Steakhouse Financial Limited: Response to Basel Committee on Banking Supervision

26-Mar-2024

Please address comments and remarks to chefs@steakhouse.financial

We welcome the Basel Committee on Banking Supervision's (BCBS) issuance of this consultative document on proposed amendments to the cryptoasset framework. We strongly support the Committee's continued efforts to establish a robust and effective framework for managing cryptoasset risks within the banking sector.

We'll begin by introducing Steakhouse Financial's experience. Following that, we'll provide commentary on two key areas. First, we'll address the treatment of stablecoins, an area where we possess significant expertise. Second, we'll analyze the Bank for International Settlements' (BIS) position on public blockchains, as it appears to lack any supporting evidence. We'll also offer comments on specific technical details that could be improved.

About Steakhouse Financial

Steakhouse Financial is a boutique consultancy specializing in cryptocurrency-related services. Our mission is to foster open and transparent financial systems. We act as a bridge between the decentralized finance (DeFi) ecosystem and traditional financial institutions, facilitating collaboration that will ultimately lead to a more prosperous future.

Steakhouse Financial has established itself as a leading expert in stablecoins. Over the past three years, we've collaborated with MakerDAO, the issuer of the prominent DAI stablecoin (boasting a market capitalization of approximately $5 billion). Our expertise extends beyond MakerDAO, as we've also provided oversight for a variety of different stablecoin projects or asset-referenced stablecoin projects. These include decentralized software such as Angle Protocol or Venus Protocol's VAI, and also include supervised stablecoins such as other stablecoin projects like Mountain Protocol. Significantly, we pioneered the application of asset-liability management within the stablecoin space and have published research papers exploring the potential of "embedded supervision" facilitated by blockchain technology and Risk Management Framework adapted to DeFi protocols.

Table of Contents

Using secondary market liquidity to infer stability is inappropriate

The consultation paper uses secondary market liquidity to infer the stability of the protocol. This is consistent with Anneke Koske's paper "Will the real stablecoin please stand up". As we explain in our response to it, the analysis is so flawed as to be essentially unusable and can be confidently thrown out. The paper featured very basic and disqualifying methodological errors, including not being able to identify reserve assets of decentralized stablecoins, when these are patently public and transparent. The premise of the paper is similarly flawed.

While secondary liquidity is important, it is unsound to base a regulatory framework on it. To provide a basic example of why this measurement technique is not suitable, it is analogous to evaluating the volatility of a government-issued fiat currency by measuring the deviation of its FX rate from par at an airport exchange desk.

Moreover, this clear fact was also highlighted by S&P Ratings in their evaluation framework for stablecoin which separate primary market redeemability and secondary market liquidity as two complementary, but not fungible concepts.

Overcollateralization is inconsistent with prior BIS guidance for banks

The consultation document employs the term 'overcollateralization' when referring to reserves. While this might appear to be a minor technicality, it actually introduces a conceptual inconsistency, which we suspect may lead to misunderstandings.

In traditional finance (TradFi), neither the Bank for International Settlements (BIS) nor national supervisory authorities require banks to be 'overcollateralized.' Instead, they mandate that banks demonstrate adequate solvency by maintaining an equity buffer on the liabilities side. This buffer is calculated as a percentage of the risk-weighted assets the bank holds on the asset side. We see no compelling reason why this same approach wouldn't be applicable to stablecoins.

It is possible that BIS is taking the view that the stablecoin business model is narrowly to serve as an e-money token and therefore is unable, or should be unable, to take on credit risk that could impair its stability. However, it is outside of the remit of BIS' competencies to determine what a stablecoin business model should be, and this should be left up to the market.

USDM, issued by Mountain Protocol and supervised by the Bermuda Monetary Authority, is an example of a low credit risk, fiat-backed stablecoin that the BIS might otherwise refer to as an 'e-money token'. However, the nature of the innovation that blockchain enables allows USDM to pay holders a reward for holding it, close to the Federal Funds rate. This is a through-and-through innovation in financial technology that allows lower

overhead costs from outsourcing core settlement infrastructure to public blockchains to be passed on as benefits to users and consumers, with no corresponding change in credit risk.

Disclosure of reserve requirements is inconsistent with existing rules

The paper discusses the requirements to be listed in Group 1b). It requires a daily disclosure of the asset composition. Group 1a) doesn't have this requirement. It would be only fair to ask the same for tokenized bank deposits, especially as the composition of their assets is, by construction, of far lower credit quality.

