main approaches: safeguards that apply automatically, referred to as exemptions or general licenses; and safeguards for which organisations have to apply for on a one-off basis, referred to as derogations or specific licenses.

Know your customer/supplier

A due diligence measure to verify the identity of a customer/supplier that involves the collection of information, including name, address and copy of government-issued ID.

Money laundering

The process of concealing the origins of money obtained from illicit activities and making it appear to have come from a legitimate source.

Money Service Provider (MSP)

A non-bank financial service provider that makes money available to third parties in other geographical locations. They can be formal or informal entities.

North-east Syria

Area under the de facto governance of the Democratic Autonomous Administration of North-East Syria that until 8 December 2024 fell outside the control of the former national government.

North-west Syria

Opposition-held area that until 8 December 2024 fell outside the control of the former national government.

Pain point

Commonly used in business, technology and user-centred design. Gartner's Sales Glossary defines pain points as "specific problems faced by current or prospective customers in the marketplace" In user-centric technology design, identifying pain points and validating how a product or tool can address them effectively is a critical step.

Sanctions

Foreign policy measures that may be adopted internationally or by regional organisations and/or individual countries. They are intended to influence the behaviour of other countries, groups or individuals without recourse to armed force. They may include financial sanctions, prohibitions on the purchase of commodities or the import of certain goods, and travel restrictions for designated individuals.

Stablecoin

Defined as a cryptocurrency intended to maintain a stable value relative to a specified asset, or a pool or basket of assets. Most stablecoins in use in 2025 are pegged to the value of a currency such as the US dollar or the euro. Widely used, currency-backed stablecoins include the US dollar coin (USDC) and tether (USDT).

EXECUTIVE SUMMARY

Humanitarian operations in north-west (NW) and north-east (NE) Syria have long relied on money service providers (MSPs) and cash-carrying practices.[2] MSPs are non-bank providers that make money available in different geographic locations. The banking sector in NW and NE Syria is volatile and the security situation unstable. Banks are largely absent and MSPs are often the only option for humanitarian operators to receive and exchange funds.

The combined impacts of international sanctions and other restrictive measures, fragmented control and systemic derisking by global financial institutions have significantly impeded humanitarians' ability to move funds into Syria reliably and transparently. This report by the Norwegian Refugee Council (NRC), with contributions from FinTech experts and other key informants, explores the potential for integrating blockchain-based crypto assets and stablecoins into humanitarian payments to improve delivery.

Financial operations in Syria currently rely primarily on:

- **Bank transfers to Damascus**, which are frequently delayed or blocked as a result of overcompliance with sanctions.
- **Cash payments via MSPs** in NW and NE Syria, which are essential but can come with high transaction fees, security risks and regulatory ambiguity. They can also be highly resource-intensive to set up and coordinate.

Organisations interviewed for this research reported that they frequently faced:

- Blocked or delayed transfers as a result of financial institutions' risk aversion
- High MSP commission fees, ranging from 1.5 per cent to 30 per cent
- Legal complexities and compliance challenges across jurisdictions related to the domestic regulatory environment and donor policies on the use of MSPs
- Excessive operational burdens for due diligence, know-your-customer/know-your-supplier (KYC/KYS) procedures and payment tracking

Blockchain and crypto assets offer a potential solution. Blockchain technology and digital assets, particularly stablecoins such as the digital US dollar, also known as the US dollar coin (USDC), that comply with the EU's markets in crypto-assets (MiCA) regulation, offer significant advantages for humanitarian transfers:

- **Transparency and traceability:** Immutable records and increase donor confidence.
- **Cost-effectiveness:** Lower transaction fees and administrative overheads compared with traditional systems.
- **Speed and agility:** Near-instantaneous transfers that bypass bureaucratic traditional banking channels.
- **Increased access:** Populations excluded from traditional financial systems, especially in conflict zones, can be reached.

Documented pilots in Afghanistan, Myanmar and Venezuela have demonstrated the feasibility of using blockchain-based systems for delivering aid, improving efficiency and reach. Blockchain offers a workaround, but it is not a substitute for traditional banking where it works well.

The regulatory landscape for blockchain-based financial tools and crypto assets is evolving rapidly, recognising their potential to increase financial inclusion globally.[3] The EU's MiCA

---

[2] NRC hosted an expert dialogue and produced a report on the *Use of Money or Value Transfer Services by NGOs* in 2022. Recommendations included improving guidance on the use of MSPs, recognising them as an essential fund transfer mechanism, providing support in settings where MSPs are widely used and undertaking mapping exercises to provide accurate data on MSP regulations and guidance to help banks and NGOs better understand them across states and jurisdictions.

[3] The UK's Financial Conduct Authority underscored the reasons for these changes in 2025, stating : *"Crypto assets offer innovations in markets, Open Banking and Open Finance offer opportunities for consumer choice, better competition, and growth"*.

regulation establishes a harmonised framework that legitimises the use of stablecoins, mandates the licensing of virtual asset service providers (VASPs) and ensures consumer protections. To remain compliant with the current regulations and strive for the lowest levels of risk, humanitarian organisations should:

- Only work with licensed crypto-asset service providers (CASPs)
- Only use regulated stablecoins, excluding algorithmic variants such as tether (USDT)
- Align operations with internal compliance and donor expectations

This report identifies **implementation pathways** across operational levels to help organisations understand practical steps that could be taken:

1. **Headquarters:** Use of CASPs to acquire, store and manage stablecoins securely, ensuring traceable and compliant fund disbursement.

2. **Country teams:** Deployment of custodial or decentralised digital wallets to manage in-country transactions, including payments to suppliers and staff salaries, reducing reliance on MSPs and enhancing flexibility.

3. **Field level:** Use of local digital wallets for disbursements to beneficiaries, enabling secure, efficient and monitored aid distribution with reduced cash-handling risks.

Risks and mitigation components were identified. While promising, the use of crypto assets in Syria must address:

- **Regulatory uncertainty in the country**, though reforms are emerging with the new authorities.

- **Organisational resistance to innovation**, which can be mitigated through collective education in the sector, leadership endorsement, staff training and inclusion in procurement policies.

- **Technological limitations**, such as connectivity and device access, which can be offset through localised wallet solutions with offline and unstructured supplementary service data (USSD) functions.

All things considered, crypto assets offer a timely and practical solution to longstanding challenges in delivering humanitarian assistance in Syria, including limited banking access, inflation and financial exclusion. Despite the first wave of sanctions relief, humanitarian organisations are likely to continue to face significant challenges in transferring funds into the country in the short to medium term, because of the chilling effect of more than a decade of complex sanctions and restrictive measures.

That said, growing international commitments to Syria's recovery create space for financial sector re-engagement and infrastructure investment. With growing technological maturity, emerging regulatory frameworks and the easing of some restrictive measures, there is a clear opportunity to responsibly scale up the use of digital assets.

This paper provides humanitarian organisations and donors with an introduction to these technologies, documented use cases and guidance on selecting appropriate tools while ensuring compliance with legal and regulatory frameworks and the humanitarian principles. It concludes with specific recommendations for different stakeholders and three general recommendations for the sector as a whole:

- **Develop collective guidance:** Invest in shared, neutral guidance on crypto assets to ensure informed, compliant implementation and reduce reliance on profit-driven service providers. Poorly executed pilots risk damaging credibility.

- **Engage donors and regulators:** Humanitarian organisations, donors and governments should align on regulatory frameworks to ensure crypto assets are permitted when traditional financial channels are constrained by derisking or liquidity challenges.

- **Continue to invest in solutions to derisking:** Blockchain offers a workaround, but it is not a substitute for traditional banking. Efforts should continue to improve access through banks, which remain the most cost-effective and scalable channel for humanitarian fund transfers. In the US, EU, the United Arab Emirates (UAE) and other major jurisdictions, banks are increasingly integrating interoperability with crypto assets such as stablecoins, which shows that the use of blockchain and banking infrastructure need not be mutually exclusive.

1 INTRODUCTION

Humanitarian operations supported by international NGOs and international organisations such as the UN and the Red Cross Red Crescent Movement in north-west (NW) and north-east (NE) Syria rely predominantly on money service providers (MSPs) and cash-carrying practices.[4] MSPs are non-bank financial service providers that make money available in different geographic locations. The banking sector in both areas is volatile and the security situation unstable. Banks are largely absent and MSPs are often the only option for receiving and exchanging funds.

Prior to the December 2024 shift in context, there were no operational banks in the areas of NW Syria controlled by the former-Syrian Salvation Government (SSG), while the Turkish Postal and Shipping Corporation (PTT) operated branches in the areas controlled by the country's interim national government. The autonomous administration in NE Syria has taken steps towards better and more centralised economic regulation, including through a decision to license local and foreign banks to operate in areas under its control.[5] However, progress since the transition has been slow, risking delays and limitations for humanitarian and aid actors who rely on functioning financial systems highlighting the continued importance of MSPs to humanitarian operations.

MSPs currently provide cash deposits for several essential transactions including:

- Liquidity for international NGO offices and local partner organisations
- Payments to NGO suppliers
- Payment of staff salaries
- Provision of direct cash assistance to programme beneficiaries

MSPs have been an integral part of the response to the humanitarian crisis in the above areas for more than a decade, but their commission rates can be high. NGOs operating in Syria were paying rates of up to seven per cent as of 2015 and in besieged areas as high as 20 to 30 per cent.[6]

The international banking sector also often blocks transfers to MSPs' accounts for the payment of services over concerns about money laundering and financing of terrorism risks, more information on this discussion can be found in NRC's paper Humanitarian Organisations' Use of Money Service Providers which explains that many MSPs used by humanitarian organisations are licensed and regulated by national authorities and subject to AML/CFT requirements, and that misconceptions about their informal nature often drive undue risk aversion.

Given the protracted nature of the crisis, humanitarian organisations recognise the need to strive for more traceable, secure and cost-efficient ways of working. This may include innovative FinTech solutions, as identified previously by NRC.[7] NRC's report on this issue shows that with context-specific design and safeguards in place, financial technologies including blockchain platforms and digital currencies have the potential to streamline and facilitate humanitarian fund transfers in poorly banked jurisdictions. Benefits include reduced costs; increased accessibility, transparency, accountability and security; and the mitigation of risks associated with fraud, money laundering and financing of terrorism.

The report found that initiatives to date had mostly focussed on last-mile domestic transfers rather than cross-border transactions. A main recommendation was to prioritise pilot initiatives in problematic banking routes for cross-border

---

4 NRC hosted an expert dialogue and produced a report on the *Use of Money or Value Transfer Services by NGOs* in 2022. Recommendations included improving guidance on the use of MSPs, recognising them as an essential fund transfer mechanism, providing support in settings where MSPs are widely used and undertaking mapping exercises to provide accurate data on MSP regulations and guidance to help banks and NGOs better understand them across states and jurisdictions.

5 Enab Baladi, *AANES issues decision allowing bank licensing in northeast Syria,* 25 January 2024.

6 Beechwood International, *Technical assessment: humanitarian use of hawala in Syria,* July 2015.

7 NRC, *Mitigating Financial Sector Derisking through Innovation: The Role of Digital Technologies in Humanitarian Fund Transfers,* 2023.

transfers. There is also growing evidence from similarly complex jurisdictions that humanitarian organisations are exploring and successfully using these technologies to solve issues related to access and the delivery of last-mile payments in locations where banking channels are limited or inaccessible, albeit in a piecemeal way.

This paper explores the potential use of FinTech solutions in the transfer of humanitarian payments into Syria with a view to adopting more sustainable and cost-efficient ways or working. The approaches proposed in the last two sections are designed to be instructional for humanitarian organisations already implementing programmes in Syria.

The paper serves as a resource for the humanitarian and donor community by providing a basic introduction to digital asset technologies, presenting a clear use case, and offering an overview of tools and solutions. It identifies the most appropriate technologies for the setting, outlines key risk factors and highlights compliance considerations in terms of applicable laws, regulations and the humanitarian principles.

The research began before the change of authorities in Syria at the end of 2024, but its recommendations were developed with a view to implementation across the country as a whole. They take into account the initial wave of sanctions relief and the anticipated and welcome shift towards recovery and reconstruction. Despite these positive developments, however, rebuilding Syria's financial institutions, re-establishing connections with the international financial system and reversing the chilling effect of more than a decade of sanctions other restrictive measures will take time.

Humanitarian and development stakeholders are expected to continue to face significant bank derisking when transferring funds into the country as a result. Reliable financial transfer channels remain essential to meeting ongoing humanitarian needs and supporting early recovery efforts. More than one year after the change in government, and despite efforts to ease and lift sanctions, organisations are still heavily dependent on MSPs to move funds into and around the country, with inherent challenges including liquidity constraints, volatile exchange and commission rates and frequent blockages of payments to MSPs for their services.

KEY TAKEAWAYS

- **Financial access constraints have led to a dependence on MSPs:** Humanitarian operations in NW and NE Syria rely heavily on MSPs because of the near-absence of functioning banks, especially in areas such as former-SSG-controlled NW Syria, where traditional banking is inaccessible.
- **MSPs play a vital role, but costs are high:** MSPs are essential for liquidity, paying suppliers and staff and distributing cash assistance, but their services often come with high commission rates that strain humanitarian budgets.
- **FinTech offers a promising alternative:** There is increasing interest in using digital financial technologies such as blockchains and stablecoins to enhance transparency, reduce costs and improve the security of humanitarian fund transfers, particularly cross-border when banking routes are problematic.

1.1 SANCTIONS, COUNTERTERRORISM MEASURES AND THEIR IMPACT ON HUMANITARIAN ACTION IN SYRIA

Humanitarian organisations are not usually the target of sanctions and CT measures per se, but such regimes still pose risks for humanitarian action. They create challenges at all stages of the project cycle and may impede access, operational efficiency and the safety and security of staff and beneficiaries. These issues have been well documented.[8]

Private entities that provide services necessary for humanitarian action, such as financial institutions, commodity providers and tech, insurance and freight companies, must also comply with sanctions and CT measures. To minimise concerns about liability, many have significantly restricted the services they are willing to offer, particularly for humanitarian operations in countries they perceive as high risk. This practice, also known as derisking, often has a significant impact on humanitarian organisations' capacity to operate.

Until recently, Syria had long been one of the world's most comprehensively sanctioned jurisdictions, subject to a range of complex and overlapping sanctions, exports restrictions, CT regulations and other restrictive policies, making it one of the most complex legal environments for humanitarians, their donors, banks and suppliers to navigate.

