Boerse Stuttgart Group Response

to the BCBS Consultation about Cryptoasset standard amendments

Stuttgart, 20th March 2024

Management Summary

Implementing the current form of the standard would make it de facto impossible for institutions to invest in tokenized securities that are issued on a permissionless blockchain such as Ethereum. Permissionless blockchains offer substantial advantages in terms of security and cost efficiency for the capital market. Therefore, most of all tokenized securities currently use this technology. When looking closely at the technological risks and future technological and regulatory developments, we strongly believe it is more appropriate to assign permissionless blockchains to Group 1 instead of Group 2. The principle of technology-neutral regulation should be maintained.

As the sixth-largest exchange group in Europe, we provide the most innovative and reliable infrastructure and trading solutions. With strategic pillars in the capital markets business and in the digital business, we connect the potential of digital solutions for future capital markets with over 160 years of experience in secure and reliable solutions as an experienced regulated player in the sector. Today, we operate a complete end-to-end infrastructure for digital assets alongside traditional capital market activities. This encompasses brokerage, custody, and operation of a multilateral trading venue.

With the SC060 standard, the BCBS is laying the foundation for more legal certainty for institutional investors in cryptoassets. This represents an important step for the further professionalization of cryptoasset markets. We welcome the fact that the Basel Committee wishes to take account of the rapid market developments in the crypto sector and is putting further refinements and clarifications to the already finalized SCO60 standard out for consultation. However, we do not share the standard's assessment on the categorization of tokenized securities that are issued via a permissionless blockchain. We would like to explain the reasons in the following.

A categorical classification of permissionless blockchains prevents innovation and contradicts the principles of technology neutral supervision

In the current consultation paper[1], the BCBS states that some seemingly unmitigable risks prevent cryptoassets based on a permissionless blockchain from being classified in Group 1. The immediate consequence would be that tokenized securities, which use a permissionless blockchain, would be at a significant disadvantage compared to securities based on another technological solution. In our opinion, this would make permissionless blockchains significantly less attractive for issuing tokenized securities in the future, as institutional investors would face excessive capital requirements.

This is diametrically opposed to the principle of technology neutrality that the BCBS itself has formulated as an objective for the regulation of cryptoassets. In contrast, EU legislators demonstrate more foresight. For example, in the current draft Capital Requirements Regulation III, they plan to apply a technology-neutral transitional regulation for the capital backing of cryptoassets.

In general, an unnecessarily restrictive regulatory framework prevents innovation in a new technology such as blockchain. An open, decentralized approach to permissionless blockchains makes it possible

[1] https://www.bis.org/bcbs/publ/d545.pdf

to realize the advantages of a decentralized infrastructure in terms of robustness, immutability and risk reduction. By contrast, access-restricted ("permissioned") DLT infrastructures increase the dependency on certain intermediaries and thus lead to a systemic concentration of risk (“single point of failure”) in the infrastructure. This is a situation that is currently viewed very critically in existing major infrastructures and attempts are being made to mitigate through regulation.

In the following, we would like to address and refute some of the concerns raised by the BCBS on permissionless blockchains.

Special characteristics of tokenized securities

First of all, we would like to discuss a fundamental structural difference between tokenized securities and other cryptoassets. Unlike other cryptoassets, tokenized securities have a legal relationship between the issuer and the investor, which is defined by the terms of issue. This legal relationship can be comprehensively regulated (in Germany implemented through the “Electronic Securities Act” (eWpG)). This enables, for example, comprehensive control and influence by a registrar, which is monitored by a national supervisory authority.

Permissionless blockchains do not involve any risks that cannot be mitigated

The BCBS remains extremely vague in its rationale for its conclusion that permissionless blockchains are unsuitable for classification in Group 1. This is not acceptable given the severe consequences. In the current consultation paper, the BCBS only deals with the topic in a short paragraph, in which the following arguments are invoked without going into the necessary depth of detail:

- Dependence of the network on unregulated third parties;
- Political, legal, money laundering and terrorist financing risks;
- Risks in connection with the settlement finality of transactions, privacy and liquidity.

We would like to discuss these arguments below in more detail.

1. **Dependence of the network on unregulated third parties**

   This argument is based on classification conditions 3 and 4 of SCO60. We fundamentally disagree with the necessary mitigation measures prescribed there. Accordingly, a network must be operated in such a way that "material risks are adequately mitigated and managed". However, according to the BCBS this is only possible if all functions in the network are subject to certain minimum supervisory requirements such as functioning risk management, certain governance structures and possibly monitoring by a supervisor.