Stablecoin supervision is not a panacea for robustness during a crisis

SCO60.11 requires issuers to be supervised. As the SVB crisis (and indeed the various bank failures across multiple jurisdictions during 2008, 2009, 2010, 2011, and more recently in 2023) showed, supervision in and of itself is not a risk mitigant.

Therefore, it is by no means a minimum requirement to demonstrate balance sheet robustness. Our rationale is that, a bank that has traditionally been run on conservative lines, such as Arab Bank in Jordan or Standard Chartered in the UK. These were not impacted by the Lehman Brothers crash in 2008 or by USD rate rises during 2022-23. One would expect these institutions to be safer managers of their balance sheet absent any regulation supervision, than a bank that "moves fast and breaks things" (SVB) would be despite strict supervision of the US Fed.

Therefore we conclude that, in the Stablecoin environment, it is not necessarily any guarantee of robustness, let alone any panacea, to simply state issuers to be under a form of supervision and accept that this magically makes them better balance sheet managers. Hence, there is no compelling need to require it. Major regulated stablecoins essentially operate as full reserve banks, and are therefore far less risky to their holders or depositors relative to traditional banks.

Also, it is worth citing an example where supervision proved to be a risk factor for a stablecoin. In the case of BUSD, issued by Paxos, the NYDFS shut down the stablecoin, without providing a clear rationale. This led to a depeg and caused losses to BUSD stablecoins users.

We recommend stablecoin supervision to be opt-in. This shouldn't be viewed as a position against stablecoin supervision, but rather about encouraging competition. A supervised stablecoin, under a sound framework and a well respected supervisor, should be clearly recognized by the market as a safer choice over time. As a market participant, Steakhouse Financial Limited advocates for supervised stablecoins over unsupervised alternatives.

BIS guidelines break singleness of money

We want to highlight the need of preserving the singleness of money. For that to happen, stablecoin issuers should be able to accept stablecoins from other issuers.

This doesn't seem possible with the current situation. The standard could be improved by addressing this particular point. For example, a supervised stablecoin issuer could be encouraged, under BIS guidance, to accept redemption of other recognized supervised stablecoins. This would help harmonize secondary market exchange rates for supervised stablecoins and, over time, attract more usage to supervised vs unsupervised stablecoins.

BIS' stance on public blockchains is opinionated, misguided, inaccurate and leads to a litany of new risks for consumers

The consultation document opens by discussing potential risks associated with permissionless, or public, blockchains. However, this analysis of risks is totally absent. Furthermore, the angle is clearly from a risk-only perspective, rather than a balanced evaluation of risks versus benefits, which might be expected from a serious technical consideration of an innovation in ledger technology.

BIS is far behind on this matter relative to jurisdictions that recognize and enshrine public blockchains as legitimate instruments of record. The Swiss DLT Act, for instance, is agnostic to the medium of recording ownership, and therefore allows public blockchains to act as securities ledgers, recognizing their unique benefits and enshrining them in law.

Furthermore, none of the risks that are obliquely addressed by BIS have any basis in evidence of reality, to the extent that one can surmise the details of this analysis, as it is not disclosed.

'Reliance on third parties' is an illusory risk on Ethereum though a meaningful one for traditional payment networks

For instance, reliance on third parties for the operation of a distributed cryptoeconomic security network is indeed a key risk for public blockchains. However, what would be expected of a serious analysis of these risks is guidance regarding to what degree a network faces this third-party risk, and thresholds over which a public blockchain could be considered to be cryptographically secure.

All the evidence suggests that Ethereum is a network with a clear ability to operate cryptoeconomic security with no or limited third-party dependencies. So this risk is mitigated, and no due diligence or oversight over these third parties is required to give stablecoin issuers on public blockchains additional confidence that the underlying network is robust.

At this stage of development, it is highly unlikely for the network or its validators to be compromised by government injunctions and sanctions that could threaten to engage in political saber-rattling such as cutting off other countries from the payment network. So far, Ethereum seems to have proven more resilient to censorship and interference from external bad actors than supervised financial systems and payment networks.

