GLOBAL DIGITAL FINANCE

SUBMITTED VIA EMAIL TO: fintech-innovation@acpr.banque-france.fr and innovation@amf-france.org

To whom it may concern,

Re: The ACPR-AMF Consultation on the Report of the Working group on Smart Contract Certification

About Global Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

The input to this response has been written and submitted on behalf of the GDF board.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail should that be beneficial as the ACPR and AMF continue their work.

Yours faithfully,
Elise Soucie – Executive Director – GDF

Response to the Public Consultation: Executive Summary

GDF is grateful for the opportunity to engage with the both the ACPR and AMF over the years.

Overall, GDF is supportive of the aim of Working Group on Smart Contract Certification to to explore the topic of smart contract certification, in the broader context of considerations around a future regulation of DeFi. We also support the groups high level principles of safety, governance, and service compliance which are aligned with the GDF mission to support best practice and high standards across digital finance markets.

GDF developed this response on behalf of our board and board advisors as part of our ongoing commitment to supporting the work of global regulators as they develop their regulatory frameworks, as well as the GDF mission to support the development of best practices and governance standards across the digital finance industry. We would also note that we support the response to this consultation put forward by our industry partners at Adan and the European Blockchain Association, and we aim to complement the points they have raised with our feedback.

The executive summary concisely summarizes our views on the specific drafting within the text. Our key points of our feedback are as follows:

1. **We encourage utilising existing technology and operational risk frameworks as a first step to mitigate smart contract risk; and**

2. **We support industry led best practice, combined with appropriate transparency rather than a top-down special regime.**

Response to the Consultation Questionnaire

GDF would note that last year we undertook a piece of work with the Global Financial Markets Association (GFMA) on responsible smart contract implementation. This Primer has informed our response to the consultation.

Q 1: Do you have any comments on the security principles set out in the document?

GDF believe that the security principles developed provide a solid basis for addressing security concerns. However, as noted in our Primer, rather than developing new security measures we would instead support the integration of established IT security frameworks (e.g., ISO 27001, NIST) that have been successfully applied across financial services. This approach ensures robust protection while avoiding duplication of efforts.

GDF believes that the primary objective of these principles should be to enhance transparency, ensure code quality, and mitigate operational risks. The scope should cover security testing, documentation, change management, and compliance with legal frameworks. Rather than reinventing the wheel, these elements should be integrated into established procedures already utilised within IT and financial risk management.

We would note the following best practice principles from the Primer[1] which can be directly applied to security principles, and have corresponding regulatory frameworks and guidance already in existence which can support their application to smart contracts:

- *Ensure smart contracts are written in clear, well-documented code that is easy to understand and audit*: Best practices in documentation should describe, for example: intended functionality of the application, what properties and invariants should be maintained under execution, controls, and cross-contract dependencies. A smart contract should have a clear scope and use regular naming conventions and in-line comments. This should also be captured in product documentation.
- *Extensively test smart contracts before deployment using various scenarios and stress tests*: This testing should include verifiable test coverage. Smart contract tests should methodically cover maximum existing use cases and functionalities to minimize unexpected and untested edge cases. Test coverage should also be transparent for both regulators and market participants.
- *Implement strong access controls to restrict who can modify or interact with the smart contract*: This should also include Privileged Access Management and firms should ensure that there are strong access controls for any privileged access or admin activity. This should also be captured in product documentation.
- *Integrate smart contracts with existing workflows with human intervention at critical points for added security:* This risk mitigation should also be streamlined with the test coverage principle noted above. Ideally, human intervention should be required whenever there is activity outside the test coverage. This should also include ledger security monitoring and alerting capabilities as well as a key management solution with appropriate cybersecurity and enforcement controls.

Q 2: Do you have any comments on the governance principles set out in the document?

GDF firmly agrees with the ACPR and AMF that robust governance is critical. However, rather than adopting a bespoke system, the certification process should incorporate existing IT and financial governance practices—such as change management, version control, and incident response protocols. These well-established methods already provide the operational rigor needed to ensure the integrity and resilience of smart contracts.

We would note the following best practice principles from the Primer[2] which can be directly applied to the governance principles, and have corresponding regulatory frameworks and guidance already in existence which can support their application to smart contracts:

- *Development and growth of internal risk and control or compliance function with appropriate resourcing:* Firms will need to consider how to develop and scale their internal operational risk and/or compliance departments to oversee, support and advise business lines with sufficient personnel to audit, maintain and upgrade any necessary coding issues. This will vary based on a firm's size, business model, and activities, proportionate to its business needs.

