FORUM FINTECH ACPR-AMF

Summary of Responses to the Public Consultation of the ACPR-AMF Working Group on Smart Contract Certification – A Proposal for Smart Contract Certification: Overview, Technical Considerations and Regulatory Discussion Points

1. Introduction

On 3 February 2025, the working group on smart contract certification, established under the aegis of the ACPR-AMF Fintech Forum, published a report which was submitted for public consultation. This report presented the working group's reflections on technical considerations and regulatory issues raised by the question of certifying smart contracts, in anticipation of possible future regulation of decentralised finance (DeFi). Following its publication, the working group (WG) invited stakeholders to share their comments in order to inform and support this exploratory work.

The report aimed to examine the possibilities of certification and the modalities of auditing smart contracts, with a view to understanding how a certification mechanism could potentially be integrated into future regulatory frameworks. It initially identified principles of security, governance, and service compliance applicable to various smart contract execution environments. The report then explored audit practices and methods that could support a certification process, distinguishing between different approaches depending on the party attributing the certification: whether issued by a public authority on the basis of an audit conducted by an accredited body, whether issued by the auditor, or whether issued by the smart contract provider themselves through a mechanism of self-certification. Lastly, the report examined different possible regulatory approaches, including that of optional certification, mandatory certification for all smart contracts, or that of certification incorporating proportionality measures.

Following publication of the report, a number of responses were received to the questions submitted for consultation. This document seeks to offers a concise summary of the consultation responses provided, which sought to clarify certain technical aspects and added the reflections of the working group in this regard. The ACPR and the AMF wish to thank the respondents, and intend to continue discussions with them and the wider stakeholder community on these aspects.

As an important reminder, the report on smart contract certification reflects the work and discussions of the working group and, as such, neither constitutes a proposal for regulatory framework, nor an official position of the ACPR, the AMF, nor from any other authority that participated in the working group.

Structure of this Summary Document

This summary document provides an overview of the responses to the consultation, briefly outlining the profile of respondents, and follows the thematic structure adopted in the report. It first addresses the proposed principles for certification standards and the modalities for auditing smart contracts. It

then analyses the responses on regulatory reflections and the certification frameworks proposed in the report, before concluding with a discussion on the European and international regulatory context and future steps.

Analysis of Responses: Profile of Respondents

The ACPR-AMF working group received 20 responses to its report on smart contract certification. Respondents represented a diverse range of profiles, including actors linked to the DeFi ecosystem (project sponsors, foundations, or blockchain associations), centralised crypto-asset actors, traditional finance institutions, consulting and auditing firms, as well as other actors such as technology providers, industry associations focused on crypto-asset activities, and individual respondents.

The table below provides a breakdown of responses by respondent category:

Type of Actor	Representation by Type
DeFi participants	**10%**
Crypto (CeFi) participants	**5%**
Audit service providers	**15%**
Traditional finance actors	**5%**
Industry associations	**35%**
Technology providers	**15%**
Other	**15%**

The approach of the ACPR-AMF working group was widely praised for providing an anchor point for discussions on potential ways to frame smart contracts within the DeFi context. Respondents particularly welcomed the factual approach taken in the report and its balanced analysis of risks and opportunities regarding the various certification mechanisms considered.

The responses serve to enrich the group's reflections on both technical themes — including security, governance, and compliance principles and audit methods — and potential regulatory pathways linked to certification schemes.

2. Summary of Responses on Technical Areas of the Report (Standards, Audit)

2.1 Standards

A majority of respondents showed agreement with the principles presented in the report, noting that these were aligned with industry best practices, albeit with certain nuances on specific points.

Security, Governance, and Compliance Principles

Regarding **security principles**, several respondents emphasised the need to adopt only general, technologically neutral principles. In particular, feedback highlighted that the principles developed in the report seemed centred on Ethereum Virtual Machine (EVM) blockchains, with less focus on other ecosystems such as Solana or Cosmos. There are technical differences in how the proposed standards can be applied, notably in coding practices and depending on the execution environments offered by these various blockchains. These comments are consistent with the hierarchical approach mentioned

in the document: “high-level principles applicable to all blockchains and their interfaces, followed by more detailed recommendations depending on the technology or technology family used.”

Some respondents also considered that the principle of segregation of duties regarding distinct business processes (principle no. 6) could be counterproductive, given the important role of the knowledge retained by the developer of the smart contract in the context of identifying vulnerabilities.

Additionally, respondents noted the value of strengthening the principle of least privilege (principle no. 5), which stipulates that each entity should have only the strictly necessary permissions in order to perform the required tasks. Responses recommended introducing safeguards and control mechanisms for smart contract administrative functions, such as requiring the use of “multisig”[1] arrangements.

