German Banking Industry Committee

Die Deutsche
Kreditwirtschaft

Comments

BCBS Consultation regarding Cryptoasset standard amendments

German Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Dr. Silvio Andrae
Telefon: +49 30 20225-5437
Telefax: +49 30 20225-5404
E-mail: silvio.andrae@dsgv.de

Berlin, March 28, 2024

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

Introduction and scope

We appreciate the opportunity to respond to the Basel Committee on Banking Supervision's December 2023 consultative document on the prudential treatment of crypto asset exposures. As the Basel Committee continues to refine its guidance on the prudent management of crypto asset exposures, we would like to take this opportunity to provide further feedback on the matter of permissionless blockchain networks and the ability of industry participants to the mitigate risks associated with them.

We are concerned that the proposed risk add-ons for crypto assets could be excessively prohibitive to banks' ability to invest in digital assets. The assumptions for the criteria which lead to these risk add-ons are not clear. This could stifle innovation and limit the growth potential of the crypto sector and lead to a significant competitive disadvantage for banks on global financial markets.

It is important to note that banks have extensive experience in adhering to anti-money laundering and anti-terrorism financing regulations, which they have already successfully incorporated into their blockchain solutions. This expertise positions banks as reliable partners in fostering a safe and legally compliant environment on blockchain networks. The associated risks are not as novel and unmanageable, as the Basel Committee assumes. We are concerned that overly stringent capital requirements may inadvertently drive banks out of the market, thereby undermining regulatory compliance in this sector. It is essential that the potential unintended consequences of such measures are carefully considered to ensure a robust and well-regulated financial system in the digital age.

We therefore suggest to re-evaluate the assertion that permissionless blockchains are universally excluded from Group 1 classification. The prudential treatment of crypto assets should be technology-neutral and risk-based. In that sense, rather than basing the assessment solely on the general type of the entire network, we propose examining the specific blockchain software environment within which a crypto asset interacts to allow for a more differentiated assessment, taking into account the actual specific risks and respective mitigating measures of individual blockchains. To reflect this, we also propose specific revisions to the qualification conditions set out below.

In this comment, we have organized our feedback as follows:

1. General remarks on the advantages of public permissionless networks
2. A proposal to assess crypto assets based on the specific blockchain environment in which they operate, rather than the whole network.
3. A recommendation to take into account the existing regulations on crypto assets
4. Proposed modifications to certain elements of the qualification conditions

General remarks regarding public permissionless networks

In our opinion, the evaluation must also consider the risk-mitigating aspects of public permissionless networks, in particular well-established blockchain ecosystems, such as Ethereum. These ecosystems offer benefits that a privately authorized, closed-source blockchain is unlikely to achieve in the foreseeable future.
Utilizing long-established permissionless infrastructures may, in fact, increase the security of assets.

Firstly, the enormous number of available validators provides a de facto network availability and stability that will hardly be achieved by individually authorized validator operators. This goes hand in hand with fewer capacity constraints and higher scalability, especially considering scalability solutions like Polygon and similar projects. Also, public permissionless chains like Ethereum provide for possibly the most diverse pool of node operators.

Secondly, permissionless networks offer a high degree of transparency and traceability of transactions. As all transactions are subject to consensus and publicly accessible, the risk of manipulation or fraud is effectively mitigated.

Thirdly, the integrity and reliability of the source code profits from the code being open-source. Although maybe counterintuitive at first glance, releasing the source code to the public can lead to significantly safer code. Because open source software's source code is available for public scrutiny, this allows security experts and developers to identify and fix vulnerabilities quickly. This level of transparency makes it easier to detect and address potential security risks and communicate them to every user of the platform immediately. The open source community encourages collaboration between developers and users, leading to faster bug fixes and security patches. Many eyes can catch errors and weaknesses that a single developer might miss, and the established Blockchain networks can draw on a large and very active community examining every change to the code immediately. Also, open-source software is usually designed with security in mind, as the developers are aware that their code will be publicly available. This can lead to better security practices and a more robust security architecture overall.

Furthermore, the risks mentioned regarding potential loss of private and public keys and large-scale cyberattacks are not necessarily higher, and might even be lower, compared to the risks in traditional infrastructure and centralized digital solutions. As stated by the German Bundesbank, "a decentralised system could boost the security of assets or information transferred across the network. Unlike a centralised settlement platform, DLT has no single point of failure – that is, a point in a system that, if it failed to work correctly, would lead to a failure of the entire system. DLT's ability to compensate for an inoperable or compromised node is often seen as providing enhanced protection against failure.
If one copy of the DL is subverted by a malicious actor, other copies of the DL containing the original data can be used to correct those changes."[1]

Similarly, risks related to secure digital storage and the potential use of crypto assets for money laundering or terrorism financing can be mitigated by requiring financial industry participants to be themselves authorizes or use professional, authorized crypto custodians.

