BC4EU response to the European Commission's legislative package on anti-money laundering and countering the financing of terrorism

29 November 2021

Anti-Money Laundering Regulation (AMLR)[1]

Blockchain for Europe (BC4EU)'s position on the AML Regulation

- BC4EU welcomes the Commission's approach to harmonise the rules on customer due diligence for crypto-asset service providers.
- Decentralised Finance, whereby there is no single entity responsible for the transfer of crypto-assets, should be clearly exempted from the scope of the Regulation.
- BC4EU opposes the ban on anonymous crypto-assets wallets as it would cut off crypto-asset users from each other, undermining the technology's promise of peer-to-peer transactions.
- BC4EU calls for the supervision of crypto-asset service providers at EU level and supports the proposed date of entry into application of the Regulation.

Customer due diligence

Blockchain for Europe (BC4EU) welcomes the opportunity to share its views on the European Commission's proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

We support the Commission's approach to harmonise the rules on customer due diligence (CDD) for crypto-asset service providers (CASPs). While we believe that compliance with the CDD requirements for transfers above EUR 1.000 (Article 15(2)) is absolutely feasible for CASPs, we note that the limit is considerably lower than the threshold above which counterparties must be reported in cash transactions in the EU, and for which EU citizens who choose to use cash currently enjoy the benefit of privacy. In fact, CASPs already apply CDD measures on all users at onboarding and before they can even transact at all (i.e., from first EUR onwards), by virtue of the 5th Anti-Money Laundering Directive (AMLD5).

However, there are sometimes great divergences between Member States in how and what CDD measures need to be done. For instance, Estonia now requires a real-time video interview with all users from outside the EU/EEA (incl. for users from strong AML jurisdictions like the UK, US, Canada

[1] Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

secretariat@blockchain4europe.eu | @BlockchainforEU | Transparency register number: 910251734425-24

etc), which are automatically all considered as high-risk, and regardless of the amounts involved. Germany is also reportedly another jurisdiction to impose real-time video interviews on its Fintech sector (e.g., see onboarding process of challenger bank N26, compared to other more streamlined ones like Revolut, which only require selfies or photos of documents and users). This is disproportionate and overly prescriptive, and not in line with the current AML regime's risk-based approach.

Indeed, there is no real AML/CTF risk when the amounts involved are low (e.g., below EUR 1.000). Taking a different approach risks making EU CASPs uncompetitive compared to large non-EU platforms, which have users all over the world and are not subject to the same standards. Instead, real-time video interviews should really be limited to Enhanced Due Diligence (EDD) scenarios (e.g., higher amounts above EUR 15.000, PEPs, and users from less stringent AML jurisdictions which are not necessarily qualified as high-risk (e.g., non-OECD countries etc.)).

Lastly, although CDD will be feasible for all actors, it will not be possible to automatically know both counterparties to every transaction when one counterparty uses a non-custodial wallet. A consumer using a non-custodial wallet should be subject to the same reporting requirements that apply currently to cash.

Obliged entities and Decentralised Finance

The definitions of CASPs in the AMLR follow those of the Markets in Crypto-Assets Regulation (MiCA) (Article 2 (13-14)). While BC4EU believes the definitions between the two proposals should be aligned, it is also important that definitions are future-proof and exclude non-financial tokens and service providers. More specifically, the AMLR must be careful to avoid situations that would lead to merchants and others in commercial transactions to be subject to CASP registration/licensing and AML obligations, e.g., including if the merchant programs or operates a trading or exchange platform for digital assets, the digital asset is a crypto-asset and the merchant is a CASP. This result would violate traditional divisions between commercial transactions and financial instrument activities. Indeed, because tokens can be digital representations of literally anything, one needs to avoid a situation where the new AML obligations blur the line between financial instrument transactions and commercial transactions, converting all things that happen to be represented in a tokenised format into crypto-assets and all merchants into CASPs. For example, any online platform that offers participants the ability to buy or sell goods that happen to be represented in a tokenised format could hypothetically be swept into the definition of CASP, and thus subject to AML rules. This is true notwithstanding the possibility that such platforms may limit the types of tokens traded to tokens that are merely representations of intellectual property rights or entitlements to physical goods. In other words, none of the above are financial instruments, and the AMLR should strictly focus on the latter category.

