Dear Sir/Madam,

Binance welcomes the opportunity to respond to the Consultation questionnaire on ‘Decentralised or disintermediated finance: what regulatory response?’ We consider this is an important contribution to the ongoing debate, at national, EU and global levels, on the risks and benefits and the appropriate regulatory framework of DeFi.

Our detailed response is attached. Below, we highlight some key points:

- Decentralised finance promises to improve financial infrastructure, which satisfies consumers’ demand for more inclusive, cost-effective, transparent, convenient and faster services;
- Replicating existing financial regulation and applying it to DeFi would be ineffective, counterproductive and would hinder innovation. It is critical for rulemakers to recognise the distinctive attributes of DeFi, notably the principle of decentralisation and the reliance on smart contracts, when assessing the options and tools to achieve policy objectives.
- Consumer protection, financial stability and market integrity must be pursued alongside the support for growth, innovation and adoption.
- Public authorities should incentivise collaboration among industry players and the development and take-up of standards, which can lay sound foundations for the development of the ecosystem.
- At this early stage of development of the industry, a self-regulatory approach has significant advantages:
  a. it leverages numerous underlying technical concepts and established standards, which take into account the specificities of the blockchain technology;
  b. it addresses the heterogeneous nature of the blockchain ecosystem by developing tailored approach through different initiatives; and
  c. it offers flexibility to keep up with the pace of innovation and respond to the evolving challenges.
- Over time, striking the right balance between standards, self-regulation and any form of regulatory oversight would be the right approach to nurture a crypto ecosystem that is responsible and continues to innovate, grow and provide benefits to consumers.

Against this backdrop, we recommend the setting up of an Observatory of DeFi, which would bring together industry representatives, regulators and other interested parties. The observatory would be tasked with gathering knowledge and proposing tools that facilitate the monitoring of DeFi protocols and developments in the market. It would promote a shared understanding of the
risks and benefits, develop technical expertise and inform the discussion on possible adapted forms of supervision.

We would envisage the following deliverables for the DeFi Observatory:

- Perform and publish public investigations and reports
- Issue opinions and warnings about DeFi projects
- Regularly map new solutions, innovations and significant protocol updates
- Help develop and propose standards, codes of conduct or voluntary compliance schemes to which DeFi protocols and entities could adhere.
- Support the development of smart contract regulation for RegTech and SupTech use.

Please do not hesitate to contact us if you have any questions about our response or require any further information.

Yours faithfully,

Binance
Presentation

Binance is a blockchain and cryptocurrency infrastructure provider. In France, Binance France SAS offers digital asset services through its Digital Asset Service Provider (DASP) status.

Binance France SAS is a centralised entity, registered with the Autorité des Marchés Financiers (“AMF”) and the ACPR for the provision of (i) custody, (i) crypto-to-crypto (iii) crypto-to-fiat services as well as (iv) the operation of a trading platform of digital assets.

The Binance trading platform is part of a broader ecosystem that bridges the gap between centralised and decentralised models, expanding the products its customers can have access to, providing a de facto CeDeFi service.

Binance has listed many tokens via the Binance platform considered to be part of DeFi, allowing users to trade these tokens against other digital assets.

In addition, the BNB Chain, which is a community-driven and decentralised blockchain, conducts thorough assessments of crypto asset smart contracts to identify potential vulnerabilities or deliberate backdoors. The BNB community also carries out on-chain analyses to detect fund concentration and possible warning signs of fraudulent activities, such as rug pulls and Ponzi schemes. It also engages with project founders and provides feedback to enhance the quality of their projects and suggest KPIs to improve oversight and reduce risk. If a project does not adhere to the suggested improvements, or if a scam is suspected, it is added to a blacklist and the community is made aware through the Red Alarm initiative on the DappBay website. To protect the BNB Chain ecosystem further, the Avenger DAO initiative has been launched. Recently, the initiative has formed a working group that collaborates with web3 security service providers. The aim of this group is to establish and propose best practices and standards for the secure development of smart contract and decentralised applications, incorporated into a Web3 Security Framework, similar to the standards developed by International Organization for Standardization (ISO).

Part 1: DeFi: definition, use cases and schematic structure

Q1: Do you have any comments on the definition of DeFi used in the paper? Does the document correctly reflect the real level of decentralisation of services?

The DeFi industry is at a nascent stage and, as argued in the recent IOSCO report on DeFi (IOSCO, 2022:1): “Currently, there is no generally accepted definition of ‘DeFi,’ or what makes a product, service, arrangement or activity ‘decentralised.’”

---

1 A list of projects and DAaps that have been assessed to be untrustworthy and carry extremely high level of risks is updated every Friday: https://dappbay.bnbchain.org/red-alarm
2 https://www.avengerdao.org/
In discussing the concept, it is important to consider the two elements that make the term DeFi ("de" and "fi"), together with the relationship between the two.

Decentralisation exists in a spectrum and is often an objective to be achieved over time, with a higher level of centralisation observed at start. The proposed criteria (i.e. architecture based on public blockchains; protocols based on smart contracts; decentralised governance; absence of a custodian) are helpful ‘indicators’ to identifying and classifying decentralised projects. However, it is important to recognise that decentralised projects may not meet all the criteria. For these reasons, we would recommend treating the proposed criteria as ‘indicative’ and keeping them under review.

Going further into the details, we would like to point out that criteria #1, on public blockchain architecture, is incompatible with Regulatory Scenario B (chapter 3.1), in which an infrastructure based on private blockchains is proposed. Furthermore, we urge careful consideration of terminology and definitions so as to avoid confusion and conflation between terms such as permissioned and permissionless, and public and private blockchain networks.

Q2: In your opinion, which use cases of DeFi are likely to develop in the future? Can they serve the real economy?

DeFi projects often mirror traditional financial services and activities, including lending and borrowing protocols, trading, insurance and assets management services. DeFi uses new and existing technologies involving blockchain, cryptography and tokenisation. It offers more choice, competition, trust and inclusion.

