ADAN, CryptoUK, GDF Report

CASP TRAVEL RULE APPLICATION:
KEY CHALLENGES AND PUBLIC/ PRIVATE SECTOR SOLUTIONS

I. Executive Summary

Current complexities to meet travel rule standards raise significant concerns among CASPs, affecting their ability to ensure compliance while potentially diminishing the competitiveness of their services.

Ahead of the 31st July deadline, the industry aims for meaningful engagement with national and European regulators and supervisors to achieve immediate compliance improvement.

The aim of this paper is thus to outline a genuine intention from the industry to work together on overcoming the perceived challenges and finding the best solutions to be achievable.

In this paper, the industry outlines the current main obstacles CASPs face and proposes a set of recommendations as transitional measures. However, the industry remains fully open to finding the best way to achieve the travel rule objectives, to prevent erosion of compliance standards, and to avoid undermining the responsible growth of our industry.

Adan, Global Digital Finance, and CryptoUK represent industry players active in Europe and other jurisdictions. Through this wide initiative, we aim to ensure broad discussions within the industry to achieve effective implementation and alignment globally.

Introduction:

- **History of the Travel Rule: The Challenges with Blanket Application**
- **Interoperability: A Persistent Hurdle Requiring Transitional Flexibility**
- **Self-Hosted Wallets: Challenges with Ownership Verification**
- **Counterparty Due Diligence: Misalignment of Expectations**
- **Fragmentation: A Complex Landscape in Need of Future Harmonisation**

We are concerned that as implemented, the current framework may create operational bottlenecks, incentivize regulatory arbitrage, and could inadvertently stifle legitimate innovation within the EU's digital asset ecosystem. We would also note that there are also ongoing interoperability issues across Travel Rule solution providers and the complex application of self-hosted wallet (SHW) verification requirements.

This report sets out the historical context of Travel Rule regulation, the challenges with a direct application to the cryptoasset industry, and how these challenges can be solved with a risk-adjusted and phased approach to implementation.

Surveyed CASPs and member firms who engaged urge the European Commission, the European Banking Authority (EBA), and the National Competent Authorities (NCAs) to consider the following key recommendations:

Near Term Recommendations

1. **Extension of the transitional deadline** (currently July 31, 2025) to July 31, 2026 to accommodate persistent interoperability hurdles that continue to challenge full technical compliance and allow sufficient time for CASPs and travel rule solution providers to complete initiatives currently underway aimed at solving these issues.

2. **Establishing a permanent public-private Working Group**, comprising European regulators, national enforcement authorities, and industry representatives, to jointly identify the challenges that obliged entities are facing and agree and coordinate risk mitigants that could support a phased approach to compliance with requirements. The joint trades and their members feel that this will ensure that the Travel Rule framework remains both robust in its purpose and workable in implementation, enhancing AML/CFT outcomes while allowing sustainable digital asset innovation in the EU.

Self-Hosted Wallet Specific Recommendations

3. **Suggesting a transitional regime to full enforcement of provisions pertaining to the verification of SHW' ownership** suggest oversight on a "best efforts" basis. This ensures that CASPs would still be expected to conduct core due diligence and exercise due care, promoting overall integrity without imposing disproportionate burdens that may

drive activity underground or to unregulated platforms and could inadvertently stifle legitimate innovation within the EU's digital asset ecosystem.

4. **Taking a risk-based approach to SHW obligations.** CASPs propose prioritising a risk-based approach to SHW ownership verification and mitigating AML/CFT risks. Specifically, industry calls to clarify that the regulatory expectations regarding transactions exceeding EUR 1,000 between CASPs and third-party SHW do not include any legal obligation to perform wallet ownership/control or identity verification obligations, as those are not prescribed by the Level I text of the TFR.

Counterparty Due Diligence

5. **The EU should support the development of a harmonised and publicly accessible register of licensed CASPs to facilitate basic verification and risk assessment across jurisdictions, reducing reliance on direct outreach and case-by-case inquiries.**

Forward Looking & Ongoing Recommendations

6. **Encouraging the NCAs and European Authorities to ensure legal consistency in the application of these rules** and to utilize the established Working Group, as proposed, to facilitate coordinated and cohesive enforcement. Differing interpretations of the TFR rules by NCAsand CASPs can pose significant challenges to regulatory coherence and consistency across the European Union. This divergence undermines the fundamental objective of the norm, which is shaped in a regulation precisely to establish a harmonized framework and oversight of crypto-assets.