[1] See pages 19-29: https://www.gdf.io/wp-content/uploads/2020/12/gfma-gdf-smart-contract-primer-report-2024.pdf

[2] See pages 19-29: https://www.gdf.io/wp-content/uploads/2020/12/gfma-gdf-smart-contract-primer-report-2024.pdf

- *Have a clear and proportionate incident response mechanism/policy*: These policies should include how and what should be done once an incident starts, and firms should have a clear business continuity plan ("BCP") as well as an information and communication technology ("ICT") plan to minimize the damage, as well as appropriate steps in place to maintain the continuity of any smart contract supporting important business services. The following table includes examples of policies and best practices that can mitigate risk.
- *Standardized requirements for smart contract audits, including for completeness and robustness while working towards a template-based approach for broader smart contract standardization*: Such requirements should incorporate best practices that exist for smart contract auditing, and should promote transparency between regulators and market participants with respect to audit processes and outcomes.
- *Agreement of contractual obligations between relevant parties*: Firms should also consider how, particularly in respect of smart contracts that are used in the context of legal agreements between counterparties, to mitigate risks in smart contract integration through incorporation of certain provisions in legal contracts between the parties, to avoid legal ambiguities. In addition, the obligations on each party to an agreement to comply with applicable laws, rules and regulations (e.g., resolution regimes and related regulations such as qualified financial contract resolution stay rules in the US or the Bank Recovery and Resolution Directive (BRRD) in the EU, international sanctions, data protection legislation, etc.) should be clearly understood between the parties.
    - Dispute resolution mechanisms as well as procedures for complying with applicable laws, rules and regulations should be considered and put in place at the outset and initial coding of a smart contract, so that appropriate mechanisms are built into the system and the parties' regulatory obligations are appropriately addressed, as would be necessary for other types of transactions in regulated financial markets.
    - It is important to note, some smart contracts may only be used internally (e.g., in the case of Books and Records Smart Contracts), so dispute resolution mechanisms may not be relevant in all instances.
    - Furthermore, the risk assessment may be significantly minimized if smart contracts are only being used within private permissioned systems where a transactional issue may be more easily addressed, such as in the event of an error by the administrator. Where there may be a potential dispute between relevant counterparties to a smart contract, the parties' agreement could also mandate certain operational and technological mitigation strategies discussed in this Section, such as requiring pre-deployment code review including user acceptance testing and scenario testing, to identify code-specific issues.
    - An independent audit/verification of the smart contract code (see best practice previously set out) or a third-party oracle (where applicable), may help to ensure that execution error is minimized. Features like time locks, kill switches, fail safes, and monitoring may allow for real-time oversight to verify ongoing transactions according to the agreement, such as by checking the transaction values and data in ongoing transactions against values in the agreement.34 Both the underlying agreement and the smart contract code can also require that both parties use multi-signature authentication to prevent premature or inadvertent execution.

Q 3: Do you have any comments on the service compliance principles set out in the document?

GDF believes that given existing regulatory frameworks, a dedicated, top-down certification regime is not necessary. Instead, we would support adapting regulatory and risk management frameworks for the nuances of smart contracts. By extending current standards and practices to cover smart contract-specific risks, regulators and market participants can benefit from a flexible, risk-based approach that fosters responsible innovation while ensuring security and reliability and meeting regulatory objectives.

Q 4: Do you wish to comment on other aspects developed in part 1 of the document?

We would strongly support a voluntary approach, and as set out under 1.4 we would support in the first instance and optional certification, and in the second instance mandatory certification with proportionality measures. GDF believes that enabling industry participants to adapt an approach that is tailored to their business model and use of smart contracts enables market participants to demonstrate adherence to best practices without imposing a one-size-fits-all regulatory burden (which may not be appropriate or proportionate in certain instances). This approach encourages innovation and the adoption of robust risk management standards while remaining consistent with existing industry practices. It would also support industry in further implementing existing initiatives such as ERC-3643.

We acknowledge the potential drawbacks noted in the paper but would note that industry best practice across other areas of security, IT infrastructure, and cybersecurity are predominantly optional with much of industry adhering to the best practice needed for their firms. While there are mechanisms in place for regulators to review and benchmark firms (e.g., TIBER testing), we believe that with appropriate transparency around optional certification, industry would implement the best practices needed to meet regulatory outcomes.

Q 5: Do you have any comments or additions to make on the audit methods set out in part 2-1?

GDF agrees with the ACPR and AMF that third-party audits are a crucial element in ensuring compliance with established best practices and that it is important to provide independent validation of the smart contract's security and operational integrity. However, these audits should align with existing audit practices within the financial and IT sectors, serving as a complement to current frameworks. They should also be flexible enough, noting that no one type of audit would be appropriate across all types and uses of smart contracts.

