September 30, 2022

Basel Committee on Banking Supervision
Secretariat
Bank for International Settlements
CH-4002 Basel
Switzerland

Re: Second Consultation on the Prudential Treatment of Cryptoasset Exposures

Dear Basel Committee on Banking Supervision:

Custodia Bank is a U.S. dollar-and-digital-asset bank ("dada-bank"), chartered to provide a compliant bridge between the U.S. dollar and digital asset financial systems. Custodia Bank is a depository institution whose application to become a Federal Reserve member bank is pending. The Wyoming State Banking Board granted our bank charter in October 2020. We received our certificate of authority to operate from the Wyoming Division of Banking in September 2022, and we will soon begin bank operations.

This comment letter will focus mostly on the Committee's proposed treatment of permissionless blockchains when used *as technology* – in other words, *as payment rails* – as distinct from their use *as assets* held by a bank.

The main concern is that the Second Consultation will create unintended consequences that will weaken the competitiveness of banks in payment technology, enabling fintechs and broader technology companies to take advantage of the unnecessary technology restrictions placed on banks by the Committee's proposed approaches. Our key concerns include that the proposed approaches: 1) neglect to differentiate the risks to banks between base-layer permissionless blockchain assets versus assets issued on permissionless blockchains that have *issuers*, 2) needlessly dictate banks' technology choices and 3) risk blocking banks from a coming payment technology pivot that will likely affect the entire industry. The letter also provides further comments on four other topics: 1) Basis Risk Test; 2) Network Design, Traceability; 3) Supervision of Involved Entities and 4) Operational Risk/2.5% Infrastructure Risk Add-On. These comments address the distinction between cryptoassets issued by a bank versus a non-bank and discuss how banks have the tools to block illicit finance from using their applications running on top of permissionless blockchains.

A. Permissionless Blockchains

The Committee noted in its Second Consultation: *"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."* (emphasis added)

The term "based on permissionless blockchains" is unclear and we recommend that the Committee clarify it. By the most conservative interpretation, the phrase would seem to imply that *any* asset that touches a permissionless blockchain – in any way – is automatically Group 2. In this letter, we presume that interpretation is correct. If so, there would be three problems with this approach.

1. It Neglects The Markedly Different Risks To Banks Between Base-Layer Permissionless Blockchain Assets Vs. Assets ***Issued*** On Permissionless Blockchains: The proposed approach neglects the critical distinction between base-layer assets (e.g., Bitcoin or Ether), which do not have an issuer, and assets that ***do*** have an issuer, such as stablecoins issued on the Ethereum blockchain or a CBDC[1] issued by Norges Bank as an ERC-20 Ethereum token. There are significant differences in the operational, market and liquidity risks to a bank between issued assets and base-layer assets (e.g., between an ERC-20 token vs. Ether itself). For example, the issuer of an ERC-20 token controls its smart contract, which means the issuer can freeze assets (e.g., for compliance reasons or to respond to law enforcement), or can burn and re-issue tokens when an owner legitimately loses their private keys. The same is not true for base-layer Ether. Consequently, the risks to banks from the two types of assets are vastly different, even though both are "based on permissionless blockchains" and, presumably, would be lumped together in Group 2 under the Committee's current proposal. The Committee should treat *issued assets* issued on permissionless blockchains as eligible for Group 1 treatment when the issuer has control of the smart contract or equivalent, the issuer is a bank, and the permissionless blockchain used by the issuer meets bank-level risk management standards.

   In a similar vein, the Committee should consider clarifying the definition of digital assets at SCO60.136(2), which expressly excludes "digital representations of fiat currencies." Does a tokenized bank deposit issued by a commercial bank qualify as a "digital representation of fiat currency," or is the "digital representation of fiat currency" exemption reserved for tokens issued by central banks only, but not commercial banks? Next, what if such a "digital representation of fiat currency" is "based on a permissionless blockchain"[2] – since that distinction seems to matter elsewhere in the Second Consultation? The Committee should provide clarity regarding these definitions and, most likely, distinguish between whether or not the "digital representation of fiat currency" is issued by a bank or a non-bank (since, if issued by a bank, it is most likely ***money***[3]).