Sanctions and CT measures have challenged, delayed and at times even obstructed the humanitarian response. NRC and the wider humanitarian community have reported the following challenges over the past 10 years:

- Major overcompliance and derisking policies from private sector companies blocking or delaying the transfer of funds to Syria
- Inability to obtain authorisation from sanctioning authorities, or excessive delays in doing so, to use services necessary for humanitarian activity provided by private companies owned by designated individuals
- Challenges and delays in obtaining authorisations to import items needed for the response, such as water pumps and mechanical or electrical parts for medical equipment
- Donor requirements that contradict the humanitarian principles

Sanctioning bodies and states have increasingly included safeguards in their sanctions and CT measures to protect and facilitate humanitarian action, including in Syria. The UN Security Council (UNSC) adopted the landmark resolution 2664 in December 2022, creating a humanitarian exemption across all UN sanctions regimes.[9] It underscores member states' intention to safeguard principled action, which turn provides more comfort for private sector stakeholders, including banks, to engage with humanitarian organisations.

States have since increasingly included humanitarian exemptions in their own sanctions regimes, but many have used their own language and definitions of humanitarian activities or introduced new constraints on their exemption's application. A variety of humanitarian safeguard models now coexist within and across jurisdictions as a result, complicating the legal environment for humanitarian organisations and others, including the private sector.[10] Simultaneously and more impactfully, few domestic criminal laws have similar exemptions, which may expose humanitarian teams to liability if they engage in transactions with groups designated or proscribed as terrorist.

---

8 For more information on the impact of sanctions and CT measures, see: NRC, *Toolkit for principled humanitarian action: managing counterterrorism and sanctions risks*, December 2024; NRC, *Principles under Pressure: the impact of counterterrorism measures and preventing/countering violent extremism on principled humanitarian action*, June 2018.

9 For more information on UNSC resolution 2664, see: International Peace Institute, *Safeguarding Humanitarian Action in UN Sanctions and Counterterrorism Regimes: The Impact and Implementation of Resolution 2664*, December 2023.

10 IPI Global Observatory, *One Year On: Where Do We Stand on the Milestone Humanitarian "Carve-out" in UN Sanctions Regimes?* December 2023.

The box at the side provides an overview of the sanctions and CT measures in place during the conflict in Syria. Since the recent change of government, there has been an initial easing of sanctions alongside international commitments to the country's recovery. Given the complexity of the existing measures, however, sanctions relief will be gradual, and further easing is likely to depend on political agreements with the new authorities. At the time of writing, the impact of the initial easing on humanitarian operations, including banking channels, is unclear. The private sector's risk appetite may take time to change after decades of comprehensive restrictive measures.

KEY TAKEAWAYS

- **Sanctions and other restrictive measures impede principled humanitarian action in Syria:** Sanctions frameworks do not prohibit humanitarian action outright, but overlapping restrictions and CT measures lead to severe disruption and delays as a result of private companies' and financial institutions' overcompliance.
- **States increasingly apply humanitarian exemptions, but they are inconsistent:** Recent developments such as UNSC resolution 2664 and national humanitarian exemptions are a sign of progress, but varying definitions and conditions, and the absence of parallel exemptions in domestic criminal laws continue to create legal uncertainty and risk for humanitarians.
- **The first steps toward sanctions easing in Syria have taken place:** The fall of the former government and the establishment of new transitional authorities have prompted some initial sanctions relief, but implementation will be slow and contingent on political developments. The impact on humanitarian operations remains to be seen.

SANCTIONS AND CT FRAMEWORKS APPLICABLE TO SYRIA

Until 2025, Syria was one of the world's most heavily sanctioned countries for decades. Before the recent easing of sanctions prompted by the change of government, the multilateral and autonomous/unilateral sanctions and CT frameworks applicable in relation to Syria included:

- **Measures applicable to the country as a whole:** These included investment and export restrictions, and "sectoral sanctions" prohibiting engagement with, for example, the energy sector – as implemented by the US, EU, UK and others.
- **Measures against the Syrian government and/or related entities:** These included asset freeze measures that prohibited making resources available, directly or indirectly, to designated entities; a US-designation as a state sponsor of terrorism - Syria was and still is banned from receiving US foreign assistance, and third-party states face commercial and diplomatic consequences if they provide assistance, along with a chilling effect on commercial and other entities; under the Caesar Act, the US can also list non-US individuals and entities providing significant support to the Syrian government's reconstruction efforts.
- **Measures against armed groups, including HTS, and related individuals/entities:** HTS is on the UN's al-Qaeda/Islamic State group sanctions list under its former name of Jabhat al-Nusra. It is also on several western countries' terrorist lists. This triggers asset freeze measures from the UN, US, EU and UK, and criminal laws on supporting terrorism in countries including the US, UK, Canada and Australia, designed to prevent and punish transfers of resources to designated groups.

1.2 MONEY SERVICE PROVIDERS AND THEIR REGULATORY FRAMEWORKS

There is a common misconception that the MSPs humanitarian organisations use operate informally, when in fact many are formally registered as financial service providers with competent national authorities.[11] This misconception is aggravated by the use of the term *hawala*, which is often taken as synonymous with informality. When organisations say they use hawala services, it may be perceived in some countries as admitting to unlawful behaviour, when in reality the MSPs involved are registered.

GLOBAL LEGAL FRAMEWORKS

There is no single global regulatory framework for MSPs. Domestic regulation and licensing requirements differ between countries. The Financial Action Task Force (FATF) recommendations set out a comprehensive framework of measures which countries should introduce to combat money laundering (ML), the financing of terrorism, and the financing of the proliferation of weapons of mass destruction.

Recommendation 14, which relates to MSPs, requires states to license them and ensure adequate regulation and supervision based on the assessed ML/terrorist financing (TF) risks to the sector. It states:

> *"Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions."*

These measures should be implemented in line with the FATF's risk-based approach to ensure that AML and CFT measures are commensurate with the identified risks.[12] Each FATF member state should embed the recommendations in their domestic regulatory framework governing financial service providers.

---

11 This is illustrated by examining how differently the regulatory bodies of the UK and Germany communicate on this matter. Germany's Federal Financial Supervisory Authority (BaFin) states that hawala banking is illegal because by definition it fails to meet KYC standards in line with AML regulations, so the authority will not grant licences for *hawala* businesses to provide financial services. The UK Office of Financial Sanctions Implementation (OFSI) states that *hawala* banking is not illegal, but that providers must comply with the domestic rules and regulations for financial service providers. As such, there is no significant difference in the types of financial services that both regulators permit, but there is a difference in their definition of *hawala* banking.

12 The risk-based approach is outlined in Recommendation 1.

States also have obligations under UNSC resolution 2462, which urges them when designing and applying CT measures "to take into account the potential effects of those measures on exclusively humanitarian activities … that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law".[13] This means states should carefully consider the impact of any restrictions on humanitarians' use of MSPs and in turn their ability to provide assistance in settings where MSPs are a vital tool.

REGIONAL AND NATIONAL LEGAL FRAMEWORKS

In the EU, so-called payment service providers must obtain a licence from member states to operate. The licensing process includes a requirement to submit detailed information, including on internal control mechanisms established to comply with the bloc's AML and CFT legislation. Humanitarian organisations are not allowed to use MSPs in the EU that do not fulfil these requirements.

Many of the countries where humanitarian operations take place have developed and improved their own domestic regulatory frameworks for MSPs in the last decade, including AML and CFT measures, to comply with FATF recommendation 14 on MVTSs.

In Jordan, for example, the provision of non-bank financial services is regulated by the money exchange business law of 2015, which requires MSPs to obtain a license from the country's central bank before providing services. Article 17 of the law states that MVTS providers must comply with Jordanian AML and CFT regulations, and article 21 that they must keep invoices and records of outgoing payments, prepare final financial statements and provide customers with copies of invoices. As a result, the FATF's 2019 mutual evaluation report found that Jordan was largely compliant with recommendation 14.

It is important that humanitarian organisations keep themselves informed of domestic legal requirements in their countries of operation to ensure legal compliance, including by requesting licenses from potential MSPs before signing a contract.

JURISDICTIONS LACKING A FINANCIAL SUPERVISORY AUTHORITY

Some jurisdictions or geographical areas lack a financial supervisory authority or are not under the control of the central government, meaning that licensing MSPs and enforcing AML and CFT rules may not be possible. These include opposition-controlled areas of Myanmar, parts of the eastern Democratic Republic of the Congo, and Darfur and other areas of Sudan.

Internationally recognised governments are entitled under international law to adopt and enforce domestic financial policies that apply across their countries as a whole, but they tend not to issue licenses to MSPs that operate in territory under the control of non-state armed groups. It follows that humanitarian organisations providing assistance in such areas may need to work with unlicensed MSPs.

In other countries experiencing internal conflicts with different fractions competing for control, separate regulatory structures have emerged. In Yemen, for example, Ansar Allah, also know as the Houthi movement, has set up its own central bank and introduced its own currency in opposition to the internationally recognised government in the south.[14] This may create competing legal obligations for humanitarian organisations using MSPs in such locations, particularly in areas where more than one party exerts an element of control.

Most donors acknowledge this operational reality and permit organisations to use MSPs which do not have a central government licence. For cross-border payments at least, registration is usually possible in the location where an organisation pays its MSP, which tends to be a more stable setting that is well integrated in the international financial system.

---

13 UNSC, Resolution 2462, 28 March 2019.

14 Associated Press, *Fight for control of Yemen's banks between rebels, government threatens to further wreck economy*, 16 June 2024.

USE OF MSPS FOR HUMANITARIAN OPERATIONS IN SYRIA

Humanitarian organisations using MSPs to transfer funds into Syria report using extensive resources to ensure compliance with domestic regulations. This includes:

- Commissioning legal advice and opinions on their use
- Applying for specific licenses as a non-operational organisation in Jordan
- Registering as a NGO in Turkey in order to open a PTT account

It is worth noting, however, that many areas outside Damascus lack a regulatory body that could issue and enforce regulations for MSPs operating there. As a result, many organisations have only been able to work towards compliance with domestic regulations in the countries where they pay for services into the MSPs official bank account, such as Dubai, Iraq, Jordan or Turkey.

Resources are also needed:

- To ensure organisations understand and comply with donor requirements or policies on the use of MSPs
- For additional internal due diligence and know-your-supplier (KYS) measures in place for contracting MSPs
- To follow up on payments to MSPs blocked as a result of bank derisking

KEY TAKEAWAYS

- **Misconceptions about MSPs:** There is a prevalent misconception that the MSPs humanitarian organisations use, particularly hawala, are inherently informal and unregulated. Most, however, are registered with national regulatory bodies that enforce corresponding obligations.
- **Diverse regulatory frameworks:** FATF has provided global recommendations for regulating MSPs and mitigating money laundering and terrorism financing risks. Domestic regulatory frameworks for MSPs, however, vary by country.
- **Frame agreements and payment in arears:** Most organisations have official frame agreements with MSPs and pay for their services in arears, once funds have been delivered.
- **UNSC resolution 2462:** The resolution urges states to take the potential effects of CT measures on humanitarian activities into account. This may include the use of MSPs, particularly in settings where they are a vital tool for sustaining operations.
- **Licensing constraints in humanitarian settings:** Humanitarian organisations try to use registered MSPs, but this is not always possible. In areas outside central government control and/or without a regulatory system for MSPs, they may have to rely on unregistered providers.
- **High compliance and risk management burdens across jurisdictions:** Humanitarian organisations using MSPs to operate in Syria have had to invest significant resources to navigate complex compliance requirements.
- **Operational and financial frictions:** Organisations also face considerable administrative burdens related to donor policies, due diligence and blocked payments to MSPs as result of bank derisking.

2 HUMANITARIAN PAYMENT ROUTES INTO SYRIA

OVER THE LAST DECADE HUMANITARIAN PAYMENTS INTO SYRIA HAVE PREDOMINANTLY TAKEN ONE OF TWO FORMS:

1 Bank transfers to Damascus to support operations in areas controlled by the former government

2 Cash payments via MSPs to support operations in NW and NE Syria

2.1 BANK TRANSFERS TO DAMASCUS

Humanitarian transfers to Damascus have proved notoriously difficult. Despite various exemptions covering transfers to government-controlled areas, organisations interviewed for this research said very few financial institutions had been willing to facilitate them. The complicated web of sanctions and CT and CFT measures in place means many financial institutions consider any transfers involving Syria to be too high risk, even if they are covered by an exemption.

One significant barrier for European banks has been the prohibition on maintaining correspondent banking relationships with the Syrian central bank under Article 22 of the EU's Syria sanctions regime. This meant that EU banks had to rely on non-EU correspondent banks to facilitate transfers to Damascus, involving extensive and costly due diligence processes.

After the earthquakes in Syria and Turkey in February 2023, the US government issued a general license that removed the requirement to apply for a specific license from Office of Foreign Assets Control (OFAC) for 180 days.[15] Despite the new license, however, payment delays and rejections were still commonplace. Thirty-three per cent of Damascus-based international NGOs surveyed after the license and other exemptions were issued said they had had a positive impact on their international bank transfers, but 50 per cent said there had been no improvement. Even when transfers were successful, organisations reported large losses as a result of the Syrian central bank's exchange rates.[16]

Some specific experiences reported include:

- One international NGO with a large treasury team said it have been unable to transfer any US dollars to Damascus since 2012, and had found only one bank willing to transfer euros.
- One Spanish NGO could not find a Spanish bank willing to facilitate transfers.
- Many French NGOs reported extreme difficulties transferring to Damascus directly using French banks.
- One international NGO managed to speak directly to a US correspondent bank about blocked transactions despite General License 23 and its accompanying guidance, which stated that banks could rely on statements from customers that the transaction was covered. The bank in question replied that the guidance did not provide enough legal comfort and that it would still require all supporting documentation for each transaction.

WORKAROUNDS

Organisations reported a number of workarounds and tools they had introduced to improve their transfers to Damascus. One used additional screening software on their payments to reduce delays and rejections. The third-party software is a know-your-customer (KYC) treasury management system that pre-screens transactions and provides an increased level of comfort for its bank. The organisation also has a

[15] Government of the US, *Treasury Issues Syria General License 23 To Aid In Earthquake Disaster Relief Efforts*, February 2023.

[16] NRC, *Analysis exemption survey Syria DINGO report,* June 2023.

specific pre-notification arrangement with its bank to make it aware of impending transfer requests.

Another organisation used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment tool, which gave its treasury team a simulation of possible payment routes.[17] This allowed the organisation to select the bank and currency that had the best chance of arriving smoothly at the chosen destination. The SWIFT tool also allowed the organisation to see where a payment may be blocked and the messages between banking partners on the transfer.