Instead of focusing on the overall network, we suggest placing a stronger focus on the isolated environment within a network the crypto assets is actually deployed in.

Firstly, we would like to address that there is a wide variety of different types of networks that could in principle be classified as "permissionless", if one only considers whether the operation of a validator node is basically open to everyone. Since the market has adapted to the security needs of financial industry participants in particular and there are now a number of blockchain solutions that, while

[1] https://www.bundesbank.de/resource/blob/707710/3f3bd66e8c8a0fbeb745886b3f072b15/mL/2017-09-distributed-data.pdf

essentially utilizing a permissionless infrastructure and its advantages, in fact offer far-reaching options for isolation of a business case, meaning that the permissionless core of a network only plays a very marginal and detached role. In these cases, the environment with which a crypto asset comes into contact is not comparable with purely public-permissionless systems such as bitcoin. We propose that isolated environments, which are separate areas specially created for the financial industry, should be considered permissioned environments for the purposes of capital requirements: The operator of these blockchain environments can design them in such a way that every participant in the environment is known and must have undergone any KYC, AML and sanction checks or other procedures before being admitted. The same measures can be applied - and made a prerequisite for participation in the isolated environment - that are also applied to traditional transactions.

The isolated environment can essentially be shielded from the rest of the network. It is possible to identify and freeze any unknown or otherwise suspicious assets before they can even enter the isolated environment. This way, a controlled space is created that allows for risk mitigation on par with that of the traditional financial sector.

When an isolated environment utilizes the validator nodes of the wider network, it does so only from a technical perspective, executing pre-defined smart contracts managed by the environment's operator. As the market has adapted to the security needs of the financial industry, a number of independent firms now offer smart contract security audits that can be employed to alleviate security concerns associated with smart contracts.

Existing authorization procedures should be considered as a mitigating factor.

Under many jurisdictions DLT-operators are subject to prudential supervision and must comply with specific statutory requirements according to local law, including minimum capital requirements, conduct of business rules, prudential rules and rules governing the relationship between the participants and the operator. Such regulated DLT-operators must assess its critical staff, the technical aspects and use of the distributed ledger technology as well as develop rules on accessing the distributed ledger, on risk management including any mitigation measures, IT and cyber risks, a detailed documentation on its arrangements related to the use of their distributed ledger technology that ensure the continuity and continued availability, reliability of the service and the integrity, security and confidentiality of any data stored by it.

The European Commission adopted on 24 September 2020 a digital finance package, including a digital finance strategy and legislative proposals on crypto-assets and digital resilience to ensure consumer protection, financial stability and a secure environment for market participants.Part of this is the Markets in Crypto-Assets Regulation (“MiCAR”) ((EU) 2023/1114) that entered into force on 29 June 2023 and will apply from 30 December 2024. MiCAR sets out rules for the authorization and supervision of crypto-asset service providers, including exchanges, custodians, and wallet providers. It also establishes requirements for the issuance and trading of crypto-assets. Under MiCAR, crypto-asset service providers are required to obtain authorization from their national competent authorities before providing services in the EU. The authorization requirements of MiCAR include approval conditions that address many (if not all) of the risks the Qualification Conditions of SCO 60 are also concerned with.

On the European level, there is also the DLT Pilot Regime ((EU) 2022/858) which is a regulatory framework that allows for the testing of distributed ledger technology (DLT) in the trading and settlement of financial instruments. Under the DLT Pilot Regime, market participants must obtain specific permission from their national competent authority to operate a DLT market infrastructure. Just like with the MiCAR authorization, many of the risks addressed in the SCO 60 are considered in the DLT Pilot Regime authorization process.

Furthermore, some EU member states have already enacted extensive regulations on certain crypto assets at national level.

Under German law, the Electronic Securities Act (eWpG) allows for the issuance of cypto securities (bearer bonds, bearer investment funds and registered equities) electronically. These crypto securities are not tokenized traditional securities, but rather are issued directly in electronic form and registered in a decentralized crypto register.

In order to ensure that these electronically issued securities do not pose any higher risks, this crypto register must be managed by an authorized crypto registrar. The business model and the technical implementation and resilience of the crypto register will be examined in detail in an authorization procedure. Part of this authorization process is the assessment of the same risks that the SCO 60 takes into account. In particular the crypto registrar must provide evidence of a tamper-proof recording system which protects registered data from unauthorized deletion and retroactive alteration. In this context it appears noteworthy that BaFin, in its Guidelines on Crypto Registrar services published on November 23, 2023, from a principal perspective declares public permissionless DLT systems as equally appropriate to fulfill the requirements of data integrity than their permissioned counterparts. If the crypto registrar obtains the authorization, the crypto securities managed in the register will then be treated by law the same as traditionally issued securities in all respects.