Moreover, when it comes to Decentralised Finance (DeFi) specifically, it is not always clear who or what would be the AML "gatekeepers". In truly decentralised projects, there is no single entity that can ensure compliance with the rules. Instead, the governance of DeFi projects is managed by the community as a whole which makes them impossible to regulate in the same way as the traditional financial system. Presumably, each time users try to bring back crypto-assets back "on ramps" (i.e., convert back into fiat and send to/from bank accounts), there must be somewhere someone in charge of KYC/CDD. These could potentially be seen as gatekeepers when users go back and forth between traditional banking and financial systems, and the DeFi world. As such, the AMLR needs to clarify when Decentralised projects are not considered CASPs. Otherwise, the framework risks placing obligations on entities such as software developers, miners and validators that have no means to comply, ultimately driving innovation out of the EU.

Ban on anonymous crypto-assets wallets

The AMLR proposal includes a provision prohibiting anonymous crypto-assets wallets (Article 58). BC4EU opposes such a measure as we feel that this would cut off crypto-asset users from each other, undermining the technology's promise of peer-to-peer transactions. The principle that crypto users should be identified is not an issue, and in fact is already applied by CASPs. However, the blanket prohibition proposed by the European Commission and the Financial Action Task Force (FATF) over anonymous crypto-asset wallets – also through the adoption of the so-called "travel rule" ("TR") - raises substantial privacy concerns for CASPs and their end-users. The TR is the rule which requires banks to collect certain minimum information from both senders and recipients of bank transactions (e.g., names, IBANs etc). If the FATF's plans go ahead (including in the AMLR), CASPs would, on top of the strict AML/KYC rules they already apply, now be required to collect users' (unverifiable) self-declarations disclosing the full identity of persons behind each private crypto wallet address their accounts interact with.

For further details on this point, please see our comments below in the context of the Transfer of Funds Regulation (TFR) proposal.

CDD obligations for owners and beneficiaries of existing anonymous crypto-assets wallets

In the AMLR proposal, owners and beneficiaries of existing anonymous crypto-assets wallets are subject to CDD obligations before they are used in any way (Article 58). The legitimate and regulated CASP industry has evolved and already implements stringent CDD processes. By default, in strong AML jurisdictions at least (e.g., North America, EU etc), all users are subject to KYC procedures, i.e., identified and verified (personal information and supporting documentation such as IDs). Moreover, ongoing monitoring of transactions (crypto-assets and fiat) is already carried out whenever certain monetary thresholds are met (EUR 15.000). This inevitably entails questions to clients about the Source of Funds (SoF), which they need to provide information on and supporting documentation for. Large crypto-asset transactions from private crypto-asset wallets are anyway typically scanned with specialised blockchain analytical tools to reveal if said wallets are known or suspected of being tied to criminal activity (N.B. dirty wallets get reported to regulators, which build databases, which the above tools connect to). Given that the identity of the person truly behind a private crypto-asset wallet cannot be verified, any information is by definition self-declaratory. However, requiring CASPs to collect such information (i.e., map the presumed individuals) represents privacy risks and increases the cybersecurity risks (e.g., hacks).

Supervision

BC4EU advocates for starting with a clean slate and moving the licensing and supervision of the CASP and broader crypto-asset sector exclusively at EU-level (e.g., EBA, ESMA and/or the new EU AML Authority (AMLA)). The priority would therefore be to hire resources (i.e., developers, lawyers, economists/tokenomics experts etc), including from the private sector, with experience in this field to help the new body regulate and engage with the sector constructively. Among others, if crypto-asset sector actors that might have committed breaches of the law but want to clean up their act/become fully compliant, they should be encouraged to do so by proactively coming to the regulators with concrete solutions to propose. Only then will a truly balanced and innovative ecosystem develop for crypto-assets in the EU.

