Crypto Asset Exposures: Critical Assessment of Infrastructure Risks

March 2024

Robert Richter, CFA is a Director at Zanders Group, lecturer at the Frankfurt School focusing on blockchain, PhD candidate at the Technical University of Munich and has a background in credit risk modelling.

Contact: r.richter@zandersgroup.com

Lukas Görnert is a Manager at 1 PLUS i GmbH focusing on crypto assets and regulation, holds a "Blockchain Expert" certificate from the Frankfurt School as well as a degree in Finance and Accounting.

Contact: lukas.goernert@1plusi.de

Justus Schleicher is a Manager at Zanders Group focusing on blockchain solutions, lecturer at the Frankfurt School and holds degrees in Business Information Systems and Management (Digital Business).

Contact: j.schleicher@zandersgroup.com

Marvin Blaich is an Analyst at Zanders Group and pursues a master's degree in "Blockchain & Distributed Ledger Technologies" at University of Applied Sciences Mittweida.

Contact: m.blaich@zandersgroup.com

We wish to dedicate this paper to the memory of Professor Philipp Sandner, who was not only a mentor but also a friend. Professor Sandner's unparalleled dedication to scholarship, mentorship, and innovation left an indelible mark on our lives and work. Although he is no longer with us, Philipp's legacy continues to inspire and influence us deeply. We are eternally grateful for the wisdom he imparted and the paths he helped forge.

I. Introduction

In December 2022, the Basel Committee on Banking Supervision (BCBS) published its final standard on the **regulatory treatment of crypto asset exposures** for banks. The standard is to be adopted by the national regulators by 1 January 2025. It categorises crypto assets into two groups, to which different regulatory requirements apply. Group 1 distinguishes between tokenised traditional assets (1a) and crypto assets with an effective stabilisation mechanism (1b). Crypto assets of Group 2 are divided into those that meet predefined criteria and are qualified for the recognition of hedging (2a) and those that do not meet these criteria (2b).

In addition, the BCBS proposed an **infrastructure risk add-on** for Group 1 assets to prevent financial losses due to fundamental risks of the crypto assets' underlying blockchain network. The initial proposal used to be "a fixed add-on to RWA [risk-weighted assets] set at 2.5% of the exposure value for all Group 1 crypto assets" [1, p. 2]. However, the consultation with stakeholders led the committee to reach an agreement on "a more flexible approach that allows authorities to initiate and increase an add-on based on any observed weaknesses in the infrastructure that underlies specific crypto assets" [1, p. 2].

In October 2023 the BCBS published a report that provides further details on the **disclosure of**

crypto asset exposures. In order to harmonise the disclosure documentation, standardised templates were created that comprise: crypto asset exposures and capital requirements, accounting classification of exposures and liquidity requirements for exposures. [2]

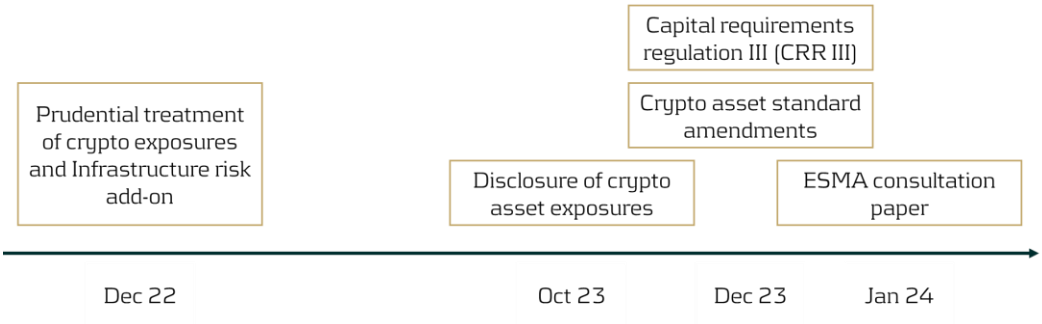
However, in a consultative document that was published in December 2023, the BCBS explains **amendments to the crypto asset standard** regarding the initial draft. Herein the Committee states that at the present time it "does not propose any adjustments to the crypto asset standard to allow for the inclusion of crypto assets that use permissionless blockchains in Group 1" [3, p. 1]. According to this, assets that are natively included into permissionless blockchain networks and apply an effective stabilisation mechanism (i.e. stablecoins), and tokenised traditional assets (e.g. digital bonds) that were issued consciously on such networks will not fall under Group 1. As a result applicable rules for such crypto assets must be exerted according to Group 2a or Group 2b, depending on the classification [1, p. 18].