For example, by reducing the need for intermediaries, DeFi protocols can introduce efficiency that reduces the cost of and / or extract better returns for users. DeFi protocols also enable more transparency. The infrastructure can increase services availability and security and enables users to keep control of their assets. The features of DeFi have the potential to serve the real economy at a global level.

However, it is also important to ensure that financial regulators think about DeFi not only in the context of ‘regulated finance’, but take into account the wider ecosystem such as Web3, NFT and Digital ID, much of which may not be regulated as finance. Otherwise, financial regulators may duplicate regulation, or regulate in a manner that fails to factor in the constituent parts of the wider interconnected ecosystem.

We set out below examples of use cases that support the development of the DeFi ecosystem:

- **Decentralised Identity** - DeFi platforms are exploring decentralised identity solutions, allowing individuals to own and control their personal data. Decentralised identity solutions offer a new way to manage personal information, providing greater privacy and security compared to traditional identity systems.
- **Prediction Markets** - Decentralised prediction markets allow individuals to hedge their investment against a particular outcome of events and earn rewards based on their accuracy. Prediction markets in DeFi offer a new way to invest in events and outcomes, providing greater transparency and accessibility compared to traditional prediction systems.

- **NFTs and Collectibles** - Non-fungible tokens (NFTs) and collectibles are rapidly becoming popular use cases for DeFi. NFTs allow individuals to buy, sell, and trade unique digital assets, such as art, music, and other forms of digital content. DeFi platforms enable individuals to verify the ownership and authenticity of NFTs, providing greater transparency and security compared to traditional methods.

- **Governance** - DeFi platforms are exploring decentralised governance solutions, enabling individuals to vote on and make decisions on products and projects they are involved in. Decentralised governance in DeFi offers a new way to make decisions, providing greater transparency and accountability compared to traditional governance systems. As DeFi continues to grow, decentralised governance will play an important role in enabling individuals to shape the future of DeFi.

**Q3: What do you think about the concentration phenomena described in section 1-5 of this document?**

It is important not to conflate the terms concentration and centralisation. Concentration in a DeFi context does not mean that a given protocol or blockchain is centralised. The term "decentralised" in DeFi describes a system that operates with decentralised governance, rather than from a pure infrastructure perspective. This includes the ability for anyone to acquire governance tokens and participate in a protocol's development that embodies the decentralised vision.

We do not see concentration as a permanent, but rather as a temporary feature that is explained by both the stage of development of some projects and the embryonic state of the industry. **We expect the distribution of funds, users and validation capacity to become more diffuse and dispersed over time, as new technologies and processes become more established and mainstream adoption increases.**

It is common practice for globally dispersed and separate company blockchain infrastructure and Dapp engineering teams to collaborate, develop and improve the ecosystem technology. This teamwork across different companies and geographies should be seen as an indicator of gradual decentralisation. Moreover, it is crucial to note that governance tokens are widely accessible on crypto assets platforms. Such a level of accessibility is inconceivable in traditional finance.

**The gradual reduction in the level of 'concentration' is already apparent in the evolution of TVL in blockchains. While Ethereum is still the dominant player (60%), it is not anywhere close to its market share (97%) at the beginning of 2021.** This coincided with the
rise of the BNB Chain and Tron, which are now second and third largest blockchains in TVL terms. The evolution of Non-Fungible Tokens (NFTs) use cases and the subsequent emergence of Decentralised Finance (DeFi) applications on other blockchain ecosystems further contributed to this process.

De-concentration has also been supported by the efforts from DeFi applications to diversify between blockchains. A case in point is Uniswap, the largest decentralised exchange with over $4bn of TVL. Uniswap first launched on Ethereum, but it has subsequently launched on other blockchains, including Arbitrum, BNB Chain and Polygon.

To conclude, we would argue the idea of a ‘winner takes all’ in the DeFi ecosystem is misplaced and outdated.

Q4: Do you have any comments on or information to add to the schematic presentation of DeFi presented in section 1-6?

![Diagram: The application architecture of DeFi](image)

Yes, we would like to make two comments.

First, on the elements included in the diagram. The diagram represents the whole Blockchain ecosystem architecture. If the intended focus is on DeFi activities, the “Centralised Applications”
rectangle might be removed. Even if it plays a critical role in the onboarding/offboarding of customers in the crypto industry, centralised applications are not part of the DeFi ecosystem per se. Layer 2 and blockchain interoperability should be kept.

Second, on Layer 2 solutions. These are not limited to Optimistic and ZK rollups, but also include side chains, state channels and nested blockchains. For instance, the most used Layer 2 solution is Polygon, which is a sidechain of Ethereum, and not exactly a “Layer 2” in the common definition of a Layer 2.

With regards to blockchain interoperability, while centralised and decentralised bridges are the most common solution to address interoperability between blockchains, there is an alternative in the form of cross-chain atomic swap. This alternative should be added to the diagram alongside bridges. Atomic Swaps enable the exchange of crypto assets between two users in a decentralised way. The main benefit of atomic swaps is that they are a fully decentralised and peer-to-peer crypto asset exchange mechanism, where users don’t have to rely on cross-chain relayers or validators.

Yet, due to atomic swaps’ shortcomings such as insufficient liquidity, scalability issues, and subpar user experience, the market has predominantly chosen decentralised bridges as the preferable solution.

**Part 2: The risks associated with DeFi**

Q5: Do you have any comments on the description (provided in section 2-1 of this document) as regards risks related to decentralised governance?

The risks related to decentralised governance described in this section do constitute some of the main risks in this field.

However, it’s important to note that decentralised autonomous organisations (“DAOs”) bring with them many innovations, not only from a financial perspective, but also from a governance standpoint. The use of tokens, smart contracts and blockchain may empower individuals to organise themselves in a much more efficient and practical manner than traditional governance systems and corporate structures.