The following report discusses each of these recommendations while also proposing initial steps towards solving these challenges. The proposed adjustments are designed to ensure that the Travel Rule framework remains both robust in intent and practical in implementation while also strengthening anti-money laundering (AML) and counter-terrorist financing (CFT) outcomes while supporting sustainable digital asset innovation in the EU. The associations remain united, and supportive of the EU authorities and the Financial Action Task Force (FATF) in achieving their objectives and remain committed to continuing to work towards these aims.

II. History of the Travel Rule: The Challenges with Blanket Application

FATF first introduced the Travel Rule in 2012 as part of its Recommendations aimed at strengthening global AML/CFT frameworks. The requirement, formally captured in today's Recommendation 16, mandates that financial institutions collect, retain, and transmit specific information about the originator and beneficiary of wire transfers. This rule was originally designed with the traditional financial system in mind, particularly interbank wire transfers conducted via centralized networks such as SWIFT, where both originator and beneficiary institutions are identifiable, regulated entities operating within clear jurisdictional perimeters.

In June 2019, FATF extended the applicability of the Travel Rule to virtual asset service providers (VASPs)[1], recognizing the growing use of cryptoassets for value transfer. While this update was well-intentioned and consistent with the FATF's "same risk, same regulation" principle, its application to the cryptoasset ecosystem has presented significant technical and operational challenges. Unlike traditional finance, the cryptoasset sector is characterized by open, decentralized networks, pseudonymous transactions, and the common use of SHW, elements that fundamentally challenge the assumptions embedded in the original Travel Rule architecture. The associations and their members broadly support the objectives of the Travel Rule; however, industry has observed that there are significant challenges with the blanket adoption of the Travel Rule to the cryptoasset sector.

One of the most critical issues lies in the absence of standardized messaging protocols and interoperable infrastructure across CASPs. In traditional finance, the widespread adoption of the SWIFT messaging system and similar platforms enables financial institutions to transmit Travel Rule information reliably. No such universally adopted system yet exists in the cryptoasset space. While multiple technical solutions have emerged, such as the InterVASP Messaging Standard (IVMS101), TRISA, the Transaction Authorization Protocol (TAP) and OpenVASP, some of these frameworks are still evolving to achieve seamless interoperability across jurisdictions, particularly within the EU where NCAs interpret obligations differently, and no system has secured universal adoption yet .

Moreover, the direct application of Travel Rule requirements to cryptoasset transactions involving SHWs poses additional complications. Unlike transfers between regulated CASPs, where both parties are subject to supervisory oversight and AML/CFT obligations, transactions with SHWs involve counterparties that are not subject to equivalent regulatory scrutiny. This asymmetry makes it challenging in many contexts for CASPs to obtain originator and beneficiary information with certainty. The FATF's guidance acknowledges this complexity and encourages a risk-based approach, including the use of additional data sources and blockchain analytics where appropriate. However, the EU's current implementation of the TFR lacks sufficient clarity on these points, leading to divergent practices and, in some cases, overly conservative compliance strategies such as prohibiting certain transactions altogether.

Applying the Travel Rule without regard to the unique characteristics of crypto asset markets risks undermining the efficacy of AML/CFT efforts while also impeding innovation. Rigid enforcement timelines, inconsistent supervisory interpretations, and insufficient transitional frameworks may drive legitimate activity away from regulated environments, weakening visibility into financial flows. In this context, a phased and risk-adjusted implementation, grounded in technical realities and aligned with FATF's flexible, principle-based standards, is essential to balance regulatory objectives with the operational viability of the cryptoasset ecosystem.

The following sections discuss each of the key challenges with the current approach in depth and aim to suggest potential solutions to mitigate the issues currently posed to the industry.

[1] Noting VASPSs will be referred to as CASPs throughout this paper, as applied in an EU context.

III. Interoperability: A Persistent Hurdle Requiring Transitional Flexibility

At this stage in its evolution the digital asset ecosystem remains fragmented across competing Travel Rule protocols. These protocols employ different technical approaches and cover varying sets of CASPs, with no standardized data transmission protocols between them as of yet. This lack of interoperability poses a major obstacle to seamless information exchange and undermines effective compliance, which could be mitigated with the support of open-source standards by vendors.