Furthermore, the final draft of the **capital requirements regulation III (CRR III)** has been released by the European Union in December 2023, which also comprises specifications about crypto assets. It primarily addresses liquidity and leverage ratio requirements for institutions and proposes a temporary quantification method for own funds requirements for exposures. Contrary to the statement of the BCBS, it does not differentiate between permissioned and permissionless blockchain networks and is therefore technology neutral. A passing of the regulation in the European Parliament is planned for April 2024 whereas its implementation is predicted for the second half of 2025. [4, article 501d)

Moreover, on 29 January 2024, the European Securities and Markets Authority (ESMA) published a consultation paper describing the conditions and criteria that qualify crypto assets as financial instruments. In accordance with the position set out in CRR III, institutions "should not view the technological structure of these assets as a key factor" [5, no. 27 p. 9]. According to the ESMA, tokenised financial instruments should not be treated differently and technology neutrality should be adhered to. [5, no. 27 & 29 p. 9 f.]

Given the dynamic developments in this area, the final position of the European supervisory authorities (EU Commission and EBA/ESMA) remains to be seen.

At the time of writing, the topic of the infrastructure risk-add on has received little attention. Currently no methodology for quantifying the add-on exists and no market standard has formed to determine the key drivers of infrastructure risk. For this reason, the paper evaluates infrastructure risks based on insights from experts in the financial sector and proposes a framework that supports their quantification (Appendix 1). We conducted a survey of qualitative interviews with leading managers from crypto asset service providers, asset managers, banks and technology providers already engaged with blockchain technology. Both the companies and the interviewees were selected according to their knowledge in this area. The results are presented in the following section of this article.



II. Infrastructure risk – interview results

The guidelines used in the interviews had a clear focus on key factors (regulation, validators, interoperability, network downtimes, and consensus mechanism) that could influence the infrastructure risk of a blockchain network as well as the identification of their drivers. Both were assessed and sorted according to the relevance from the interviewees' perspective. Due to their previous involvement in crypto asset projects, the participants have several years of experience. The interviewees' projects were based on different networks, allowing us to distinguish between permissionless and permissioned implementation approaches and their motivation. What all projects have in common are the considerations in choosing a network based on the blockchain trilemma[1] .

Regulatory compliance

Blockchain-based financial services are still relatively new and depending on local jurisdictions, companies must comply with different regulations. According to the interviewees regulatory compliance is essential when integrating crypto assets into the current business model and offering it to customers. The reputational risk of losing trust of customers due to missing consultation or wrong behaviour could threaten the existing business of the company. This risk may be higher for companies when utilising a permissionless blockchain network as they have less influence on its processes. In order to avoid such issues, the interviewees independently agreed that the availability and selection of partners participating in the process is a crucial factor for any financial institution conducting a blockchain project. On the one hand this comprises the financial services providers, on the other hand software and technology companies. Therefore, comprehensive quality requirements are necessary in order to ensure ongoing functionality and a regulated playing field. In addition to that, licenses for business models such as crypto custody and registration of crypto securities are essential which can either be included through an appropriate selection of partners or the company obtains the necessary licenses itself. The software that is used in the blockchain project can be developed inhouse or purchased externally (make or buy principle). Solutions for the custody of crypto assets already exist, however, financial institutions also develop their own applications. This has several reasons including the overall security standards required.