Others transferred funds to banks in neighbouring countries and did not tag them as destined for Syria. They then used regional banks to transfer into the country.

At the time of writing, more than one year after the change in government in Syria and subsequent easing of sanctions, the very few international bank transfer routes into Damascus available to NGOs had not yet resumed because of the fluid situation as the new authorities work on the transition. Nor does the international financial system have clarity on the status of existing assets in the country.

The EU lifted its sectoral sanctions in May 2025, but retains those directed at the former president, Bashar al-Assad, and his supporters, and those related to security. The US has also announced an easing of its sanctions, but most of the restrictive measures targeting the country and the previous government are still in place. It will take time to untangle the huge number of restrictions. This creates an environment for the international financial system in which banks are unable to consider either establishing or restarting transfers to Damascus. As one put it: *"The things banks hate most are uncertainty and lack of clarity."*

2.2 MSP CASH PAYMENTS INTO NW AND NE SYRIA

PAYMENTS THROUGH POSTA VE TELGRAF TEŞKILATI (PTT)

Organisations registered in Turkey are able to use PTT's transfer services. Like many national postal services, PTT is 50 per cent owned by the Turkish government. This route has predominately been used by partners of the Syria pooled funds administered by the UN Office for the Coordination of Humanitarian Affairs (OCHA). The process involves an organisation transferring funds from its PTT account in Turkey to an account in one of PTT's branches in NW Syria, where they can be cashed out. The account in Syria may be a local partner's account, an MSP account or the organisation's own account.

Many organisations choose to transfer to an MSP's PTT account because it means their staff do not have to face the risk inherent in carrying large amount of cash to offices and programme areas. Some organisations also contract the MSP agents to distribute programme cash.

Organisations using PTT were positive about the costs involved, with commission rates ranging from 1.5 to three per cent, but they said branches did not always have enough liquidity, especially in US dollars. This meant they would have to cash out in Turkish Lira and incur exchange rate losses.

OTHER ROUTES

Not all organisations operating in NW and NE Syria are registered in Turkey, excluding them from using PTT. The Turkish government declined to register some, while other chose not to apply for registration with a state that could be categorised as a party to the conflict in the interests on neutrality. Nor are PTT services available in all areas of Syria. Organisations unable to use PTT relied on MSPs to provide and deliver cash to their offices and programme sites, and to pay suppliers and staff.

[17] Swift, Payment controls homepage, undated.

To do so, organisations generally put out tenders and sign contracts with selected MSPs. Once an MSP has provided its services - delivering funds into Syria, the organisation reimburses it into its bank account outside the country. MSPs tend to have accounts in Dubai, Iraq, Jordan and Lebanon. Many organisations said they had experienced problems with such payments being delayed or rejected for a number of reasons:

1. The sending bank saw that the payment was for services related to Syria and regarded the transaction as high risk.
2. The sending bank saw the payment was to an MSP or hawala provider and regarded the transaction as high risk.
3. The NGO did not have the correct registration in the country where the MSP had its bank account. In Jordan, for example, organisations paying for services provided in NE and NW Syria must be registered as a non-operational NGO.
4. Payments to MSPs in Iraq were suspended as a result of central bank restrictions on US dollar accounts. Some MSPs only accept payment in US dollars, while those that accept other currencies increase their prices to account for exchange rate losses.
5. US dollar payments from European NGOs to Jordan were regularly blocked as a result of being tagged as involving Syria or under suspicion of involving Syria. Many organisations were forced to transfer in euros and then incur exchange rate losses and fees to pay MSPs in US dollars.

Organisations interviewed said they spent significant time and resources on finding and securing payment channels. Most worked in a number of ways and with various service providers. They said they always needed contingency plans because no single channel was reliable 100 per cent of the time.

Many organisations expressed concerns for the safety and security of staff when they had to receive cash from MSPs, and many were looking for solutions that removed that necessity. Most said they kept little or no cash on their premises, but options for safe storage in NW and NE Syria are extremely limited in the absence of banks.

Some organisations contract third parties to distribute MSPs' cash to beneficiaries, adding a further two to three per cent to their costs. Others used a Turkish e-voucher service alongside MSPs. They provide households with a card which includes information for the MSP about how much money to pay the beneficiary. This reduces cash-handling risks and removes data protection concerns. The system also reduces the need for financial and security staff and has allowed one organisation to cuts its costs even when accounting the expense incurred for using the e-voucher service.

KEY TAKEAWAYS

- **Payments into Syria have predominantly taken one of two forms:** Bank transfers to Damascus to support operations in areas controlled by the former government, and cash payments via MSPs including PTT for operations in NW and NE Syria.
- **There are severe banking restrictions on Damascus transfers:** Despite humanitarian exemptions, transfers are extremely difficult as result of sanctions, CT measures and EU prohibitions on correspondent banking with Syria's central bank. Many banks refuse to process Syria-related transactions, leading to high costs, delays and exchange rate losses.
- **Organisations have adopted workarounds and risk-mitigation tools:** These include the use of screening software, SWIFT route simulations, pre-notifications to banks and indirect transfers through regional banks. These tools are intended to reduce transaction rejections and delays, but they require significant time and expertise.
- **Organisations unable to use PTT face significant issues:** Payments to MSPs are often delayed or blocked because of compliance concerns over Syria and transactions involving MSPs, currency restrictions and NGO registration status.
- **Security risks and workarounds:** Handling cash in insecure environments poses serious risks to staff, and organisations increasingly use e-voucher systems and third-party agents to distribute funds as a result, improving staff safety but adding extra costs.

3 INTRODUCTION TO BLOCKCHAINS AND DIGITAL CURRENCIES

3.1 WHAT ARE BLOCKCHAINS AND DIGITAL ASSETS?

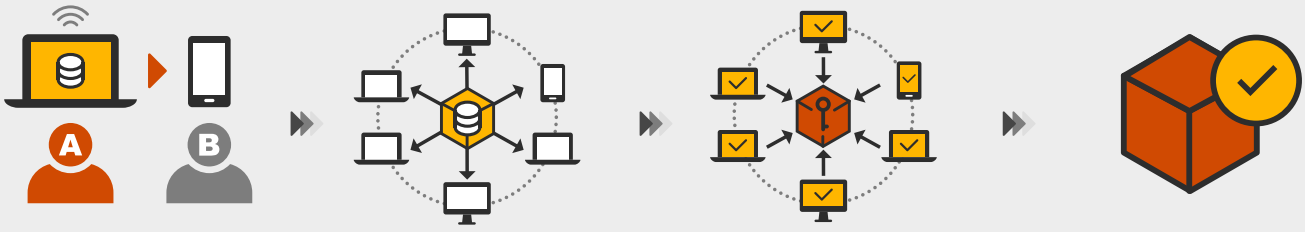
A blockchain is a digital ledger that records transactions in a secure and transparent way. Instead of being stored in one central location, it is distributed across a network of participants who maintain, update and validate it together. Transactions can involve a wide range of assets, both tangible, such as cash, cars, property or land; and intangible, such as intellectual property, patents, copyrights or branding.

Because blockchains use cryptographic methods to secure these records, they ensure that the transaction history is consistent, unchangeable and linear.[18] Cryptographic methods refer to the encryption mechanisms used to protect the secrecy and integrity of data within a blockchain network. They form the foundation of blockchain technology, enabling trust among participants and making the system truly decentralised.[19]

Most blockchains are public and permissionless, meaning anyone with an internet connection can access them. Examples include binance smart chain, bitcoin, ethereum, hyperledger fabric, polygon and solana. Some, however, are private or hybrid, meaning access is restricted. These are often used by businesses and large organisations for specific purposes, such as managing collaborations or sharing data securely (see figure 1).

The technology gained prominence after the 2008 financial crisis when Satoshi Nakamoto proposed blockchains as the foundation for an alternative financial system.[20] Bitcoin is an example of a cryptocurrency, a decentralised form of digital money designed for use over the internet. Cryptocurrencies are a type of digital asset that rely on distributed ledger technology (DLT) to record and transfer economic value. Unlike e-money, which represents digital versions of fiat or physical currencies, crypto assets operate independently of traditional banking systems.

Figure 1: How a blockchain works.[21]



Someone **requests transaction**

The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes**

The network of nodes **validates the transaction and the user's status using known algorithms**

A verified transaction can involve cryptocurrency, contracts, records, or other information

18 Gupta M, *Blockchain for dummies*, 2018.

19 Christie A, *Can distributed ledger technologies promote trust for charities?* A literature review, July 2020.

20 Nakamoto S, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009.

21 PWC, *Making sense of bitcoin, cryptocurrency and blockchain*, undated.

Digital Crypto-assets, as defined in the E.U.'s Markets in Crypto-Assets Regulation (MiCA)[22] are relatively new, and regulated way to store and transfer value online. Unlike traditional money or assets, they exist only in digital form and rely on blockchain technology to ensure security and transparency. **Crypto** assets improve on traditional electronic records because they can be programmed, interacted with, easily transferred and independently verified without the need for a central authority such as a bank or government.[23] **Crypto** assets are:

- **Programmable:** They often include smart contracts, self-executing agreements that carry out actions automatically when certain conditions are met. This means transactions or agreements can happen without manual approval.
- **Interactive:** They can move freely and work seamlessly with different applications and other assets within the same blockchain system.
- **Portable:** Owners control crypto assets through cryptographic keys, which are similar to passwords. This allows people to store, access and transfer assets directly using a self-hosted wallet without the need for a middleman such as a bank.
- **Auditable:** Because a blockchain records every transaction permanently, users can review the history of a digital asset, verify its details and ensure its authenticity.

Crypto assets include cryptocurrencies, stablecoins and central bank digital currencies (CBDCs).[24] Most crypto assets purchased, held and used by the public are cryptocurrencies and stablecoins. Crypto assets are the bedrock for the blockchain financial ecosystem, also known as decentralised finance or DeFi.

Cryptocurrencies are a type of digital asset. They run on blockchain technology and are mainly used for financial transactions. Their value can be linked to fiat currencies, creating stablecoins, or tied to other cryptocurrencies or market-driven algorithms such as Ampleforth. Some cryptocurrencies also serve specific purposes within blockchain networks, such as supporting infrastructure or paying for services.

Stablecoins are a type of crypto-asset designed to maintain a steady value relative to an established currency such as the US dollar or a commodity such as gold, offering more stability compared with highly volatile unbacked cryptocurrencies. The US digital currency (USDC), which is tied to the dollar, is an example of a stablecoin. It was created by the peer-to-peer payments technology company Circle.[25] There are three types of stablecoin:

- **Fiat-backed stablecoins** are collateralised by physical currency reserves or equivalents, which provides stability dependent on the issuer's creditworthiness.
- **Crypto-backed stablecoins** rely on other cryptocurrencies as collateral, employing mechanisms such as over-collateralisation.
- **Algorithmic stablecoins** maintain value through supply-demand balancing mechanisms but have been criticised for their volatility.

A key difference between these crypto assets is the type of digital wallet they use. These are defined as digital tools, software applications or services that manage one's digital assets, including cryptocurrencies.

A cryptocurrency wallet does not store crypto assets but instead holds private keys that grant its owner access to and control over them, prove ownership and authorise transactions on the blockchain. Centralised systems such as CBDCs and fiat-backed stablecoins tend to use custodial wallets, and third parties such as government institutions or FinTech companies including PayPal and Revolut manage the funds.[26] Decentralised systems rely on non-custodial wallets, giving users full control of their assets.

---

22 ESMA, *Markets in Crypto-Assets Regulation* (MiCA), 2023.

23 CDAP/CCAF, *Considering crypto assets for humanitarian cash-based transfers*, 2023.

24 Idris I, *Humanitarian digital transfers in challenging contexts*, 2024.

25 OKX Learn, *7 top stablecoins to watch in 2025*, March 2025.

26 Dwyer G P, *The Economics of Bitcoin and Similar Private Digital Currencies*, May 2014.

KEY TAKEAWAYS

- **A blockchain** is a type of digital ledger that records transactions in a secure and transparent way across a network of participants who maintain, update and validate it together.
- **Cryptocurrencies** are a type of digital asset that run on blockchain technology and are mainly used for financial transactions. Their value may be tied to a physical currency, other cryptocurrencies or market-driven algorithms.
- **Stablecoins** are a type of crypto-asset designed to maintain a steady value relative to an established currency such as the US dollar or a commodity such as gold.

3.2 DECENTRALISED FINANCE: BLOCKCHAIN-BASED FINANCIAL PRODUCTS

Decentralised finance (DeFi) is a blockchain-based system that allows people to lend, borrow, trade and earn interest without relying on banks or other traditional intermediaries. It uses smart contracts to automate financial transactions, making them more transparent, secure and efficient. One of DeFi's key strengths is composability, meaning that different applications can seamlessly connect, share resources and access pooled funds or liquidity.

This creates a highly flexible system with several advantages over traditional finance (TradFi), including lower fees, greater accessibility, transparency and automation. DeFi also enables global lending and borrowing at reduced costs. Unlike cryptocurrencies such as bitcoin or ethereum, which function as digital money, DeFi focuses on replacing and improving banking and investment services through decentralised and programmable financial tools.[27]

As blockchain adoption grows, new service providers are emerging to help individuals and businesses interact with the technology without the need for in-depth expertise. These include regulatory and compliance technologies, known as RegTech, to help with legal and security requirements, compliant transaction monitoring and reporting, and exchange, trading, investment and custodial services that facilitate buying, selling and storing digital assets. These are collectively known as crypto-asset service providers (CASPs) or virtual asset service providers (VASPs), and they play an increasingly important role in global blockchain adoption.

KEY TAKEAWAYS

- **DeFi eliminates the need for traditional intermediaries:** Decentralised finance is a blockchain-based system that allows people to lend, borrow, trade and earn interest without relying on banks or other traditional intermediaries.
- **Smart contracts enable transparency and efficiency:** DeFi uses smart contracts to automate financial transactions, making them more transparent, secure and efficient.
- **Composability improves flexibility:** DeFi applications are designed to be interoperable, enabling different services to integrate and share liquidity, which creates innovative and adaptable financial ecosystems.
- **A new ecosystem of service providers is emerging:** As blockchain adoption grows, CASPs and VASPs are offering tools such as trading platforms, custody services and compliance tech, helping individuals and businesses engage with DeFi without the need for in-depth expertise.

3.3 BLOCKCHAINS AND CRYPTO ASSETS IN THE HUMANITARIAN SECTOR

Blockchains and crypto assets have the potential to transform humanitarian aid by improving financial inclusion, efficiency and transparency. Because blockchains are transparent, decentralised and immutable – meaning records cannot be changed – they can be used for a range of applications, including cross-border payments, aid distribution, supply chain management and digital identities.