This lack of interoperability has been acknowledged in FATF's Targeted Updates published in 2023 and 2024.

This fragmentation also makes it difficult to distinguish between CASPs that are non-compliant and those that are making best-effort compliance attempts using non-interoperable systems thus making the determination and reporting of 'repeatedly failing' CASPs extremely challenging. In Adan's recent survey, CASPs outlined that they often prioritize selecting solutions that provide the greatest reach to other CASPs, including interoperability with the greatest number of protocols to ensure effective communication, minimize transactional disruptions, and ensure a seamless user experience.

CASPs and protocol operators are engaged in productive efforts to address these challenges, but meaningful implementation will take time. We would note that this industry is still nascent, and while rapidly evolving, a phased approach to implementing and enforcing requirements will be beneficial in encouraging high standards across the ecosystem, while also giving industry the time it needs to develop best practice and embed them across all protocols and CASPs.

The EBA itself acknowledges this reality, noting that "not all are interoperable, which means CASPs might have to use multiple systems." However, surveyed CASPs and association member firms emphasized that this approach introduces several prohibitive complications including:

- *Operational burden:* Running multiple systems is resource-intensive and unsustainable,
- *Technical complexity:* Integration of different protocols can destabilize internal systems and require significant development effort, and
- *Increased costs:* The operational costs associated with onboarding multiple solutions are significant. Maintaining multiple systems disproportionately affects smaller CASPs, limiting their competitiveness.

Furthermore, such an approach places the full burden of solving interoperability gaps on CASPs alone which is a disproportionate and inequitable expectation.

The period between the regulation's application date (December 30, 2024) and the end of the transitional period foreseen in the EBA guidelines (July 31, 2025) appears to inadvertently underestimate the operational strain created by this fragmentation. The post-December 2024 rise in transaction volumes only compounds the issue.

Recommendation 1: Surveyed CASPs advocate extending the transitional deadline to July 31, 2026. This extension is not a dilution of AML/CFT safeguards, but a pragmatic step that would:

- Provide time for ongoing interoperability solutions to mature;
- Enable scalable system development for cross-protocol data exchange, through open-source standards; and
- Avoid operational paralysis or non-compliance driven by unrealistic technical constraints.

Industry stakeholders note that such an extension aligns with the intent behind the original transitional period in the long term and would contribute to achieving a robust, scalable compliance framework.

Recommendation 2: The industry also advocates for establishing a permanent public-private Working Group, comprising European regulators, national enforcement authorities, and industry representatives, to jointly identify the challenges that obliged entities are facing and agree and coordinate risk mitigants that could support a phased approach to compliance with requirements.

CASPs broadly support the foundational objectives of the TFR and the EBA Travel Rule Guidelines. However, as explained in this document, CASPs encounter significant systemic hurdles in implementing the Travel Rule Regulation. These are not simply firm-level compliance obstacles but represent industry-wide structural barriers that, if unaddressed, risk undermining the regulation's objectives.

The Working Group would support coordinating efforts among all relevant actors, including solution providers, to ensure that the Travel Rule framework remains both robust in intent and practical in implementation, leveraging open standards to guarantee cross-vendor interoperability, strengthening AML/CFT outcomes while supporting sustainable digital asset innovation in the EU.

IV. Self-Hosted Wallets: Challenges with Ownership Verification

In the case of transfers to or from a SHW, CASPs should collect information on both the originator and the beneficiary (Art. 14(1)). Furthermore, Regulation (EU) 2023/1113 imposes heightened requirements for transfers exceeding EUR 1,000 involving SHW, mandating Originator CASPs to verify that the address is controlled by the originator (Art. 14(5)) and Beneficiary CASPs to verify that the address is controlled by the beneficiary (Art. 16(2)). This provision reflects regulatory concern around the potential misuse of SHW for illicit activities.

It is important to note that, in certain cases, a SHW may not be controlled by the CASP's customer but by a third party. Some market participants interpret the EBA Guidelines as effectively extending the measures applicable to first-party transfers under the TFR to third-party transfers exceeding EUR 1,000, even though such requirements are not explicitly stated in the TFR text. Under this interpretation, two main challenges arise:

1. Verifying the ownership of the wallet, as the CASP may not have a direct relationship with the third party; and
2. Identifying the third party itself, for the same reason.

