Response of Deutsche Börse Group

on the Basel Committee on Banking Supervision's

second public consultation on the prudential treatment of banks' cryptoasset exposures

Frankfurt am Main, 27th September 2022

Introductory remarks

Deutsche Börse Group (DBG) in its capacity as a financial market infrastructure provider uses modern IT and technological solutions to operate and service the financial sector worldwide. DBG's technologies are at the core of its operations and are an integral part of the regulated services we operate. We ensure the efficient functioning of markets, including but not limited to market data, trading, provision of indices, clearing, securities custody.

DBG clearly sees the advantages of new technologies and is actively seeking to use them. We have been familiar with the handling of financial market instruments and different asset classes for decades and we understand very well the risks associated with new types of cryptoassets.

We are currently working on the use of cloud technology and distributed ledger technology (DLT) / blockchain as well as automation of processes. We use these technologies in a rather gradual, granular and tested manner, hence continuing to guarantee transparency, stability and investor protection at all times. In addition, DBG is a majority shareholder of Crypto Finance AG. The Crypto Finance Group provides financial institutions professional and prudentially regulated access to the cryptoasset market.

In this context, we acknowledge the Basel Committee on Banking Supervision´s (BCBS) valuable work at monitoring developments in cryptoassets, and its efforts in coordinating its work with other global standard setting bodies and the Financial Stability Board.

DBG welcomes the efforts undertaken by the BCBS to further develop a prudential treatment for crypto-assets and conducting a second consultation. We already participated in the first consultation and appreciate that some of our comments have been taken into consideration (like the recognition of netting and hedging on page 18). Hence, we welcome the opportunity to participate in the second BCBS´s consultation and kindly ask you to consider the following remarks:

Exposure limit of 1% for banks

The proposed 1% exposure limit on group 2 cryptoassets lacks justification. It is in our view not adequately motivated by sound risk management and financial market policy practices. We note that the proposed methodology has no precedent in financial market regulation when comparing it to other economically more volatile and less predictable asset classes (such as other complex financial instruments). Crucially, conceptually similar overall market exposure limits on individual asset classes for banks have to the best of our knowledge not even been proposed during the 2008 global financial crisis despite the urgency of corrective measures at the time. Given the limited economic significance of cryptoassets, we fail to see such urgency at this point in time.

We note that such a restrictive limit on gross cryptoasset exposures would effectively render any business economically less viable in an emerging market segment with increasing market capitalization not only for crypto-native banks and but any associated financial institutions that fall under the ambit of the proposed BCBS standards. It also leaves insufficient room for different jurisdictions to base their own adaptions or interpretations of the limit. Such regulatory leeway for local authorities and policymakers is in our view essential to adequately cover and supervise the wide spectrum of cryptasset-based hubs and micro-economies that have emerged in recent years in different financial centers around the globe.

While we are generally not in favor of the introduction of such exposure limits, any such concept should for the reasons above be left at the sole discretion of national regulators and policymakers. In addition, we would like to remind the Committee that the proposed RWA coefficient is already a strong tool to limit exposure to group 2 cryptoassets that achieves the same goals of managing market and liquidity risks with significantly less detrimental side-effects.

Based on the considerations above, we are of the strong opinion that the overall exposure limit of 1% has no sufficient scientific basis, introduces major harmful effects on any prudentially supervised bank that wishes to introduce cryptoasset-based services without providing additional protective measures and should therefore be rejected in the finalized standards in its entirety. Any exposure limit that is perceived as necessary should be left at the discretion of national regulators and be issued on a case-by-case basis.

Considerations regarding the Basis Risk Test

The proposed basis risk test is in our view not sufficiently specified in terms of applicable sources for market prices, in terms of which aggregation method(s) to apply in case multiple sources are used and in terms of the time granularity of data. If not amended, this can in our view introduce unwanted room for regulatory arbitrage worsened by the fact that the test is an inclusion/exclusion criterion. In our market data analysis (cf. our Basis test analysis in Annex 1 below) we demonstrate that equally reasonable choices of market price sources and aggregation methods lead to severely different results for the basis risk test.

Furthermore, the current formulation of the test, based on counting the number of breaches in the peg-to-market value, does not provide a meaningful measure of the effectiveness of the stabilization mechanism. According to our analysis, a sudden price spike can be caused by a variety of reasons (e.g., a sale followed by arbitrageurs taking the opportunity and re-establishing the peg value) and does in our view not constitute a break of the stabilization mechanism per se. Thus, the basis risk test should take into account the duration of market price breaches by excluding breaches shorter than six hours.

