Cardano Foundation

9 October 2024

Bank for International Settlements (BIS)
Centralbahnplatz 2
CH-4002 Basel

Submitted via online form on BIS' website
(https://www.bis.org/bcbs/commentupload.htm)

Subject: BIS consultation on principles for the sound management of third-party risk

Dear Madam or Sir,

We appreciate the Basel Committee issuing updated outsourcing principles for banks and welcome the opportunity to provide comments in the respective public consultation.

The Cardano Foundation is an independent Swiss not-for-profit organization that oversees and supervises the advancement of the public, permissionless blockchain protocol Cardano and its ecosystem. As the custodian of the protocol and the owner of the Cardano brand, the Foundation works to drive adoption and partnerships, grow the wider blockchain community, shape legislation, and commercial standards, and ensure stakeholder accountability.

Kindly find our comments below. We would gladly address any follow-up questions or contribute to further discussions with the BIS.

Yours sincerely,

Nicolas Jacquemart

CLO, Dr. iur.
Cardano Foundation
nicolas.jacquemart@cardanofoundation.org

1 Operational resilience and technological neutrality

Operational resilience is not only paramount for financial institutions and their infrastructure, but for any type of critical infrastructure in this digital age. It is our conviction that decentralized and open-access digital infrastructures such as public permissionless blockchains (hereinafter "decentralized infrastructures"), when utilized correctly, have the potential to materially mitigate key risks faced in the financial market today. The Cardano Foundation advocates for an open, non-discriminatory and proportionate regulatory approach, allowing the implementation of technological solutions irrespective of their architecture.

All infrastructure architectures come with trade-offs. A diverse and resilient financial market leaves it to the financial institutions to assess respective costs and benefits, mitigate risks, and ultimately decide on what best fulfills their business requirements. Applicable regulatory regimes should ensure appropriate compliance and risk management standards are upheld, but should refrain from preemptively constraining financial institutions' architectural choices (i.e. remain technologically neutral). We believe the current draft principles for the sound management of third-party risk (hereinafter the "Third-Party Risk Principles") unduly favor legacy (i.e. centralized and permissioned) architectures in a number of ways. If adopted in their current form, this outcome would stand in contrast to the BIS' stated objectives of improving the operational resilience and risk management of financial institutions.

In the following, we will lay out (i) some of the key advantages of decentralized infrastructures, (ii) the implications of the suggested counterparty-centric risk management standards and (iii) the Cardano Foundation's recommendations on how to create a more technologically neutral framework for third party risk management.

2 Key advantages of decentralized infrastructures

Decentralized architectures have an untapped potential to increase the resilience of, and therefore trust in, financial institutions and the financial market at large. In particular, we would like to draw your attention to the following key advantages.

2.1 Avoidance of single-entity dependencies and vendor lock-in

Decentralized infrastructures, such as Cardano, can avoid or at least significantly reduce two key risks in the current third party service provider landscape of financial institutions. Firstly, due to their decentralized data processing model, they decrease single-entity dependencies for infrastructure operation. Secondly, they can significantly reduce or even outright avoid vendor lock-in (e.g. gatekeeping through proprietary technologies). Given the ever-increasing

concentration of cost-competitive cloud computing services in the hands of only three (!) large providers[1], reducing these exposures should be a key goal of any standard setting work. While we acknowledge that decentralized infrastructures can come with their own dependencies (e.g. open source community dependency, governance dependencies), their decentralized nature generally disincentivizes concentrations of power by distributing responsibilities among operators. As has been shown by infrastructures such as Cardano, this can create remarkably resilient, reliable and adaptable digital infrastructures.[2]

2.2 Increased resilience through decentralization

By distributing data processing, control and other infrastructure functions across a multitude of nodes in a network, a decentralized system can be designed to be overall more secure, reliable and resilient than a centrally controlled alternative. Mature infrastructures with a decentralized architecture achieve service level metrics that can compete with or outperform legacy digital infrastructures. Reliance on a trusted third party is replaced with distributed redundancy and fault-tolerant data processing spread across a global network.

2.3 Transparency and auditability

Decentralized infrastructures allow for enhanced data assurance and auditability by providing a tamper-proof, participant-immutable ledger containing all transactions. This enables real-time data assurance, cuts down on reconciliation costs and risks, and significantly reduces the reliance on and effort required by information intermediaries such as auditors. This can reduce operating overhead, boost financial institution competitiveness and lower consumer costs. So-called scaling solutions, such as zero-knowledge proofs, simultaneously allow for cryptographically secured limitations on data disclosure, in line with regulatory requirements.

2.4 Composability and open source development

Decentralized infrastructures provide for composability, i.e. their capabilities can be selected and assembled in various combinations to satisfy specific financial institution requirements. This offers financial institutions more flexibility and choice in how to approach outsourcing, can reduce switching costs, and fosters infrastructure competition and innovation. Because development takes place in an open source environment, financial institutions and regulators have more visibility on future developments (and hence risks) and much more opportunity to exercise

[1] As per Q1 2024, Amazon AWS holds 31%, Microsoft Azure holds 25%, and Google Cloud holds 10% of global market share in cloud infrastructure according to Statista's data, published 21 May 2024.