Ultimately, obtaining all the necessary information relies heavily on the good faith of both the customer and, eventually, on the third party willing to disclose the required data.

The insufficiency of verification processes often results in CASPs banning transfers, as it seems unreasonable for a third party to disclose personal information to a CASP that is not their service provider. Additionally, it is inefficient and impractical to allocate resources for onboarding and know your customer (KYC) procedures for third parties who are not clients of the CASP.

The EBA guidelines may be interpreted to indicate that there is an obligation to conduct further verification procedures, particularly those related to identity checks. Hence, the lack of such procedures could attract scrutiny during inspections if authorities find them necessary. This challenge dissuades CASPs from engaging in this type of transfer, ultimately leading to potential business losses and undermining transaction intel (end-customers instead transfer funds to their personal wallets and then to the intended recipient, effectively bypassing any controls the CASP could reasonably apply to third-party transactions).

The EBA Guidelines outline several non-exhaustive ownership verification methods, including cryptographic signatures, small deposit tests, and attended/unattended remote verification. While we welcome that CASPs are free to use other methods beyond the EBA Guidelines, CASPs emphasize that:

- Not all technical methods are possible/effective across all asset types, (e.g., wallet ownership on UTXO-based chains like Bitcoin cannot be accurately verified by Satoshi tests); and
- Manual processes are not scalable and pose operational risks.

These concerns were consistently raised during the EBA's public consultation (Nov 2023 – Feb 2024).

Rigid application of ownership verification introduces excessive friction for legitimate users and potentially driving activity offshore. Likewise, CASPs have begun to automatically ban these types of transfers altogether. This ultimately diminishes the rigorous KYC verification and monitoring mechanisms that are foundational to AML efforts.

According to this report's survey, transactions involving third-party-controlled SHW present a significant difficulty for CASPs, with 90% of surveyed CASPs reporting challenges in gathering the information and establishing the ownership. A poor user experience can lead to a notable shift towards peer-to-peer (P2P) transfer methods to bypass the complex and time-consuming procedures.

The regulation itself, including Recital 44, highlights the importance of a risk-based approach—yet all currently listed methods presuppose direct ownership verification. This prescriptive stance risks overshadowing more proportionate, outcome-oriented approaches.

Recommendation 3: As a transitional measure, CASPs suggest a de-prioritization of the supervision and enforcement of provisions pertaining to the verification of third-party SHWs' ownership and suggest oversight on a "best efforts" basis.

In practice, this approach still mandates responsible and proactive practices by CASPs without reducing accountability frameworks.

The approach would aim for pragmatism and a responsible way to manage risks effectively. CASPs are still committed to upholding high standards of integrity and combating financial crime. This entails implementing robust due diligence internal policies and procedures specifically designed to address risks associated with SHW transactions; defining clear criteria for identifying and assessing ML/TF risks; continuing to promptly file SARs/STRs whenever suspicious activity is detected and providing evidence of policy implementation to demonstrate to authorities that their policies and necessary set-ups for "best efforts" oversight are genuinely implemented and operational.

Therefore, this ensures that CASPs would still be expected to conduct core due diligence and exercise due care, promoting overall integrity without imposing disproportionate burdens that may drive activity underground or to unregulated platforms and could inadvertently stifle legitimate innovation within the EU's digital asset ecosystem.

This flexible approach encourages responsible and proactive practices. To transition from a "best efforts" framework to something measurable and consistent across the industry, the previously working group is the ideal mechanism to jointly identify ''best practices''.

In parallel, CASPs propose a risk-based approach to SHW ownership verification and mitigating AML/CFT risks. We believe that this, coupled with analytics tools which can support risk management, can meet regulatory objectives with regards to SHW transfers while also implementing high standards for risk mitigation.

Recommendation 4: CASPs propose prioritising a risk-based approach to SHW ownership verification and mitigating AML/CFT risks. Specifically, industry recommends clarifying that the regulatory expectations regarding transactions exceeding EUR 1,000 between CASPs and third-party SHWs do not include any legal obligation to perform wallet ownership/control or identity verification obligations, as those are not prescribed by the Level I text of the TFR.

Further expanding on the need for this recommendation, industry specifically supports a clarification of the EBA guidelines where if the SHW is owned or controlled by a third party who is not a customer of the CASP, the requirements from Article 19a of Directive (EU) 2015/849 apply. We would encourage the explicit clarification that a risk-based approach to identity verification is deemed to be fulfilled by collecting additional information from other sources (e.g., blockchain analytics, third-party data, verifiable credentials, or recognized authorities' data) or using other suitable means to ensure the originator/beneficiary's identity is known - should be adopted by CASPs on a risk-based basis.