Considerations regarding the Redemption risk test for inclusion in group 1b cryptoassets

Based on the results of our internal model for redemption risk (based on liquidity and systemic risk considerations) we agree with the general specification of this test. We emphasize that the implementation of the redemption risk test should focus more on the quality of the reserves rather than just on overcollateralization (cf. our Redemption risk analysis in Annex 1 below).

Infrastructure risk add-on

Please refer to our response to last year´s BCBS consultation on that matter (see Q8). We agreed back then with BCBS, that the risks associated with cryptoassets are at least partially different to those related to “traditional assets”.

However, we are still of the view that they need to be addressed from an IT-security/operational resilience perspective and not necessarily via the tool of additional capital requirements in order to help the technology develop.

This especially applies to Group 1 (tokenised traditional assets and cryptoassets with effective stabilization mechanisms) that meet the proposed classification conditions.

Hence, we are critical, when it comes to the proposed "infrastructure risk add-on" for several reasons.

- First, it goes against the principle of "technology neutrality", since no comparable capital add-ons are applied to other technologies used within banks. In particular, it is in our view not obvious why banks have to apply an add-on additionally to the obligations of determining and monitoring compliance of cryptoassets with the classification conditions (60.25) especially as conditions 3 and 4 seem to address the dimension of DLT infrastructure already. While we recognize that every technology bears an intrinsic risk, which has to be managed appropriately, we do not see why this form of treatment of the technology would be justified or why the existing regulatory tools to introduce specific operational risk add-ons on a case-by-case basis are not sufficient.
- Second, a blanket 2.5% add-on does not capture the important technological and conceptual differences between e.g. single-chain cryptoassets, multi-chain cryptoassets, cryptoassets issued by central authorities, cryptoassets on permissioned/permissionless blockchains, etc. and is therefore not a suitable means of distinction.
- Third, an add-on that is independent on infrastructure quality does not give an adequate incentive to infrastructure users/developers to improve the stability and reliability of the infrastructure.
- Fourth, the draft paper only mentions *"infrastructure risks"* and "*unforeseen risks"* (page 2 and respectively 4), while paragraph 60.57 only states that cryptoassets "*may pose various additional risks*". Hence it is not sufficiently clear which concrete risks are addressed here (see also our request for clarification on risk management further below) and it is not specified how the 2.5% add on would actually cater for that risk.

We would either propose that local supervisors and regulators are empowered to introduce a risk-based add-on that takes

(I.) the individual specifications and properties of the underlying DLT as well as
(II.) the associated financial institution(s) that wish to deploy the DLT-based service

into account or reconsiders the risk-based add-on in general and applies a more differentiated approach. We would propose a differentiation according to be defined criteria, like:

1. The "add-on" would not be necessary in the context of infrastructures, if the infrastructure is offered or will be used by a regulated entity with respective financial markets regulation in place (e.g. authorization/licenses). Hence these entities are already subject to rules and regulations focusing, among others, on IT security and operational resilience [like "*Digital Operational Resilience Act"* in the EU and various regulations at the Member States level]. This concept has been foreseen e.g. in the context of "stablecoins" issued by regulated financial entities already and could be integrated in the context of prudential requirements as well.
2. The "add-on" should not apply in controlled "DLT-permissioned environments" where there is a clearly "responsible operator/consortium of operators" as they could made liable, the participants are known and risks therefore could be adequately addressed, without putting the burden of a "flat add-on".
3. To avoid any double regulation, the "add-on" should also not be applicable, if on Member State or jurisdiction level provisions for DLT-based infrastructure are already in place [like the "*Markets in Crypto Assets Regulation*" and the "*Digital Operational Resilience Act*" being also applicable for the whole financial sector, including banks, in the EU]. If such regulatory requirements would be in place, they would cover already the risks related to IT security, risk management and investor protection in order to protect market stability as well as rules to hold "own funds". A duplication of requirements should be prevented in any case.

Classification conditions and permissionless chains

In general, we would like to confirm that the use of DLT for certain settlement or recordkeeping purposes does not necessarily subject the related asset to the cryptoasset exposure framework.

On page 4, BSBC asks for feedback on permissionless blockchains and states "*As currently specified, it is highly unlikely that any cryptoassets based on permissionless blockchains will be able to meet the classification conditions to be included in Group 1*". At the same time BCBS asks for comments on "*what modifications to the classification conditions would be required to permit the inclusion in Group 1 of cryptoassets that use permissionless blockchains*". The following comments are focusing on "tokenized traditional assets" and especially securities.

