Effective AML policy for crypto-assets and CASPs in the EU

Anti-Money Laundering Regulation (AMLR)

Blockchain for Europe (BC4EU) welcomes the European institutions' swift progress in developing harmonised rules to combat money laundering and terrorist financing in crypto-assets markets in the EU, including the recently updated Transfer of Funds Regulation (TFR) and the new Anti-Money Laundering Regulation (AMLR). Now more than ever we need transparent and effective rules on crypto-assets at EU level which allow to protect consumers and fight against financial crime, while providing legal clarity for companies setting up in Europe.

In this spirit, this document presents BC4EU's position on some key issues we noticed in the original European Commission's proposal and current approach presented by the co-legislators in their respective positions on the AMLR. Our objective is to provide specific recommendations to support the establishment of a transparent, balanced, and effective EU legal regime for crypto-assets and CASPs.

Achieving legal clarity through a risk-based approach to AML

We believe the AMLR should provide for a consistent and risk-based approach to customer due diligence (CDD), particularly enhanced due diligence, so that companies can streamline their onboarding processes and apply requirements that are commensurate with the risks involved. In addition, we should also make the best use of the latest technological developments and of the inherent transparency that blockchain technology brings. This calls for a regulatory regime that allows for the use of DLT analytics tools to detect the origin or destination of crypto-assets, thus facilitating the job of AML and law enforcement authorities. Finally, we believe there are some aspects that require further clarification to ensure the AMLR application provides legal certainty and remains consistent and fully aligned with the Markets-in-Crypto-Assets (MiCA) Regulation and the TFR.

Lack of consistency around definitions of DAOs and DeFi arrangements adopted across various EU regulations

The proposal of the European Parliament to make arrangements that self-identify as Decentralised Autonomous Organisations (DAOs) and Decentralised Finance (DeFi) subject to AML/CFT requirements, without providing clear definitions of these concepts, creates an unclear vision of what is expected to

be within the scope of application. Furthermore, it creates a risk of legal inconsistency with the rest of the new crypto-assets regulatory regime in the EU. In fact, EU institutions had purposefully decided to leave decentralised entities outside of the MiCA regulatory scope due to their early stage of development and the need to further study the sector to identify the associated risks before appropriately addressing them.

We would thus strongly encourage the co-legislators to stick to the political agreement reached during the negotiations on the MiCA Regulation and keep the reference to decentralised entities consistent with the wording enshrined under Recital 12a of the MICA Regulation, instead of introducing new confusing and contradicting language in the new Recital 11a (Amendment 140) in the AML Regulation.
Moreover, the political agreement reached clarified how the Commission will be tasked with assessing the development of DeFi markets within its Report on the application of the Regulation (Article 122). Based on this assessment, the Commission would then truly be able to evaluate the adequate regulatory treatment of decentralised crypto-asset systems.

We also welcome the decision by both co-legislators to align the AMLR provisions on transfers to self-hosted wallets (SHW) with the political agreement on the TFR, which also aims to fight money laundering, illicit finance, and sanctions evasion. We would thus further appreciate the decision to introduce a clear reference in the AMLR, as it was done in the TFR, to the use of blockchain analytical tools as appropriate ways of conducting risk-based enhanced monitoring of transactions.

Avoiding unfeasible requirements for Non-Fungible Tokens (NFTs)

A foundational notion in the MiCA Regulation is that not all crypto-assets are the same and that their regulation needs to recognize the differences among classes of crypto-assets. In this spirit, the European Parliament's proposal to impose the same KYC and CDD requirements for "persons buying or selling a single NFT" as the ones imposed on credit and financial institutions, is a disproportionate approach and inconsistent with MiCA. Casting a too wide net will severely limit economic activity, endanger personal privacy, and permit surveillance of consumers to an unprecedented level. This would clearly hinder the development of a digital asset market in the EU, as it will effectively put unachievable requirements for anyone willing to own or trade any digital asset.

It is essential to remember that blockchain technology, which is fundamental for crypto-assets and NFTs, is known for its transparency, which will enable regulators to achieve full oversight over the crypto environment. Instead of turning against the potential of digital ownership, lawmakers should embrace the technology and create balanced requirements that will not stop the growth of innovation in the EU. To achieve this, proportionality and a risk-based approach are key.

Ensuring the regulatory framework supports the innovation of Web 3.0, and avoiding an increase of risk of non-compliance of regulated entities

Self-hosted wallets (SHWs) are core elements of Web 3.0. Just like web browsers have given consumers broad access to the internet, SHWs are essential for users to access the next generation of the World Wide Web that is decentralised and allows for benefiting from blockchain-based programmability, automation, and creation of verified digital identities. However, Article 58 of the AMLR proposal prohibits regulated entities from providing anonymous wallets and accounts to clients. Users will therefore no longer be able to access a SHW service provided from regulated entities, although SHWs play such an important role in individual data ownership, digital empowerment and personal privacy - key concepts that lie at the core of the EU's data protection principles enshrined in the GDPR. As a result, users will be pushed towards unregulated entities in search for privacy when accessing Web 3.0. At the same time, such prohibitions will increase the risk that, in order to answer the need of their users for anonymous SHWs, regulated entities might do it outside of their regulated organisation, which will effectively lead to less, not more, overall compliance in the sector. Last but not least, if European entities are limited in their abilities to build products involving SHWs, institutions from the outside of Europe will fill in the gap, putting the development of the entire Web 3.0. domestic market in a disadvantaged position compared to the rest of the world.

To avoid these unintended consequences, a solution could be to adopt the language proposed by some of the amendments submitted in the European Parliament (e.g., AM 910), which would exclude from the scope of Article 58 all those CASPs that do not have direct access to private user data or user funds and solely function as software providers.

Protecting citizens' right to personal privacy and pseudonymity on the chain

Users' right to personal privacy online is put further at stake by the Council's own version of Article 58 AMLR, where the latest amendment would prohibit regulated entities from keeping "anonymity enhancing coins" as well. While we understand the regulators' objective of combating money laundering and terrorist financing, for which a key aspect is the identification of those involved in suspicious transfers of assets, we urge EU policymakers to not let misconceptions undermine their good intentions. It is crucial to remind that blockchains are not anonymous but pseudonymous, meaning that each user is directly associated with a public blockchain address rather than an identity. This means that blockchain transactions provide little privacy to users, who should have a legitimate right to decide whether they want to disclose the destination of their funds and the amount of their transactions to other users of the network.

Considering that regulated entities are already required to KYC new users when establishing a business relationship, prohibiting them from keeping anonymity enhancing coins as well would be redundant at best, and at worst it would stifle innovation in the EU Web3.0 sector and push users that have a legitimate interest in using these tokens towards unregulated entities and markets. We continue to advocate for KYC/CDD processes to be established at the on-ramps/off-ramps of blockchain networks, meaning on those entities and services that allow users to bring funds in and out of a blockchain network. That is where the identification of users brings added value to AML investigations, as everything that happens within a public blockchain can anyway be monitored and traced back to these entry & exit points.

About BC4EU

BC4EU is a trade association representing international blockchain industry players at the EU level. We work with policymakers, academics and our member companies to support their work in developing clear and consumer-friendly European regulatory frameworks for blockchain-based innovation. Over the past years, we have contributed to EU policies such as the AMLD5, MiCA, TFR, DAC8, taxation, data act, eIDR, as well as discussions around the Digital Euro.