[27] Alamsyah A et al, *A review on decentralized finance ecosystems*, February 2024.

Many organisations, including UN agencies, have explored blockchains for humanitarian purposes. One of the most notable projects is Building Blocks, launched by the World Food Programme (WFP) in 2017.[28] It started as a pilot in the Azraq refugee camp in Jordan, where 10,000 participants used blockchain-based virtual wallets to buy food from merchants. Instead of cash, vouchers or debit cards, transactions were validated through iris-scanning technology, reducing the risk of theft and improving efficiency. It became the world's largest blockchain-based humanitarian assistance programme.

Crypto assets have the potential to be particularly useful in regions with cash-based financial systems. This includes areas with limited banking access, high inflation, currency instability and low financial inclusion. While blockchains offer many advantages, however, their use requires careful planning to address risks, regulatory challenges and local settings. Without careful design, new technologies can unintentionally reinforce political and economic inequalities rather than reduce.

Some key benefits of using crypto assets in humanitarian settings include:

- **Lower costs:** They reduce transaction and operational expenses.
- **Faster payments:** They automate disbursements for quicker aid delivery.
- **Greater transparency:** They improve accountability for donors.
- **Better fund movement:** They facilitate aid to financially isolated areas by circumventing the correspondent banking system and its derisking behaviour.
- **Stronger supply chain tracking:** They provide visibility in complex humanitarian logistics.
- **New donation channels:** They encourage innovation in funding aid efforts.

Crypto assets can also help to solve payment challenges at the field or programme level, where organisations and systems that often lack mutual trust and access to the same transaction information have to work together. KYC requirements are a major obstacle with the traditional banking system, because many people in crisis zones lack the required identity documents. Crisis zones are also often in highly sanctioned jurisdictions, making the traditional banking system reluctant to allow transactions.

Crypto assets provide a safe and secure and safe way to circumvent this derisking behaviour. They can reach people who are unable to meet KYC requirements and are excluded from financial systems, ensuring aid reaches those who need it most.

Any transfer of data, crypto assets and/or cryptocurrencies on a blockchain is also highly traceable and verifiable for audit records, which has been touted as a significant advantage of the technology.[29] Global regulations such as the EU's markets in crypto-assets (MiCA) regulation further strengthen traceability requirements and functionality through the application of FATF's "travel rule" to cryptocurrency and digital-asset transactions.[30]

Other major benefits include lower international transfer costs and greater flexibility for users. Unlike mobile money, which is tied to specific network providers, crypto assets can be used across different networks. As adoption moves beyond pilot programmes, they could also help people access affordable financial services by enabling them to build an account and transaction history, a crucial first step toward long-term financial inclusion.

That said, using crypto assets comes with trade-offs and challenges, including concerns about energy consumption, privacy, scalability and unequal access:

- **Energy consumption:** Some blockchains, such as the Bitcoin blockchain (the first blockchain, originally built to support the Bitcoin

[28] WFP, *Building Blocks*, undated.

[29] World Bank, *Exploring blockchain for disbursement traceability*, November 2020.

[30] KPMG, *The travel rule: Transfer of crypto-assets in Germany and European Union*, April 2024.

cryptocurrency)use a consensus mechanism called Proof of Work (PoW), in which data miners compete to validate transactions by solving complex puzzles. This requires vast computing power, which consumes huge amounts of energy and raises environmental concerns. However, newer blockchain consensus algorithms are increasingly energy efficient or "carbon-zero".

- **Unequal access:** Because PoW mining relies on powerful computers and stable internet connections, it can exclude regions with limited infrastructure, deepening the digital divide.
- **Scalability:** Crypto assets depend on access to smartphones or computers, which is increasing globally but such devices are not universally available. Those without them or with limited technological literacy may struggle to participate in DeFi.
- **Internet connectivity:** Even for those with devices, unreliable internet access in some parts of the world can make it difficult to use crypto assets effectively.

To begin addressing these challenges, some humanitarian organisations have opted to use private permissioned blockchains (such as WFP), which have restricted access and require the organization itself to manage the network. Others, such as Oxfam, and Mercy Corps, have predominantly adopted the use of public blockchains, particularly those that are more accessible to users in emerging markets, and that are more efficient, such as the Celo, Polygon and Algorand blockchains. The expanding blockchain ecosystem offers a spectrum of choices for organizations to adopt, based on their needs. Stablecoins, which are pegged to traditional currencies, are preferred because they reduce the risks associated with cryptocurrency volatility.

Many organisations have introduced training to improve technological literacy and ensure participants are able to use DeFi tools effectively. Many have also started to pilot the use of crypto assets in their programmes, and there is a growing body of research that explores how blockchains and digital currencies could expand the financial tools available to humanitarians.[31]

KEY TAKEAWAYS

- **Improved access in fragile settings:** Crypto assets can enhance humanitarian aid delivery in areas with limited banking infrastructure, high inflation and financial exclusion, enabling fund transfers where traditional systems fail.
- **Enhanced efficiency and transparency:** Blockchains' transparency, decentralisation and immutability help to deliver faster, cheaper and more accountable assistance.
- **Usefulness in complex settings involving many stakeholders:** Crypto assets can help to solve payment challenges at the field or programme level, where organisations and systems that often lack mutual trust and access to the same transaction information have to work together
- **Scalability and equity are challenges:** Access to devices, internet connectivity and technological literacy are essential but not universal, potentially widening the digital divide and limiting the inclusive potential of blockchain-based solutions.
- **Strategic implementation is essential:** The successful integration of crypto assets in the humanitarian sector requires careful planning in terms of regulatory compliance, operational risks and context-specific challenges.
- **Use of stablecoins and permissioned blockchains helps to mitigate key risks:** Humanitarian organisations prefer stablecoins for their price stability, and permissioned blockchains to avoid high energy use and improve control, access and security.
- **Global regulation and adoption are expanding:** Frameworks such as the EU's MiCA regulation and FATF's travel rule have improved transparency and functionality, while pilots and research continue to test crypto assets as viable long-term tools for humanitarian responses.

[31] NRC, *Dialogue series on solutions to bank derisking*, 2022-2023.

3.4 CASE STUDIES: CRYPTO ASSETS IN HUMANITARIAN PROGRAMMING

Humanitarian organisations have been exploring the use of blockchains and digital assets, including stablecoins and tokenised fiat currencies, through pilots and some larger-scale initiatives since 2018. The technologies have often been tested for cash and voucher assistance (CVA), but they have not always served as direct alternative payment channels. Instead they have primarily been used to address challenges and maximise new opportunities in aid distribution.

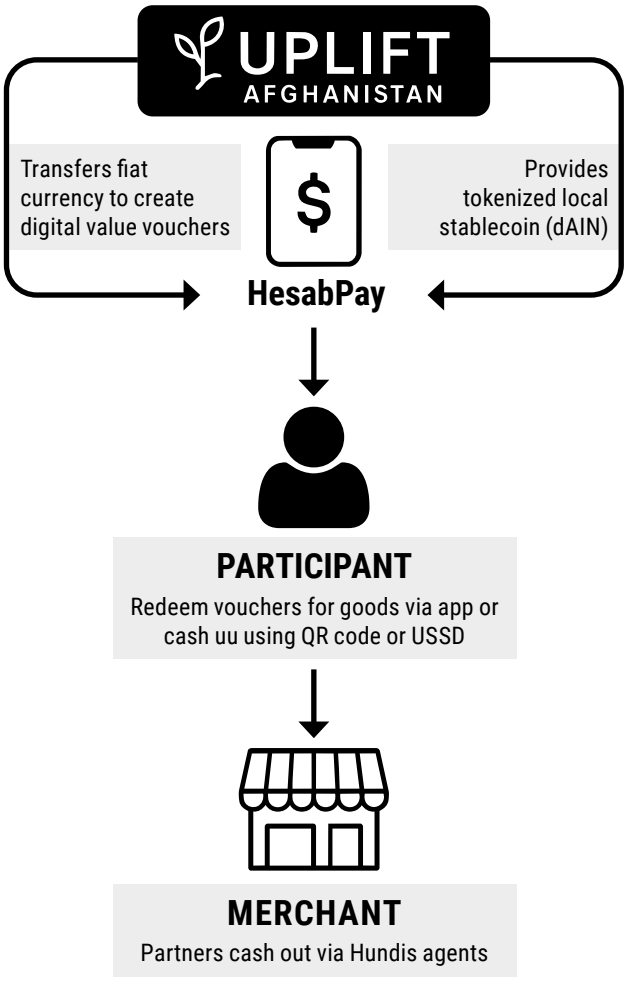
Stablecoins in particular have played a key role in settings where derisking and sanctions have significantly impeded humanitarian action. The following section explores case studies from Afghanistan, Myanmar and Venezuela, where blockchain-based end-to-end payment solutions have been used to navigate these restrictions and ensure aid reaches those in need.

AFGHANISTAN: HesabPay's digital payments

HesabPay, a licensed platform in Afghanistan, digitised humanitarian cash transfers using stablecoins. Beneficiaries received bi-weekly payments for two months, delivered as digital value vouchers denominated in the local dAFN stablecoin, created by tokenising fiat currency. The vouchers were redeemable for goods at any HesabPay-enrolled merchant. Beneficiaries received value vouchers on their phones, ensuring accessibility and reducing logistical challenges.

Integrated with the Algorand blockchain, HesabPay ensured secure transactions while maintaining user privacy. The programme was highly cost efficient and transparent. The pilot achieved significant scale, serving more than 500,000 users and 3,000 merchants. Its success was also a result of the system's ability to expand to rural areas and integrate with a number of humanitarian partners.[32]

Figure 2: Funds flow diagram for pilot in Afghanistan.



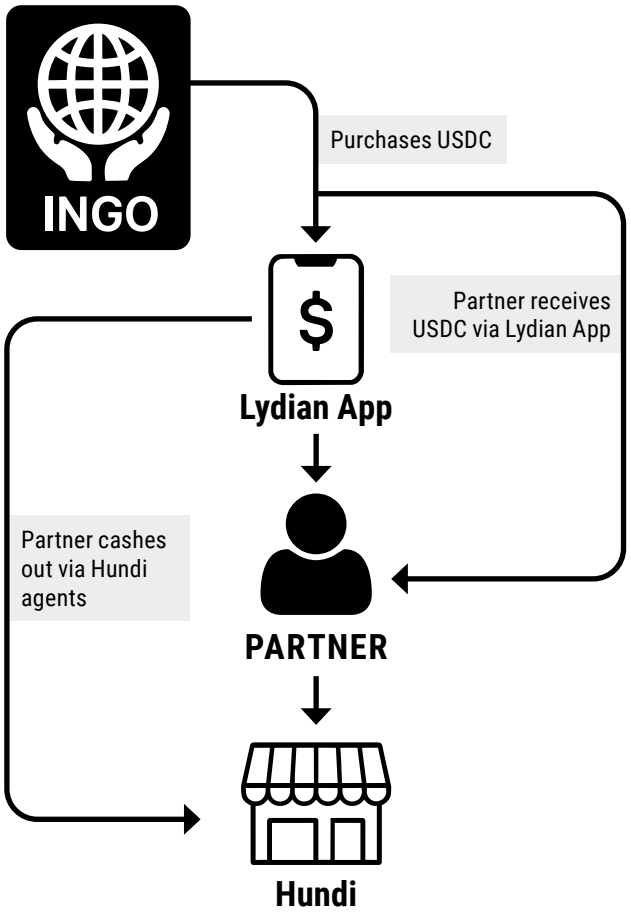
[32] Callen M et al, *Can digital aid deliver during humanitarian crises?* October 2024.

MYANMAR: Mercy Corps' stablecoin initiative

In 2024 Mercy Corps piloted stablecoin-based payments to address challenges in Myanmar posed by sanctions, domestic banking surveillance, restrictions on NGO financial access and a liquidity crisis. Its global finance team purchased USDC and used a bulk disbursement platform to send payments directly to local partners' digital wallets. Setting up the wallets was simple. Partners received an automated message, clicked a link and the Lydian app instantly created them.

Funds could then be exchanged for local currency through Hundis, informal financial agents with strong liquidity networks. The system was affordable, fast, secure and flexible, allowing partners to relocate as needed to support internally displaced people (IDPs) while avoiding financial surveillance. The pilot reduced costs and risks, with potential for expansion given donor approval.

Figure 3: Funds flow diagram for pilot in Myanmar.

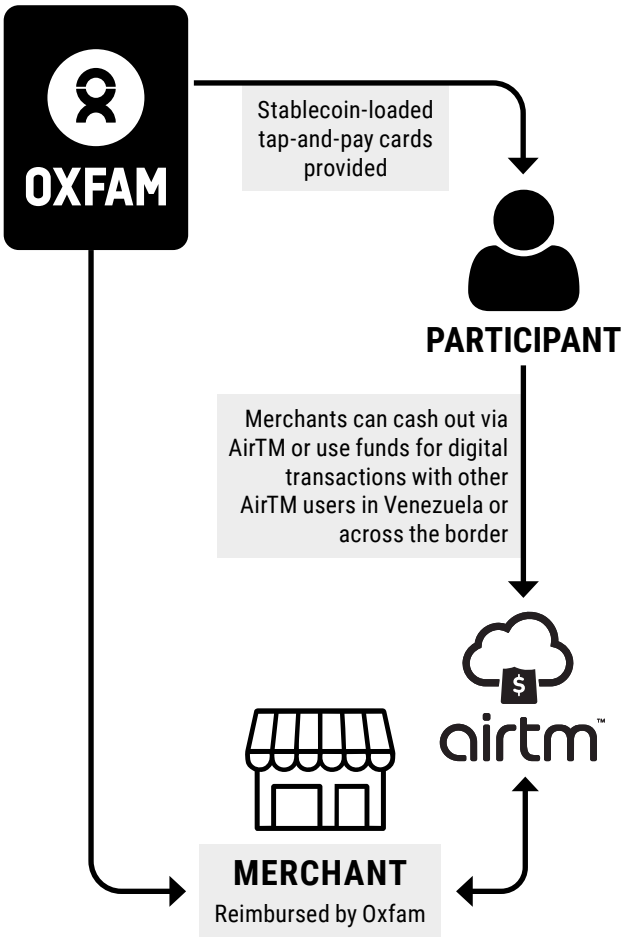


VENEZUELA: Informal cryptocurrency adoption and Oxfam pilot

Venezuela's economic crisis and the impact of sanctions led more than 7.7 million people to flee the country and has left the country "de-banked", but cryptocurrencies have served as portable and discreet assets for fund transfers across borders. The country ranked third in the world in terms of cryptocurrency adoption in 2020. The adoption of bitcoin was unprecedented because of its relative stability compared with the bolívar, appreciation over time and independence from government control.

