Rechtbank Rotterdam (sector bestuursrecht)
De voorzieningenrechter
Postbus 50951
3007 BM Amsterdam

Nijmegen, 11 February 2021

Subject: Procedure Bitonic / DNB (zaaknummer ROT 21/452)

Dear Madam, Sir,

In my capacity as chairman of the Verenigde Bitcoin Bedrijven Nederland ("**VBNL**") and on behalf of numerous crypto service providers, I kindly send you this letter following the receipt of a written response from the Dutch Central Bank ("**DNB**") on 10 February 2021 (the "**Response Letter**") on a letter sent to DNB and the Ministry of Finance on 2 November 2020 (the "**Request Letter**"). In the Request Letter a substantiated request was made to DNB to withdraw the whitelisting requirement that was announced by DNB on 21 September 2020 during a webinar and published on 23 September in a factsheet.[1] The Response Letter is unsatisfactory. Multiple crypto service providers who are or wish to be active in the Netherlands have different experiences with DNB than the way described in the Response Letter. These crypto service providers include both crypto service providers that are already registered in accordance with the Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, "**Wwft**"), crypto service providers that are still in the process of becoming registered as well as crypto service providers that have withdrawn from the registration process due to the disproportionality of the registration requirements. Moreover, these crypto service providers include companies incorporated in the Netherlands as well as crypto service providers incorporated in other jurisdictions.

With this wide support from crypto industry in the Netherlands, I kindly draw the attention of the Court to the following. In this letter I will refer to 'we' to reflect that the content of this letter is endorsed by numerous crypto service providers who, at this stage, prefer to remain anonymous as they fear that this letter could otherwise harm their existing relationship with DNB.

We have taken note of the request for a preliminary injunction, as submitted by Bitonic B.V. (**Bitonic**) on 25 January 2021. By sending this letter, we support the initiative that Bitonic has taken. The whitelisting requirement imposed by DNB as part of the registration process pursuant to the Wwft applies equally to other crypto service providers active in the Netherlands. With the whitelisting requirement DNB provides substance guidance to an open standard how crypto service providers should organize their internal controls to ensure compliance with the sanctions rules and regulations. By imposing the whitelisting requirement, DNB goes beyond its authority and discretion. It is the responsibility of institutions themselves to put in place adequate measures to ensure compliance with sanctions rules and regulations. We therefore endorse the preliminary request of Bitonic that aims at suspending (and eventually withdrawal of) the whitelisting requirement as imposed by DNB. We will further explain the rationale for this endorsement below, but we will first briefly consider the Response Letter of DNB dated 10 February 2021.

1 https://www.dnb.nl/en/sector-information/supervision-sectors/crypto-service-providers/integrity-supervision-of-crypto-service-providers/sanctions-act-1977/screening-counterparties-in-incoming-and-outgoing-customer-transactions/

Response Letter DNB
On 10 February 2021, the undersigned received the Response Letter of DNB on our Request Letter of 2 November 2020. We understand that both the Request Letter as well as the Response Letter are already part of the prosecution file. Therefore these will not be re-attached to this letter.

We emphasize that it is not contested that crypto service providers fall under the scope of the sanctions rules and regulations. This responsibility is taken very seriously. The point of contention is that crypto service providers have experienced that DNB de facto imposes the requirement on crypto service providers that *in addition to identifying relations* within the meaning of the sanctions laws and regulations, crypto service providers are required to undertake measures to *verify the identity of those relations*. Crypto service providers have experienced that DNB only deems measures sufficient and adequate if crypto service providers verify that a person holds (a copy of) the private key which gives access to a crypto wallet. Other measures which would enable crypto service providers to have sufficient identity data in respect of a relation to screen such relation against the sanctions lists, have not been accepted by DNB in the registration process. Effectively, DNB does impose the whitelisting requirement on crypto service providers, whilst – taken note of the Response Letter – DNB knows and agrees that no such verification requirement applies on the basis of the sanctions rules and regulations.