Currently, the disconnection between the texts of the EBA Guidelines and the level I of the TFR is leading to different interpretations both from market players and supervisors. Given the ambiguity, some CASPs are opting to prohibit these transfers when that's an unintended consequence.

To accurately assess risk, CASPs can make use of powerful tools such as blockchain analytics[2]. When, through those tools, the risk is deemed low, CASPs can then have more confidence in relying on the customer's self-declaration that they control the wallet. When high risks are detected, CASPs should verify wallet ownership via a suitable method, like verifiable credentials attesting to KYC compliance from other regulated banking institutions, that is both appropriate and proportionate to the risk.

This approach is already embraced in jurisdictions such as the UK and aligns with Recital 17 of the Travel Rule Regulation, which takes a more outcomes focused and risk based, principles approach to SHW ownership verification and risk assessment.

Regulatory guidance supporting a risk-based approach to SHW would be widely supported by industry, would encourage adoption of technology-driven compliance practices and implementation of tools which can support firms in a compliance first approach, while still taking a proportionate and risk-based approach to meeting regulatory objectives.

[2] Analytics tools, when coupled with appropriate internal governance and risk assessment methodology can offer:

- Enhanced risk assessment: Real-time transaction monitoring and pattern recognition;
- Scalability: Automated processing of large volumes of on-chain data;
- Efficiency: Reduced manual intervention and faster compliance;
- Traceability: Improved visibility into transaction paths and counterparty risk.

V. Counterparty Due Diligence: Misalignment of Expectations

A core challenge with the EU's implementation of counterparty due diligence (CDD) requirements is that CASPs struggle to verify whether a counterparty is properly licensed or registered, owing to the lack of consistent, publicly accessible registers across jurisdictions. Furthermore, assessing adherence to AML/CTF obligations is often only possible through direct engagement, which is not scalable given the sheer number of counterparties and the rapid, cross-border nature of digital asset transactions.

These limitations are magnified by the presence of unregulated or under-regulated entities, making it exceedingly difficult to determine potential exposure to illicit finance or sanctioned actors.

Local transposition of FATF requirements adds to these challenges, as some jurisdictions have opted not to incorporate certain requirements in their version of the Travel Rule. Even when counterparty due diligence is required, there are divergent approaches in how thoroughly this due diligence is applied, with FATF explicitly stating that CVDD (R.16) "is distinct from the obligations applicable to cross-border correspondent relationships" (R. 13), while jurisdictions like the EU cite the "ongoing and repetitive" nature of the relationship to determine that they constitute a type of correspondent relationship.

In practice, this has resulted in some jurisdictions not including such analogous EU requirements in their version of the Travel Rule, leading to variations in how the CVDD is applied.

The FATF acknowledged this issue in its June 2023 Targeted Update, observing that VASPs face significant difficulties conducting effective due diligence on other VASPs.

In response, firms have developed pragmatic temporary solutions such as:

- *Alternative address sourcing:* Asking clients to provide alternate CASP addresses that may be better known or more trusted.
- *Blacklist monitoring:* Maintaining lists of CASPs with which they do not transact, though enforcement is often manual given current solution limitations.
- *Client warnings:* Notifying clients about high-risk counterparties and advising them to avoid engagement.
- *SHW redirects:* Encouraging redirection of transactions to SHWs with pre-verification steps, delaying receipt until Travel Rule data is validated.

A due diligence practice is to send inquiries to unknown CASPs to verify certain information before processing transactions. While industry-led standardisation efforts are underway, including templates supported by industry associations, there remains a high degree of fragmentation. Without a consistent template, each CASP and depending on the jurisdiction, may require different information or display it in various formats, making the evaluation process more complicated and lengthy. Jurisdictions differ in what data is required, how it is displayed, and the legal interpretation of what constitutes a sufficient CDD process.

Recommendation 5: The EU should support and promote the development of a harmonised and publicly accessible register of licensed VASPs to facilitate basic verification and enhance the risk assessment across jurisdictions, reducing reliance on direct outreach and case-by-case inquiries.