Cryptocurrencies have proven also proved useful beyond being a safe-haven asset, enabling Venezuelans to send, receive and store funds, purchase essentials and earn income. The country also pioneered blockchain-based alternative payment channels during crises, particularly through the use of stablecoins pegged to the US dollar.[33]

Figure 4: Funds flow diagram of pilot in Venezuela with Oxfam.



[33] Hart S U, *From Promise to Practice: A cross-institutional analysis of design trends, enablers and challenges in blockchain-enabled cash and voucher delivery*, January 2024.

Oxfam Colombia worked with Oxfam Australia, Sempo, which provides blockchain-enabled cash transfers for humanitarian aid distribution, and the Airtm digital wallet in late 2020 to pilot its UnBlocked Cash project, which used stablecoin-backed vouchers for vulnerable populations near the Colombian border. The project addressed challenges including restricted operations caused by political tensions, risky cash delivery, the deflating bolívar and the lack of reliable financial service providers. The project had previously been piloted in 2019 in Vanuatu, Papua New Guinea and Zimbabwe, and won the 2020 EU Horizon prize for Blockchain for Social Good in Aid.[34]

For the Venezuela pilot, local merchants were provided with smartphones, while participants received tap-and-pay cards preloaded with stablecoin. The cards acted like digital vouchers, allowing participants to purchase goods from enrolled merchants. Instead of waiting for reimbursements from Oxfam, merchants cashed out their earnings directly through Airtm. This gave them flexibility. They could keep their funds in stablecoins, convert them to Colombian pesos or use them for digital transactions with other Airtm users in Venezuela or across the border.

Because Oxfam managed the Airtm wallets, they could correct user errors, such as accidental transactions, and monitor for misuse, which was crucial given their lack of presence on the ground. The pilot came to end in January 2021 when the Venezuelan government suspended humanitarian cash transfers, but the Airtm app has since expanded and now serves millions of users across Latin America.[35]

KEY TAKEAWAYS

- **Oxfam's pilot in Venezuela** in collaboration with Sempo and Airtm took advantage of the growing cryptocurrency adoption locally, and Airtm's digital wallets enabled Oxfam to correct user errors and monitor for misuse.
- **Mercy Corps' pilot with stablecoin-based payments in Myanmar** enabled it to address challenges posed by sanctions, domestic banking surveillance, restrictions on NGO financial access and a liquidity crisis.
- **HesabPay was used in a stablecoin-based pilot in Afghanistan which was highly cost efficient and transparent, significantly reducing aid diversion risks.** Beneficiaries were able to use digital vouchers at any HesabPay-enrolled merchant.

3.5 REGULATORY LANDSCAPE: KEY COMPLIANCE CONSIDERATIONS

The development of global regulatory frameworks for blockchain solutions is evolving rapidly, a positive development after years of maladapted, unclear and piecemeal regulation across jurisdictions. Global supervisory bodies such as BIS (Bank of International Settlements) and FATF have issued regulatory guidance, but its broad nature has not prevented confusion and in some jurisdictions.[36]

Regulatory guidance on stablecoins is clearer, with a general rule of "same risk, same regulation".[37] This generally results in the classification of currency-backed stablecoins as assets equivalent in risk to holding hard currency in a bank account, while other types of stablecoins are treated as having a higher risk profile.

[34] Oxfam, *UnBlocked Cash Project: using blockchain technology to revolutionize humanitarian aid*, undated.

[35] Musialkowska I et al, *Looking for a safe-haven in a crisis-driven Venezuela: The Caracas stock exchange vs gold, oil, and bitcoin*, April 2020.

[36] BIS, *Prudential treatments of cryptoasset exposures*, December 2022; FATF, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*, July 2024.

[37] Latham & Watkins, *BIS Issues Final Guidance on Stablecoin Regulation*, August 2022.

One of the most common concerns about cryptocurrencies is their potential use for illicit activities as a result of their encrypted and pseudonymous nature. Regulators across a number of jurisdictions have issued warnings, but it is important to note that criminal activity represents only a small fraction of global cryptocurrency use. The vast majority of illicit financial transactions still occur in fiat currencies. A 2021 Europol report states: "The overall number and value of cryptocurrency transactions related to criminal activities still represents only a limited share of the criminal economy when compared to cash and other forms of transactions."[38]

Given concerns about the illicit use of virtual assets, global firms such as Chainalysis and Elliptic work closely with regulators and law enforcement to track and blacklist service providers and digital wallets linked to such activity.[39] Their tools enable real-time monitoring and analysis, strengthening oversight and compliance within the cryptocurrency ecosystem.[40] Advanced financial forensics applications that take advantage of the transparency of transactions on public blockchains are continuously being developed to trace, track and stop the use of crypto-assets for illicit transactions.

The Atlantic Council provides a live cryptocurrency regulation tracker, which highlights that crypto assets are legal and under some form of regulatory oversight in 60 countries. It shows that cryptocurrencies are legal in 33 countries, partially banned in 17 and banned in 10.[41] The database also reveals shows a clear trend towards countries legalising the use of cryptocurrencies, and helpfully groups regulatory efforts into four general areas:

1. **Tax policy:** Focused on income tax, capital gains tax and corporate taxes
2. **AML/CFT measures:** Focused on requiring financial institutions to monitor transactions and report suspicious behaviour to government agencies
3. **Consumer protection rules:** Including advertising regulation, data storage and transfer rules, cybersecurity provisions and investor accreditations
4. **Licensing and disclosure obligations:** Examining whether businesses and investors have licensing, disclosure and reporting requirements in place

---

38 Europol, *Cryptocurrencies: tracing the evolution of criminal finances*, January 2022.

39 Chainalysis, *OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses,* August 2023.

40 Elliptic, *Tactics, Techniques & Procedures Report For Law Enforcement*, 2023.

41 Atlantic Council, *Cryptocurrency Regulation Tracker homepage*, undated.

Most rules and regulations for fiat transactions are applied in the same way to virtual asset transactions. This includes rules governing due diligence, such as KYC and know-your-business (KYB) requirements, enhanced measures related to specific transaction types, jurisdictional risks and transaction reporting. Most relevant for this report is that FATF's travel rule is also applied in the same way, requiring due diligence and reporting on transaction purposes and use of funds in cross-border transfers.

As DeFi products rarely offer payments, credit, investment and savings functions in a single product, however, these compliance requirements can also be easier to comply with, compared with those imposed on larger financial institutions such as banks. Digital wallets, for example, are most commonly simple "payment apps", designed for sending and receiving funds and which require the same onboarding process as other apps such as PayPal and Apple Pay, and mobile money wallets such as M-Pesa.

This report does not cover the use of all cryptocurrencies but focuses on stablecoins, which offer greater stability and tend to operate within private permissioned networks, making them more suitable for humanitarian applications because they are regulated and can be monitored.

KEY TAKEAWAYS

- **Stablecoin regulation is advancing quickly:** Global regulatory frameworks for blockchain technologies, especially stablecoins, are evolving after years of fragmented oversight, with regulation in place in more than 60 countries to date. Stablecoins are increasingly regulated under the principle of "same risk, same regulation," often treated similarly to traditional bank deposits when backed by fiat currency.
- **FATF and BIS guidance exists but is often broad:** Global bodies such as FATF and BIS have issued regulatory guidance, but it has not fully resolved confusion at the national level, where interpretation and enforcement vary widely.
- **Standard financial regulations apply to virtual assets:** The same compliance rules that apply to fiat transactions, such as KYC, KYB, AML/CFT and the travel rule, also apply to virtual assets. DeFi applications such as digital wallets, however, tend to face lighter requirements given their limited financial functions.
- **Stablecoins are better suited for humanitarian use than other cryptocurrencies:** Unlike volatile assets such as bitcoin, stablecoins offer price stability and tend to operate in permissioned, regulated networks. These characteristics make them more viable for humanitarian organisations, for whom risk and compliance concerns are paramount.

4 OUTLOOK AND RECOMMENDATIONS: USING CRYPTO ASSETS IN SYRIA

4.1 INTRODUCTION TO USING CRYPTO ASSETS IN SYRIA

Beyond the immense human, economic and social toll on Syria, one of the lasting effects of the country's civil war is its fragmentation into areas controlled and influenced by different and often competing groups. With continued political instability and a backdrop of more than ten years of sanctions, it is likely to be some time before the Syrian banking sector is fully functional across the country and has access to the international financial system.

Digital currencies offer a potential workaround by enabling seamless value exchange without the complications of converting between various currencies, a key advantage given the diverse range of international aid organisations working in Syria. Unlike traditional financial systems, which rely on intermediaries, digital currencies streamline transactions, making them significantly more agile. This agility has been particularly important since the fall of Assad in December 2024. As governance structures evolve, humanitarian organisations have had to adapt quickly. This includes early adopters of stablecoins to facilitate the transfer of humanitarian funds to, and within Syria, notably by GIZ & UOSSM, using stablecoins for health worker payroll; and (2024) and Mercy Corps (2025), for cash support to Syrian farmers.

The remaining sections of this paper provide guidance for humanitarian organisations seeking to use blockchains and digital currencies to overcome the difficulties they face in getting funds into Syria, whether for programme delivery or paying salaries and suppliers. The solutions described are also intended to safeguard organisations, programme participants and donors by minimising risks and maximising compliance.

As such, they should be in line with the following guidance:

1. Only use MiCA-compliant US dollar stablecoins
2. Organisations and/or licensed VASPs outside Syria should procure stablecoins using fiat currency, whether US dollars or euros, from an account at a regulated institution.
3. Use of one or more of the DeFi applications easily accessible via the internet.
4. The chosen DeFi applications should allow for two types of transaction: bulk disbursements, for salaries and cash programmes; and targeted or single disbursements to suppliers and implementing partners.
5. Use strong controls to confirm that digital currency transfers are strictly limited to humanitarian use and involve only trusted partners and vetted recipients.

KEY TAKEAWAYS

- **The agility of digital asset-based transactions is particularly important** in Syria's post-war setting, where governance structures are evolving and humanitarian organisations have to adapt quickly.
- By reducing reliance on slow-moving bureaucratic banking channels, **digital currencies can accelerate local development, ensuring funds reach people on the ground** without the delays caused by sanctions or risk-averse banking policies.
- **Blockchain technology also opens up new funding avenues in Syria.** Many organisations are eager to support the emerging "tech for good" movement, which uses decentralised technologies for social impact, financial inclusion and humanitarian aid.

4.2 STAYING COMPLIANT

The EU's MiCA regulation is a comprehensive legal framework adopted to regulate the crypto-asset market. It was approved in April 2023 and began to come into effect in phases in 2024. MiCA is intended to create a unified regulatory framework for crypto-assets across the EU, ensuring consumer protection and financial stability, and fostering innovation. MiCA regulates crypto-assets not covered by other EU financial services legislation, such as stablecoins and utility tokens. It excludes NFTs and some decentralised De-Fi platforms for the time being.

MiCA is framed as the broadest and most relevant and advanced regulatory regime adapted to current uses of cryptocurrencies. It largely treats crypto assets and related services as mainstream market activities implemented by a diverse range of individual and institutional stakeholders. This makes it the preferred framework for assessing the risks and challenges of using DeFi, crypto asset providers and stablecoins in humanitarian transactions. MiCA imposes stringent requirements on issuers of stablecoins, referred to in the regulation as "asset-referenced tokens" and "e-money tokens". It requires stablecoins used for cross-border transfers to:

- Maintain adequate reserves and liquidity to ensure reliability and prevent systemic risks
- Adhere to clear governance and risk-management standards
- Be subjected to regulatory oversight by the EU authorities

It also provides significant protection for individuals and organisations seeking to use digital assets. VASPs must obtain licenses to operate across the EU, and these protect consumers because service providers must clearly disclose risks to users, ensuring transparency in how stablecoins are issued and used.

MiCA is timely in providing more clarity and assurance in compliance for cross-border transfers, providing harmonised rules that make it easier for entities to operate across EU member states without conflicting national regulations. This development is particularly relevant for De-Fi platforms facilitating payments or remittances across member states and internationally.

MiCA ultimately serves as a baseline to ensure that humanitarian organisations' use of digital asset-based products or pilots in Syria is legally compliant. Two of the largest humanitarian donors to Syria, the EU and Germany, where the use of currency-backed stablecoins is legal, fall under its provisions.

There is a growing market of regulated VASPs in the EU that can offer support and expertise in the procurement of stablecoins and their transfer to the digital wallets of country teams, partners, staff and suppliers. These VASPs provide decentralised financial services and products, such as digital wallets and traceable disbursement and transaction reporting mechanisms that are bound by MiCA in terms of minimum requirements for consumer protection, data privacy and service disclosures.

As with most regulations, however, MiCA includes some limiting factors that need to be accommodated when considering use in Syria. Its stablecoin rules are mostly suitable for moving humanitarian funds, but only certain coins are compliant. Widely used ones such as USDT, which is common in emerging markets and the Middle East, may not qualify because MiCA excludes algorithmic stablecoins.

KEY TAKEAWAYS

- **MiCA is intended to create a unified regulatory framework** for crypto-assets across the EU, ensuring consumer protection and financial stability, and fostering innovation.
- **MiCA provides more clarity and assurance** in compliance for cross-border transfers by harmonising rules, which makes it easier for entities to operate across EU member states without conflicting national regulations.
- **Only certain stablecoins are MiCA-compliant.** Widely used ones such as USDT, which is common in emerging markets and the Middle East, may not qualify because MiCA excludes algorithmic stablecoins.

4.3 HOW CAN STABLECOINS ADDRESS CURRENT CHALLENGES?

The main challenges that humanitarian organisations with operations in Syria experience in relation to financial access, and which can potentially be resolved by using stablecoins are:

- **Blocked or delayed cross-border transfers:** Bank derisking means that the movement of funds into Syria may be blocked or significantly delayed by the need to use a number of intermediaries, which also complicates traceability and transparency.
- **Donor concerns, high costs and risks with MSPs:** Direct transactions with MSPs, especially through banks, are expensive, can involve increased risks and are often disrupted. Fees can be unpredictable because of limited liquidity. Managing KYC requirements and contracts with various MSPs, along with donor due diligence, can be a major burden for organisations.
- **Field-level cash handling:** Most organisations in Syria rely on physical cash for payments to offices, field sites, suppliers and staff. This creates serious risks of theft and fraud, and is costly and time-consuming, often leading to delays.