Regarding **governance principles**, some respondents felt that more emphasis should be placed on the risks associated with centralised governance, and suggested various methods to mitigate these risks. In particular, it was suggested that measures to control the concentration of decision-making power over smart contract or protocol changes could be introduced, especially within DAOs, through mechanisms to counter risks of vote manipulation, such as quadratic voting, the establishment of quorum rules, or transparency requirements in the case of vote delegation.

One response notably highlighted that a certification mechanism, by mandating a governance audit, requiring the implementation of protective mechanisms against governance attacks, and obliging disclosure of voting rights distribution and changes in governance token allocations, could help attest to the level of decentralisation of protocols. Respondents also emphasised the importance of taking into account the governance stages taking place off-chain[2].

Thirdly, regarding **principles of service compliance**, many respondents disagreed with the inclusion of the notion of “reasonable gas fees[3]”, some arguing that a “reasonable” amount would be too difficult to define, while others highlighted that protocol designers have limited means to control costs, which depend largely on the underlying blockchain infrastructure. Some pointed out that recommendations on gas fee optimisation already exist in certain audit reports and that, barring exceptional cases, protocols always have an interest in minimising these fees. One respondent suggested incorporating a cost/performance analysis during the audit instead.

Several respondents also highlighted the difficulty of embedding regulatory obligations directly into smart contracts, arguing that regulation should apply at the application layer (e.g. at the interface or intermediary level that enables access to the smart contract), rather than at the level of programmed logic. One respondent added that such regulatory requirements at the smart contract level would necessitate developer control over the code to ensure compliance (given that financial regulation consists of rules devised off-chain, that cannot be automatically translated), which would not necessarily be something desirable.

Smart contract lifecycle, best practices, and international standards

On considerations relating to the **lifecycle of smart contracts**, respondents questioned the practical implementation of the principle prescribing the security of the smart contract throughout its lifecycle, including during subsequent modifications.

[1] Also known as multi-signature arrangements.
[2] Technical environment outside the blockchain (opposite of “on-chain”).
[3] On some blockchains, gas fees are payments owed by the initiators of transactions so that they can be carried out on these blockchains.

Responses emphasised that the dynamic nature of blockchain technology and of the innovations associated with it was not sufficiently taken into account overall. While mentioned in the report, some respondents stressed the importance of introducing timelock[4] and rollback[5] mechanisms related to code updates, and suggested clarifying materiality thresholds for "subsequent changes" that would impact any updates to certification.

One respondent also highlighted the importance of addressing the "end-of-life" stage of a protocol. According to this view, a phased decommissioning policy, with clear user notification and secure disengagement, would greatly contribute to enhance trust in protocols and help avoid incidents that might occur at later stages.

Finally, a large majority of respondents urged regulatory authorities to engage closely with industry players in order to best define standards and principles aligned with current best practices and / or based on existing frameworks (e.g. ISO 27001, NIST, OWASP, EthSecurity, EthAlliance), highlighting the importance of a coordinated application of such standards at the international level. This approach is reflected in the report, which underscores the role and necessary consultation of industry actors in standard-setting.

2.2 Audit

A majority of respondents agreed with the options explored by the working group in relation to different audit methods, and with the challenges and issues identified in relation to these.

Audit types: Use of automated tools and formal verification methods

Some respondents sought to delve further into the technical aspects of the report, showing divergent views in response on conducting audits in multiple phases. Certain respondents believed that any certification framework should encourage audits in multiple "layers" using different methods, arguing that analysis of a smart contract should continue after deployment and throughout the smart contract's lifecycle. They highlighted the importance of continuous monitoring, which could rely on automation enabled by blockchain technology.

Conversely, some respondents argued that conducting a multi-phased audit – one that would for instance take place on the source code, and another on the deployed code – would introduce new challenges, including the need to allow updates to deployed smart contracts in order to address issues identified during the second audit. This could contribute to the creation of a new attack vector, increasing the costs and timeline of certification.

The use of formal verification methods in smart contract audits was also an important discussion point. While respondents acknowledged the value of these methods, it was suggested that such methods be applied only to contracts deemed critical, given the significant resource requirements and the limited availability of specialised experts. Determining the level of criticality of a smart contract also echoes the idea of proportionality criteria (discussed in section 3 below). Additionally, several respondents

[4] A time lock introduces a delay before an update is introduced, allowing users and auditors to review it before it takes effect.

[5] A rollback system would allow for an update to be cancelled in the event of a problem, thus helping to avoid potentially catastrophic incidents.

indicated that a combination of manual audits and automated verification tools is an already established best practice within the industry.