As to the risks identified in section 2.1, they currently relate mostly to concentration of voting powers. It is worth noting that not all DAOs operate in the same way. Some have sought to de-link voting rights, which are granted to those who effectively participate in the governance of the DAO, and the holdings of tokens. Others set out voting rights by agreement within the DAO based on certain objects or purposes set out in its constitution. This can include circumstances where holders of large voting rights must self-declare to promote transparency and democracy, otherwise their votes will not be counted towards quorum/voting threshold. This is akin to the experiments related to
cooperative societies, such as the European Cooperative Society (SCE) in the EU. Such mechanisms prevent the concentration of powers in DAO members who may have more financial capacity.

In addition to that, there are significant technological hurdles to collecting data related to DAOs. For this reason, we believe that introducing rules (e.g. minimum level of dispersion of governance tokens) at this juncture would be counterproductive, inefficient and hinder the development of alternative governance solutions. **Public authorities should refrain from regulating DAOs in a way that steers the market in one direction, because it may not be the best one for innovation. However they should provide clarity and stability on the legal existence of DAOs.**

**Q6: Do you think that layer 1 solutions can exacerbate the security issues of the blockchain infrastructure?** What about layer 2 solutions? In your opinion, are there significant differences in this respect between the layer 2 solutions considered?

We take the questions in turn, starting with layer 1 solutions.

Layer 1 solutions are the blockchain themselves, hence, by definition, they can’t **exacerbate security issues.** By nature, Layer 1s tend to be more secure than Layer 2s. However, blockchains aren’t built the same and Layer 1 security depends on the technical features of the Protocol (e.g. size of the blocks, consensus mechanism, cryptography algorithms).

It would be reductive to assess the level of security of blockchains as different as Bitcoin, BNB Chain and Ethereum against a single framework, based on a single or a few factors or indicators. We would favour a more detailed, bespoke analysis that takes into account the above mentioned technical features as well as the interactions between them.

While recognising the explanatory power of the so-called trilemma framework blockchain - decentralisation, security, and scalability -, we would note that security often takes priority. **This goes a long way to explain the absence of hacks at Layer 1 level when the aforementioned blockchains are considered.**

We would like to make three main points about the security of Layer 2 solutions.

First, to overcome scalability obstacles of Layer 1 and offer a service apt for financial applications, it is crucial to incorporate Layer 2 solutions into the DeFi infrastructure, despite the additional complexity they may introduce.

Secondly, it’s essential to understand that Layer 2 solutions employ a variety of technologies to achieve their objective of enhancing Layer 1 scalability. These solutions are not limited to Optimistic and ZK Rollups. Some leverage sidechain technologies, such as Ethereum’s Layer 2
solution, Polygon. This is more mature than Rollups. Others, like the Lightning Network, utilise state channels.

Using ZK Rollups is computationally demanding and intricate, and integrating with the Ethereum Virtual Machine (EVM) is not a straightforward task. Nevertheless, they can offer a seamless, more secure user experience while increasing the number of transactions being validated every second. Unlike Optimistic Rollups, which default to assuming transactions are valid until challenged, ZK Rollups ensure transaction security through cryptographic proofs. This discrepancy has implications for transaction finality (the time it takes for a transaction to be considered irreversible), with ZK Rollups achieving instant finality, while Optimistic Rollups must endure a challenge period.

Third, zero-knowledge and optimistic rollups are relatively new. Providing an accurate risk assessment of these technologies would be challenging as they are evolving. Theoretically, they are mathematically proven and don’t impair the security of the underlying Layer 1 blockchain, and, as such, don’t pose inherent risk to the system. However, like any IT system, they also depend on the security of the underlying system and on its secure configuration and usage.

Q7: Do you think that the use of rollups or similar solutions will result in less transparency of information for an observer?

Not necessarily. Zero-knowledge technology is a means to improve scalability, even if it can also be used to enable privacy or even anonymity. Ultimately, this depends on the objectives of a given project. For instance, Loopring using Zero Knowledge Proofs offers complete transparency, akin to Layer 1 solutions. Furthermore, layer 2 solutions, such as zkBNB and opBNB are designed to store the redacted data on decentralised storage solutions, where anyone can access it for further investigation and statistical reporting.

Q8: Do you have any comments on the description (provided in section 2-3) of the risks related to the application layer of DeFi?

The public nature and the blockchain architecture enables entities to engage with any smart contract deployed on the blockchain. This openness and transparency is a key feature of blockchain technology, fostering the trust we place in it. While not negative, this characteristic necessitates a heightened emphasis on secure engineering practices to ensure superior code quality. Given the high level of complexity and financial risk in developing DeFi applications, it underscores the increasing demand for seasoned engineers with substantial cybersecurity, distributed systems, smart contracts and blockchain knowledge, who can navigate the landscape of decentralised applications safely. The public nature of decentralised applications can also contribute to the development of more secure algorithms. Given their exposure, these algorithms are extensively tested by members of the community through bug bounty programs.
As outlined, the executable code within smart contracts can exhibit vulnerabilities. Similarly, the most adopted programming languages in the industry also have their own vulnerabilities and some have been prevalent in the industry for over three decades. Therefore, the issue doesn't lie in the smart contract computer code itself, but in how it is utilised. **As the industry matures, so does the solidity of the programming language, enhancing its quality and security.** This is done for example via EIP (Ethereum Improvement Proposals), an off-chain proposal system where developers vote and decide the priority of improvements to be added to the programming language.

Furthermore, the use of composable DeFi protocols in a decentralised application could **increase its susceptibility to risks.** Even projects that maintain high safety standards can be affected by interfacing with less secure projects. This underlines the importance for projects to uphold rigorous standards of quality and security. Additionally, continual evaluation, collaboration, and communication between partner projects should be given utmost priority.