Registration obligation
In order to be active as a crypto service provider in the Netherlands, crypto service providers are required to register with DNB pursuant to Article 23b Wwft. Article 23c Wwft, as specified in further detail in the Implementation Decree Wwft 2018 (*Uitvoeringsbesluit Wwft 2018*), lays down the prerequisites with which crypto service providers have to comply in order to become registered (the "**Registration File**"). On the basis of Article 23d Wwft, section 1 Wwft, DNB can reject a registration request if either (i) a crypto service provider does not provide a complete Registration File, (ii) if DNB is not convinced of the accuracy of the Registration File and/or (ii) if the persons subjected to a reliability assessment pursuant to Article 23h Wwft cannot be found reliable.

Sanctions rules and regulations
One of these prerequisites relates to having risk based administrative procedures and internal controls ("**AO/IC**'") in place to ensure compliance with the Sanctions rules and regulations. The Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling toezicht Sanctiewet 1977*, "**RtSw**") describes in more detail what DNB expects from institutions within the meaning of Article 10, section 2 of the Sanctions Act 1977, which includes crypto services providers. The AO/IC measures must enable an institution to monitor its administration in such a way that it can detect and freeze financial assets of a sanctioned person and to prevent that it disposes financial assets or services to a sanctioned person.

It follows from the complementary notes to the RtSw[2] that an *intended* choice was made for *principle based* standards rather than rule based standards. This means that the institution itself needs to determine in which way it monitors its administration to ensure compliance with the sanctions rules and regulations. It is clarified that the institution can put this into effect on a *risk oriented basis*. It is also clarified that it is expected that *the institution itself makes a risk assessment* which forms the basis of its AO/IC.

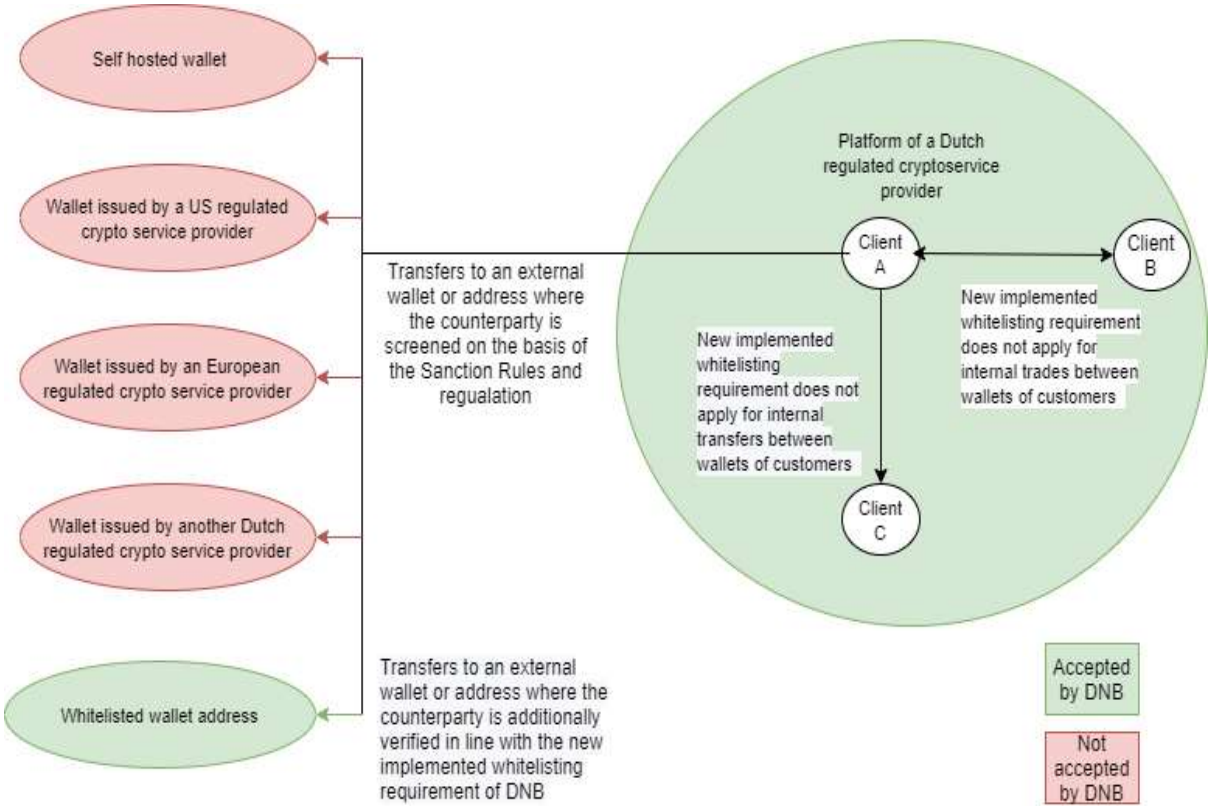
This principle based approach as well as the own responsibility in this respect of an institution also follows from recent guidelines published by DNB as well as the Ministry of Finance.[3]