Public blockchains do not entail any clear, specific, political, policy or legal risks

BIS further outlines political, policy and legal risks from using public blockchains, but refuses to elaborate. What possible unique risks with a political, policy or legal dimension could exist from a bank accepting stablecoins issued on a public blockchain? Once again, one only needs to look at jurisdictions that recognize public blockchains as legitimate ledgers to understand that policy and legal framework dimensions of risk for stablecoins are outside of the purview of BIS guidance. A Swiss bank should have no issue holding or settling stablecoins on public blockchains relative to permissioned, or restricted blockchains (which one could also, by the way, refer to as databases with concentrated third-party dependencies and heightened risk exposure).

Public blockchains are deeply unsuitable for criminals and money laundering and do not represent a unique vector for AML/CFT risk transmission for well-run financial institutions

AML and CFT risks are also cited as a source of risk for banks in handling stablecoins, but no further elaboration is made. The reader is expected to accept, at face value and without evidence, that public blockchains increase the risk of AML and CFT. All of the available evidence[1] from reputable and knowledgeable forensic analysis demonstrates that public blockchain transactions involving criminal or sanctioned activity exist at a much lower rate than the same proportion of transactions within the regulated banking space.

The AML risk for a bank interacting with stablecoins or public blockchains exists at the offramp to fiat fulcrum, which should anyway be subject to KYC/AML controls already. Provided that the bank does not engage in criminal tumbling or mix sources and uses of customer funds to and from stablecoins on public blockchains, there is no meaningful increase in AML/CFT risk from accepting stablecoins on public blockchains. Therefore, considering that the risk of AML/CFT is mitigated by KYC processes at the bank level, no new requirements on interactions with stablecoins would mitigate any additional risks of AML/CFT.

[1] Chainalysis reports on Criminal Transactions

Lack of privacy on public blockchains is not coherent with AML/CFT risk and does not constitute a source of balance sheet risk for a bank holding stablecoins

One of the main reasons public blockchains are so unsuitable for money laundering or criminal activity is the fact that transactions are transparent and public. The BIS notes no contradiction in describing the lack of privacy as a source of risk from stablecoins on public blockchains. It would be a more persuasive argument to lean on either one (AML/CFT) or the other (lack of privacy), but insisting on both is insisting on a contradiction.

There is, certainly, some element of concern around the lack of privacy from the perspective of a user who, for e.g., deposits stablecoins from a public blockchain into their bank account. But this privacy issue, by itself, does not change anything with respect to the balance sheet risk incurred by a bank accepting these stablecoins. It may well be a source of risk personally to the user in some regard, but that user is presumably already aware of the tradeoffs, by being a stablecoin user in the first place.

A bank could conceivably run netting and clearing with another bank by exchanging balances over a public blockchain, but in that case there are no privacy issues with respect to the user. There might be some disclosure of balance sheet composition during these netting transactions, but we would argue that this is an improvement from a prudential supervision perspective, relative to a situation where 100% of the assets of a bank are completely opaque and only reported four times a year to the public with no verification guarantees, or disclosed under duress while the bank is collapsing (Credit Suisse).

In closing, the BIS lists ‘privacy’ as a source of risk to bank robustness from accepting public stablecoins, but we are unable to identify any such risk and believe this risk concern is not real and can therefore be disregarded, along with the others.

Settlement finality on public blockchains and Ethereum in particular are actually a risk mitigant relative to traditional T+n clearing with no counterparty risk

Regarding settlement finality, public blockchains and Ethereum in particular already offer substantially improved settlement guarantees relative to T+n clearinghouse settled transactions in traditional finance, and with no third-party exposure or counterparty risk.

Ethereum’s migration to a Casper Proof-of-Stake consensus algorithm provides an improvement over probabilistic finality in Proof-of-Work algorithms. Today, Ethereum achieves immutable finality within two epochs, or approximately 12 minutes, with further plans to achieve single-slot finality which would bring it down to less than 12 seconds.

Granted, Ethereum's consensus algorithm was stressed in May 2023, when an inactivity leak spread to 60% of validators through client bugs. However, during this period of partition intolerance, Ethereum is designed to prioritize liveness which means that transactions continued to take place as normal and users interacting with Ethereum would not have noticed anything amiss.

Furthermore, because of client diversity among the validator network, the blockchain was able to continue operating essentially as normal and finality was recovered after burning a total of 28 ETH across the whole network of offline validators, or less than 0.0006 ETH per offline validator. The robustness of Ethereum's settlement finality is already extremely high and tolerant to failure. The BIS' concerns over risks concerning settlement finality must therefore be either rooted in a lack of understanding of how public blockchains function, or intentional misdirection over the source of risks in public blockchains.