As it stands today, numerous measures have been implemented to ensure secure code development. These include the use of audited secure smart contract templates, testing frameworks, simulation frameworks, monitoring tools, automatic incident response and both static and dynamic code analysis tools dedicated specifically to the secure development of smart contracts. These tools have been developed as open-source resources, making them accessible to anyone. However, it is important to acknowledge that the technical proficiency required to effectively evaluate and utilise these tools is quite high. This is why some ecosystems have started developing their standards and best practices that could be leveraged by the projects. For instance, **the BNB Chain started the AvengerDAO initiative gathering industry security experts to establish industry defined standard and best practices aggregated under a Web3 Security Framework, built in a collaborative fashion.**

This scenario also shows the opportunity for academic institutions to provide new **specialised courses tailored to blockchain application development.** These could encompass decentralised software architecturing, decentralised application development, blockchain engineering and operations, and web3 cybersecurity.

On the potential tampering by validators, there are various approaches under development to address the problem of transaction reordering and the exploitation of arbitrage opportunities that adversely affect end users. Other initiatives are focusing on returning arbitrage profits to the community as a means of ensuring fair distribution.

In terms of data reliability, the inability of smart contracts to access data outside the blockchain poses certain limitations, such as calculating the prices of crypto assets. Various solutions have been crafted to circumvent this problem by utilising on-chain liquidity pools data for such computations. However, these mechanisms are intricate and present both financial and engineering challenges and risks. But large DeFi projects have successfully implemented a safe on-chain crypto asset calculation, even if it could be considered non-optimal.
Oracles, both centralised and decentralised, are proposed solutions as they facilitate on-chain data provision for crypto assets. However, centralised oracles pose a risk to the decentralised applications using them as they represent a single source of risk. They are a single source of truth and a critical component that could deliberately or inadvertently misrepresent crypto asset prices. Since centralised oracles do not offer transparency regarding their computation mechanism, primarily for security reasons, there's an increasing demand for decentralised oracles that provide transparent data along with verification means. It is important to note, however, that decentralised oracle services typically incur higher costs. Finally, given the criticality of oracles, we agree with ACPR's assertion that clear standards for oracles could help improve their resilience and integrity.

Q9: Do you have any comments on the identification of DeFi risks for retail customers (section 2-4-1)?

The description of risks to retail customers is comprehensive. However, we would stress that most of these risks are inherent to the products and digital means of access and, to an extent, are also present in traditional finance.

Furthermore, where there are specific risks arising from DeFi, we believe these should not be considered in isolation. Instead, it is important to weigh them against the benefits of DeFi, which include: financial inclusion and access to financial services, less intermediaries and costs, quicker execution or broader access to capital.

Q10: Do you have any comments or additions to make to the description (provided in section 2-4-2) of the systemic vulnerabilities of the DeFi ecosystem (endogeneity of investments, significant leverage effects, role of automated position liquidation mechanisms)?

We have no comments.

Q11: Do you agree with the proposal concerning the regulation of stablecoins issued by DeFi protocols? (refer to section 2-4-3: “if a decentralised service claims to create or use a crypto-asset with an official currency as a reference, this crypto-asset must be an EMT within the meaning of MiCA or an equivalent asset)

No. The mere referencing of a ‘fiat currency’ should not result in a crypto asset being classified as an e-money token (EMT).

In our view, the classification of e-money token should be reserved to crypto assets that “purport to maintain a stable value against” the fiat currency, as per the MiCA definition.
Conversely, crypto assets that (only) reference a fiat currency and are issued in a decentralised manner should be treated like other crypto assets: an entity offering or seeking admission to trading of that crypto asset would have to produce a white paper outlining how they operate and the risks associated with them, in particular the risk that they deviate from the peg.

This differentiated approach should enable users to clearly distinguish between EMTs (or regulated stablecoins for the lack of a better term) and other crypto assets that fall short of that classification. It would be a pragmatic way to ensure user protection, while not hindering innovation and experimentation.

As a final point, we would like to stress that **not all ‘DeFi stablecoins’ are the same. There is a material difference between collateralised stablecoins and algorithmic stablecoins, which should be appropriately reflected in the white paper** as well as in regulators’ statements and analysis. The collapse of UST last year exposed the difficulty of designing a robust stabilisation mechanism based on algorithms or endogenous collateral. In contrast, collateralised stablecoins, such as DAI, experienced limited deviations from the peg, despite sharp drops in the value of unbacked crypto assets, and those deviations were mostly above the peg.

**Q12: Do you have any comments on the description of the potential AML/CFT risks of DeFi (section 2- 4-4)?**

We agree with that assessment that pseudonymity does not equate to anonymity. The underlying technology (i.e. transactions on blockchains leave a permanent trail), existing industry guardrails, including fiat on/off ramps, centralised exchanges and on/off chain analytics companies help to manage and mitigate the risk of AML/CFT.

In this context, it is worth noting that blockchain analytics companies have consistently reported that **the criminal transactions, while meaningful, constitute a relatively small proportion of the total crypto transaction volume.** According to the Chainalysis Crypto Crime report, criminal activity accounted for 0.24% of all blockchain transactions in 2022.

Technology is also evolving in a way that can contribute to further mitigate AML risks. Binance has recently launched its Soul Bound Token, Binance Account Bound (BAB). Soulbound tokens are non-transferable and aim to solve identity verification problems on the web3, by serving as a digital verification tool for users who have performed KYC. In theory, SBTs could allow people to establish their own digital reputation and assess another person's on the blockchain. An SBT can function as the Web3 version of the "identity card". In addition to the Binance ecosystem, third party protocols will be able to use BAB tokens for many use cases. Experiments could be encouraged for certain use cases in DeFi for example.
Q13: In your opinion, are there any other risks that should be taken into account which are not mentioned (or not given sufficient attention) in the document? 

No.

Part 3: Avenues for a regulatory framework

Section 3-1: Ensuring a minimum level of security with respect to infrastructure

Q14: Should public blockchains be governed by a framework or by minimum security standards (refer to section 3-1, regulatory scenario A)?

Minimum security standards have the potential to foster trust and increase security in public, private blockchains and the ecosystem. This would be relevant and have a positive impact on a number of industries, not only DeFi *strictu sensu*.