The emerging use of artificial intelligence (AI) in smart contract audits was recognised by some respondents as a tool that could help define the audit scope more precisely, though it would not be able to replace other audit techniques. This point is highlighted in the report.

Following the logic of developing a proportional approach, some respondents suggested lighter requirements for fully immutable smart contracts, arguing that the governance and governance-related risks of such contracts are theoretically negligible or non-existent. According to these responses, the concept of total immutability would resolve the risks of code modifications that would be contrary to user interests, thereby justifying the application of reduced requirements in this case.

Audit scope: Smart contracts and external dependencies

Respondents also debated the scope of audits, questioning whether they should focus solely on the audited smart contract, include all contracts it interacts with, or extend to all external dependencies (e.g. oracles and other off-chain elements). Some advocated for a comprehensive approach that would incorporate these dependencies as far as possible, or at the very least, where this would be deemed impossible, clearly inform users when a certification would not cover certain components (such as an oracle).

Audit triggers and the duration of certification

Regarding the criteria that would trigger an audit, proportionality was a key concern for many respondents, and closely linked to the notion of smart contract criticality. Most felt that a risk-based approach should be adopted as suggested in the report, based on criteria such as Total Value Locked (TVL)[6], the criticality of the contract, its number of external dependencies, or other factors. Establishing clear proportionality criteria is therefore crucial in order to determine what changes would be deemed significant enough to require a new audit. Such a proportional approach would also guide the validity period of a certification.

Some respondents, however, opposed implementing such proportionality criteria, citing the complexity of developing relevant metrics and the challenges of practical application.

Views also diverged regarding the duration of the validity of an audit and of the resulting certification. While many supported the proposal of a three-year validity period, in line with standards from other industries, others suggested alternative durations and renewal methods. Several respondents suggested that a duration of three years would be too long and proposed a model similar to SOC 2 audits[7], which involve a full recertification process every two years, incorporating lighter periodic annual reviews in between.

A significant number of actors argued that the validity period for an audit and certification should not be fixed but instead proportionate to the complexity of the audited smart contract, which could for instance be assessed on the number of interactions or external dependencies of the smart contract, or its degree of mutability.

---

[6] Total Value Locked: A commonly used DeFi indicator to assess the footprint of different protocols, measuring the amount of assets locked within a protocol.

[7] SOC 2 is a voluntary standard implemented by technology and cloud computing companies to ensure data privacy compliance. The standard is published by the American Institute of Certified Public Accountants (AICPA).

Finally, some respondents highlighted that continuous monitoring mechanisms would be more effective in detecting non-compliance with certification requirements, enabling proactive re-audits rather than waiting for the next scheduled audit to take place.

Audit providers

Regarding the question of the provision of audit services, respondents encouraged the working group to consider existing decentralised audit solutions such as bug bounties, community audits, or audit competitions. These approaches were presented as capable of meeting the report's requirements while allowing for the audit of smaller projects.

Given the current shortage of experienced smart contract auditors, which was also referred to in a majority of responses, respondents suggested the importance of including third-party or individual auditors, whose expertise would be demonstrated through certifications or specific training.

In light of this, certain respondents also emphasised the need to develop a structured approach for smart contract auditor training, or for certifying auditors. One respondent proposed that the core competencies of auditors should be standardised, to allow for the recognition of international auditors that would be deemed equivalent, rather than limiting recognition to auditors certified in the jurisdiction where the smart contract certification is issued.

3. Summary of responses on proposed regulatory avenues

Respondents highlighted the importance brought by the distinction made between approaches to different certification regimes proposed in the report, and expressed their preferences among the proposals put forward. Among those responding to this section of the report, 85% favoured the idea of an optional certification regime.

Regarding the idea of an **optional certification regime**, respondents indicated they felt that this option this would offer greater flexibility and preserve the competitiveness of the European crypto-asset ecosystem, while adequately addressing emerging risks. Such a regime would promote the establishment of best practices without imposing constraints, allowing actors to obtain certification once their business model would have matured. Certification would thus be viewed as giving more of a competitive advantage in this scenario.

Regarding the idea of a **mandatory certification regime**, several respondents noted the potential risks of centralisation that could result from such a scheme. Some argued that it could contradict the principle of decentralisation, particularly by creating barriers to entry for independent developers and start-ups, who may struggle to meet compliance requirements. The main criticism focused on potential costs and delays linked to imposing certification, which could undermine the competitiveness of the European ecosystem. Respondents also highlighted that, given the immaturity of the DeFi sector, the idea of regulation at this stage could be premature.

Regarding a **mandatory regime with proportionality measures**, opinions were more divided. Though some of the criticisms made in relation to the idea of mandatory certification were extended to this approach as well, several respondents supported the establishment of proportionality criteria for a more tailored application based on the individual specificities of smart contracts.