2. It Dictates Banks' Technology Choices, Which May Impact The Fungibility of Money: Blockchains, at bottom, are just a form of database technology. Bank regulators have historically not dictated banks' technology choices, such as whether a bank should deploy database software from Oracle or Microsoft, for example. Yet, by lumping together all assets "based on permissionless blockchains"

[1] Custodia acknowledges the Committee's statement that the Second Consultation does not describe prudential treatment of CDBCs, and that it "will give further consideration to the treatment of CBDCs if and when they are issued." However, subsequent to the release of the Second Consultation in June 2022, Norges Bank announced in September 2022 that its prototype CBDC is an ERC-20 token issued on Ethereum (i.e., a permissionless blockchain). This and similar examples of *bank-issued* stablecoins that already exist on permissionless blockchains suggests that the Committee should not lump together all assets "based on permissionless blockchains" into Group 2. In Custodia's view, the more appropriate distinction is which type of entity issues them (i.e., banks or non-banks). If issued by central or commercial banks, then such assets would substantively and legally be ***money***. The technological form of such money should not dictate its risk weighting; rather, what should matter is whether or not a bank issued the instrument. https://www.finextra.com/newsarticle/40967/norwegian-central-bank-taps-ethereum-for-cbdc-work

[2] *Supra*, note 1.

[3] In the U.S. specifically, a further distinction would be necessary between a depository institution vs. a non-depository trust bank. Depository institution liabilities are money, but trust liabilities are not.

into Group 2, that is what the Committee's proposal would seem to do – simply by creating a disincentive in terms of capital cost[4] for banks to use a permissionless blockchain as a technology choice. Consequently, if the proposal were to be adopted as drafted, some forms of bank-issued money (such as tokenized bank deposits or bank-issued stablecoins[5]) could automatically be categorized as Group 2 cryptoassets simply by nature of the bank's choice of which database technology to use. Applying disparate risk weightings to different forms of ***money*** based on which technology the bank uses would be precedent-setting, and such an approach would make money non-fungible (among other unintended consequences). The definition of "money" in most of the world's legal systems does not dictate its specific form. Rather, the key distinction is that *banks* issue the money – specifically, the central bank and commercial banks,[6] which are special types of legal entities bestowed by statute with the right to, among other things, issue ***money***. It is this distinction (bank vs. non-bank) that the Committee should maintain, rather than a distinction based on the technology choice of the banks issuing the money.

Moreover, the practical effect of the Second Consultation approach, if enacted, would also be to block banks from choosing to engage with permissionless protocols *as payment rails* for fiat currency. This could hamstring banks relative to non-banks in the face of growing competition from the technology sector as permissionless blockchain protocols scale. ***Non-banks are already using permissionless blockchains as payment rails for settling payments outside banking systems.***[7] In the face of this, Custodia Bank believes a necessary technology pivot is coming for the banks – namely, to use these very protocols as payment rails for fiat currency – which the Committee's current proposal would block if it were adopted as currently drafted.

3. It Risks Blocking Banks From A Coming Tech Pivot That Will Likely Affect The Entire Industry: The Committee's current proposal, if enacted, would have the unintended consequence of preventing

[4] One challenge with the proposed 1250% risk weighting for Group 2 cryptoassets is its calibration to the standard 8% exposure level, which results in a 100% capital charge at the 8% level. However, in practice most banks target capital ratios greater than 8%. This means such banks would need to hold greater than 1:1 capital for exposure to Group 2 cryptoassets – and the better capitalized the bank, the greater the excess capital cost involved with handling Group 2 cryptoassets. An alternative approach for the Committee to consider, instead of applying a 1250% risk weight, would be simply to require 1:1 capital for all Group 2 cryptoassets, plus the already-contemplated operational risk capital charge in SCO60.105 to compensate for operational risk caused by differences in settlement timing (as discussed in this June 2021 post: https://www.forbes.com/sites/caitlinlong/2021/06/24/bis-proposed-capital-requirements-for-cryptoassets-vital-move-but-theyre-too-low-for-bitcoin/?sh=2845aa02546f).

[5] *See*, *e.g.*, https://www.bitcoinsuisse.com/cryptofranc.

[6] In the U.S. specifically, a further distinction between a depository institution and a non-depository trust bank would need to be made. *Supra*, note 3.

[7] *See*, *e.g.*, the significant progress in Lightning Network adoption, use and development by non-banks (including by both fintechs and broader technology companies), including by Square/CashApp, Strike (both for online purchases via integration with Shopify and point-of-sale purchases via integration with NCR), MicroStrategy (building Lightning Network software-as-a-service), Lightspark (started by the former Facebook Libra team), Blockstream, NYDIG, Lightning Labs and others. Lightning Network is a Bitcoin layer 2 protocol that scales Bitcoin. Lightning Network payment channels are analogous to payment clearinghouses and correspondent banks in that they provide netting, thereby scaling the base-layer money and increasing its transaction velocity (since not every transaction needs to be settled in the base money). Lightning Network's throughput capacity roughly equals that of Visa, and payments made over Lightning cost virtually zero. Each payment channel is anchored to base-layer Bitcoin, but has no limit on its transaction velocity. As an internet-*native* payment technology already in use, both fintechs and broader technology companies now have access to payment rails for settling payments *outside banking systems*, and it is scaling rapidly. It will take Lightning a few years to lay down scaling infrastructure before hitting its tipping point at scale. But make no mistake, it's happening.