At the present juncture, given the pace of development of the technology, any framework or minimum standards for blockchains should be developed by the industry and their adoption should be voluntary. This objective is to nurture a crypto ecosystem that continues to innovate, grow, while providing benefits and protecting all its stakeholders.

Public authorities would have a role to play in supporting collaboration and dialogue between industry players and providing incentives for the adoption of the standards, ideally positive incentives. We would consider the imposition of any standards or oversight framework as premature.

Any framework or minimum standards should build on or take into account the established initiatives⁴, which have assessed the underlying technical concepts such as cryptography, secure server management or secure network management.

Q15: Should public authorities supervise the concentration level of validation capacities on public blockchains? If so, through what kind of measures?

There is a strong case for monitoring the concentration level of validation capacities on public blockchains to identify potential threats to the blockchain ecosystem if a single entity or group could potentially take advantage or control over the network.

---

⁴
A first step would be to monitor the number of active participants or calculate the decentralisation of the network using known criterias such as the 'nakamoto coefficient' (i.e. in layman's terms, this is the number of entities that hold the majority of the network).

There are already services on all major public blockchains providing the total number of nodes in the network as well as their geo location (e.g https://www.ethernodes.org/). Public authorities, together with the industry, could explore options to build on these existing and public tools, for instance through self-regulation bodies or an observatory.

**At this stage, introducing a blunt threshold would arguably be counterproductive, including by limiting the ecosystem growth** (by creating additional challenges to add new validators to the network as it grows), and creating a selection bias (as projects might prioritise quantity instead of quality).

Furthermore, it is important to acknowledge that new blockchains might be more prone to threats from large validator pools that could temporarily infiltrate the network to stage an attack. Although 'hard forks' can technically counteract 51% attacks, hard forks don't align with the core tenets of decentralisation and should not be seen as a standard system feature. Given the advanced state of global mining pools and specialised hardware, 51% attacks are a legitimate concern for new blockchains using Proof of Work consensus protocol. In a Proof of Stake blockchain, a 51% attack can theoretically be performed if one entity owns more than 50% of the total staked tokens. However, this issue is not present in Proof of Authority consensus blockchains, as the identities of validators are known.

**Q16: Do you agree with the analysis provided in the paper on the merits and limitations of private blockchains (section 3-1, regulatory scenario B)? Should private blockchains operated by private operators be regulated through a supervisory framework, if at all?**

☐ Yes
☐ No
Why?

No, we believe the analysis is not balanced nor comprehensive.

**Private blockchains offer several advantages, such as faster transaction processing, more efficient consensus mechanisms, data privacy and a streamlined decision-making process for updates and security enhancements.** These features make private blockchains particularly suitable for enterprise-level applications, where organisations require control and have a greater focus on compliance with availability and efficiency metrics.

However, private blockchains also come with certain trade-offs. By relying on a limited number of trusted players, private blockchains sacrifice some degree of decentralisation and openness that public blockchains offer. This can make **private blockchains less resistant to censorship and susceptible to the influence of the controlling entities.** The reduced level of
decentralisation could also limit the potential for community-driven innovation, as seen in public blockchains. The level of innovation observed on Ethereum the past 5 years would not have been possible without the permissionless characteristic of the Ethereum blockchain.

We believe that public and private blockchains can co-exist and complement each other. Banks can operate their own private chains and even offer their own "DeFi" (CeDeFi) services, without hindering public blockchains from providing similar services.

Cautious users may prefer to rely on banks as intermediaries for accessing these services, while more adventurous users may choose to eliminate the custodian and directly manage their funds and investment strategies on public blockchains services. Ultimately, having more service providers promotes healthy competition, leading to lower costs and improved services for the end customer.

On the question of how private blockchains should be supervised, it is crucial to differentiate between various use cases for private blockchains. Many private blockchains do not involve financial crypto assets, but instead function as databases for data storage and timestamping among private actors within a consortium. This makes such blockchains very similar to the existing database solutions and as such, there is likely no need for a supervisory framework.

On the other hand, private blockchains that connect to public blockchains as side chains or through bridges may benefit more from adopting security standards than from a supervisory framework. This would help ensure the safety of consortium participants and prevent any malicious behaviour from individual actors who might act against the majority's interests.

Q17: Should public players directly manage the blockchains that provide the infrastructure for DeFi operations?
☐ Yes
X No
Why?

No, direct management of blockchain infrastructures for DeFi by a public entity is likely to be impractical and unrealistic in the same way that the public players don't offer infrastructure services such as cloud services.

Q18: Do you have any other regulatory proposals to make with a view to ensuring a minimum level of security for the blockchain infrastructure?
Yes
X No
If so, what are they?
Section 3-2: Providing a suitable oversight framework in view of the algorithmic nature of services

Q19: Is a certification mechanism an effective solution to determine the scope of "safe" smart contracts (for a given state of knowledge)? Would alternative solutions achieve the same result?

A global certification mechanism would help to mitigate risks in the DeFi sector. It would enable projects to better safeguard and manage their assets and applications and offer additional protection to users and investors.

Such a framework would address:

1. Recommendations for smart contract security, addressing vulnerabilities and flawed patterns to avoid.
2. Instructions for securing popular DeFi popular services, such as liquidity pools, lending pools, and governance smart contracts, as well as oracle usage.
3. Wallet security guidelines for both projects and users, as wallets are the critical keys for accessing on-chain crypto assets.
4. An aggregation of the latest best practices in software engineering for development teams and software project management practices, including DevSecOps and zero trust approaches, considering the technical expertise needed to comprehend blockchain infrastructure and DeFi architectures.
5. High-level guidance on maintaining business continuity throughout various market cycles.

