Enabling KYC and AML verification in DeFi service

Mesquita Borba Maranhao M, Suzana; Seigneur, Jean-Marc

Enabling KYC and AML verification in DeFi services

Suzana Mesquita de Borba Maranhão Moreno
University of Geneva
Geneva, Switzerland
Suzana.Mesquita@etu.unige.ch

Jean-Marc Seigneur
University of Geneva
Geneva, Switzerland
jean-marc.seigneur@unige.ch

Abstract

This paper proposes an approach to comply with KYC/AML regulations supporting self-hosted wallets, empowering users to voluntarily comply by selecting the most suitable compliance analysis provider when participating in regulated use cases and to take more informed decisions considering the intrinsic risks of their own transactions. This voluntary approach creates an infrastructure for DeFi services self-regulation and enables the development of new DeFi use cases compliant-by-design with KYC/AML requirements. By introducing innovative KYC/AML techniques based on dynamic computation, the approach supports financial inclusion and privacy-preserving techniques in regulated DeFi services, while respecting the risk-based FATF recommendations. The proposed approach can be implemented in a complementary way to existing intermediary-based regulations, like centralized KYC and AML and the Travel Rule.

1. Introduction

Money laundering is the process of making money generated by criminal activity appear lawful by using the financial system. The United Nations Office on Drugs and Crime estimated in 2013 that between 2% to 5% of global gross domestic product (GDP) per year is a result of money laundering and less than 1%, probably around 0.2%, is seized and frozen [1].

A relevant coordinated initiative to combat money laundering was the creation of FATF in 1989. The Financial Action Task Force [2] is an independent inter-governmental body that develops and promotes policies to protect the global financial systems against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF has developed a series of recommendations that are recognized as the international standard for combating financial crimes. These recommendations include preventive measures that apply to traditional financial systems and, more recently, to virtual asset service providers. Countries that follow FATF recommendations must promote measures to make these recommendations a reality in the public and private sectors. Two sets of regulations are relevant in the context of compliance verification on user transactions involving cryptoassets: the usual KYC/AML regulation and the Travel Rule. Both are verified by the intermediaries during some of their client operations.

Regulations based on intermediaries cover only part of cryptoassets transactions because blockchain and other types of distributed ledger technologies enable the possibility of performing transactions without involving intermediaries when between two self-hosted wallets. There is an ongoing discussion if and how DeFi and the self-hosted wallet should be monitored by

regulators[1]. Until now, FATF is not explicitly giving a broad recommendation to regulate transactions among self-hosted wallets because (a) the available data on the P2P market is not reliable enough to make an informed policy decision, (b) the intermediated transactions are still relevant enough to allow for effective implementation of the standards and (c) P2P transactions that are visible on public ledgers enable financial analysis and law enforcement investigations [3].

At the same time, there are new services trying to be more compliant with the regulation of traditional financial institutions, the so-called institutional DeFi [4]. For example, there are permissioned lending pools in DeFi that require KYC and AML checks on users. This requirement can be satisfied in at least two ways: by interacting with custodial wallet users [5] (since the custodial provider may do the required verifications in their customers) or by requiring a personal or a corporate user to do KYC/AML with a specific service provider linked to a fixed blockchain address to be whitelisted [6]. As far as the authors know, there is no standard way to approach these KYC/AML verifications, so the user is not able to select the KYC/AML provider he/she wants.

This paper proposes an approach to comply with KYC/AML regulation supporting self-hosted wallets, empowering users to voluntarily comply by selecting the most suitable compliance analysis provider when participating in regulated use cases and to take more informed decisions considering the intrinsic risks of their own transactions. This voluntary approach creates an infrastructure for future DeFi services regulation and enables the development of new DeFi use cases compliant-by-design with KYC/AML requirements. By introducing innovative KYC/AML techniques based on dynamic computation, the approach supports financial inclusion and privacy-preserving techniques in regulated DeFi services, while respecting the risk-based FATF recommendations. The proposed approach can be implemented in a complementary way to existing intermediary-based regulations. In fact, it can be applied to comply with the FATF recommendations to collect Travel Rule data from self-hosted wallets when interacting with virtual asset service providers (VASPs), which is an issue when implementing Travel Rule.

The remainder of this paper is divided as follows. Section 2 discusses some background concepts. Sections 3 and 4 detail the proposal, dividing the explanation between what is done in the edge (Section 3) and how the information generated by the edge is verified (Section 4). Section 5 discusses some considerations to implementation, while Section 6 concludes the work. Finally, Section 7 presents some references linked throughout this paper.

2. Background

This section aims to provide a high-level introduction to concepts that will be needed in the remainder of the paper.

Compliance background and innovative technologies

KYC (Know your customer) is a process to identify and continuously verify customers during the business relationship with a financial institution with a primary goal to comply with a set of regulatory requirements [7]. Anti-money laundering (AML) is a set of laws, regulations, and procedures intended to prevent money laundering and maintain secure financial institutions.