the banks from being able to pivot to using permissionless blockchains *as payment rails* for fiat currency. We believe scaling technology for permissionless blockchains has arrived, and that banks will need to pivot to using it in the next few years – just as telecom companies pivoted to using Voice Over Internet Protocol ("VOIP") when its scaling technology (broadband) arrived, circa 2003. Back then, at its pivotal moment, telecom regulators saw what was coming, properly recognized that superior new technology had arrived and enabled the incumbents to adopt it. Within a flash, their old copper-wire networks became obsolete – but the telecom companies that operated the outdated networks did not become obsolete, because they successfully pivoted to using the new technology before the unregulated providers beat them to it and had a chance to build durable network effects.[8]

The analogy to telecom is apt because Bitcoin is a "Money Over Internet Protocol," as is Ethereum, potentially. Bitcoin and Ethereum move value data around the internet *natively*, just as VOIP moves voice data around the internet *natively*. Most people disparage Bitcoin, Ethereum, et al. as protocols that can't scale and can't possibly threaten the incumbent financial industry, just as they denigrated VOIP. But the scaling technology is now here – it's called the Lightning Network, which is a Bitcoin layer 2 protocol.[9] Its throughput capacity roughly equals that of Visa, and payments made over Lightning cost virtually zero. There are other scaling technologies, too. If we're right and scaling technologies for internet-*native* money protocols have arrived, then many legacy systems operating in the financial system today will be obsolete within a handful of years.

But the "aha!" of these "Money Over Internet Protocols" isn't cost or scale. There are two "ahas" that matter far more: integration speed/cost and developer communities.

- Integration speed/cost: Anyone in the world can become members of these emerging payment networks in the span of a few hours, using equipment that costs a few hundred dollars.

  Banks' IT systems will never be able to compete with that. The paradigm has shifted: payment system integration time is now measured in hours, not in months or years – and in a few hundred dollars, not a few million dollars. It's obvious which approach will win.

- Developer communities: Open, permissionless protocols have huge developer communities, which compounds the speed of their ecosystem development and network effects. Network effects are all about compounding. The code libraries and developer tooling available for Bitcoin and Ethereum are critical infrastructure that banks' proprietary systems cannot replicate. Moreover, these developer communities organically create interoperability. Banks' "walled garden" systems with closed groups of developers will never be able to keep up with their pace of innovation.

---

[8] https://www.forbes.com/sites/caitlinlong/2022/09/23/banks-are-about-to-face-the-same-tsunami-that-hit-telecom-twenty-years-ago/?sh=86996157a7a8

[9] Together, the Bitcoin Protocol (BP) and its Lightning Network Protocol (LNP) are joining the ranks of other open network protocols akin to TCP/IP. The Bitcoin Protocol has movable units of scarce value that can flow within its network, similar to the Internet Protocol (IP). The Lightning Network Protocol (LNP) acts as a second layer built on top of BP, which permits nearly instant and cheap exchanges of data packets on BP, similar to how the Transfer Communication Protocol (TCP) does it with the Internet Protocol.

Recommendation: Again, our comments presume that the Committee meant by the phrase *"based on permissionless blockchains"* to include any asset that touches a permissionless blockchain. If that presumption is correct, Custodia Bank recommends that the Committee consider carving out ***issued assets*** from the term "based on permissionless blockchains," thereby making them eligible for Group 1 treatment, when the issuer has control of the smart contract or equivalent, the issuer is a bank, and the permissionless blockchain used by the issuer meets bank-level risk management standards. If the Committee accepts this recommendation, it could adjust Classification Condition 2 to recognize the ability for the bank, as issuer, to set legal terms by contract with its customers (including for settlement finality, which is commonly set by contractual agreement in other instances across traditional financial markets today). The Committee would also need to adjust Classification Conditions 3 and 4, as further explained below.

B. Comment on Classification Condition #1: Basis Risk Test

The Committee noted that its initial proposal to require a Group 1b cryptoasset's stabilisation mechanism to be effective at all times received several comments, expressing concern with the "calibration of the test and cliff effects." In its Second Consultation, the Committee introduced a second threshold to reduce cliff effects.