2 Government Gazette, 28 September 2005, no. 188 / p. 21, paragraphs 1.2 and 4.3.

3 'Leidraad DNB Wwft en Sw', lastly amended in December 2020, p. 69, available here: https://www.dnb.nl/media/dzicty20/dnb-leidraad-wwft-en-sw.pdf; Ministry of Finance 'Leidraad Financiële Sanctieregelgeving', 12 August 2020, p. 9-10, available here: https://www.rijksoverheid.nl/documenten/rapporten/2020/08/12/leidraad-financiele-sanctieregelgeving.

Whitelisting requirement DNB

The whitelisting requirement imposed by DNB on crypto service providers deviates from the sanctions rules and regulations, the complementary notes to the RtSw and the guidelines published by, amongst others, DNB itself.



The whitelisting requirement puts a disproportionate burden on crypto service providers and results in a non-level playing field. The whitelisting requirement namely obliges crypto service providers to verify the identity of a holder of an external crypto wallet. If crypto service providers facilitate transactions in crypto-assets to any external crypto wallet, DNB requires crypto service providers to whitelist such external wallet first. An external crypto wallet is a wallet provided our clients themselves. A statement of our client in respect of the identity of the holder of such external crypto wallet does not suffice for DNB. This would, however, enable crypto service providers to check whether such person is listed on any sanctions lists, similarly to the way other financial institutions are expected to comply with the sanctions rules and regulations. This suffices for any other institution falling under the scope of the RtSw and DNB's integrity supervision.[4]

DNB seems to have evolving insights in this respect as it comes to crypto service providers though. In the draft explanatory notes to the Registration Form intended for crypto service providers, DNB pointed out the following to crypto service providers[5]: *"Houdt u er rekening mee dat u minimaal de naam van de ontvangende partij bij een transactie nodig heeft om deze aan de sanctielijsten te kunnen screenen. Dit moet ook uit de procedures en maatregelen blijken*."

4 Guidelines DNB AML Act and Sanctions Act, see footnote 3, p. 73.

5 Draft Explanatory notes to the form for registration as a crypto service provider, p. 16. This paragraph was deleted in the final explanatory notes published on the website of DNB.

DNB offers two whitelisting methods (other than providing a crypto wallet by the crypto service provider itself):

- screen sharing or video conferencing at the time of logging in; or
- signing of a transaction or sending back a small amount of crypto-assets to the crypto service provider on request.[6]

DNB also approves the screenshot method that is derived from the screen sharing method. Instead of real time observing that a person logs into his external crypto wallet, DNB accepts the alternative of sharing 'near real time' screenshots of a person being logged into such external crypto wallet.

DNB does not make a distinction between (i) external wallets held by clients which have been identified and which identity has been verified as part of the on-boarding processes of a crypto service provider in accordance with the Wwft and (ii) external wallets held by third parties. This means that crypto service provider have to bother fully identified and verified clients with the additional whitelisting requirement before crypto service providers can accept a transaction from or to an external wallet of such client. This also means that far-reaching identification and verification procedures have to be performed vis-à-vis third parties, such as third-party beneficiaries of a crypto transaction, before facilitating a transaction to an external wallet of such third party. In other words: if a client wants to make a payment with crypto-assets in a shop, this cannot be facilitated.

Moreover, these whitelisting methods are practically unfeasible as regards third-party holders of an external crypto wallet. This was considered during the parliamentary debate on the draft bill implementing AMLD5. Similar measures were explicitly dropped by the legislator in respect of the customer due diligence that needs to be performed in respect of a *client* pursuant to the Wwft because of the (partial) impracticability of such measures and a more risk based approach was taken going forward.[7] If the legislator already deemed such measures impracticable concerning the crypto service provider's own clients, how can it reasonably undertake such measures regarding a third party?