[1] https://www.cnbc.com/2021/11/04/defi-the-wild-west-of-crypto-is-set-to-face-regulatory-crackdown.html

One FATF recommendation of AML is to do Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD), which may involve KYC and other pieces of information like verification on the origin of funds and the origin of the wealth of a customer.

The traditional way some institutions do KYC is by asking for government-issued docs to prove identification and utility bills to prove address. Innovative approaches include biometric data, location technologies and decentralized social trust, including graph-based approaches like BrightID[2], verifiable credentials together with decentralized identity [8] [9], token-based computation [10] and peer-to-peer social trust [11]. Some of these innovative ways are minimizing the data leaked by the user during an identification, enabling compliance while preserving user privacy. For example, it is possible to compose solutions enabling a person to claim that he/she is not involved in financial crimes based on their work reputation and their income in the last years without revealing his/her own identity.

More information on KYC and AML can be found in the work of Moreno et al [7].

Know Your Transaction or KYT is a financial industry term that refers to the process of examining financial transactions for fraudulent or suspicious activities including money laundering[3]. This technique is especially relevant to transparent DLT/blockchain protocols because sophisticated algorithms can be used to infer the risk of a specific transaction. KYT techniques enable VASPs to monitor their customer and to minimize the risk of money laundering. There are specific services focused on providing KYT solutions to blockchain networks, e.g., ChainAnalysis[4]. It is also possible to offer KYT services in a wallet to provide risk-based information related to user transactions. This is the case of the Metamask Institutional[5] wallet.

DeFi and Compliant-DeFi

Decentralised Finance (DeFi) is an umbrella term for a collection of financial products which rely on smart contracts and blockchains to enable open, peer-to-peer (P2P) financial services and automate specific procedures [12].

DeFi transactions may happen between self-hosted wallets without involving any intermediary. For example, it is possible to send cryptoassets from one user to another or to engage in a lending protocol without involving any intermediary. And any KYC/AML verification as well. Despite the growth of DeFi services, and the increasing number of self-hosted wallet users, there is still an ongoing debate about how these wallets and DeFi services should be regulated.

The lack of compliance prevents some users, especially institutional ones, to be involved in these services. There are some new DeFi models trying to comply with regulations to attract these institutional users to their services. For example, as already discussed, there are permissioned lending and borrowing pools to compliant users only [5] [6]. In the long run, with more time to increase regulation, the concept of regulated DeFi may become more common to institutions and individuals as well.

---

[2] https://www.brightid.org/

[3] https://ciphertrace.com/glossary/know-your-transaction-kyt/

[4] https://www.chainalysis.com/

[5] https://metamask.io/institutions/compliance/

Identification on DLT/blockchain use cases

Identity is an essential requirement for many blockchain use cases. There are at least two well-known types of identity solutions linked to blockchain projects. The first one is well-known as decentralized identity and aims to increase privacy and control of the user data. It is common to use some W3C standards in the implementation of this use case, like decentralized identifier [8] and verifiable credential [9]. One example of scenario using this solution is a person that creates his/her own identifier and receives education credentials linked to this identifier issued by a university. Following a different implementation, Binance announced[6] that they will offer a non-transferable NFT token to users who pass KYC identification following the theoretical proposal of Vitalik [10].

A second solution aims to create a proof that an entity in real life manages an asymmetric key pair or a DLT/blockchain address, as a decentralized name service. In the example above, the university may generate a proof to become a public well-known issuer. There are no privacy requirements. One example of a project implementing this idea is called Lacchain DNS[7]. In this project, an entity can link an existing digital certificate to a blockchain address and this link is available on-chain on an EVM-based network called Lacchain. It enables smart contracts on this network to verify on-chain that a blockchain address belongs to a specific entity.

3. Compliance Analysis in the Edge

This section describes how to perform KYC/AML analysis on the edge of a DLT/blockchain solution to achieve our desired guidelines. By edge, we mean linked to the user wallet and possibly one or more off-chain services.

We identified two main flows for compliance in the edge. The first one is a flow to request that the trusted third party analyze KYC/AML of a person[8], generating an on-chain proof for this analysis. The user wallet should store a reference for this proof and enable the user to add a reference for this proof on further transactions to be sent to a DLT/blockchain network. The second flow is to request that the trusted third party analyze a transaction and include the result of this analysis attached to the transaction to be sent.

This section will analyze these two flows using a compliant wallet. A compliant wallet is an application that can interact with a compliance analysis service to request KYC/AML analysis. The compliance service is hosted by a trusted third-party, which can be private or public sector institutions and can be remunerated by doing this analysis. A compliant wallet should allow the Originator to select which service(s) to use in a free market. For simplicity, this paper will consider the involvement of a unique compliance analysis service. A more elaborated proposal can also support the participation of multiple compliance analysis services enabling a future verifier to consider multiple KYC/AML analyses.

---

[6] https://cointelegraph.com/news/first-binance-soulbound-token-bab-targets-kyc-user-credentials

[7] https://github.com/lacchain/lacchain-dns

[8] For simplicity we will assume that who sends the transaction is always a person. Someone could argue that it could be a system, a set of people, a people in behalf of an institution etc, but we will not cover these cases in this paper.