In addition to the existing frameworks that ensure the security of web applications and their infrastructures, organisations can also follow complementary guidelines and recommendations from ISO, OWASP, Cloud Alliance, and NIST.4

In the absence of standardised practices and comprehensive knowledge from auditors, projects seek multiple audits/alternative solutions to ensure that all issues have been properly identified. Incentivising the industry to develop standards can lay the foundation for a thriving ecosystem.

In this context, we would like to re-emphasise the AvengerDAO5 community based initiative, which has gathered industry security experts in a working group to establish industry defined standards and best practices aggregated under a Web3 Security Framework. As part of this initiative, BNB Chain is under weekly monitoring and relevant projects are regularly informed about security best practices status. This includes ongoing work within the BNB Chain compliance function to enable certificates to further support on-chain transparency and verifiability.

5 https://www.avengerdao.org/
However, with the diverse range of blockchain protocols, consensus algorithms, smart contract programming languages, and layers 2, among others, it is important to prioritise the technologies most used by the largest part of the industry. Furthermore any certification mechanism would have to undergo a continuous process of evolution and incremental adaptation. This is crucial in addressing the most critical ecosystems first and keeping up with the ever-evolving landscape of blockchain technology.

**Q20: Do you agree with the description (provided in section 3-2-1) of the various techniques offered to audit the computer code of smart contracts, including their respective strengths and limitations?**

The description of the challenges and methods concerning smart contract security is comprehensive. The public nature of smart contract code can be a double-edged sword; while it enables the community to identify vulnerabilities, it also potentially exposes vulnerabilities to attackers. Solutions to ensure the security of smart contracts often involve specialised risk assessment tools, human audit, formal proof mechanisms and the usage of standardised, audited smart contract templates. However, each of these methods has its limitations:

1. **Standard Smart Contracts:** Over the years, various blockchain ecosystems have proposed different standards for smart contracts to promote reusability, ease of integration with other applications, and enhanced security. In the BNB Smart Chain ecosystem, the BEP20 standard was introduced, drawing inspiration from the Ethereum ERC20. This standard is primarily viewed as a Utility Token used by decentralised applications. Such standards can be considered reliable as they have been thoroughly audited by both the community and professional auditors, ensuring its security. With time, some companies began to offer more sophisticated standard smart contracts for specific use cases. Examples include Proxy contracts, which allow for updates to existing contracts, and contracts that provide access control mechanisms to manage smart contract functionalities. However, standard smart contracts do not cover all the use cases in the DeFi industry. As of now, only individual smart contracts are standardised, but there are no standards for functional, end-to-end business-oriented use cases.

2. **Human audits:** While auditing can help detect flaws in smart contract code, the high demand for such services has led to a shortage of skilled personnel, and even experienced auditors may fail to identify vulnerabilities. Also, as the industry grows and the decentralised application architecture and offered services increases in complexity, the human factor becomes a bottleneck, in terms of time and in terms of audited coverage.

3. **Formal proof mechanisms:** Although these methods can be automated, they are not yet widespread due to their high cost, limited number of experts, and compatibility requirements. Moreover, even if the program complies with a set of specifications, the validity of these specifications still needs to be checked.
4. **Automated risks assessment tools:** Tools that detect smart contract vulnerabilities are crucial in this field. Open-source solutions help projects identify common vulnerabilities in their smart contracts during the early stages of development. More comprehensive options can be found through specialised service providers. However, these tools might not detect all vulnerabilities, particularly those related to specific market conditions, specific composability vulnerabilities or complex business flows relying on external dependencies.

Complex business flows with multiple smart contracts interacting may also present undetected vulnerabilities. Furthermore, a crypto asset might be secure on its own but could become vulnerable when interacting with other decentralised applications. For example, the association of certain types of crypto assets with decentralised exchange liquidity pools.

5. **Monitoring and Alerting:** Various monitoring tools have been established throughout the industry to aid projects in receiving alerts about possible security breaches. While receiving this kind of information is crucial, the notifications are not entirely actionable due to the brief interval between the alert and the actual event.

6. **Artificial intelligence:** There is much speculation about employing new AI technologies to enhance smart contract code. However, tools like ChatGPT are still generic AI models. While they may effectively detect simple to medium vulnerabilities, they might not identify critical ones because they are new or because they require a high degree of expertise. As of now, relying solely on these technologies is not considered sufficient for ensuring comprehensive smart contract security.

7. **Standards and Best Practices:** It is crucial to utilise the techniques, tools, and services mentioned earlier in order to safeguard the security of the DeFi ecosystem. However, it is of greater significance that these resources are employed in accordance with established standards and best practices, ensuring an acceptable level of security and quality for decentralised applications in the DeFi ecosystem. These guidelines should be defined by industry leaders and cybersecurity experts, drawing upon technical and business use cases, to guarantee security, user experience, usability, and scalability of solutions.

It is essential to acknowledge that best practices and standards are ever-evolving concepts that must adapt to accommodate the industry's new use cases and technologies. This approach ensures that standards do not hinder the growth of the industry, but rather continue to support its progress, while protecting the stakeholders.

The emergence of collaborative communities working together to improve code and detect vulnerabilities, preferably at global level, is promising for the assurance of smart contract security. With the shared interest in maintaining safe and reliable smart contracts, developers, users, and blockchain administrators are likely to contribute their expertise to ensure robust security measures are in place.
Q21: Can you identify examples of smart contracts that should not be certifiable due to the nature of the services they provide?
X Yes
☐ No
If so, which ones?

Smart contracts that should not be certifiable are those that explicitly involve illegal activities and objectively harmful content, such as smart contracts that create ponzi and pyramid schemes or enable market manipulation.

Q22: What do you think of the rules put forward in this paper (section 3-2-2, item a) on how to certify smart contracts (pre-certification of called components, certification life cycle)?

As the industry matures, we believe there will be a need for more comprehensive standards and / or rules, including on certifying computer code. However, at this stage, efforts should be put on defining best practices, to be used as a basis for industry standards. This would include systematically analysing smart contracts and their dependencies to ensure that smart contract code is free from vulnerabilities. The initial focus should be on aspects that are crucial to the proper functioning of DeFi smart contracts. Life cycle analysis, static analysis, dynamic analysis, and software composition analysis provide a good starting point.