The second threshold does not solve the issue, though, because differences in the peg-to-market value are not within an issuer's control. A peg-to-market-value difference could easily diverge temporarily due to simple supply/demand imbalances that have nothing to do with the ability of the issuer to redeem the obligation at par. What really matters is the issuer's ability to redeem at par.

But there's more: if a cliff of any sort is enacted by the Committee and it applies to bank issuers of such instruments, it's a "gotcha" that will inadvertently hand short-sellers an easy-to-aim-at target for any bank that someday comes under capital pressure. Short sellers may find it easier to cause a peg break in a bank-issued stablecoin (and thereby trigger the capital requirement cliff for the bank) than to short the bank's stock.

The Committee noted it is considering an approach whereby stablecoins issued by regulated entities "will generally be lower risk than those issued by unregulated entities." In Custodia's view, the Committee should go even further by making the distinction between a ***bank*** vs. a non-bank issuer. Again, banks issue ***money***. If a bank issues such an instrument and holds 100% of its reserves in central bank deposits or short-term government obligations, it should be exempt from the Basis Risk Test. Subjecting such a bank-issued instrument to the Basis Risk Test would set an adverse precedent by breaking the fungibility of money.

C. Comment on Classification Condition #3: Network Design, Traceability

The Committee noted: "Networks that fulfill this condition would be those where the key aspects are well-defined such that **all transactions and participants are traceable**" (emphasis added).

Custodia Bank's comment here is that – if that specified standard were to apply literally – banks would not be able to use the internet ***at all***. No transactions and participants are currently traceable on ***any*** internet networks, because that's not how the internet works. All data that travels across the internet is, at bottom, 0s and 1s – it's "dumb data" that requires software applications to make the data useful and, as in this case,

to make "all transactions and participants" traceable. Banks already run such software applications today in the normal course of business.

As Custodia Bank understands it, the Committee's main concern with traceability is a compliance one – namely, the ability to associate "transactions and participants" with people (i.e., ultimate beneficial owners). But that's exactly what banks already do today – they convert "dumb data" (0s and 1s) exchanged over internet networks into account records associated with people. Whether or not such networks use a blockchain architecture should not make a difference. What should matter is whether banks can convert that data into an accurate record of their customers' accounts.

It is not realistic for the Committee to require that ***networks*** must be able to associate data with people, and indeed that is not what bank regulators require of non-blockchain networks today. Every bank uses TCP/IP today. Criminals and sanctioned countries also use TCP/IP, but banks' software applications and operational processes block them from using banks' systems. There is no compliance or identity built into TCP/IP, just as there is no compliance or identity built into Bitcoin or Ethereum – remember, again, all data on these base-layer networks is "dumb." Yet, all banks use TCP/IP because they have the tools to block access to their applications running on top of TCP/IP. Same thing with Bitcoin and Ethereum – banks have the tools to block illicit finance from using their applications running on top of Bitcoin and Ethereum. It's easier to police illicit activity on permissionless blockchain systems than it is in legacy systems.

Custodia Bank recommends removal of the entire paragraph in Classification Condition #3 that includes the phrase "all transactions and participants are traceable" (at SCO60.22(1), second paragraph) because that paragraph – if read literally – would preclude banks from using TCP/IP today. Of course Custodia understands that is not the Committee's intention, but that's also the point – it's not possible to distinguish TCP/IP from the requirements set out in that paragraph, and yet bank regulators are comfortable with banks using TCP/IP. It is not realistic to hold Bitcoin, Ethereum, et al., to a different standard, nor is it possible to define a standard for permissionless blockchains that would not risk inadvertently blocking banks from using the internet.

Like TCP/IP, the same case could be made for banks' use of TLS (transport layer security), because encryption – if taken literally – also fails the "all transactions and participants are traceable" standard for the simple reason that the data cannot be associated with people or transactions until it is decrypted by a software application.[10]

Custodia Bank believes the first paragraph of Classification Condition #3 at SCO60.22(1) is sufficient because it addresses the critical prudential risks pertaining to the use of cryptoasset networks by banks, and accomplishes the Committee's policy goal without risking an unintentionally broad condition described in the second paragraph of SCO60.22(1).

[10] The same technology that provides encryption – cryptography – is also what allows the generation of keys for a blockchain. As a side note, one of the co-authors of the TLS Security Standard – the security standard now ubiquitously used across the internet – is an adviser to Custodia Bank.

D. Comment on Classification Condition #4: Regulation and Supervision of Involved Entities

Custodia Bank recommends that the Committee exclude wallet providers from the list of entities subject to Classification Condition #4 in SCO60.24.

