Montpellier, 9 June 2025

Dear EDPB Members,

I welcome the Guidelines 02/2025 on processing of personal data through blockchain technologies. However, I would like to draw the Board attention on four important elements concerning cryptocurrencies using the blockchain technology such as bitcoin, which appear to me to not have been sufficiently clarified, unless I am mistaken. They relate to the right to self determination, to the identification of the data controller, to data storage and to confidentiality and privacy by design (currently rendered impossible by disproportionate EU legislation).

The right to self determination

The right to privacy and to data protection, under Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the European Union Charter of Fundamental Rights (EUCFR), is a right to confidentiality but also a right to data availability and to make those data public. This freedom of choice is also a component of private life, since it is "an inherent part of a person's autonomy, independence, dignity and self-development"[1]. Self-development and freedom of choice enable in turn self determination[2], which was considered by the German Federal Constitutional Court as participating to the value and dignity of the person and a "a fundamental prerequisite for the functioning of a free and democratic society".[3]

As a result, individuals are entitled to choose a technology of which a core function implies traceability, for the other benefits it brings. Prohibiting this technology, on the ground that it stores tracks indefinitely, would lead to deprive these individuals of their freedom of choice, in a "paternalistic 'best interests' decision-making" approach that would override or ignore the "will and preference of persons" who are in a position to give their opinion, to quote a decision from the ECtHR.[4] The ECtHR also prohibits the complete extinction of a right, in particular where less intrusive alternative measures are available.[5]

[1] ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134.

[2] Liudmyla Serdiuk *et al.*, Personal autonomy as a key factor of human self-determination, December 2018, DOI:10.21277/sw.v1i8.357, https://www.researchgate.net/publication/329776846_PERSONAL_AUTONOMY_AS_A_KEY_FACTOR_OF_HUMAN_SELF-DETERMINATION.

[3] BverfGE, 15 December 1983, 3 – 1 BvR 209, 269, 362, 420, 440, 484/83, especially §144 and 146 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

[4] ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134.

[5] ECtHR, 2nd ch., 27 November 1996, Hertel v. Switzerland, n° 25181/94, https://hudoc.echr.coe.int/eng?i=001-3380.

It is possible to make a parallel with the TCP/IP protocol, which enables to communicate on the Internet, and on which IP addresses, which are personal data where static or stamped, are publicly available. Additional features and tools may enhance anonymity, such as the use of Virtual Private Networks (VPN) – but they are regularly blocked[6] and subject to legal ban attempts[7], precisely because they enable confidentiality. In any case, a prohibition of the use of the protocol would basically condemn Internet. In the same line, a prohibition of the blockchain technology on the ground that it is impossible, technically, to suppress information since traceability is at the core of its functioning (as it ensures certainty), would be dramatic for people who count on bitcoin (as an example) to live despite the closing of their bank acount or more simply to have a store of value. Further, it would deprive individuals of their right to self-determination.

The data controller

In the case of the use of blockchains like the Bitcoin one, individuals decide themselves to broadcast a transaction on the network, using a tool that is generally a wallet. They pay a fee to a miner who will solve a mathematical problem in order to incorporate the transaction in the blockchain. As a result, individuals are the ones who decide the means and purposes of the data processing, and consequently they are the data controller of the processing involving their data and the ones of the party who will benefit from the results of their transaction (the sending or the reception of bitcoins). Since they process their own data within the framework of their domestic sphere, the GDPR does not apply to them. I am certain that it is for you obvious but, since the GDPR is sometimes misunderstood, a clarification on that point would simplify a lot of future discussions.

Miners can certainly be seen as processors, since they process the transaction in order to incorporate it in the blockchain, but they basically do it at the request of the natural person who has broadcasted the transaction. On the same line, centralised exchanges should be seen as processors in relation to the tools they provide natural persons with, which empower those natural persons to broadcast transactions. Of course, they are also controllers of the additional processing operations they need to undertake in order to render their services.

There might also be subsequent data controllers, for example in case the data published in the blockchain are collected by other natural or legal person, for other purposes such as legal investigations.

Data storage

Data storage, as your Board recalls it, must be limited to the achievement of the processing purposes. The purpose of buying bitcoins, thereby accepting the registration of own personal data in the blockchain, is to be and to stay entitled to claim the property of these bitcoins, and to eventually changing them into another cryptocurrency or euros. It is therefore important that the data registered in the blockchain stay there indefinitely, since it is the condition of property, present and future. A parallel might be drawn with a notarial deed, the notary being in charge of keeping owners'

[6] Wikipedia, VPN blocking, https://en.wikipedia.org/wiki/VPN_blocking; Aurelija Einorytė, VPN bans: How they work and who's behind them, 21 February 2024, https://nordvpn.com/blog/vpn-ban/.

[7] See for example The Huffington Post, Interdire les VPN ? Finalement la majorité retire son amendement, 17 September 2023, https://www.huffingtonpost.fr/politique/article/interdire-les-vpn-finalement-la-majorite-retire-son-amendement_223203.html.

identity, during the time this data preservation enables to claim a property, including in case of legacy.