While every technology bears a risk, which needs to be managed appropriately, we do not see why the tokenized securities should not be eligible to fall into group 1 regardless of the underlying technology. From our point of view and referring to the important and well-established principle of "technology neutrality" in financial market regulation: instead of focusing on the technical characteristics of the DLT, the regulatory environment should be taken more into account. Especially, as long as the tokenized security confer the same legal rights as traditionally issued assets or when transferring tokenized securities between regulated intermediaries.

In case jurisdictions allow for securities issued on a DLT, they fall in the same regulatory scope as "traditionally issued" assets (e.g. Germany, Switzerland, France and Luxembourg). According to our analysis, there is as a general rule also a dedicated financial service license required to perform such tokenized securities services, hence the same or at least comparable rules and standards apply as for traditional securities services. We note that the aforementioned standards do not only apply when it comes to the adherence to established capital/liquidity & market stability-oriented regulatory provisions, but also to the extent that conduct-related standards are concerned. As tokenized securities are therefore treated similarly from a regulatory perspective, we conclude that they must also be treated the same, when it comes to capital requirements.

Regardless of whether the network is organized in a central or decentral manner, in both cases dedicated authorization procedures need to be fulfilled, which includes several requirements related to questions on the organization, operational resilience, risk management, compliance and other important prudential safeguards. This also implies that in these jurisdictions there is always a liable and supervised actor (e.g. a registrar in Germany) present, which fulfills important functions on the network and the register. In addition, the access to specific functions of the register based on smart contracts can be restricted by an entity, which would be often supervised, like the registrar in Germany[1].

[1] In the German context, issuances of securities by means of a DLT / Blockchain is possible under strict conditions only. In particular, a registrar is responsible for maintenance of the register running on a DLT protocol. Here, while generally anyone who desires to participate (issuers, validators, investors) can do so (in case of a permissionless protocol), regulation requires the registrar to only allow those applicants to make use of the register if they meet the participation criteria (e.g. trustworthiness needs to be proven). This includes also a dedicated onboarding procedure. This means, a whitelist of participants is created and that others who fail to meet the participation and KYC/AML criteria cannot access the register. As a consequence, a regulated entity would offer business with regard to securities issued by means of DLT.

In the context of this consultation, banks would therefore interact with regulated entities which brings a high level of security already, regardless of the protocol used and stands in strong contrast to early developments in the unregulated cryptoasset trading market.

In summary, we propose to consider more the principle of technology neutrality and also to take the regulatory environments of actors more into account. We conclude that at least as far as securities in the sense of "tokenized traditional assets" are concerned and the respective regulatory requirements are met, they should be able to meet the classification conditions and therefore be eligible for group 1a, irrespective of the DLT/blockchain technology used.

Different treatment needed, if DLT is used, but no "cryptoasset" is changing owners or is even moved

If DLT is used as a form of "database" / "datastore" and only information is digitally recorded, this should a priori not be in scope of the proposed recommendations. Hence, it is our understanding that the consultative document does only make a statement on the use of DLT or similar technologies by the banks, their clients and the banks´ service providers, as long as they do expose the banks (directly/indirectly) to cryptoassets. Consequently, it does only require the "add-on" with regard to capital requirements for the use of DLT as such.

To make it more concrete, in the case of HQLA^X the "traditional assets" remain custodied through a regulated custodian. The Digital Collateral Record (DCR) manifested on the DLT represents a "record of ownership" that can be transferred on the DLT without requiring physical settlement, is recognised as a ledger update by the regulated custodian, and provides unequivocal legal title transfer between parties, allowing access directly to the referenced securities through the regulated custodian. The lack of physical securities movements and involvement of the regulated custodian reduces the operational risks associated with such securities movements, and the DCR has no value independent of the traditional assets. Additionally, there is no operational or technical failure of the DLT that would jeopardise the ability of the rightful owner from accessing the traditional assets through the custodian. This model, where the 'cryptoasset' is a data record (not a token with an independent valuation and lifecycle), should be represented as a separate category or subcategory in the BCBS classification.