Transaction validation

The validator network that verifies transactions on the blockchain represents an infrastructure risk. The interviewees in our sample had different opinions on this matter. Some interviewees were off the opinion that checking or registering validators becomes more important due to regulatory guidelines which will tighten in the future. Such processes can be implemented more easily in permissioned blockchain networks. Furthermore, institutions interacting with blockchain networks might need to be able to verify the identity of validators and whether they are located in sanctioned countries, requiring them to perform background checks. According to the interviewees, digital bond issuances that are performed on a permissionless blockchain (e.g. Polygon, Stellar) therefore have a higher risk of regulatory implications in the future. Permissionless networks have no restrictions and allow anyone to participate in the validation process as long as they are able to provide the appropriate hardware and software requirements and behave according to the rules. Thus it cannot be guaranteed that these are not operated in sanctioned countries. Some validators manage to completely disguise their identity as well as the location of the node. Hence, performing a "know-your-validator" verification is more complicated or even impossible for permissionless networks.

[1] The blockchain trilemma is a concept that describes the three factors "scalability", "decentralisation" and "security", which cannot be achieved all at once and must be balanced differently by each project.

Looking at the location of traceable nodes, a minority of them are operated in sanctioned countries such as the Russian Federation, Iran or Venezuela. An arbitrarily chosen set of node data on the Polygon blockchain showed that 52 (129 in a second test) of 5,000 nodes were located in sanctioned countries, which is approximately 1% (2.6% respectively) of the total set [6]. While some interviewees states that the relevance of these nodes for the blockchain network can be considered negligible, others claimed that this introduces regulatory issues.

Interoperability

Within permissionless networks, individual participants do not have any influence on the protocol, which is considered an advantage for security. This can be a challenge for companies that want to develop their applications on such a platform, as they are dependent on the prior configuration. A permissioned setup allows for more customisability of processes, resulting in more flexibility for the company and its business model. However, in terms of the entire ecosystem, permissionless blockchain networks offer better interoperability. Different blockchains (e.g. Ethereum, Avalanche, Tron) can communicate with each other and bridge crypto assets. According to our interviewees, the issuance of digital bonds on Ethereum Virtual Machine(EVM)-compatible networks would be highly interoperable. This applies to some extent to permissioned blockchain networks. Initially they are more encapsulated and are not intended to exchange messages or perform transfers outside the platform. However, the ERC-3643 token standard enables a bridge between permissioned and permissionless networks.

While permissionless blockchains can be used by anyone and might include bad actors, permissioned platforms can only be accessed by selected participants. The interviewees partially favoured the benefit of interoperability provided by permissionless blockchains. Others stated that permissioned blockchain projects will probably not be given up, but rather further enhanced in the future. However, this approach creates a “network of networks” where interoperability becomes substantial, in order to unify these encapsulated solutions to one ecosystem. Hence, multiple solution providers could be required once again to bridge crypto assets over different permissioned networks. Overall this could lead to a system which is similar to the traditional process, thus, neglecting all the benefits blockchain technology could provide. This especially comprises the reduction of the number of participants through disintermediation. Both perspectives were represented in the interviews and could define the future landscape of blockchain technology platforms in the financial services industry.

Network downtimes

An infrastructure risk, that is broadly known are outages of networks. In the recent years the permissionless blockchain Solana had several downtimes [7]. This lead to nodes being offline and transactions not being executed. In order to prevent the loss of funds and be able to verify the latest state, interviewees stated that they keep copies of the ledgers. Moreover, a secure pricing mechanism must be guaranteed, which is difficult for blockchain networks that do not operate properly. Network outages can also happen to permissioned blockchains depending on the degree of decentralisation and their individual validation rules. Since they tend to employ fewer validators, downtimes of a few nodes could halt the whole network. While some interviewees considered the decentralisation aspect as fundamental for the stability of the network, others view this aspect as less critical. Ultimately it is important to find a suitable trade-off between the total number of validators and the amount that is required to continue processes.