Confidentiality and privacy by design ...

Obviously, confidentiality is of utmost importance and your guidelines emphasise its necessity, using especially encryption and/or other obfuscation techniques. Where ownership can be claimed while ensuring that owners' identity is only revealed to legitimate third parties, efforts must be made in this direction. In the same line, notaries must ensure the confidentiality of the personal data processed under their responsibility, in order to make sure that they will only be used to serve the purpose of the processing.

This rule applies to blockchains that enable the ownership of cryptocurrencies and their use. It is important to recall here that banking information (which means more widely information relating to amounts held and transactions performed), irrespective of it being sensitive information or not, even though it is of a professional or business nature, is considered to be protected as an element of private life by the ECtHR.[8]

For the very reason of the sensitivity of financial information, there are very interesting research projects, on different blockchains, aiming at adding confidentiality layers, including on the Bitcoin blockchain, in order to enable an anonymised or strongly pseudonymised use. An example is the zero-knowledge-proofs technology.[9] Some technologies currently permit such confidentiality already, for example mixers such as Tornado cash[10] and the Monero cryptocurrency[11]. I fully agree with you that they should be encouraged.

... rendered impossible by disproportionate EU legislation

However, this approach, which respects human rights and which is compliant with both the ECHR and the EUCFR, faces a wholly disproportionate EU legislation which, in financial matters, imposes basically the transparency of all transactions, under the guise of combating money laundering and the financing of terrorism, while both the need of the measure and its positive effect on crime have not been demonstrated.

Indeed, this legislation (AML package) imposes in particular:

- The requirement to be identified, as well as the recipient, for any transaction involving the sum of more than 1000 €[12]. This condemns the use of privacy cryptocurrencies such as Monero and anonymous wallets.
- More generally, the practical prohibition of mixers and other technology enabling confidentiality, including self-hosted wallets since they are considered as posing "high risks"[13]. In the Netherlands

[8] ECtHR, ch., 7 July 2015, M.N. and others v. San Marino, appl. n° 28005/12, § 51-53, https://hudoc.echr.coe.int/eng?i=001-155819.

[9] Howard Wu, Why Wall Street Won't Embrace Crypto Without Zero-Knowledge Privacy, 11 May 2025, https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide.

[10] Arkham, Understanding Tornado Cash, 23 September 2023, https://info.arkm.com/research/understanding-tornado-cash.

[11] Monero, project website; https://www.getmonero.org/.

[12] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance), Article 5-10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1113.

and in France, Courts' decisions have further, *inter alia*, considered that the making available or the use of anonymisation tools is not inherent to privacy (as it should) but is an indicator of potential criminality.[14] A recent French law on drug-trafficking considers that the use of privacy enhancing techniques constitutes a presumption of money laundering.[15]

As a result, cryptocurrencies owners are required to undergo:

- Extremely intrusive "Know Your Customer" tests, which include the collection of the name, postal address, copy of a valid ID card with photography (and therefore biometric personal data), total assets, cryptocurrency wallets number (which enables to track the amount of assets)[16] which will probably leak and be used in the future by malicious persons, since stakeholders have shown their weaknesses regarding security.[17]
- Concerning anybody, including persons "with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime"[18], whereas such degree of intrusion would require it.
- Making disapear the very possibility to keep a certain financial confidentiality, whereas this confidentiality is protected under the right to private life;
- In order to pursue a purpose, whose pressing social need has not been "convincingly established"[19] by States[20], whereas reports show the very low level of criminal activity related to cryptocurrencies.[21]

---

[13] Regulation (EU) 2023/1113 already mentioned. Recital 17 states: "Certain transfers of crypto-assets entail specific high-risk factors for money laundering, terrorist financing and other criminal activities, in particular transfers related to products, transactions or technologies designed to enhance anonymity, including privacy wallets, mixers or tumblers". See also Recital n°58.

[14] James Reddick, Tornado Cash co-founder convicted of laundering $1.2 billion by Dutch court, 14 May 2024, https://therecord.media/tornado-cash-money-laundering-verdict-netherlands-alexey-pertsev; La Quadrature du Net, Outils de chiffrement lors du procès du 8 décembre : du fantasme à la réalité, 14 décembre 2023, https://www.laquadrature.net/2023/12/14/outils-de-chiffrement-lors-du-proces-du-8-decembre-du-fantasme-a-la-realite/; Cryptoast, L'Europe rend-elle Bitcoin illégal sans le dire ?, 6 May 2025, https://cryptoast.fr/europe-rend-elle-bitcoin-illegal-dire/.

[15] Proposition de loi visant à sortir la France du piège du narcotrafic, final version, 29 April 2025, Article 7 p. 23, https://www.assemblee-nationale.fr/dyn/17/textes/l17t0102_texte-adopte-provisoire.pdf.

[16] See for example the Binance KYC from the end of 2024; Cryptoast, L'UE veut surveiller toutes les transactions crypto : vers la fin de l'anonymat on-chain en Europe ?, 14 May 2025, https://cryptoast.fr/ue-veut-surveiller-toutes-transactions-crypto-vers-fin-anonymat-on-chain-europe/.