Other requests for clarifications and comments

- Both classification conditions 3 and 4 for inclusion into group 1b cryptoassets (paragraphs [60.22] to [60.24]) require that entities performing "transfers" be regulated, supervised, and sufficiently mitigate and manage any material risk. We ask BCBS to clarify whether this includes transfer of cryptoassets between private retail individuals, as this could in our view prevent any cryptoasset based on permissionless blockchains from being included in group 1b.
- We ask BCBS to clarify whether the capital add-ons of paragraphs [60.15] and [60.57] should follow the same methodology (increase in risk weight), due to their similar wording but very different amounts (100% vs 2.5%).
- The BCBS paper mentions at several occasions "*subject to appropriate risk management standards*". We would prefer, if "appropriate" could be further detailed to be more precise on the necessary requirements.

***

We hope that our comments as well as the Annex 1 hereafter will be helpful for the upcoming consultations and are available for any clarifications and further discussions.

Annex 1

This Annex contains **supporting evidence** regarding the quantitative classification conditions for Group 1b cryptoassets (stablecoins). Specifically, we conducted a data-based and methodological review of the **Basis risk test** and the **Redemption risk test**. A detailed analysis will appear in a peer-reviewed paper by Furlan et. al at a later point in time.

Quantitative classification conditions for Group 1b cryptoassets (stablecoins)

A. Basis risk test

i. Introduction

Based on the BCSBS consultative paper, we have examined the effectiveness of the proposed testing methodology and the derived quantitative classification conditions for a classification as a Group 1b cryptoasset ("stablecoin").

According to the BCBS proposal, the number of days where the peg-to-value difference exceeds 10 basis points is a decisive element for passing the test. However, the basis test as formulated in the current version of the consultative document is ineffective as a measure of the peg stability and introduces unwanted potential for regulatory arbitrage, if not specified accurately.

We observed from the consultative document that it is currently not specified which prices should be considered to check the condition and which time granularity would be relevant (e.g. low / high /open / close prices): depending on which price is chosen and how the events are defined, the result of the baseline test will be different. We have therefore examined four possible methodologies for price discovery (see ii. Scope of the analysis) and compared the respective differences (see iii. Results of the analysis).

ii. Methodology of the analysis

In our subsequent analysis, we used hourly OHLCV (Open High Low Close Volume) candles from the open source-database Cryptocompare[2] for the 12 months between August 1st 2021 and July 31st 2022. Due to the lack of specification provided in the consultative document, we examined four different methodologies to obtain a representative price for the stablecoin:

1. Using hourly low prices from all available venues, compute the hourly volume-weighted average of prices across venues. If the hourly price falls below 1 – 10bp during one given day (respectively, 1 – 20bp), that day is counted as a breach.

2. Using hourly low prices from all available venues, compute the hourly maximum of low prices across all venues, discarding all prices where hourly volume is less than 10k USD. If this hourly price falls below 1 – 10bp during one given day (respectively, 1 – 20bp), that day is counted as a breach.

3. Same methodology as point 2 but excluding hourly volume below 1mn USD.

[2] See https://www.cryptocompare.com/.

4. Using hourly open and close prices from all available venues, compute the hourly price for all venues as the average between open and close price. Then compute the volume-weighted average price as in point 1.

iii. Results of the analysis

It can be seen from the table below that the definition of which price to use for the test has a large impact in the results:

Token	Method	Number of breaches (10bp)	Number of breaches (20bp)
USDC	average of hourly low prices	142	93
	maximum of hourly low prices (excluding venues with hourly volume lower than 10k USD)	1	1
	maximum of hourly low prices (excluding venues with hourly volume lower than 1mn USD)	54	43
	average of hourly open/close prices	11	2
USDT	average of hourly low prices	80	25
	maximum of hourly low prices (excluding venues with hourly volume lower than 10k USD)	7	0
	maximum of hourly low prices (excluding venues with hourly volume lower than 1mn USD)	50	2
	average of hourly open/close prices	41	4

iv. Considerations regarding the effectiveness measurement

Secondly, the basis risk test as described in the consultative document is not a meaningful measure of the effectiveness of the pegging mechanism. The test does not specify the pattern of intraday prices that defines a breach event. There are patterns that have no power to break the peg but cause only short-term fluctuations such as mistrades, errors, attacks on the peg without enough market power share, or simple market operation. Such downward price deviations from the peg are quickly compensated by the mechanism by driving prices back to the peg. Such events or patterns should not be included in the test.