We believe in the importance of leveraging existing work and expertise from industry, used in the development of tools, services and smart contract standards helpful to smart contract certification. At this stage, regulators should concentrate on providing incentives for the development and the take-up of standards.

Overall, the stated approach seems comprehensive and aims to address the essential aspects of code certification, especially in the DeFi sector. However, striking the right balance between effective certification processes, costs of implementation, audits and the DeFi industries needs may be a challenge worth considering.

Q23: Should smart contracts embed a number of regulatory requirements in their code in the future?
☐ Yes
☐ No
Why?

Not necessarily. The heterogeneous nature of smart contracts, which stems from the variety of programming languages, platforms, and protocols used in their development, poses significant challenges to the creation of a regulatory framework that is both effective and fit for purpose and does not hinder innovation.
Maintaining a permanent dialogue with the DeFi industry and incentivising the development of and adoption standards would be an appropriate first step to help overcome these challenges. Any proposal to require embedding regulatory requirements on smart contracts should be subject to further discussion and it should, in any case, be limited to circumstances where there is a critical policy objective and the adoption of industry standards has been limited.

It would be crucial that any requirements do not hinder composability, scalability, or increase gas consumption, thereby affecting the usage costs to end users.

Q24: Who should set the security standards for smart contracts (refer to section 3-2-2, item b) and why?

In theory, security standards could be set by either (a) market participants themselves; (b) by public authorities; (c) by standard-setting agencies (e.g. International Organization for Standardization), which brings together the industry, regulators and the public.

At present, given the nascent stage of DeFi, we believe the industry should play a leading role in the development of any standards, leveraging on practical knowledge and the collaboration between the various players. This would ensure that any standards keep up with the pace of innovation and support it, rather than hinder it.

We believe there is scope in this process for involving public authorities, possibly through standard-setting organisations or observatories. Collaboration can lead to the development of standards that are widely adopted, address public concerns and are aligned with policy objectives.

Q25: Should interaction with uncertified smart contracts be discouraged or prohibited (refer to section 3-2-2, item c)?

☐ Discouraged
☐ Prohibited
X Neither discouraged nor prohibited

Why?

No. Interaction with uncertified smart contracts should not be discouraged nor banned. Restricting interactions would be challenging due to the diverse range of platforms, protocols and programming languages. It could also limit the innovation, utility, and interoperability of smart contracts across the DeFi ecosystem.

Instead, public authorities should focus on providing positive incentives for intermediaries to engage with certified smart contracts. As DeFi develops and certification options become more widely available, regulators may consider introducing negative incentives.
But prohibition should remain a measure of last resort. If restrictive measures are adopted, the focus should be on those smart contracts with the biggest potential impacts, i.e. those that provide functions or services deemed critical.

It is worth noting that certification is not mandatory for more traditional software or hardware companies. Certification serves as a means to ensure that companies adhere to and implement techniques that guarantee quality and an adequate level of security in software applications.

In addition, it is essential to acknowledge that the standards, best practices and certifications typically lag behind innovation. It is imperative that we do not hinder companies from both pursuing innovation and acquiring customers or developing their businesses due to a lack of certification.

**Q26: Who should bear the certification costs of smart contracts (refer to section 3-2-2, item b) and why?**

As a rule, the entity that owns and/or manages the smart contract should bear the costs of certification, as their smart contract is a service they are offering to the community. It should also be noted that it is possible for smart contracts, if programmed accordingly, to add fees when interacting with them.

However, the ultimate decision of who should bear the certification costs of smart contracts will depend on the specific context and nature of the smart contract, and should be discussed between industry participants, regulators and standard setters. Industry standards or regulation could also influence the certification cost allocation.

**Q27: Do you have any comments on the description made of the risks inherent in the decentralised oracle model? Can these risks be mitigated using a certification mechanism tailored to the specifics of these applications (refer to section 3-2-3)? Do you have any comments or alternative proposals for a framework governing the activities of oracles?**

Decentralised oracles play a significant role in providing reliable and accurate information to power various DeFi applications, but, as mentioned in the Discussion Paper, they can be susceptible to poor data quality, collusion, manipulation, and operational risks.

A decentralised oracle certification system could be one way to help mitigate these risks. However, certifying oracles in the DeFi space presents significant challenges for regulators due to the dynamic nature of the technology and the rapidly evolving industry landscape. Self-regulation could be a way to effectively address these challenges.
It's crucial to note that the majority of existing decentralised exchanges (DEXes) do not tend to utilise decentralised oracle solutions. They predominantly rely on large liquidity pools, sometimes belonging to other DEX's, to determine an asset's price. Weighted averages is an example of a robust solution to help safeguard users from abrupt market price shifts, such as those instigated by oracle price manipulation. However, a downside of this method is its perceived slower response to price fluctuations, especially during market downturns.

Circuit breakers can also be beneficial in situations of significant hacks, substantial market volatility or where oracles display unexpected behaviours. We are not currently aware of any DeFi decentralised applications that have implemented automatic incident response mechanisms consistent with the use of circuit breakers.

As concerns the proposal to provide data through a centralised entity, we believe that such an approach goes against the ethos of decentralisation that the blockchain ecosystem seeks to promote. This approach also has the potential to make the ecosystem more susceptible to single points of failure, as their infrastructure may not be as decentralised as a network of oracles.

Q28: Do you have any other regulatory suggestions that could contribute to reducing the risks associated with the application layer of DeFi?
☐ Yes
X No
If so, what are they?
No additional comment. Please refer to Q19

Section 3-3: Regulating the provision of and access to services

Q29: Do you think that in some cases it may be necessary to "recentralise" specific sensitive activities (section 3-3-1)?
☐ Yes
X No
If so, which ones? If not, why?