[2] For instance, the Cardano network is maintained by a diverse set of participants, geographically as well as in terms of operators and providers used (see e.g. Cardano Blockchain Insights here and here); furthermore, the Cardano network has since inception in 2017 worked without any interruption boasting 100% uptime, while sustaining ongoing transaction activity as well as continuously adapting and increasing transaction diversity (see e.g. Transaction History here).

influence over infrastructure development. This applies particularly to small and midsized banks that typically have very limited leverage with cloud providers.

2.5 Lower barriers to entry and reduction of cost

Decentralized infrastructures allow for significantly lower barriers to entry, allowing a much wider range of participants to utilize it and contribute to its operation. This simultaneously increases the operational resilience of the infrastructure through further distribution. Reducing the number of intermediaries through peer-to-peer interactions can significantly reduce the transaction costs and operational overhead for participants. Finally, decentralized infrastructures are an inherently cooperative model[3] that spreads the cost of maintaining the system across a broad base of participants, making it more cost-efficient to maintain, upgrade and scale in the long term.

3 Rethinking counterparty-centric risk management

At its core, the deficiencies in technological neutrality contained within the Third-Party Risk Principles stem from the explicit (and in many places implicit) requirement that services may only be provided by an identifiable counterparty. Financial institutions are expected to enter into specific formal arrangements regarding the outsourced functions with the third party service provider (henceforth “TPSP”). It is more likely than not[4] that this will effectively preclude financial institutions from relying on decentralized infrastructures for any material services they do not wish to run on premises, for the following reasons:

- Truly decentralized infrastructures do not and should not have a single controlling entity. Hence, there is no single available counterparty acting as a dedicated service provider to enter into a legal relationship with. Instead, because the software necessary to interact with and participate in the operation of the infrastructure is generally freely available, the operators of decentralized infrastructures are heterogeneous (e.g. private individuals, enthusiasts, professionals or companies). These participants do contribute to the data verification and consensus building. However, none of them individually can represent the performance characteristics of the entire infrastructure, nor assume this as a liability. Instead they are independent and redundant components of a network performing according to the defined technical parameters.

[3] It is worth noting that historically this was how some key financial market infrastructures were created: As a cooperation between large national financial institutions to achieve better market penetration and manage costs.

[4] While it is conceivable that national regulators could interpret the Third-Party Risk Principles to not apply to the utilization of decentralized infrastructures because of a lack of an outsourcing in the sense described therein (and some financial institutions have attempted this argument), we do not believe this would align with the clear intent of the standard.

- While certain services associated with decentralized infrastructures may therefore be available from an entity that would qualify as a TPSP (e.g. monitoring of a decentralized infrastructure, running a set of infrastructure nodes), the operation of a decentralized infrastructure is the product of an only loosely associated collective. For this "service", no TPSP that would satisfy the Third-Party Risk Principles is available.

- This lack of a centralized counterparty is an intentional design feature of decentralized infrastructures. For centralized legacy systems, a financial institution must rely on a TPSP and formal legal arrangement to ensure a system functions as promised, is maintained properly, and – if not – to assign relevant liability. In decentralized infrastructures, this reliance is shifted to the technical design and the attributes conveyed by decentralization and distribution. The associated risks are fundamentally different and can be suitably addressed with non-traditional mitigants (see below).

We argue that adequate and technologically neutral TPSP risk management principles should not require the allocation of legal obligations and liability to a specific counterparty via a formal arrangement in every service arrangement. Rather, they should ensure a financial institution's general ability to conduct an appropriate risk assessment and implement effective, holistic risk controls for the relevant risk characteristics. This also better aligns with the Committee's conclusion that neither the third-party life cycle nor the risks themselves behave in a linear progression.[5]

In the context of potential outsourcing to a decentralized infrastructure, a financial institution should still be required to determine and assess the risk environment in accordance with their risk strategy and appetite as per the proposed principles 1-3. However, instead of requiring the allocation of identified risks to an (unavailable) single counterparty, the financial institution **should be able to mitigate the applicable risks through the sum of alternative suitable measures** (see illustrative examples below). This approach would create a significantly more proportionate and technologically neutral outsourcing framework. Whether or not decentralized infrastructures are competitive with centralized ones will be left up to market forces, allowing for infrastructure competition on a level playing field.

The alternative risk mitigation measures could consist of a combination of the following non-exhaustive elements, the requirements of which can be further calibrated to the materiality of an outsourcing arrangement.

[5] Cf. p.5, no. 14 et seq of the Consultation Document.

3.1 Assessing infrastructure design and code base

Financial institutions should evaluate the technological foundations of the decentralized infrastructure and participate, or contract a third party to participate, in its maintenance. Rather than relying on a contractual counterparty for the operation of the infrastructure, the verification of the design and code base are crucial. The focus should be on evaluating the integrity of the architecture and its ability to meet operational and security requirements. Such evaluations ensure that material risks are addressed at the design and technology level in lieu of dependance on contractual obligations of a TPSP.