[17] etheralpha /kycisbad, https://github.com/etheralpha/kycisbad; see also Medium, How KYC/AML poses a serious threat to your privacy and should not be used at all, 22 January 2019, https://blog.opportunist.global/how-does-kyc-aml-pose-a-serious-threat-to-your-privacy-and-should-not-be-used-at-all-88f7acd3f3b; 1miau, Pourquoi le KYC est extrêmement dangereux - et inutile?, Bitcoin Forum, 3 February 2020, https://bitcointalk.org/index.php?topic=5222860.0; Trend, Data Breach 2025: Meta, Coinbase, AT&T, Google, Apple, M&S, and More [May], 22 May 2025, https://news.trendmicro.com/2025/05/22/meta-coinbase-att-google-apple-data-breach/; Aaron Drapkin, Apple, Meta, and Twitter have all disclosed cybersecurity attacks over the past 12 months. We track the latest data breaches, 29 May 2025, https://tech.co/news/data-breaches-updated-list.

[18] EUCJ, gr. ch., 6 October 2020, La Quadrature du Net and others, C 511/18, 512/18, 520/18, §147-149, https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6083397. In the same line see ECtHR, 3rd Section, 7 November 2017, Zubkov and others v. Russia, appl. n°29431/05 and 2 others, §127, https://hudoc.echr.coe.int/eng?i=001-178343.

- In a manner that is not only ineffective, but also counter-productive. Side effects are indeed huge: reports show that the cost of compliance is today higher than the amount of money recovered from fraud[22], while it poses unacceptable risk of kidnapping and unlawful detention to all cryptocurrencies owners[23], who are not autorised by law to protect themselves through anonymisation techniques.

  The disproportion of this legislation is not acceptable in a democratic society governed by the Rule of Law. Since it comes into direct conflict with the EDPB guidelines, these guidelines could be an opportunity for the Board to use its position and authority to question the AML legislation, which, if it is not revised by the European Parliament within a fairly short space of time, will undoubtedly be, sooner or later, challenged before the CJEU and/or the ECHR.

Sincerely yours,

Estelle De Marco

---

[19] ECtHR, ch., 25 February 1993, Crémieux v. France, appl. n° 11471/85, § 38, https://hudoc.echr.coe.int/eng?i=001-57805; see also ECtHR, plen., 22 October 1981, Dudgeon v United Kingdom, appl. n° 7525/76, § 60, https://hudoc.echr.coe.int/eng?i=001-57473 (There must be a need for legislation in order to preserve society or sections of it, and the demonstration that not adopting it would result in adverse effect on the public); Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 February 2014 (WP211), §3.13, 3.17 and 3.19; Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, adopted on 9 November 2004 (WP99), p. 4.

[20] ECtHR, 4th sect., case of Piechowicz v. Poland, 17 July 2012, appl. n° 20071/07, § 212, https://hudoc.echr.coe.int/eng?i=001-110499; ECtHR, gr. ch., case of M.A. v. Denmark, 9 July 2021, appl. n° 6697/18, § 148, https://hudoc.echr.coe.int/eng?i=001-211178; ECtHR, 3rd sect., case of M.N. and others v. San Marino, 7 July 2015, appl. n° 28005/12, § 80-81 (§ 81: "The Court considers that the Government should normally be able to illustrate the practical effectiveness of a remedy with examples of domestic case-law"), https://hudoc.echr.coe.int/eng?i=001-155819.

[21] Alexandre Stachtchenko, Les dérives de la surveillance financière menacent nos démocraties, 16 May 2024, https://medium.com/@AlexStach/les-d%C3%A9rives-de-la-surveillance-financi%C3%A8re-menacent-nos-d%C3%A9mocraties-323fbdc1ccbf. The author demonstrates that risks linked to cryptocurrencies are not demonstrated, whereas KYC and AML procedures enable to recover about 0,05% of funds linked to criminal activity, at the world level. He also shows that the effectiveness of successive laws imposing transparency never demonstrated their effectiveness. See also Renaud Lifchitz, Loi « narcotrafic » : ma lettre ouverte aux députés, 7 May 2025, https://inbi.fr/loi-narcotrafic-ma-lettre-ouverte-aux-deputes/, who shows that crime related to cryptocurrencies represents 0,14% of the total in 2025.

[22] Alexandre Stachtchenko, Les dérives de la surveillance financière menacent nos démocraties, already mentioned. The author shows that each euro recovered from crime implies 200€ of compliance cost.

[23] More than 200 physical assaults against bitcoin owners, often accompanied by torture and sometimes fatal, were reported worldwide: https://github.com/jlopp/physical-bitcoin-attacks; see also Pauline Armandet, "On sait combien vous possédez de cryptos": un expert alerte sur de nouvelles législations moins protectrices, 5 May 2025, https://www.bfmtv.com/crypto/on-sait-combien-vous-possedez-de-cryptos-un-expert-alerte-sur-de-nouvelles-legislations-moins-protectrices_AN-202505050572.html.