Incorporating appropriate regulatory oversight through legal frameworks or statutes in sensitive cases could help ensure the safety and stability of the DeFi ecosystem while retaining its decentralised qualities. Still, care must be taken to strike a balance between regulations and autonomy to prevent stifling innovation and growth in the DeFi space.

Q30: What do you think of the proposals on how to achieve this goal (incorporation requirements, making players with effective control liable, legal status for DAOs)? Do
you have any suggestions regarding the legal status of DAOs?

Establishing a legal status for DAOs to provide clear oversight and control, while also respecting the decentralised nature of DeFi, is worth exploring. This will require further work to develop proper governance structures and appropriate legal frameworks, similar to those found in foundations, that are representative of the DeFi ecosystem’s unique characteristics, aims and objectives.

Additionally, there is a lot of work that has already happened globally in relation to DAO foundations and global consistency regarding regulatory expectations should be pursued. We also look forward to the report by the HCJP and stand ready to contribute to this discussion in that context.

Q31: Do you agree with the description provided of the risks associated with "CeDeFi" on the one hand and "crypto conglomerates" on the other (box 6)?

The integration of CeFi and DeFi (CeDeFi), with appropriate guardrails, could lower many of the observed risks (e.g. money laundering, bad actors, security risks linked to scams, hacks, mismanagement of crypto wallets, simpler user experience, unsuitable products, conflicts and the safeguarding and administration of assets), whilst enabling DeFi to develop.

It is also critical not to paint all crypto companies with the same brush. Unscrupulous actors do not define this innovative and fast-growing industry. Reflecting on the crises of last year, it's important to recognize that it was FTX's misuse of customer funds and its failure to ensure that assets under custody were greater than its liabilities to customers that ultimately caused its insolvency. Responsible players in the industry have robust measures in place to prevent that from happening.

At a minimum, exchanges should follow these simple rules to protect user assets and ensure financial soundness: 1) hold user assets in custody 1:1 (bitcoin for a bitcoin, dogecoin for a dogecoin); 2) never trade against their users, or use customer funds in any unauthorised manner; 3) have no debt in their capital structure.

Q32: What requirements should apply to intermediaries facilitating access to DeFi?
X Information requirements
X Duty of care and duty of advice
X White paper publication requirement
X KYC requirements
☐ A comprehensive framework inspired by MiCA
☐ Other
Why?
Further work is needed on these matters, including how broadly the term ‘intermediary’ is defined. The relevance of any policy determined by relevant stakeholders e.g. G7 and global standard setting bodies will also need to be factored in. This may include:

- how the ‘scope of liability’ is decided to ensure it is appropriate.
- whether a liability regime should be modelled on existing legal precedent, if possible.
- the role of courts as the ultimate adjudicator on matters of liability.

Q33: Should the same rules apply to all intermediaries in DeFi (including, where appropriate, decentralised web interfaces)?

X Yes
☐ No
Why?

Please see the previous response.

Q34: Should access to financial products be conditional on customers’ financial literacy level and risk appetite?

X Yes
☐ No
Why?

Where critical financial decisions are at stake, it could be justifiable to consider what the appropriate level of access to DeFi products should be based on the level of financial literacy and risk appetite of customers. But, if implemented, any restrictions on access should be balanced and appropriately justified.

As a rule, adults should be allowed to make their own financial decisions. Provided they are offered sufficient information and have the chance to access appropriate advice, in most circumstances, individuals should take responsibility for assessing whether a financial product aligns with their needs and risk tolerance.

Furthermore, developing a standardised assessment to measure financial literacy and risk appetite accurately is challenging. For example, some of the currently available suitability tests pose a number of challenges, since wealth is not a proxy for knowledge nor risk appetite.

Finally, we believe market participants have a critical role to play in promoting education and financial literacy, in particular in a novel market such as crypto.

Q35: Do you have any other suggestions for regulating the provision of and access to services?
☐ Yes
Avenues for a regulatory framework: cross-cutting aspects

Q36: How can proportionality requirements (for small players) be taken into account in the various regulatory avenues put forward by the document (or proposed by you)?

Proportional regulation promotes financial stability, reduces unnecessary regulatory burden and compliance costs and ensures effective use of scarce supervisory resources. Combined with sensible industry standards/certification, it can contribute to lower the cost of barriers to entry and help smaller players compete in this innovative market.

In assessing the need for and scope and detail of standards and rules, we encourage regulators to take a risk-based and gradual approach. Standards and rules should be developed over time and be focused, as much as possible, on the largest protocols and services. Exemptions should be considered where these are critical for the early development of projects (e.g. as recognised in the discussion paper, minimum requirements on the number of validators can present a significant hurdle to the development of new blockchains).

Q37: What regulatory avenues -whether or not they are proposed in the document- could overcome the problems related to the possible extraterritoriality of actors (from a national or European point of view)?

The risks linked to extraterritoriality are not exclusive to DeFi, in fact they increasingly arise in traditional finance, in particular when financial services are provided through the internet. While regulators must not ignore these risks, they should not place undue emphasis on them to justify the introduction of additional regulation. This would be both ineffective and counterproductive.

As argued in other sections of this response, at the current stage of development of the industry, regulators should focus on providing positive incentives for the industry to adopt standards and, where appropriate, develop shared standards. These would increase consumer confidence and reduce the risks of extraterritoriality, even if indirectly.

Finally, the discussion and development on any standards should happen at global level as much as possible. By avoiding regulatory fragmentation, whilst ensuring equivalency, alignment or mutual recognition of any standards and rules, and the cooperation and information exchange between supervisors, regulators can help mitigate this problem.
Q38: Who should, in each case, monitor the implementation of the different regulatory tracks (whether they are put forward in this document or proposed by you)? With what means?

As argued above, at this stage, we believe the industry should play the leading role in developing any standards for DeFi. Where relevant and appropriate, regulators, in particular global standard-setting bodies, should support this process by monitoring and increasing the visibility of practices they would like to encourage and that address their policy objectives.