In the hypothetical scenario of a complete and utter collapse of the Ethereum blockchain, what implications would this hold for holders of a stablecoin like EURCV issued by Société Générale? As the issuer, Société Générale possesses the ability to freeze the contract entirely. Alternatively, if freezing is not feasible, they could capture a snapshot of all holdings prior to the critical event. This snapshot would allow them to identify holders based on two methods: either through existing KYC (Know Your Customer) procedures, or by leveraging the inherent traceability of public wallet addresses within the cryptographic system. Once holders are identified, Société Générale could then facilitate transactions in a traditional, off-chain manner until a transition to a new blockchain platform is complete.

Public blockchains do not constitute a source of liquidity risk relative to restricted blockchains

Finally, BIS cites liquidity as a source of risk for banks from interacting with stablecoins on public blockchains. No further elaboration is, once again, volunteered, so the reader is left to their own imagination to discover what those risks could be. It is not, for example, made clear how accepting stablecoins on permissioned, or restricted blockchains, would mitigate liquidity risks relative to accepting stablecoins on public blockchains. As described earlier, relying on secondary market liquidity for gauging redemption risk, particularly for supervised stablecoins, is inappropriate and does not apply.

By focusing exclusively on 'risks', many of which are illusory and not real risks in the first place, the BIS seems intent on pushing the industry away from public blockchains altogether. This would mean maintaining bank dependence on centralized intermediaries and replicating the conditions of systemic risk that built up during 2007-2008 and led to the collapse of hundreds of banking institutions over the following years.

By fighting public blockchain adoption, BIS is increasing systemic risk in the global financial system

Rather than reducing risks to bank balance sheets, by fighting the development of market innovations with clear prudential and regulatory benefits, the BIS is actually working to increase systemic risk in the global financial system, rather than mitigate it. As a mitigation to this actual risk to bank robustness, we would encourage the BIS to be open to the possibilities that stablecoins and public blockchains offer for prudential supervision and financial robustness, rather than focus on inventing spurious risks to deter their use.

Finally, the consultation document does not fully consider the varying degrees of control that issuers have over different asset classes issued on public blockchains. Notably, issuers within Group 1 likely possess significant control mechanisms for their respective assets

Most stablecoin contracts grant administrative rights to their issuers. These rights allow issuers to pause transfers, freeze addresses, and manage the movement of stablecoins. These extensive controls enable them to maintain administrative power even within the open environment of public blockchains.

Furthermore, unlike traditional financial systems with third-party intermediaries, issuers can operate their own blockchain validation node. This node acts as their source of truth, essentially replicating the control they already exercise over their assets.

To put it another way, a centralized stablecoin issuer, like Société Générale, can operate its own public blockchain node. This node serves as their primary source of truth, independent of information provided by other nodes on the network. This would be no different from a bank storing transactions on an internal database and providing APIs for third parties to operate on it.

Alternatives to public blockchains (restricted blockchains) have no market value and forcing banks to adopt them would put them at a disadvantage

Moreover, in our discussions with many financial institutions, we never found any that thought permissioned, or restricted blockchains, have any significant value. Activity is on permissionless blockchain (as shown by BlackRock issuing a fund on Ethereum). Keeping regulated banks outside of this area of innovation would put them at a clear disadvantage.

Basel Committee on Banking Supervision is coloring outside the lines

In closing, as a final thought, and to recap the above risks that the consultation paper outlines, i.e. "Similar analysis applies to political, policy, and legal risks, AML/CFT risks, and risks around settlement finality, privacy, and liquidity":

Besides liquidity risk, most of these risks fall squarely outside of the scope of this working group or of traditional drivers of capital/liquidity requirements. For example the risks and recommendations pertaining settlement finality are actually covered by the relevant BIS-IOSCO CPMI on Application of the Principles for Financial Market Infrastructures to stablecoin arrangements (cf. https://bis.org/cpmi/publ/d206.pdf). One could say the same with regard to AML/CTF, the responsibility of which is with the FATF.

Therefore, it is safe to say that the Basel Committee on Banking Supervision is coloring outside the lines with scope creep and exceeding its mandate in absence of explicit recommendations from these working groups to mitigate the risk with capital requirements.