Breaking a peg requires a strong shock on the stablecoin supply (i.e., generating excess supply) or on the reserve asset values (i.e., implosion of asset prices). The cause for such a "shock" can be significant attacks or possible contagion of asset price shocks channeling to the reserves. The statistical patterns of price movements derived from such events show *an essential negative price drift* in a short period, i.e. successive price deviations become stronger, and the distance to the peg value increases. This pattern may be stopped and reversed if countermeasures are strong enough to stabilize the market and avoid a sell-off leading to a lasting value decrease of the stablecoin.

As supporting evidence, we conducted an analysis of the duration of price deviations, when prices are computed following the methodology 1 above. It can be observed that the majority of price deviations is short-lived for USDC and more substantial for USDT:

Token	Breach duration (hours)	Number of breaches (10bp)	Number of breaches (20bp)
USDC	**1**	142	93
	3	7	3
	6	0	0
	9	0	0
	12	0	0
	24	0	0
	48	0	0
USDT	**1**	80	25
	3	44	5
	6	34	3
	9	30	3
	12	30	3
	24	16	3
	48	7	0

v. Conclusion for the Basis risk test

Based on the results above, we propose to **include the duration of the price deviation as a criterion** in the basis risk test, for example by **excluding from the count all price deviations that are shorter than 6 hours**.

B. Redemption risk test

i. Introduction

According to the BCBS proposal, the value of reserve assets needs to be sufficient to enable the cryptoassets to be always redeemable for the peg value to pass the Redemption risk test. This requires that the reserve assets are liquid assets in any period, i.e., they can be bought and sold in arbitrary size to restore required over-collateralization or to buy back stablecoins without having a price impact.

However, the TerraUSD incident demonstrated that without a "reserve quality requirement" the liquidity assumption fails to hold true in periods of stress. Furthermore, some reserve reports of stablecoin issuers highlight that a significant fraction of traditional assets which failed to keep their value during the financial crisis of 2008 are used as reserve assets. Therefore, the quality of the reserves and contagion risk need to be considered in the redemption test for it to be effective.

ii. Methodology of the analysis

To take into account value, liquidity, quality of assets and contagion, a network analysis provides insights into which factors matter to ensure redemption stability. Our analysis incorporates the main reserve providers in the traditional asset space (U.S. Government, banks, corporates, money market funds) as well as cryptoassets. The interlinked web of the different balance sheets and flows provides insights into which factors matter to ensure redemption stability at the network node of stablecoin issuers. Furthermore, such an analysis also shows the price impact on reserve assets that would result from a mass stablecoin redemption, addressing the concerns raised, among others, by the Federal Reserve in June 2021.

iii. Results of the analysis

Our preliminary analysis shows that the quality of underlying assets (both in terms of price stability and redeemability under stress) is more important to the stablecoin price stability and systemic stability than overcollateralization.

The following example, obtained from the systemic risk model with simple but realistic assumptions on balance sheet size and liquidity, shows the maximum redemption percentage that can be incurred by a stablecoin without defaulting, with respect to both overcollateralization and reserve assets composition.

	Overcollateralization percentage					
Percentage of liquid asset	**0.1%**	**0.2%**	**0.5%**	**1%**	**2%**	**3%**
0%	2%	4%	10%	20%	41%	62%
10%	2%	5%	13%	25%	51%	76%
20%	3%	6%	16%	32%	65%	97%
30%	4%	8%	21%	42%	84%	100%
40%	5%	11%	28%	56%	100%	100%
50%	7%	15%	38%	77%	100%	100%
60%	10%	21%	54%	100%	100%	100%
70%	15%	31%	78%	100%	100%	100%
80%	21%	42%	100%	100%	100%	100%
90%	24%	49%	100%	100%	100%	100%
100%	22%	45%	100%	100%	100%	100%

The table above shows that overcollateralization is only effective in conjunction with a high percentage of liquid assets, and that with a low percentage of liquid assets, there is only a limited advantage in increasing overcollateralization.

iv. Conclusion for the Redemption risk test

The following insights should be part of the design of the redemption risk test:

(a) The redemption risk test should distinguish between stablecoins that are backed by only cash and short-term liquid assets (e.g. treasury bills) and stablecoins that are backed by less liquid assets that potentially introduce counterparty and systemic risk.

(b) For treasury bills and bonds, access to the repo facilities of the Federal Reserve Bank of New York plays a key role in the ability of the stablecoin issuer to obtain funding.

(c) Stablecoins backed by cryptocurrencies have higher risk of a downward spiraling effect in the stablecoin price, where sales of crypto reserves and consequent price reduction could trigger a loss of confidence in the crypto market leading to higher stablecoin redeems, in a feedback cycle.