Entry into application

The AMLR will enter into application three years after its entry into force (Article 65). This means it will become applicable somewhere around the second half of 2025. We believe that the earlier the crypto-asset sector moves towards direct supervision at EU level (including by the EU AMLA), the better. Three years should be more than enough time for the sector to adapt, and for the EU AMLA to hire resources, including from the private sector, which understand the crypto-asset sector and are able to engage with it constructively. Moreover, CASPs and crypto-asset businesses throughout the EU should ideally all be under the direct supervision of EU-level regulators, including the EU AMLA. There is currently a lack of trust between the crypto-asset sector and many national regulators, and so a new reset via the EU AMLA would be strongly advocated by the sector. At the very least, CASPs should be able to fall under the competence under an opt-in system, and/or via further eligibility criteria (e.g., via a European Company/Societas Europaea status (i.e., directly or indirectly via parent company), recognition of any cross-border intra-EU activity etc).

Traceability of crypto-asset transfers[2]

Blockchain for Europe (BC4EU)'s position on the Transfer of Funds Regulation (TFR)

- BC4EU supports the exemption of person-to-person transfers of crypto-assets.
- The adoption of the "travel rule" through the TFR raises substantial privacy concerns for CASPs and their end-users. CASPs would, on top of the strict AML/KYC rules they already apply, now be required to collect users' (unverifiable) self-declarations disclosing the full identity of persons behind each private crypto-asset wallet address their accounts interact with.
- The more balanced solution, in our view, would instead be to focus on so-called "blockchain analytical tools" which can increasingly and effectively track and trace suspicious wallets and transaction flows, without compromising legitimate privacy.
- In parallel, CASPs would keep carrying out strong AML/KYC checks, which would ensure the safety and integrity of transactions conducted on CASPs across Europe.

Person-to-Person transfers of crypto-assets

Blockchain for Europe (BC4EU) supports the European Commission's proposed exemption of person-to-person transfers of crypto-assets in the TFR proposal (Article 2(4)). It is crucial that the exemption remains part of the final text in order to preserve one of the fundamental promises of blockchain technology.

Information obligations for the originator

Under the proposal, the originator must ensure that transfers of crypto-assets are accompanied by certain information on the originator (Article 14). As mentioned above, the adoption of the so-called "travel rule" ("TR") raises substantial privacy concerns for CASPs and their end-users. The TR is the rule which requires banks to collect certain minimum information from both senders and recipients

[2] Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)

of bank transactions (e.g., names, IBANs etc). If the Commission and FATF's plans go ahead (including in the AMLR), CASPs would, on top of the strict AML/KYC rules they already apply, now be required to collect users' (unverifiable) self-declarations disclosing the full identity of persons behind each private crypto wallet address their accounts interact with.

The stated purpose of course is to fight the illicit activity risks (such as ML/TF), which crypto-assets can pose. However, transposing a rule which makes sense in the traditional banking world without first really understanding the transparent nature of blockchain technology (whose ledgers are inherently public), raises huge privacy implications. Indeed, with a crypto-asset wallet address, one has absolute visibility on its current balance and full transaction history (including other counterparties/addresses). All one needs to do is go on a specialised search engine like Blockchain.com or etherscan.io and type the given wallet address. This is fine as long as the identity of the crypto wallet owner remains unknown, as all transactions and money flows on the blockchain will be publicly available pseudonymously.

The moment you start to map the ownership/identity of persons behind these wallets, you essentially know everything about them, in a way which even IBANs alone could never do (i.e., one cannot find out a person's balance and entire transaction history simply by typing their IBAN into a search engine). In addition, users' self-declaration about IBAN details are easily verifiable, in contrast with crypto-asset wallet addresses which are impossible to verify. Such unlimited sensitive Personally Identifiable Information (PII) should therefore not readily be available to anyone (including governments, banks, or even hackers who might malevolently gain access to CASPs' client databases), at least without certain checks and balances. This is why the CASP industry is now reaching out to privacy regulators (and we call on the European Commission to do the same) to give them an opportunity to weigh in against the FATF's and the European Commission's plans to implement the TR.

The more balanced solution, in our view, would instead be to focus on so-called "blockchain analytical tools" (e.g., crypto wallet scanning services like Chainanalysis), which can increasingly and effectively track and trace suspicious wallets and transaction flows, without compromising legitimate privacy. Indeed, each time known or suspected activity is detected on a CASP platform, the crypto-asset wallets associated with them are reported to regulators and law enforcement. These eventually make their way into databases of dirty wallets, and any other wallets that touch them, in turn, become suspicious (as all transactions are anonymous but fully public). Wallet scanning services connect to such databases (as might be done in the case of Politically Exposed Persons and International Sanctions lists).