Scope of certification

Respondents also addressed the question of the scope of certification, specifically the possibility of reconciling protocol-level certification with that of its underlying smart contracts. Some felt this was possible if respecting the modular nature of DeFi and while done in consideration of all characteristics of a protocol, including interactions among smart contracts and their vectors of centralisation, characterised by the use of any element constituting potential single points of failure (such as bridges, oracles, or off-chain elements).

Other respondents argued for distinguishing between smart contracts and protocols, rejecting the idea of an overall protocol certification in favour of other models, for example based on the idea of a shared codebase[8], suggesting that certifying one address could extend to all addresses using the same codebase.

Certification Mechanism: Certification issuance

Regarding the mechanism that would allow for the issuance and publication of the certification, respondents reflected on methods that would best help ensure disclosure and display of certification status. As envisaged by the working group, proposed solutions generally included on-chain access to a smart contract's certification status (certified, uncertified, revoked, etc.), for example via NFTs on-chain, or through the granting of a certificate.

Some actors also brought a distinction between a static certification model (which would apply for a given period), and a dynamic model where monitoring would be continuous rather than periodic. Some also suggested developing a continuous certification model, with automated checks carried out constantly on-chain or off-chain, with results automatically published as an on-chain certificate. One respondent mentioned the possibility of building a monitoring protocol that could be managed by the body responsible for the accreditation of smart contract auditors or by the regulator, which would directly oversee upgrades or other relevant changes made to a protocol.

One respondent also proposed adopting a system similar to SSL/TLS certificates[9] for web browsers. They argued that such a system would require maintaining a registry, potentially an open registry (e.g., an Ethereum contract registry or an off-chain database API that wallets could query), that would automatically signal or indicate the revocation of expired certificates. Implementing this would require a certificate issuance and monitoring infrastructure overseen by a government body or industry governance mechanism. The respondent suggested that the registry should ideally operate in a decentralised way, or as a common good maintained by a consortium, bringing together experts in blockchain, security, audit and regulators, in order to avoid single points of failure.

Some respondents also supported the idea of an ex-post oversight regime led by regulators, in which all forms of audit (decentralised audits, bug bounties, audit competitions, etc.) would be recognised. Some further emphasised that such a scheme would require a clear definition of the supervisory powers granted to these authorities.

[8] The codebase corresponds to the entire source code of a software, component or system.

[9] SSL/TLS certificates are digital files used to secure communication between a client (such as a web browser) and a server (such as a website) by enabling encryption of the data exchanged. When someone accesses a site over HTTPS, the browser verifies the SSL/TLS certificate to establish a secure connection.

One respondent also mentioned other approaches to regulating DeFi, such as requiring protocols to set up a fund or insurance pool to cover certain risks, including hacking risks, referring to the concept of a "surplus cushion" within certain protocols, that acts as an insurance policy against certain losses.

4. Conclusion

The consultation from the Working Group's report on smart contract certification helped to enrich the thought process within several areas as indicated below.

On **standards**, feedback from the consultation generally showed agreement with the proposed principles, which were judged as broadly consistent with industry best practices, while calling for certain adjustments. Respondents recommend more general, technologically neutral security principles, highlighting the limitations of standards overly focused on EVM blockchains, and recommend making the most of decentralized functions that can reduce security and governance risks. On service compliance of smart contracts, reservations were expressed about the idea of "reasonable gas fees" and the direct integration of regulatory requirements into smart contracts. Finally, there was a strong call for international coordination around existing standards.

On **audits**, respondents generally agreed with the approaches proposed by the working group while suggesting for more nuance. Support was brought to the idea of a multi-layered approach combining manual audits, automated tools, and, in the case of critical contracts, formal verification methods. A proportional approach was favoured, both to trigger the audit and to define its scope and period of validity, though some pointed to the potential complexity of implementing such an approach. Respondents also highlighted that audits should cover external dependencies. Lastly, they encouraged the recognition of diverse auditing actors or methods, including decentralised audits, bug bounties, and certified third-party experts.

On **the exploration of regulatory avenues**, a large majority of respondents supported the idea of an **optional certification regime**, viewed as more flexible and in support of innovation, allowing for good practices to develop without hindering entry by new actors. The idea of a **mandatory regime** was criticised for risks of centralisation and the imposition of constraints that would be perceived as disproportionate, especially for smaller projects. The idea of a **regime with proportionality** received more mixed reactions. **The scope of certification** sparked debate between respondents, some advocating for a protocol-wide approach, while others preferred the idea of a certification by codebase. Finally, respondents favoured the idea of **public, dynamic, and verifiable on-chain certifications**, potentially managed via a decentralised registry, a consortium or by public authorities.