Ensuring these pain points are addressed was a core focus in selecting and evaluating the solutions proposed in the next section. That said, not all of the difficulties associated with transferring funds to, and within, Syria can be wholly addressed with blockchain solutions. It is more realistic to assume that they will reduce the severity of pain points rather than resolving them completely. This is because of "real world" issues such as access to the internet and electricity, flaws with digital devices and significant contextual risks, such as conflict and insecurity.

Nor is it feasible to exclude MSPs from any of the solutions proposed for two reasons: first, because they are the primary source of liquidity in Syria; and second, because cash is still in demand among local populations, suppliers and organisations.

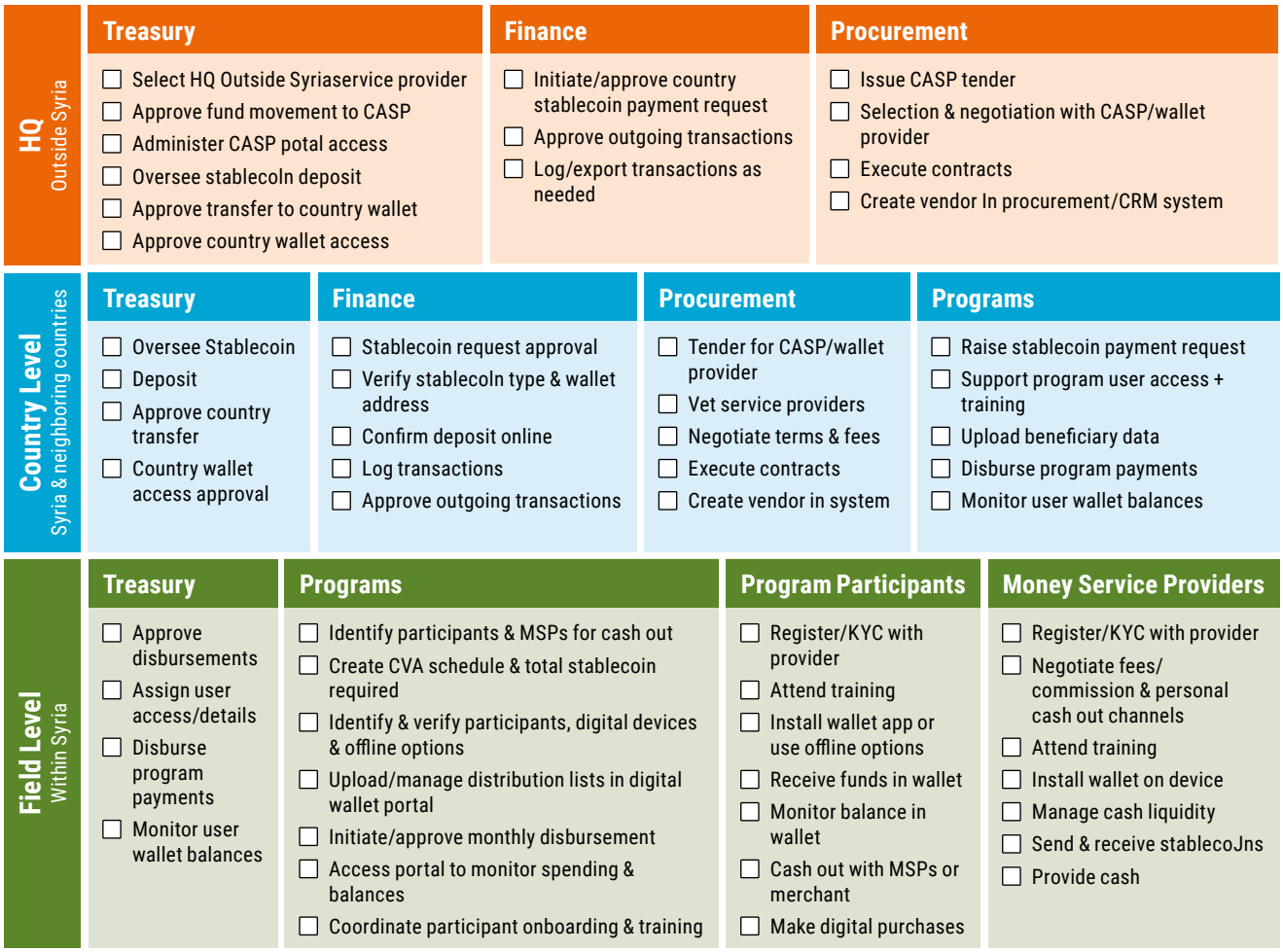
Looking forward to the possible broader use of emerging technologies, something Syria's central bank is reportedly discussing, MSPs have a potentially central role to play in digital currency adoption and the availability of cash-out channels for humanitarian organisations, staff and beneficiaries. The central bank issued guidance in February 2025 encouraging humanitarian organisations to use digital payments rather than cash in their programmes.[42]

KEY TAKEAWAYS

- Not all of the challenges associated with transferring funds to and within Syria can be wholly addressed with blockchain solutions.
- **It is not feasible to exclude MSPs from any of the solutions proposed** because they are the primary source of liquidity in Syria and because cash is still in demand locally.
- The Syrian central bank issued guidance in February 2025 encouraging humanitarian organisations to use digital payments rather than cash in their programmes.[43]

[42] HCT Cash Working Group, *Update on meeting with Central Bank*, 26 February 2025.

[43] *Ibid.*



4.4 POTENTIAL SOLUTIONS FROM HQ TO FIELD LEVEL

In each solution, the chosen blockchain infrastructure is important but mostly invisible to users. It functions as a behind-the-scenes layer, similar to electricity or a mobile phone network, which powers the system. The main interface that users interact with is the blockchain application, which they access via a smartphone or laptop to transfer of funds from one digital wallet to another, similar to transferring funds from one account to another using an online banking interface. Stablecoins are the unit of transfer used to represent the movement of US dollar funds from one wallet to another over the blockchain network.

The solutions presented here reflect services and systems that are readily available to humanitarian organisations and have been tested in settings including Syria. HesabPay and Mercy Corps, for example, have piloted the transfer of USDC stablecoins into digital wallets held by farmers in NE Syria so they can buy fertiliser digitally from agricultural suppliers. UOSSM and DigiBankar have teamed up in NW Syria to disburse salary payments to health workers in USDC.

In both cases, anecdotal reports suggest more MSPs in Syria now use digital wallets and can convert stablecoins to cash in varying amounts, reducing the need to handle large sums of physical cash. These examples are a useful reference point in terms of feasibility, showing that they can be adopted successfully. Informal feedback from digital wallet providers also indicates uptake by individuals and businesses independently of the humanitarian sector to receive remittances, transfer money quickly and easily between friends and family or to earn income online.

As Syria's political landscape evolves, particularly in terms of sanctions, tech products and services are likely to develop quickly, as seen with emerging technologies such as blockchain. New service providers, such as digital wallet apps, crypto platforms and stablecoin issuers, are likely to be entering or preparing to enter the Syrian and related markets, including for diaspora remittances.

The solutions presented here draw lessons from the existing pilots based on feedback from stakeholder interviews and consultations, indicating a common flow of funds across stakeholders working in Syria. **This flow assumes that humanitarian funds are typically handled at three levels, according to the structure of most organisations.**

1. **HQ level:** Headquarters or offices outside Syria where donor funds are received and held, and where transfers originate. Funds are sent to Syria in large amounts for programmes and operations.

2. **Country level:** Country offices in Syria and neighbouring countries such as Jordan, where finance, operations and programme staff determine who funds should be transferred to, in what amount and for what purpose.

3. **Field/programme level:** Offices or project sites in Syria where staff are located, programmes are implemented directly or by local partners and beneficiaries receive assistance.

This breakdown helps to clarify who in the organisation will use the proposed technology and how. It also highlights where fund transfer issues occur and who is affected. The below visual provides a simplified overview. Full details are provided in the operational blueprint in Annex 1. This discusses how each solution should be designed for each level of operations, presented in a standard format describing the solution, who will be using it, how it will function and what service provider type and basic steps are recommended to implement it.

THE USDC STABLECOIN

As noted in section 4.1, for all solutions described USDC is the primary digital asset used for several reasons.

- It is MiCA-compliant.
- Its interoperability across blockchains ensures that users have maximum flexibility in choosing service providers.
- It is highly transparent, because a live and public record of US dollar currency and equivalent asset reserves backing USDC is published monthly by Circle, the stablecoin issuer.[44]
- It is effectively a digital equivalent of the US dollar, the primary currency used by humanitarian operations in Syria and widely accepted as the main medium of exchange.

In short, USDC is not only most likely to be compliant with existing regulatory frameworks governing crypto assets across jurisdictions. It is also most likely to satisfy donor compliance requirements, a major concern for humanitarian organisations. That said, research and service providers suggest that USDT, a fully decentralised stablecoin, is the most widely used in Syria despite not being MiCA-compliant.

This suggests that stakeholders involved in digital fund transfers may choose to swap USDC for USDT for further transactions within Syria. Given its liquidity and availability on a number of blockchains, USDT is likely to be accessible on most digital wallets in Syria, allowing third parties to acquire it independently of humanitarian transactions that will be in USDC.

KEY POINTS

- In each solution, the chosen blockchain infrastructure is important but mostly invisible to users, functioning as a behind-the-scenes layer that powers the system.
- The solutions described are organised around three levels of humanitarian aid flows: **HQ level, country level and field/programme level.**
- **It is assumed that USDC is used for all solutions described** because it is most likely to be compliant with regulatory frameworks governing crypto assets across jurisdictions, and also most likely to satisfy donor compliance requirements.

[44] Circle, *Transparency and stability*, undated.

4.5 CHALLENGES AND RISKS

4.5.1 REGULATIONS AND COMPLIANCE

If an organisation uses a regulated service provider, it's generally safe to convert money from a bank account into stablecoins and send it to a digital wallet owned by the organisation or a trusted partner. Some people believe that cryptocurrencies are illegal, but this is not true in many places where humanitarian organisations operate.

The EU, for example has clear regulations such as MiCA. Just like any other service, organisations need to carefully check each provider's licenses, compliance standards and regulatory status. There are currently no clear laws on crypto assets in Syria, but this could change, especially as local institutions have begun exploring ways to regulate cryptocurrencies and digitise the Syrian pound.[45]

4.5.2 ORGANISATIONAL INNOVATION

The bureaucratic nature particular to international humanitarian organisations can create challenges when changing processes. That is a standard part of organisational innovation. Stablecoins and digital wallets should be qualified as financial tools, similar to fiat currencies and bank accounts. Ensuring that the use of these systems aligns with internal organisational processes, such as procurement and approval responsibilities and timeframes, should be planned into the process of exploring the use of these tools.

Staff should be ready to review existing processes and adapt them as needed to comply with organisational practice. A country office payment request form may be modified to create a crypto-payment request that includes fields for key information such as the CASP name, type of stablecoin and digital wallet address for deposit.

Adopting new ways of working can seem difficult because of a lack of clarity or information. Organisational change can also fail as a result of a lack of ownership and endorsement by decision makers. A key factor in successful organisational innovation is the use of "nudges" and the provision of "behavioural enablers" who are openly endorsed by senior management teams to improve acceptance and adoption.[46] This may include:

- Communicating the objectives and goals of the change in processes.
- The creation of standard operating procedures (SOPs) and/or organisational guidelines ideally issued or owned by treasury or other senior management.
- Encouragement of key staff to participate in service provider interviews and live demonstrations to better understand how the new systems work.
- Providing training to staff involved in using the tools.
- Making learning opportunities available to other curious staff, which can ease concerns and increase confidence in adopting new approaches.
- Considering the recruitment of specialists with deeper knowledge of blockchain ecosystems, service providers and cryptocurrencies to advise on key steps in implementing new processes.

KEY TAKEAWAYS

- Just like the procurement of any other service, organisations need to carefully **check each provider's licenses, compliance standards and regulatory status.**
- **There are currently no clear laws about crypto assets in Syria**, but this could change, especially as local institutions have begun exploring ways to regulate cryptocurrencies and digitise the Syrian pound.
- **Stablecoins and digital wallets should be qualified as financial tools, similar to fiat currencies and bank accounts.** Ensuring that the use of these systems aligns with internal organisational processes, such as procurement and approval responsibilities and timeframes, should be planned into the process of exploring the use of these tools.

[45] OneSafe, *Syria's Bitcoin Initiative: Implications for Global Crypto Banking Landscape*, January 2025.

[46] Harvard Business Review, *Breaking Down Barriers to Innovation*, March 2020.

5 CONCLUSION AND RECOMMENDATIONS

5.1 HARNESSING CRYPTO ASSETS FOR HUMANITARIAN ASSISTANCE IN SYRIA

The use of crypto assets presents a significant opportunity to overcome longstanding challenges in delivering humanitarian assistance in Syria. Limited banking access, rampant inflation, currency instability and low financial inclusion continue to obstruct the timely transfer of funds. When carefully designed and deployed, crypto assets can help to mitigate these constraints. Importantly, they offer a potential solution to the problem of cross-border derisking.

Humanitarian operations in Syria often require coordination among organisations and financial systems that lack mutual trust and access to shared data. Digital-asset technologies can provide transparent, verifiable and secure transaction records, helping to rebuild trust across the chain and enabling greater financial access.

The convergence of three important factors – technological maturity, the emergence of enabling regulatory frameworks and increasing pressure from shrinking aid budgets – makes this a timely and viable moment to explore crypto assets as a tool for humanitarian finance. The commitment to financial inclusion further strengthens the case for their adoption.

The humanitarian sector, however, has been slow to build collective knowledge and institutional readiness for these technologies. This knowledge gap has constrained the scaling of promising pilots, even in settings such as Syria where the need is urgent and the case for use clear.

Recent developments, such as the initial easing of some restrictive measures on Syria, create new openings. These policy shifts offer the potential for economic recovery, infrastructure investment and gradual financial sector revitalisation. Change will be incremental. It will take time for the chilling effect of sanctions and restrictive measures to subside, and for banks and the private sector to shift from perceiving Syria as a risk to seeing it as a viable investment environment.

Digital asset solutions are already being used in Syria. They are not a panacea, but carefully governed FinTech solutions offer humanitarian

organisations a pathway to building more resilient, transparent and inclusive financial ecosystems, especially in crisis-affected and unbanked areas.

This paper serves as a resource for the humanitarian and donor community by providing a basic introduction to digital asset technologies, presenting a clear case for their use and offering an overview of tools and solutions. It identifies the most appropriate technologies for the setting, outlines key risk factors and highlights considerations in terms of compliance with applicable laws, regulations and humanitarian principles.