   These minimum requirements always serve to ensure the stability of a particular company or operator. However, the security and integrity of a DLT infrastructure are not based on the security of individual operators or institutions, but on its technical protocol, size and decentralization. The resulting independence from individual operators also means that there is no single point of failure. It would therefore be a mistake to view decentralization and lack of access permission as weaknesses or risks. It is precisely these features that are crucial for the security and resilience of a network. Even if not every single component can be checked, the network as a whole can be evaluated and checked very well. The number of nodes, the code, the smart contracts, network stability and security are some of the aspects that are publicly accessible and can be checked at any time. In addition, threshold values could be set in relation to the size of the network or its decentralization.

Permissionless blockchains are accessible to the general public. The source code used is - by definition - open source. The procedures and technical implementations are therefore subject to a constant public peer review process. This reduces the risk of cyberattacks. The governance structures are publicly accessible and verifiable. The open source concept also has advantages in terms of interoperability between different blockchain technologies. This enables the issuer of a security, for example, to react to any security problems that may arise in the infrastructure by switching to a different underlying technology. Corresponding plans must be included in the BCM concepts of the parties involved in issues. For example, the German eWpG has already implemented a legal framework that obliges issuers and registrars to take appropriate measures in such cases. This can also be required by the supervisory authority.

2. **Risks from the areas of politics, law, money laundering and terrorist financing**

The BCBS mentions political, legal, money laundering and terrorist financing risks, among others, without going into further detail. Two scenarios must be distinguished, regarding money laundering and terrorist financing in particular:

Transactions on a blockchain make it possible to clearly identify the owner of assets, at latest with the new Transfer of Funds Regulation (TFR) that has come into force in the EU. Tokenized securities cannot be acquired without identifying the investor. This traceability of transactions and immutability minimizes the risk of money laundering ex ante and significantly increases the detection rate ex post. Effective money laundering prevention and the prevention of terrorist financing are therefore much more possible in DLT infrastructures. It is therefore not a risk that cannot be mitigated.

In addition, the possibility of indirect terrorist financing is sometimes raised, as individual unregulated operators in public DLT infrastructures could use their rewards to finance terrorism. However, like the internet, a permissionless blockchain should be viewed as a general digital infrastructure. And just like the internet (without the traditional financial system would be unthinkable), the individual operator cannot be regulated, but the use of the infrastructure can.

Finally, it is not clear to us how one can conclude that a potential money laundering risk could be countered by strict capital requirements or exposure limits.

In contrast to permissionless infrastructures, it can be assumed that permissioned systems are much more dependent on individual companies or jurisdictions due to their lower level of decentralization and therefore involve a higher risk in these areas.

3. **Risks linked to the finality of transactions, privacy and liquidity**

The problem of a lack of settlement finality is also repeatedly discussed. In this case, there is a risk of an invalid transaction (for example due to a "fork" or a "reorganization"). This problem actually exists with blockchains that are based on a proof-of-work mechanism. Although this risk decreases exponentially over time, 100% finality is theoretically never achieved. In contrast, this problem does not exist with proof-of-stake consensus mechanisms (which are practically exclusively used for tokenized securities) due to the limited quantity and known currently staked coins. With Ethereum, transaction finality is guaranteed after approx. 10 minutes (two epochs).

A legal solution has already been found in Germany: For example, the issuer of a tokenized security can make provisions in the terms of issue as to when a transaction is considered final. If a transaction that has become final according to these specifications becomes invalid again

in the protocol, the status defined as final can be restored by applying of the administrative rights of the registrar for the token.

Apart from the mentioned risks and mitigation options, the planned "infrastructure add-on" gives the supervisory authority the opportunity to examine the technologies used for their risks and, to secure them with additional capital requirements. This creates pressure to further develop the technologies used to mitigate emerging risks and maintain interoperability. However, this measure should only be used in justified exceptional cases and as a last resort by the supervisory authority.

Conclusion

In summary, we strongly advocate maintaining the principle of technology neutrality. It should not be rejected prematurely. This prevents innovation and reinforces existing monopolies and access restrictions. Thus, we propose that tokenized securities should be allowed to be included in Group 1a regardless of the underlying blockchain technology applied. Instead of blanket bans on certain technologies, fundamental concerns regarding technology-specific risks should therefore be discussed in an open-minded manner.