Consensus mechanism

The consensus mechanism ensures that only transactions and blocks that comply with the protocol rules are added to the blockchain.[2] The interviewees do not consider the consensus mechanism to be a predominant factor in the selection process of a blockchain network for financial services. Hence the technicality of the consensus mechanism is not a key priority for financial institutions. However, the interviewees all deem ESG considerations as relevant. Therefore, energy-intensive networks that apply proof-of-work are not included in the selection process, due to bad effects on sustainability objectives. According to an interviewee using a permissioned blockchain network can further enhance ESG criteria compared to permissionless chains.

III. Conclusion

The infrastructure risk introduced by the BCBS concerns capital requirements of institutions utilising blockchain technology. Since the fixed add-on does not apply, authorities can initiate and increase it based on identified weaknesses, the drivers on which to base this analysis first need to be identified. This article outlined the main risk drivers of infrastructure risk as perceived by industry leaders as shown in Table 1. In addition, future developments will show the reaction of institutions to the recent developments, taking into account the different positions of the BCBS (permissioned-friendly) and the European Union (neutral).

[2] Examples for consensus mechanisms are proof-of-work, proof-of-stake or proof-of-authority.

Appendix 1: Infrastructure Risk Quantification Framework

Table 1 - Infrastructure Risk Drivers and Importance

Category	Subcategory	Priority	Comment
Regulation	Regulation in place	high	Not a risk driver, but a requirement for banks.
	Licenses	high	Make or buy
Validators	Location validators	medium/high	Know your validator, sanctioned countries. Differences in opinions across interviewees.
	Number of validators	medium	
	Transparency	low	Not considered good for FIs, but good for regulator
Interoperability	Customisation	medium	Permissioned: Fundamentally high but low on "upper level" Permissionless: Fundamentally low but high on "upper level"
	Multi-chain support	medium	
	Disintermediation	medium	
	Accessibility	medium	
Network downtimes	Availability	high	Current state, secure funds and track amounts
	Reliability	high	Use must be guaranteed
	Decentralisation	medium	See number of validators, open-source development
Consensus mechanism	Security	low	PoA: Known validators PoS: Security considered good
	ESG	medium/high	Energy consumption

Legend	
High	All/most interviewees agreed
Medium	Half the interviewees agreed
Low	Few interviewees agreed

References

[1] Basel Committee on Banking Supervision (December, 2022). Prudential treatment of cryptoasset exposures. [Online]. https://www.bis.org/bcbs/publ/d545.pdf [25 January, 2024]

[2] Basel Committee on Banking Supervision (17 October, 2023). Disclosure of cryptoasset Exposures. [Online]. https://www.bis.org/bcbs/publ/d556.pdf [25 January, 2024]

[3] Basel Committee on Banking Supervision (December, 2023). Cryptoasset standard amendments. [Online]. https://www.bis.org/bcbs/publ/d567.pdf [25 January, 2024]

[4] Council of the European Union (4 December, 2023). CRR III 2021/0342 (COD) article 501d. [Online]. https://data.consilium.europa.eu/doc/document/ST-15883-2023-INIT/en/pdf [25 January, 2024]

[5] European Securities and Markets Authority (29 January, 2024). Consultation paper. On the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. [Online]. https://www.esma.europa.eu/sites/default/files/2024-01/ESMA75-453128700-52_MiCA_Consultation_Paper_-_Guidelines_on_the_qualification_of_crypto-assets_as_financial_instruments.pdf [1 February, 2024]

[6] PolygonScan (n.d.). Nodes. [Online]. https://polygonscan.com/nodetracker/nodes [25 January, 2024]

[7] Solana (n.d.). Incidents. [Online]. https://status.solana.com/history?page=4 [25 January, 2024]