As set out under Q2 we support *Standardized requirements for smart contract audits, including for completeness and robustness while working towards a template-based approach for broader smart contract standardization.*

GDF would note the following best practice[3] for smart contracts already being implemented across industry including:

- Audits should be undertaken by independent auditors with sufficient knowledge, skills and expertise in smart contracts and blockchain.
- Given the transparent nature of blockchain networks (including permissioned networks), it may be possible for certain audits to occur on an automated and constant basis, as opposed to taking place on a periodic basis.

[3] See page 24: https://www.gdf.io/wp-content/uploads/2020/12/gfma-gdf-smart-contract-primer-report-2024.pdf

- Where smart contract code is developed / provided / managed by third party providers, appropriate audit and access rights should be granted to financial entities and their regulators in the relevant vendor contracts.
- Firms can integrate international standards applicable to software more broadly, such as ISO/IEC 27001.
- Audits can also be conducted in line with smart contract-specific standards which may be developed by industry.30
- In addition to audits around software code, carry out audits relating to external data which feeds into the smart contract such as via data oracles, as well as audits on internal governance, risk controls and compliance functions around smart contract development and deployment processes.

We would also highlight that generally, a financial entity's ICT systems and processes would be audited on a periodic basis, particularly those that support critical business functions and operations. Given that smart contracts are designed to execute autonomously and may be used in combination with sensitive data, smart contract code should in particular be audited for security issues or errors.

Smart contracts may also consume off-chain data through external systems such as data oracles, which themselves may be susceptible to manipulation– appropriate auditing practices will therefore help to mitigate security and data accuracy risks in relation to such oracles.

Q 6: Do you have an opinion on the validity period of a certification?

GDF would support a risk-based approach to the validity period that is outcomes focused and principles based to account for the numerous uses cases and implementations that may exist for smart contracts. We would also support recertification being triggered by material changes in the smart contract's code, significant shifts in the operating environment, or the emergence of new vulnerabilities—not solely on a fixed, time-based schedule. Overall, we believe the certification process should incorporate a flexible, iterative review mechanism that draws on ongoing industry developments and stakeholder feedback. This dynamic approach aligns with the adaptive nature of existing IT and financial compliance reviews and would also future proof the regime.

Q7: Would you like to comment on other aspects developed in part 2 of the document?

We would note that while certification can enhance market confidence and reduce systemic risks, the implementation of such a regime should also conduct a cost benefit analysis. Furthermore, as noted in the consultation, this should take into account the proportionality provisions set out in MiCA. By leveraging existing frameworks, as set out throughout our response, rather than creating a parallel, specialized regime, costs are minimized. A voluntary, best-practice–driven approach could enable firms to gain the benefits of enhanced security and transparency while avoiding the operational and financial burdens of a top-down, mandatory certification process.

Q 8: Do you have any comments or remarks on the developments relating to the regulatory bases (objectives, scope, proportionality criteria, different possible regulatory schemes)?

We support the overarching regulatory objectives and are supportive of the outcomes that the ACPR and AMF seek to achieve. However, as noted throughout our response we would support these being worked towards in a way that utilises existing technology and operational risk frameworks as a first step to mitigate smart contract risk enables industry to work with the public sector to implement industry led best practice, combined with appropriate transparency rather than a top-down special regime. Overall, we support the regulatory objectives being achieved through the optional certification scheme combined with appropriate incentives to drive industry adoption and uptake.

Q 9: What is your opinion on the discussion developed in III-1.2.3 tending to reconcile the certification of protocols and that of the underlying smart contracts?

While we appreciate the aim of ensuring that the underlying protocol is secure and meets appropriate standards, we believe further consideration is needed as to what constitutes a 'protocol' in this sense. Additionally, in terms of certification, we would also raise a concern surrounding the audit of base layer ones such as the Ethereum or Bitcoin blockchain. First, we would raise a question as to the practical feasibility. For example, the requirement for firms to conduct due diligence, analyse, and detect any and all suspicious activities on "an underlying DLT", is in effect to mandate that a firm has supervision and risk management over the whole of the blockchain. GDF feels that this is neither proportionate, nor appropriate and instead encourages a focus on the certification, audit, and best practice being applied to the smart contracts within a firm's control and reasonable liability.

Overall, we would support ensuring that part of the audit process for smart contracts takes in to account the robustness of any other smart contract it interacts with as well as the robustness of the underlying base layers. To facilitate this, we would support a disclosure-based element of the final certification regime enabling greater transparency for the users of the smart contracts.

GDF believes that combining these approaches would mean that users are aware that the smart contracts don't operate in isolation, and that they have appropriate and proportionate transparency around specific risks (e.g., if there is a hard fork or attack on the underlying base layer, or oracle exploit, users would be aware that they could be at risk irrespective of whether the smart contract audit passed the audit.)

Q 10: Do you wish to comment on other aspects developed in part 3 of the document?

Overall, we support the development of industry led and governed solutions with appropriate transparency and visibility to both regulators and the wider private sector.