Whitelisting requirement beyond DNB's powers

Despite these considerations of the legislator, DNB holds the view that the aforementioned whitelisting measures are required in order for a crypto service provider to comply with the sanctions rules and regulations. There is no legal ground for the whitelisting requirement. DNB is not in the position to impose the whitelisting requirement that *de facto* results in restrictions to the business operations, markets and services of crypto service providers. These whitelisting measures are burdensome, costly and user unfriendly. The whitelisting requirement cannot be reasonably applied to third-party beneficiaries of a transaction. It is emphasized that DNB itself takes into account that a beneficiary can be unknown to an institution.[8] DNB does not expect other financial institutions to undertake further measures to identify such unknown persons, let alone to *verify* the identity of such persons. The whitelisting requirement to which crypto service providers are subjected, however, *do* require crypto service providers to undertake such extreme measures. There is no level playing field with any other institution that falls under the scope of the RtSw. DNB does not require these measures from any other institution than from crypto service providers.

Disproportionate negative impact of whitelisting requirement

The whitelisting requirement has led to the situation that no registered crypto service providers in the Netherlands currently facilitate transactions to third party crypto wallets. The whitelisting requirement substantially deteriorates the competitive position of the Dutch crypto industry. There is no level playing field on a national level because this whitelisting requirement does not apply to any other institution falling under the scope of the RtSw or under DNB's integrity supervision, neither a level playing field exists on a European level. To the best of our knowledge, this or a similar obligation does not apply to crypto service providers in any other European Member State.

---

6 See footnote 1.

7 Parliamentary Papers House of Representatives, 2018/2019, 35 245, no. 3, p. 28.

8 Guidelines DNB AML Act and Sanctions Act, see footnote 3, p. 72 and p. 74.

The clients of crypto service providers passed their respective extensive customer due diligence on-boarding processes. Requesting them to whitelist one or more of their own external wallets in addition to that is unreasonably burdensome. Sharing screenshots or effectuate screen sharing or video conferencing at the time of logging in is an infringement on one's privacy. There is no legal ground for processing these personal data as crypto service providers do not have a legal obligation to verify the identity of such person for the purpose of compliance with sanctions rules and regulations. Signing a transaction or sending a small amount of crypto-assets (so called 'pennycheck') can be very costly due to the transactions costs involved. Moreover, neither of these whitelisting methods exclude the risk of circumvention such as the use of a front man.

Clients of crypto service providers experience the whitelisting requirement as burdensome and a number of crypto service providers registered in accordance with the Wwft experience loss of clients. This is not a surprising outcome; these clients can transact in the exact same crypto-assets with crypto service providers in other jurisdictions where the whitelisting requirement does not apply.

Alternative measures
During the registration process, many crypto service providers have discussed these whitelisting measures and suggested other, less burdensome but still effective, control measures. They have experienced that DNB was not willing to comment on any suggestions prior to having described these in detail in the AO/IC and related documents. Some crypto service providers who spent time and energy in presenting alternative measures on a substantiated basis to DNB experienced a reluctant stance taken by the regulator. Other than the screenshot method, none of the other suggested measures has been deemed sufficient by DNB.

It became very clear that DNB would only accept the Registration Requests if at least one of the above mentioned whitelisting measures are adopted by the crypto service providers. This is surprising because DNB *de facto* prescribes how crypto service providers should comply with the sanctions rules and regulations whilst this should be their own responsibility.

Due to the deadline of the transition period expiring on 21 November 2020, stakes were too high and the majority of crypto service providers chose to accept the whitelisting requirement because they would otherwise no longer be able to continue their operations in the Netherlands as they would not be timely registered in accordance with the Wwft.

Conclusion
It is emphasized that crypto service providers take their responsibility under the sanctions rules and regulations very seriously. As mentioned, they have discussed several alternatives to the whitelisting measures of DNB that would be in line with the rationale of the sanctions rules and regulations and would enable crypto service providers to comply with these requirements in a less burdensome, less costly and less user-unfriendly manner. With the wide support of crypto service providers active in the Netherlands, I therefore endorse the request for a preliminary injunction as submitted to your Court by Bitonic and express the hope that your Court rules in favour of this request.

I keep myself available to answer any questions your Court may have.

Yours sincerely,

on behalf of numerous crypto service providers active in the Netherlands,

Mr. Patrick van der Meijde,
Chairman Verenigde Bitcoin Bedrijven Nederland