In parallel, CASPs would anyway still carry out strong AML/KYC checks, so potential criminals would be unlikely to use them to cash out their large criminal proceeds, i.e., criminal activity (e.g., ML/TF, ransomware attacks etc) that rely on crypto-assets like Bitcoin, do not occur in the open (i.e., CASPs like Coinbase where all users are subject to KYC procedures), but in the criminal underworld of the darknet. These are two parallel worlds that rarely meet. Legitimate CASPs are, therefore, the wrong target to address any potential AML/CTF concerns, as in fact, they are at the forefront of this battle.

In any case, regardless of what personal information is ultimately collected by CASPs, financial privacy is important and due process should be required in order for governments or anyone else to gain access to financial information (holdings or transactional). Naturally, this right of privacy is not absolute, just like the right of ownership is not absolute. Private parties may have a claim on a financial asset or an informational asset. Similarly, governments may under certain circumstances seize or require reporting concerning either type of asset. However, if any party seeks to seize it or require that a financial institution report information, the standard should be one of due process where the

actor makes a sufficient showing with respect to the owner and their assets before seizure or reporting is permitted.

Information obligations on the beneficiary

In the proposal, the CASP of the beneficiary shall verify the accuracy of the information on the beneficiary in cases of transfers of crypto-assets exceeding EUR 1.000 (Article 16). Most regulated CASPs already apply Enhanced Due Diligence (EDD), notably by requesting information and evidence of the client's Source of Funds (SoFs), whenever incoming or outgoing (fiat or crypto) transactions exceed EUR 15.000. Verifications at EUR 1.000 could be logistically challenging for CASPs to handle, and not really in line nor proportionate with AML law's key principle of the Risk-Based Approach (RBA). Again, it is important to remind regulators that criminals who use crypto-assets for illicit purposes do so on the darknet, not via regulated CASPs. So, applying extra checks on such a low amount as EUR 1.000 (which does not represent a material ML/TF risk), would equate to shooting a fly with a bazooka, and still missing the mark.

Final remarks on the ongoing negotiations

BC4EU is extremely concerned about the recent push by EU Member States to remove certain derogations for crypto-asset transfers falling under the 1.000 EUR threshold. We feel that this approach is disproportionate and not in line with the principle of technology neutrality, as well as with the aim to create a level playing field with financial instruments. It will mean that transfers of funds in fiat are treated more leniently compared to transfers of crypto-assets, despite the lack of evidence to suggest the latter represent a higher inherent money-laundering risk. As outlined above, merchants, intermediaries and vendors who participate, whether virtually or physically, in generally low-risk commercial transactions are outside of financial institution style regulatory and licensing requirements. This should remain the case regardless of the technology used. Blockchain databases should be treated no differently than other databases and the same should apply to the assets tracked on them. Ultimately, the removal of this derogation will drive out European entities simply because they have no means to comply with onerous verifications for every single small transaction.

Lastly, we urge the legislators to avoid aligning the TFR proposal with recent global developments such as the Updated FATF guidance on Virtual-Asset Service Providers (VASPs). The latter would effectively impose disclosure obligations on entities that have no means to comply, such as software developers. Indeed, DeFi projects have no single entity that can comply with such obligations and treating them as financial intermediaries will only put Europe at a competitive disadvantage globally.

About BC4EU

Blockchain for Europe (BC4EU)[3] is a trade association representing international blockchain industry players at the EU level. We work with policymakers, academics and our member companies to develop a European regulatory framework to support and promote blockchain-based innovation. Over the past two years, we have contributed to EU policies such as the 5th Anti-Money Laundering Directive, the Markets in Crypto-Assets Regulation (MiCA), and the 8th Directive on Administrative Cooperation (DAC8). We continue to participate in the regulatory dialogue and remain available for further information on our comments and suggestions.

[3] *EU transparency register ID: 910251734425-24*