Again, we suspect that the Committee included wallet providers on this entity list mostly due to compliance concerns (and possibly also due to vendor risk concerns, but each bank can separately address vendor risk when choosing a wallet provider). As discussed above, there's no need for compliance to be built into wallet software. Banks can build compliance into their technology stacks without requiring it to be integrated into wallet software itself. The real policy question is *whether* the banks can comply with anti-money laundering/countering the financing of terrorism ("AML/CFT") requirements, not *which technology* they use to do it. The policy goal of implementing bank-level compliance standards can be met without the prudential capital requirements dictating a bank's technology choice. It is not realistic to assume wallet providers would become regulated and supervised – partly because, as software companies (or, in some cases, open-source software projects), it's not clear that they would even be eligible to become regulated and supervised financial institutions.

Including wallet providers on the entity list could lead to the unintended consequence of blocking the banks from using software that becomes ubiquitous as the internet-*native* protocols scale and become organically interoperable, thereby hamstringing banks from keeping up with customer preferences. Again, banks are likely to use the protocols *as payment rails* (including for fiat currency) in their own businesses. Blanket regulation should not block banks from using the best wallet software.

E. Comment on Operational Risk and 2.5% Infrastructure Risk Add-On

Operational Risk: Custodia Bank agrees with the Committee that there is heightened operational risk for cryptoassets, mostly arising from settlement risk[11] (due to the fast settlement cycles of most cryptoassets, which are generally much faster than the settlement cycles of traditional assets[12] – except in countries already operating programmable, real-time gross settlement payment systems). The guidance in SCO60.125 through SCO60.132 (and especially SCO60.130) should capture the heightened operational risk for those banks that have not separately addressed settlement risk.[13]

Infrastructure Risk Add-On: The capital charge for "cryptoasset technology risk" in SCO60.130(1) overlaps with the infrastructure risk add-on in SCO60.57-SCO60.58. In the context of the above comment about the sufficiency of operational risk capital charges (which already specifically address "cryptoasset technology risk"), it is not clear why prescribing a blanket 2.5% infrastructure risk add-on for Group 1 cryptoassets is necessary. This is particularly true because the four specified items in SCO60.130(1)(a)-(d) already cover the very same technology risks as the infrastructure risk add-on. Rather than establishing a blanket 2.5% add-on charge for infrastructure risk, a more flexible approach would be to propose the 2.5% as a rebuttable

[11] Banks that actively manage the settlement risk by avoiding all leverage with cryptoassets, and/or when issuing cryptoassets as bank liabilities by remaining 100% reserved in central bank deposits (or in other sovereign-guaranteed assets that settle as fast as cryptoassets settle), for example, inherently have lower operational risk.
[12] *See* https://www.forbes.com/sites/caitlinlong/2021/06/24/bis-proposed-capital-requirements-for-cryptoassets-vital-move-but-theyre-too-low-for-bitcoin/?sh=2845aa02546f
[13] *Supra*, note 11.

presumption included in the guidance in SCO60.130(1) for "cryptoasset technology risk," thereby allowing banks to demonstrate differentiation to their examiners based on their actual risk. There is a significant difference in the security and maturity of various blockchain protocols. A bank whose business plan is to quickly serve every new, untested blockchain protocol should have a MUCH higher risk capital charge than a bank that services only Bitcoin, for example. As drafted, the 2.5% infrastructure risk add-on does not permit examiners this flexibility, in either direction.

F. Closing

It is a fact that legacy payment systems are already in competition with internet-*native* payment protocols, which enable their users to settle payments *outside banking systems*. By one estimate, to date approximately 3% of U.S. bank deposits have already migrated to the crypto industry – and that happened mostly before technology to scale these protocols arrived. But it has now arrived. This means regulations implemented today that block banks from adopting the new protocols, as they scale and as customers increasingly demand them – including to use them as payment rails for fiat currency – could turn out to have the unintended consequence of costing the banking industry dearly, as fintechs and broader technology companies simply go around banking systems to settle payments.

At its pivotal juncture 20 years ago, telecom was a heavily regulated industry – just like banking is today at its pivotal juncture. How, then, did the telecom companies pivot to become software companies and avoid obsolescence by internet-*native* technology (VOIP) when it scaled? Answer: regulators enabled them to make that pivot.

That's what banks will become, too – software companies running applications on top of internet-*native* money protocols – but only if bank regulators let our industry make the same pivot. If they don't, then it will be obvious, looking back 10 years from now, why the tech industry won.

Custodia Bank would be happy to answer questions you may have about the content of this letter.

Sincerely,

Caitlin Long
Founder & Chief Executive Officer

Sincerely,

Rich Radnay
Chief Technology Officer