5.2 RECOMMENDATIONS

The following general recommendations emerged from the findings of this research:

1

Invest in clear collective guidance for the sector, recognising that a failed pilot can significantly damage donor perception and any potential uptake. The risk is highest when organisations and staff are not well informed about the technologies involved and compliant options. Organisations currently rely heavily for guidance on service providers, which may prioritise customer onboarding, highlighting the need for neutral, sector-wide support.

2

As a sector, discuss the current regulatory environment and donor policies on the use of digital asset technologies with donors and governments. Donors should permit their use when the sector is left with few other options as a result of bank derisking, financial access restrictions or liquidity constraints.

3

Blockchain is a workaround, not an answer to the problem. We should continue to seek to facilitate humanitarian transfers with traditional banking institutions and financial regulators. We still need banks to facilitate these transactions. The smooth transfer of humanitarian funds through the traditional banking system remains the go-to option for many organisations.

THE FOLLOWING RECOMMENDATIONS ARE FOR CONSIDERATION AND ACTION BY THE SPECIFIED STAKEHOLDERS:

HUMANITARIAN ORGANISATIONS AND CASH COORDINATION PLATFORMS

Humanitarian organisation senior management groups

- Verify the regulations governing blockchains and crypto assets in your organisation's primary jurisdiction. There is often a misconception that the use of these technologies is illegal, but most regulators in the Americas and Europe, and a growing number in Asia and the Middle East have established frameworks that permit and govern and the use of crypto assets and blockchains.
- Explore the use of these technologies in regions where your organisation experiences financial access issues, and analyse if there is a case for them to be integrated as a tool in your treasury department.
- Ensure pilots and initiatives using crypto assets are documented and shared with other NGOs to spread learning.
- Work with other organisations on the development of policy governing the use of these technologies to ensure clear procedures are in place for staff.

Cash coordination platforms

Global cash coordination platforms and in-country Cash Working Groups (CWGs) should ensure that any consideration or use of crypto assets within humanitarian programming includes:

- Structured learning and knowledge-sharing components, enabling global and country-level actors to build a shared understanding of relevant technologies and to develop practical skills for design, implementation, and risk management.

- Strong localisation commitments, including engagement with and investment in the national FinTech and digital payments ecosystem, to avoid parallel systems and strengthen local capacity.

- Context-specific analysis of DeFi applications, such as blockchain-based solutions, to assess whether and how they could support continuity of payments, financial access, and the early recovery or resilience of the national financial sector.

- Dedicated resources and technical support for coordination leadership, including funding, guidance, and training for global platform leads and CWG chairs to enable informed facilitation, oversight, and peer learning.

FINTECH COMPANIES WANTING TO WORK WITH THE HUMANITARIAN SECTOR

- Support humanitarian organisations in developing well-documented risk assessments for use when looking at FinTech solutions for programming.

- Communicate the extent to which FinTech solutions are compliant with current regulations and focus on risks associated with specific donor requirements and programme audits.

- Ensure user-centred design processes. Thoroughly evaluate humanitarian organisations as a primary user of the technology, in addition to end users such as staff and beneficiaries. Humanitarian organisations often have financial processes and management requirements that may need to be adapted to the use of new technologies.

DONORS AND TECHNICAL BODIES

- Allow humanitarian organisations to use digital currencies for cross-border and domestic payments when they are left with few other options as a result of bank derisking, financial access restrictions or liquidity constraints.

- To facilitate consistency and mitigate risks, donors should work together to develop a shared position on the safe and effective use of digital currencies, with the aim of aligning policies and approaches across institutions.

- Put clear policies and procedures in place to facilitate organisations' timely use of digital currencies, given the urgent nature of humanitarian programming.

- Consider allocating support for coordination mechanisms that pool organisations' knowledge of using digital currencies in rapidly changing settings, and work towards maximising cost-effectiveness and managing risks effectively.

- Technical bodies supporting the new Syrian government in the recovery of the country's financial infrastructure should ensure the regulation of crypto assets is a key workstream to integrate the uptake of the technology into the official financial system.

- Ensure the MSP community is consulted as part of the rebuilding of Syria's financial sector. MSPs have provided the Syrian population with basic financial services at a time when it has effectively been debanked.

POOLED FUNDS

- Explore how the use of digital currencies can improve pooled-fund impact, traceability and reporting.

- Where relevant allow organisations to use digital currencies, recognising that they face varying levels of financial access as a result of differences in banking relationships and registration status.

- Consider the development of a policy on their use to provide partners with clarity.

ANNEX 1

OPERATIONAL BLUEPRINT: STABLECOINS FOR HUMANITARIAN ORGANISATIONS

This technical annex outlines a practical roadmap for organisations wishing to explore the use of stablecoins and digital wallets at the HQ, country and field/programme level. It includes guidance on the allocation of responsibilities at each operational layer, the required infrastructure, relationships with service providers and a typical flow of funds.

Before implementing this approach, organisations should conduct a thorough internal risk assessment to evaluate whether and how digital asset solutions align with their operational landscape. This includes identifying key pain points and cases for use, using the main report above as a reference framework. Given the wide variation in organisational structures, legal and regulatory obligations, donor and compliance requirements and risk appetites, this annex is not intended as a one-size-fits-all SOP. Rather, it provides a blueprint that should be adapted to fit each organisation's needs and compliance frameworks.

Three tables are included in this section, each corresponding to a different level of operations:

1. **The HQ-level table** outlines requirements and actions related to institutional readiness, digital asset acquisition, compliance and custody setup.
2. **The country-level table** provides guidance on wallet management, fund receipt, internal controls, partner engagement and reporting systems.
3. **The field/programme-level table** focuses on field-level payment mechanisms, recipient interfacing, risk mitigation and reconciliation practices.

The fund flow used for this blueprint follows this path:

1. **Donor → NGO HQ** in fiat currency
2. **NGO HQ → Digital** exchange or stablecoin issuer: Fiat is converted into stablecoins such as USDC
3. **NGO HQ → NGO** country office wallet: Stablecoins are sent on-chain
4. **NGO country office → Local implementers/ vendors/recipients:** On-chain transfers or off-ramping via local providers if needed.

1. FOR HQ

This HQ-level section is intended to answer the question: how can humanitarian organisations access stablecoins and other digital currencies? Over the course of this research, stakeholders repeatedly expressed a need for guidance in this area.

SOLUTION: USE A CRYPTO-ASSET SERVICE PROVIDER

Crypto-asset service providers (CASPs) are readily available in the EU, North America, the Middle East and Asia. They offer retail and institutional services for large organisations and other institutional customers seeking a straightforward and non-technical way to convert fiat currency into crypto assets to store, invest, send and receive funds compliantly.

There are two types of CASP that humanitarian organisations may choose to use: crypto custody and brokerage firms, and cryptocurrency exchanges. This paper recommends the first option, assuming most organisations are new to blockchain technology and need a more flexible, hands-on service with advisory support for staff still learning about it. These providers also tend to have existing relationships with stablecoin issuers, a partnership that may otherwise be difficult for organisations to secure. Their services are, however, likely to be more costly in the short term than using a cryptocurrency exchange.

- **Crypto custody and brokerage firms (recommended)** provide advisory services and often an online portal where funds from a bank account can be converted into crypto assets and currencies. They also invest and trade crypto assets on their customers' behalf, similar to a traditional brokerage firm. Services include "white glove" accompaniment and other bespoke services that clients can tailor. Fees are charged according to the services provided and typically include a monthly payment.

For humanitarian organisations, CASPs would not focus significantly on investment or trading. Rather, they would provide services such as:

- **Acquiring stablecoins:** Converting fiat currency received from an organisation into USDC or another stablecoin.
- **Holding stablecoins:** Taking custody of stablecoins on behalf of an organisation to avoid the complications and extra work of creating one or more crypto-wallets.
- **Stablecoin management:** Executing orders from one or more authorised parties within an organisation to send stablecoins to the digital wallets of one or more designated recipients.
- **Accounting:** Maintaining an auditable transaction record, including the time, date, number and volume of stablecoin transactions.

ADDRESSING PAIN POINTS: WHY IS IT USEFUL?

The pain points addressed at HQ level primarily relate to the initial cross-border transfer of funds to country or programme teams. The solutions below remove costly intermediaries, and transactions are near instant, excepting any internal processes required for approval, accountability and a clear audit trail. They also improve compliance by keeping funds under the control of the organisation or a regulated provider from origin to destination, considered the most derisked part of the humanitarian funds flow.

Humanitarian organisations should view these HQ-level actions as the core organisational infrastructure or backbone needed to use cryptocurrencies safely in programmes. Once set up for Syria, the same infrastructure can also be used for other problematic and derisked jurisdictions, such as Myanmar and Venezuela.

IMPLEMENTATION: WHO DOES WHAT?

Approval and coordination at HQ level is needed across all teams that have a decision-making role in opening bank accounts, service provider procurement, and approving/coordinating outgoing payments to country teams. As with all organisational changes, there must be a designated lead to coordinate the process and ensure accountability across the stakeholders involved. The table below lists key users/teams and the roles required to support the process, acknowledging that the roles may vary from one organisation to another.

Table 1: Who does what? HQ-level stakeholders

User	Role in organisation	Actions
TREASURY	**Senior staff responsible for opening bank accounts and managing balances**	Approve/select service provider
		Manage/approve movement of fiat funds from bank to CASP for stablecoin conversion
		Admin access/use of CASP online portal/interface
		Oversee/confirm deposit of stablecoins in digital wallet
		Manage/approve onward transfer of funds to country-level digital wallet
		And/or approve country-team access to digital wallet if a shared wallet is used
FINANCE	**Senior staff responsible for approving and documenting movement of funds to country of operation. May also include accounts payable.**	Approve country-office request for stablecoins (at US dollar transfer value). This may for be a one-off payment or monthly cashflow.
		Confirm stablecoin deposit in wallet via online portal
		Log transactions on accounting platform, or instruct staff to do so.
		Monitor/approve all outgoing transactions from country-level digital wallet
PROCUREMENT	**Senior staff responsible for managing contracts with financial service providers**	Issue tender for CASPs
		Selection/vetting of CASPs
		Negotiate terms and fees
		Review/execute contract with CASPs and digital wallet provider (see next)
		Create vendor in procurement/customer relationship management (CRM) system

KEY TAKEAWAYS

- Humanitarian organisations should view these HQ-level actions as the core organisational infrastructure or backbone needed to use cryptocurrencies safely in programmes. Once set up it can be used in other jurisdictions.
- Using cryptocurrencies as a solution at the HQ-level creates an alternative payment channel, preventing blocked or suspended transactions and onerous due diligence linked to derisking.
- Using cryptocurrencies improves traceability and reduces transfer costs and counterparty risks by cutting out intermediaries in third-party jurisdictions and avoiding fees for routing funds through secondary bank accounts.

2. FOR COUNTRY TEAMS

Country teams are responsible for secondary country-level transactions with suppliers, staff, local partners and beneficiaries. They experience pain points at two levels: blocks and delays in receiving funds, and high overheads for sending funds for operational transactions such as supplier payments and salaries and for programme-related transactions such as partner payments and cash distributions.

SOLUTION: USE DIGITAL WALLETS

A digital wallet, also known as a crypto-wallet, is the mechanism by which a country team would receive and access stablecoin funds sent from HQ. This might involve designated country staff accessing a wallet controlled by HQ, or the country office managing its own wallet, similar to a bank account. Organisations could consider a scenario where HQ owns and operates one digital wallet at the HQ level, and the country team owns and operates another wallet at the field/programme level. This also ensures better compliance in aligning wallets with the jurisdiction in which they are being operated.

WHAT TYPE OF DIGITAL WALLET?

The digital wallets recommended for humanitarian organisations tend to fall into two categories:

1. **Decentralised wallets:** These give users full control of their cryptocurrency, with sole access to funds and private keys, similar to a bank account password. No third party can recover funds if the key is lost. This offers greater security and flexibility, but it also requires users to manage their wallets responsibly.

2. **Custodial wallets:** These are managed by a company that holds users' private keys, similar to a bank holding a customer's funds. They are easier to recover if passwords are lost, but require trust in the provider. Custodial wallets tend to be more expensive and less interoperable than decentralised ones.

The type of wallet that humanitarian organisations choose to use should be always subject to a research and vetting process to ensure they are accessible by the stakeholders that will use them to transact. Organisations may choose to use a mix of both types of wallet. Digital wallets, even custodial wallets, are extremely cheap to procure and maintain.

To provide some general guidance, organisations should consider using decentralised wallets if:

- There is a strong appetite for training staff and institutionalising skills and knowledge of how blockchains, cryptocurrencies and DeFi tools work.
- There are plans to adopt the use of stablecoins at scale for various purposes, such as payroll, receiving donations and programmes; and for high-volume transactions and across countries. This is because decentralised wallets are more secure and less prone to cyber-threats.
- There are strong organisational procedures to govern wallet and key management, especially in high-turnover settings. There should also be clear protocols for handling faulty transactions, because decentralised wallet transfers cannot be reversed.

Organisations should consider using custodial wallets if:

- Key staff are unfamiliar with the technology and unlikely to learn because of feasibility constraints such as lack of time and/or resources or high staff turnover.
- There may a need to claw back or reallocate funds, such as unused project budget balances or grants to partners. Custodial wallet providers have control over the movement of funds between wallets and can correct and/or reverse transactions.
- A number of users need access to a single wallet. Custodial wallets often provide tiered access permissions to determine who can view, access or use them to make transactions, and to limit transaction amounts. This is also possible with decentralised wallets, but the burden is on the organisation to learn the skills to do so securely and responsibly.

A vital consideration in the selection of digital wallets is access – who needs it, from where and how? An internationally available digital wallet, for example, may be more appropriate for HQ users who work in a single language and have good access to the internet and smartphones. Local wallet providers, in contrast, are almost always better suited to country-level use by non-senior staff, partners, suppliers and beneficiaries. Local wallets are discussed in field/programme level section below.

ADDRESSING PAIN POINTS: WHY IS IT USEFUL?

It has long been established that it is necessary and useful to have access to alternative transfer mechanisms that bypass the international banking system and more specifically the correspondent banking system. Hence the frequent use of MSPs as intermediaries.[47]

The use of DeFi technologies addresses a multitude of pain points for a variety of country-level users:

- Country teams, local partners and beneficiaries can effectively use digital wallets in the same way as bank accounts, but without using a bank. This shields transactions from the effects of derisking.