3.2 Collective risk assurance

While there might not be one single entity acting as a legal counterparty and assuming liability for the system overall, anchor groups of participants – such as professional node operators, and key technical developers – often play important roles in maintaining and securing decentralized infrastructures. While these participants do not have centralized control authority, they may contribute to essential components of the infrastructure's reliability, security, and operational resilience (e.g. network monitoring).

Financial institutions can leverage these anchor groups by conducting targeted due diligence on relevant actors who meet specific criteria for technical competence, reliability, and alignment with institutional risk standards. For example, professional node operators can be assessed based on their operational track record, infrastructure robustness, and capacity to contribute to the network's security. Technical developers can be evaluated for their role in decision-making processes, their accountability mechanisms, and their contributions to the continuous development and maintenance of the infrastructure.

By identifying and selecting a group of these contributors, financial institutions can form a risk management framework based on a collective assurance model, where different participants together provide sufficient coverage to mitigate potential risks. This approach allows institutions to conduct due diligence on specific, identifiable actors within the decentralized network who carry out critical tasks, thereby offering a level of risk assurance comparable to traditional outsourcing models, even in the absence of a single counterparty. Furthermore, to the extent feasible, financial institutions could also enter into agreements or formal partnerships with selected members of these anchor groups to further mitigate identified risks.

3.3 Financial institutions as infrastructure participants

Rather than relying entirely on third-party participants, financial institutions could choose to actively participate in the operation of the decentralized infrastructure, for example, by running

nodes, contributing to open source development, or engaging in the infrastructure's governance processes. This provides financial institutions a proactive risk management tool and enhances their oversight when outsourcing to a decentralized infrastructure.

This direct involvement provides institutions with several advantages, such as:

- **Enhanced control and oversight**: By operating a node, financial institutions gain direct access to the infrastructure's real-time data and operations, improving their ability to monitor transactions, ensure compliance with internal and external requirements, and manage risks. This reduces dependence on third-party service providers for critical information and offers greater transparency into performance and security.

- **Increased resilience and alignment with institutional needs**: Active participation in decentralized infrastructures enables financial institutions to contribute to the overall security and resilience of the network while shaping its evolution to align with their strategic priorities and risk management requirements. By running a node or engaging in protocol governance, institutions can influence key decisions regarding the system's operation, updates, and governance structures, ensuring that their interests – such as regulatory compliance, security, and operational efficiency – are represented. This involvement also distributes responsibility across an even wider network of participants, further mitigating operational risks.

- **Reducing third-party risks and maintaining internal expertise**: By actively participating in decentralized systems, financial institutions not only develop in-house expertise in blockchain technology, cryptography, and decentralized governance but also reduce reliance on third-party providers. This empowers institutions to assess risks more effectively and enhances decision-making.

4 Conclusion and Recommendations

The proposed Third-Party Risk Principles express a clear preference for traditional, centralized service models by assuming the presence of a single legal counterparty in all outsourcing arrangements. This assumption overlooks the inherent benefits of decentralized infrastructures which can significantly enhance operational resilience, security, and cost efficiency for financial institutions. By requiring a legal counterparty for every material outsourcing, the Third-Party Risk Principles effectively preclude decentralized infrastructures from being fully integrated into the financial system, limiting innovation and drawing into question the principle of technological neutrality.

Decentralized infrastructures present an opportunity to reimagine third-party risk management, leveraging technical design, distributed governance, and collective risk assurance models to mitigate risks without depending on a single counterparty. Financial institutions should have the flexibility to adopt decentralized technologies and utilize alternative risk management approaches that address the unique characteristics of these systems.

We propose to adjust the Third-Party Risk Principles, in particular the principles 3-6, making them more open, in order to reflect the following recommendations:

- **Adopting a truly technologically neutral approach**: The Third-Party Risk Principles should be revised to ensure that they do not inherently favor centralized architectures. Instead, they should allow financial institutions to assess and select the most appropriate technology based on their risk profile and operational needs, without being constrained by the need for a centralized service provider.

- **Allowing alternative risk management approaches**: Rather than relying solely on a counterparty-centric model, the regulatory framework should accommodate decentralized infrastructures by allowing financial institutions to implement alternative risk mitigation measures, such as rigorous code base assessments, collective risk assurance through anchor groups of participants, and direct participation in decentralized governance.

- **Enabling direct participation for risk mitigation**: Financial institutions should be encouraged to directly engage with decentralized infrastructures – through running nodes, contributing to governance, or supporting development – as a proactive approach to risk management. This would enhance transparency, control, and resilience while reducing reliance on third-party providers.

We are convinced that adopting a more proportionate, technologically neutral and flexible regulatory framework that accommodates the unique benefits of decentralized systems will result in more resilient, efficient and innovative financial institutions and markets.