Moreover, regulated smart contracts are characterized by several risk-mitigating aspects:

- tokenization agents are authorized to reverse transfers which happen without instruction (e.g. to recover otherwise lost assets), to mint new assets or to burn assets.
- the use of whitelists ensures that only known and verified participants are able to own an asset.
- the possibility of freezing assets, e.g. in case a participant is sanctioned.
- redundant data backups to ensure clarity and transparency of the legal situation also off-chain. Thus, in case of an emergency, assets can be transferred to other DLTs or be redeemed into traditional assets.
- the tokenized traditional assets embody a stable right, independently of the DLT network used or the status of the permission, which generally exists through contracts between the parties and/or applicable laws.

In light of the robust authorization processes embedded within regulatory frameworks like MiCAR, the DLT Pilot Regime, and national legislation such as Germany's Electronic Securities Act, it is evident that these mechanisms address the same risks as those outlined in SCO 60. Consequently, we believe it would be unjustified to conflate regulated crypto-assets and regulated services with unregulated crypto assets. Doing so would also undermine the work being done by authorities and legislative bodies in fostering a secure and well-regulated digital financial ecosystem. We are of the opinion that recognizing the clear distinction between regulated and unregulated crypto assets for the purposes of capital requirements is crucial to encourage further innovation and to create a consistent and future-proof environment within the realm of digital finance.

Therefore, a paragraph should be added to SCO 60 that takes existing authorization procedures into account as a mitigating factor.

Considerations regarding specific risks addressed in the SCO 60 Qualification conditions

SCO 60.17: Risk governance and risk control policies

As mentioned above, any measures desired by the operator can be taken to mitigate risks, especially non-financial risks, in isolated environments. The operator of such an environment can have complete control over which participants are admitted to the isolated environment and implement functions that ensure the traceability of all transactions accordingly.

In practice, quarantine procedures using a multiple wallet structure are put in place for unknown assets to ensure adherence to anti-money laundering regulations and sanctions regimes. This guarantees that the isolated environment is shielded from the rest of the network and allowing for the identification and freezing of suspicious assets before they can enter the isolated environment.

From our perspective, the existence of a controlled environment within the blockchain space parallels the situation in the traditional financial industry. In both cases, there is a regulated and supervised sphere run by regulated entities in which actors operate within a secure, legal framework. By implementing quarantine protocols and other risk mitigation measures, the financial industry participants in the Blockchain industry can create a controlled space that is analogous to the regulated environment of traditional finance, thereby in the same way promoting security, stability, and compliance with legal and regulatory requirements in this space.

To mitigate cyber risks and risk associated with the loss of data, Banks can use experienced IT-service providers to implement several firewalls to protect a system. In addition, security information and event management systems are implemented that recognize predefined patterns that indicate specific malicious actions, such as manipulation of data, unauthorized or conspicuous access to databases, etc. Comprehensive authorization management systems and backup structures are a standard feature of any decent digital project anyway and can be utilized and adapted to further mitigate the risk involved with crypto assets.

We therefore propose not to focus on the entire ‘network’ within the SCO 60.17, but rather on the specific blockchain environment in which the crypto asset was issued.

SCO 60.17: Redeemability

In our opinion, the risk of crypto assets not being redeemable can be mitigated by the obligation to use authorized crypto custodians (e.g. according to MICAR). Professional backups can virtually eliminate the risk of losing private keys. With a sufficient number of validator nodes or access nodes that store a complete copy of the blockchain (as is the case with the long-established public permissionless blockchain projects), it is unlikely that crypto assets get irretrievably lost.

SCO 60.19: Appropriate risk management standards for validators – smart contract audits

As mentioned above, there are firms that specialize in security research and also offer to audit smart contracts. As self-executing contracts with predefined terms directly written in code, a smart contracts security, reliability and efficiency can be tested and certified just as any other piece of code. Another critical aspect of smart contract audits is the detection of hidden functions or vulnerabilities in the code, such as backdoors, that could potentially be exploited by dishonest actors. In response to the financial industry's need for secure software solutions, the market is already working on establishing standards in this area.

We believe that appropriate risk management standards, as necessitated by SCO 60.19, can be effectively demonstrated by obtaining a smart contract audit certification from a reputable firm, and we propose to amend the standard accordingly.