[47] NRC, *Humanitarian Organisations' Use of Money Service Providers*, April 2025.

- Transaction size doesn't matter because costs are low irrespective of the amounts involved, meaning that users can cash out funds incrementally as appropriate based on security and liquidity risks.
- Unlike bank transfers, digital wallet transactions are borderless. As stablecoins are procured and sent from HQ level, cross-border transfers are cheap, easy and fast.
- USDC stablecoins held in country-level wallets help to stabilise grant and transfer values, and offer the same protection against currency volatility to staff, local partners and cash-programme beneficiaries.
- Transfers are instant, traceable and direct, removing the cost and need for cash handling by a number of intermediaries.

IMPLEMENTATION: WHO DOES WHAT?

The main variations at the country level are dependent on the organization size, type, and it's own internal policies. There are also variations between workflows: (a) approvals to make a transaction; and (b) user access required to enter and monitor information required to initiate the transaction. For (a), there may be differences in the assignment of approval and decision-making roles. . Approval of transaction using stablecoins, regardless of the type of digital wallet or service used, should still follow the sector standard with country-level approval matrices or delegation of authority rules, for example with a country director approving a digital wallet transaction.

An additional scenario (b) to consider involves programme-level staff in approvals and tasks requiring direct wallet access to initiate transactions (such as enrolling participants in a CVA program), rather than approvals for making the transactions themselves. It is also possible that procurement staff may require involvement, for example if suppliers agree or request to be paid in stablecoin, the procurement focal point is best placed to ensure service agreements reflect this arrangement, and can collect information on the digital wallet of the provider (in lieu of a bank account number) in order to initiate a transaction for a Country Director to approve. **In all cases, staff at country level should expect to access the digital wallet platform via smartphone, tablet, or desktop, similar to other users in the organization.**

Table 2: Who does what? Country-level stakeholders

User	Role in organisation	Actions
FINANCE	**Senior finance staff responsible for approving and documenting movement of funds at country level**	Approve country-office request for stablecoins (at US dollar transfer value). This may for be a one-off payment or monthly cashflow.
		Verify transaction request - stablecoin type and wallet details
		Confirm stablecoin deposit in wallet via online portal
		Log transactions on accounting platform or instruct staff to do so
		Monitor/approve all outgoing transactions from country-level digital wallet at country level
PROCUREMENT	**Senior staff responsible for managing contracts with financial service providers**	Issue tender for digital wallet provider if necessary
		Selection/vetting of CASPs
		Negotiate terms and fees
		Review/execute contract with CASPs and digital wallet provider (see next)
		Create vendor in procurement/CRM system
PROGRAMMES	**Senior programme staff responsible for related payment and cashflow requests and payments to local partners and cash programmes**	Raise payment request specifying stablecoin amount and send to finance
		Work with wallet provider to support enrolment and access for programme users
		Upload/manage programme-user details in digital wallet payment management interface/online portal
		Disburse programme-level payments of authorised amounts using digital wallet payment management interface/online portal
		Monitor/approve wallet balances of programme-level users to ensure funds received and track spending

KEY TAKEAWAYS

- A digital wallet, also known as a crypto-wallet, is the mechanism by which a country team would receive and access stablecoin funds sent from HQ.
- A vital consideration in the selection of digital wallets is access – who needs it, from where and how?
- Decentralised wallets are ideal for organisations with a strong desire to train staff, use stablecoins at scale and ensure security, while custodial wallets are better suited for organisations with staff unfamiliar with the technology, and/or the need to recover funds or have multi-user access with tiered permission.

3. FOR IMPLEMENTERS

Using stablecoins for last-mile payments concerns field-level implementation, particularly of CVA programmes. It can also extend to other uses, such as tracking in-kind distributions, digital financial inclusion programming, paying staff, purchasing goods from local suppliers and disbursing grants to partners. CVA is used as the primary example because it is characterised by a key tension that complicates humanitarian organisations' work in Syria and other complex jurisdictions: it is broadly adopted, but also the most problematic from a derisking and cash handling perspective.

Years of evidence show that CVA is by far the most cost-efficient and effective programme type. Yet they and multi-purpose cash approaches (MPCAs) specifically have amplified the impacts of derisking, because banks and other financial stakeholders consider them the highest risk transactions. This perspective was reinforced throughout the consultations with financial institutions for this research.

SOLUTION: LOCAL WALLETS

Local wallets are best adapted to the local setting and the diversity of users in that setting, including programme beneficiaries. Local wallet providers, such as those currently operating in Syria (see page 34), offer the most suitable interfaces. They can be used in the local language, making them easier to understand.

They can also be accessed via unstructured supplementary service data (USSD), which is similar to SMS, for users who don't have smartphones. They are designed to work even in areas with low internet connection or offline. Transactions are shown in the local currency, making them more familiar for users, and the local provider offers customer support.

Most importantly, local wallet providers have already developed their own country-level liquidity networks, making cashing out possible through channels that users are familiar with. For humanitarian organisations, local providers are also motivated to expand liquidity networks to support large-scale operations and high-volume transactions, because both wallet and liquidity providers benefit from fees and commissions. These costs, however, tend to be consistently lower than for other transaction types.

WHICH LOCAL WALLET TYPES AND PROVIDERS ARE SUITABLE FOR CVA?

Local wallet providers in Syria offer products that can be used for MCPAs. The choice of which wallet should depending on the programme design and monitoring needs, but they can be grouped into the two categories discussed below. There are also international digital voucher services operating in Syria that are blockchain-based and can feasibly integrate the use of stablecoins, similar to the Oxfam examples earlier in this paper.

The categories below are not technical or formal terms, but are intended to enhance understanding of how digital wallets can be used at the field level:

1. **General-use wallets:** These are the most widely accessible type of digital wallet. They are not specifically designed for cash programmes, and they are fully owned by the individual. They can be used for personal

purposes such as earning income or receiving remittances. They are also more flexible for organisations to use beyond programmes, for operational purposes such as payroll. They have the following characteristics:

- They require a smartphone and connectivity to make payments.
- They allow for bulk disbursements. Organisations can make and manage stablecoin disbursements to any number of individual wallets for any purpose.
- They are anonymised. Disbursements are only identified by phone number or wallet address, with no personal data accessible to the organisation or sender. This enhances data privacy and security, but it limits the platform's ability to automate processes such as participant monitoring and detailed reporting.
- They are relatively cheap.
- They are more decentralised and available to the public, and can be opened, accessed and kept indefinitely by the user.

❷ **Programme-adapted wallets:** These wallets have specific features designed for implementing and monitoring CVA programmes, but they also share features with general-use wallets and the custodial wallets described in the country-level section above. Features include:

- **Users without smartphones:** To accommodate field-level programme participants without smartphones, digital payment cards and QR codes are available. These are tethered to a digital wallet on the blockchain and can be used to pay for goods digitally or cash out funds at liquidity points similar to ATMs.
- **Offline functionality:** The wallets can be used to make payments when connectivity is unavailable, an advantage in remote field sites that lack connectivity, or where connectivity is expensive.
- **Enhanced monitoring:** The wallets have a custodial aspect, allowing individual data to be linked to each wallet, visible to the organisation via an online interface. This enables monitoring of household trends, such as spending patterns by gender and transaction patterns over time, including the percentage of cash entitlement spent.
- **Transaction controls:** The wallets have specific controls in place for organisations that have to meet stringent donor and audit compliance obligations. They include the ability to set limits on transaction amounts, restrict transactions to specific “whitelisted” wallets, such as those of programme beneficiaries, and reverse transactions in case of fraud, error or the scaling back of programmes.
- **More costly:** The service providers for these wallets can help with training staff and beneficiaries, supporting pilot design and implementation and managing custodial functions. This increases costs for the organisation, but it doesn’t usually affect end users.
- **Bulk disbursement:** The majority of digital wallet solutions used in humanitarian contexts today also include bulk disbursement functionality, and are relatively easy to adapt to multi-purpose cash payments or payroll.

Bulk disbursement function is especially important for humanitarian organisations to understand, because programme staff are likely to be the primary users of these interfaces. They are easily accessible online via a laptop or desktop, making them the primary in-office tool that programme staff will use.

Bulk disbursement platforms work in a very similar way to digital voucher platforms such as Red Rose and Genius Tags. Beneficiary data can be uploaded via spreadsheets, and wallets can be generated for beneficiaries directly from the dashboard, potentially pre-empting the need to be physically present. A bulk disbursement platform also allows a number of staff members to interact with the organisations' stablecoin, and user permissions can be set to limit who can and cannot disburse funds or view specific data.

ADDRESSING PAIN POINTS: WHY IS IT USEFUL?

The pain points addressed at the HQ and country levels also apply to the field/programme level. Humanitarian organisations and programme participants at the field level are affected by upstream problems related to derisking. The impacts are indirect but their consequences are far more severe, because they translate into delays and even the suspension of lifesaving interventions. These pain points are not discussed again here. In terms of those felt directly by programme-level stakeholders, the use of digital wallets addresses two major issues:

- **High risk and cost of MSP transactions:** The use of digital wallets eliminates direct transactions with MSPs, because payments are digitised and only cashed out at the participant level. This reduces MSP intermediaries, fees and compliance requirements. MSPs can still provide cash-out services directly to participants, but they are no longer involved in the initial payment process.

- **Cash-handling risks:** Digital wallets eliminate the security risks involved in cash delivery at field sites, because funds are transferred directly from the organisation to beneficiaries.

Digital wallets offer other general benefits over and above addressing the pain points discussed above. The Myanmar case study shows that cost savings lead directly to increased coverage and number of households assisted, allowing organisations to deliver more for less. Digital wallets are of particular benefit in Syria, given that rebuilding accessible financial systems will take years even with sanctions easing. They also allow users to save US dollars securely at a time of hyperinflation.

Using digital payments can help markets to become more resilient by lowering costs associated with accessing dollars, especially when liquidity is scarce or difficult to obtain. For organisations integrating digital tools into cash programmes, providing smartphones and digital wallets supports both payments and savings, improving financial inclusion.

Digital wallets also have the potential to support financial autonomy. They are fully owned by individuals and immutable because they are built on the blockchain. As such they offer lasting benefits that extend beyond the end of programmes. Owners can continue to use them to earn income, receive remittances, hold household funds securely and interact with other digital assets. In short, digital wallets give people direct control over their money, unlike banks.

IMPLEMENTATION: WHO DOES WHAT?

The main stakeholders involved in putting digital wallets to use at the field level are programme staff and others with whom funds are exchanged as part of programme activities: local implementing partners, beneficiary households and MSPs in or near field sites. Programme staff functions are mainly focused on bulk disbursement and monitoring from the country-level digital wallet.

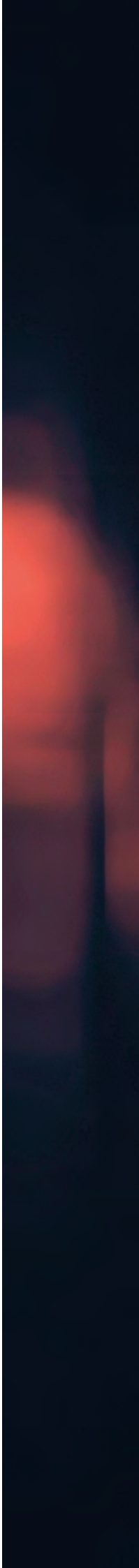
There is also coordination involved in working with digital wallet providers to identify implementing partners, beneficiary households and MSPs that may need to be onboarded to ensure funds can be sent, received and cashed out. Implementing partners, beneficiary households and MSPs will interact directly with their own digital wallets on a smartphone, feature phone or using a payment card. Although organisations are not responsible for this, MSPs are likely to work on their own with the digital wallet provider to set up liquidity channels, such as cashing in to a bank account or cashing out at another MSP.

Table 3: Who does what? Field/programme-level stakeholders

User	Role in organisation	Actions
INTERNAL USERS		
FINANCE	**Senior finance staff responsible for approving and documenting movement of funds at country level**	Assign user access levels for bulk disbursement functions according to delegation of authority/approval matrix
		Initiate and approve bulk disbursements
		Verify transaction request - stablecoin type and wallet details
		Log transactions on accounting platform or instruct staff to do so
		Confirm, monitor and approve all outgoing transactions from country-level digital wallet via online portal
PROGRAMMES	**Senior programme staff responsible for program level payments, monitoring staff**	Identify programme participants including local merchants if digital spending is expected. Recommend trusted MSPs in programme areas for cash-out services.
		Raise payment requests specifying total CVA distribution amount in stablecoin, including distribution schedule
		Work with wallet provider to support enrolment and access for programme users
		Verify which digital devices programme participants will be using - smartphone, feature phone or card/QR code
		Upload/manage distribution lists in digital wallet bulk payment management interface/ online portal
		Initiate and/or approve monthly disbursements using digital wallet bulk payment management interface/online portal
		Access bulk disbursement interface to monitor spending trends and wallet balances of programme users, including data export if needed
		Coordinate with digital wallet service provider to identify, onboard and train programme participants and if necessary MSPs
EXTERNAL USERS		
PROGRAMME PARTICIPANTS	**Local implementing partners, beneficiary households or businesses**	Attend training and user-testing sessions
		Complete KYC/onboarding with service provider
		Install digital wallet application on personal device
		Check balances and receipt of funds on distribution dates
		Pay for goods digitally at merchants that accept stablecoins
		Contact identified MSPs for cash out when needed
MSP	**Informal and formal money transfer agents**	Complete KYC and onboarding with digital service provider
		Negotiate fees and commissions with service provider
		Attend training and user-testing sessions
		Install digital wallet application on personal device
		Receive stablecoin payments from programme participants in exchange for cash
		Pay for goods digitally if desired
		Work with service provider to integrate personal cash-out channels such as bank or mobile money accounts

KEY TAKEAWAYS

- **CVA programmes and MPCAs have an increased risk of being impacted by derisking,** because banks and financial institutions see them as high-risk. Local digital wallets address this issue by bypassing the traditional financial system altogether.
- **General-use wallets are flexible, low-cost and privately owned by individuals, suitable for personal and non-humanitarian uses.** They require smartphones and connectivity, and have limited monitoring and reporting features.
- **Programme-adapted wallets are specifically designed for humanitarian programmes**, offering offline functionality, enhanced monitoring and transaction controls. They support users without smartphones. They are more costly as result of additional features and support, but provide better tracking and compliance.
- **Digital wallets offer lasting benefits after a programme finishes.** Owners can continue to use them to earn income, receive remittances, hold household funds securely and interact with other digital assets.



NORWEGIAN
REFUGEE COUNCIL