VI. Fragmentation: A Complex Landscape in Need of Future Harmonisation

Another significant challenge faced by CASPs is the fragmented global landscape of travel rule implementation. Jurisdictions may establish different distinct de minimis thresholds, as well as differing requirements for the originator and beneficiary data that must be collected and transferred, or different counterparty due diligence requirements. Consequently, CASPs encounter challenges in data-sharing with counterparts in regions where such regulations are not yet in effect or possess divergent requirements. Before sharing Travel Rule data, CASPs must establish legal basis and asymmetrical regulatory requirements across jurisdictions complicate this process.

On the one hand, two counterparties operating in jurisdictions that do not impose similar obligations under their travel rule regimes may be less inclined or unable to voluntarily share the required information for lack of legal basis.

For example, if a jurisdiction fails to fully align its Travel Rule regulation to FATF Recommendation 16 or has weak privacy or data protection laws, it becomes challenging or impossible to complete a full two-way Travel Rule exercise. In the Oct 2021 Guidance, the FATF prescribed the need for the originator VASP to assess the counterparty VASP's ability to receive and protect the data (paragraphs 199 onward), and if compliance is genuinely impossible, to apply strong risk mitigations, which could be several actions, including refusing the transaction. Without these enhanced risk mitigation measures in place (which need to have been previously accepted by the regulator), the transaction should not take place. Currently, such a mechanism does not exist in the EU—a gap that is especially significant given the strict GDPR requirements concerning data transfers outside the EU.

This could be a future consideration for clarification by the European regulator.

On the other hand, the design of travel rule protocols often reflects jurisdiction-specific needs. These gaps in regulatory alignment have a knock-on effect on the interoperability of travel rule protocols used by CASPs, particularly when a protocol has been developed for the needs of a specific jurisdiction.

This necessitates the adoption of risk mitigation strategies and may inadvertently foster the development of fragmented, jurisdiction-specific compliance solutions, thereby underscoring the critical need for globally harmonized and interoperable travel rule protocols to facilitate efficient and compliant cross-border virtual asset transfers. Some CASPs have opted to forbid transactions outside the EU as a result despite unfavourable liquidity (thus global competitiveness) consequences.

VII. Policy Recommendations and Collaborative Path Forward

To ensure that the Travel Rule framework is both effective and future-proof, Adan, GDF and CryptoUK reiterates the recommendations from the surveyed CASPs:

Near Term Recommendations

1. Extension of the transitional deadline

2. Establishing a permanent public-private Working Group

SHW Specific Recommendations

3. Suggesting a transitional regime to full enforcement of provisions pertaining to the verification of SHWs' ownership

4. Taking a risk-based approach to SHW obligations

Counterparty Due Diligence

5. The EU should support and promote the development of a harmonised and publicly accessible register of licensed VASPs to facilitate basic verification and enhance the risk assessment across jurisdictions, reducing reliance on direct outreach and case-by-case inquiries.

Forward Looking & Ongoing Recommendations

6. Encouraging the NCAs and European Authorities to ensure legal consistency in the application of these rules

The EU has an opportunity to lead in shaping the future of crypto regulation by embracing pragmatic, innovation-friendly policies. An inflexible implementation risks driving legitimate actors offshore, diminishing EU oversight, and weakening AML/CFT outcomes. A balanced approach ensures compliance is effective and sustainable.

Effective implementation of the EU Travel Rule is essential for combating illicit finance in the digital asset sector. However, current challenges—particularly those related to interoperability and SHW verification—demand pragmatic policy adjustments.

By implementing the above recommendations and working collaboratively across the public and private sector to mitigate pressing risks, the EU can build a regulatory framework that is both robust and adaptable. This will ensure that the fight against financial crime is not only effective but also compatible with innovation, growth, and the responsible evolution of the digital economy in the Union.

The collective associations and their memberships stand ready to work in close partnership with the European Commission, the EBA, national competent authorities, and fellow stakeholders to refine and implement a workable, forward-looking Travel Rule framework.

ADAN

CryptoUK

GDF GLOBAL DIGITAL FINANCE

CONTACT ADAN:

w: www.adan.eu

@adan_asso

Adan

CONTACT CRYPTOUK:

w: www.cryptouk.io

@CryptoUKAssoc

CryptoUK

CONTACT GDF:

e: hello@gdf.io

w: www.gdf.io

@GlobalDigitalFi

Global Digital Finance