The risk-based approach recommended by FATF can be applied in both flows. The compliance analysis may be based on traditional or on innovative ways to do KYC/AML and may include a dynamic way to compute risk [11] [13]. This latter approach supports financial inclusion and privacy-preserving techniques, avoiding the disclosure of personal information in lower-risk and undesired scenarios.

Finally, an authentication mechanism between the wallet and the compliance analysis service can be created to reuse information managed in previous interactions. So, for example, if the user changes the DLT/blockchain address in use, the compliance service can reuse previous KYC/AML proofs.

3.1. Analyzing KYC/AML of an Entity in the Edge

The overall model to do the compliance analysis of an entity followed by sending transactions to the DLT/blockchain network is depicted in Figure 1. In this flow, the same result of a compliance analysis can be reused in many user transactions if the Originator uses the same DLT/blockchain address[9]. The remainder of this subsection will describe the steps of Figure 1.

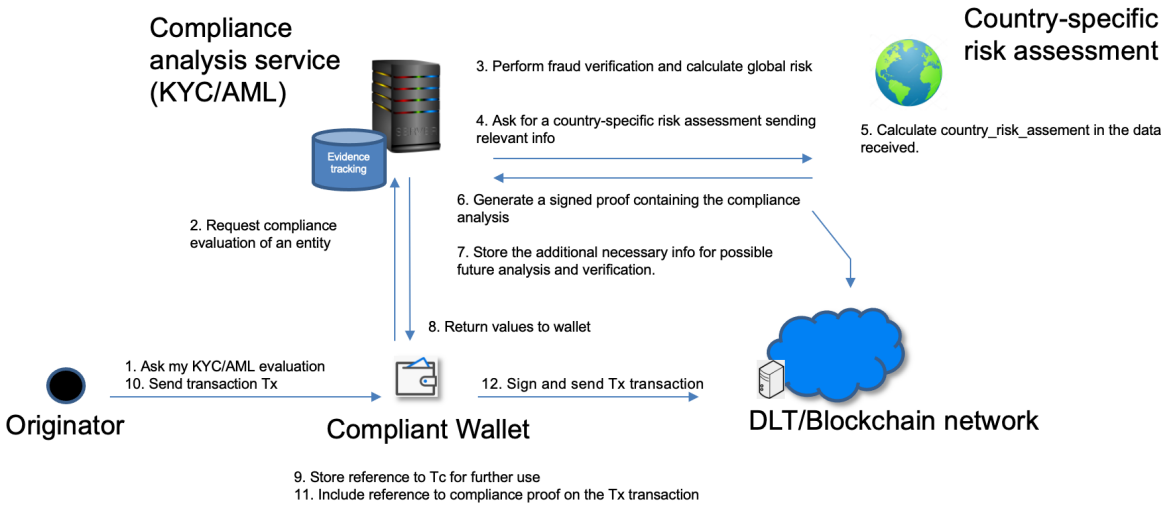

Figure 1: Analyzing KYC/AML compliance of an entity (steps 1-9) and sending a transaction linked to the compliance proof (steps 10-12).

Step 1: Ask KYC/AML evaluation of an entity

The Originator sends KYC/AML proofs to the wallet (e.g., proof of identification, proof of address, proof of income) and a DLT/blockchain network that wants to save the result for his/her compliance analysis.

Step 2. Request compliance evaluation of an entity

The wallet receives the data. The compliant wallet will first determine:

[9] One could also argue that the user could user other address since he/she can proof that he/she owns both addresses. Although it can work, it will also reveal the link among the two addresses, which many be not desirable.

- If it is a custodial wallet - a proof of VASP identity, the country where the user is registered for using of VASPs services and the compliance level[10] associated with the user, determined when the user followed the VASP KYC/AML process.
- the country to be considered for analysis – If the wallet is custodial, it can be the country where the account is registered (as in the previous bullet). If the wallet is non-custodial or if the custodial wallet cannot send the required information described in the first bullet, it should be the country where the user is located, which can be determined for example by using GPS service in the Originator's device, by searching in a global service or by asking the user;
- the chainID associated with the information about the DLT/blockchain network sent by the user.

Then, the wallet will send these pieces of information together with the data received from Step 1 to the compliance analysis service.

Note1: the wallet should let the user configure the URL of the compliance analysis service to be used in the same way that wallets enable users to configure the gateway to submit the transaction to the DLT/blockchain network. In this way, the user can change the compliance analysis service if desired.

A standardization work is important to determine (1) the requirements and tests to be considered a compliant wallet and (2) chainIDs linked to supported DLT/blockchain networks. KYC/AML standardized formats would help to simplify the overall KYC/AML analysis and verification. To enable broader interoperability, it is important to have a standardization of the compliance level considered by VASPs.

Step 3. Perform fraud verification and manage global risks

The compliance analysis service will be executed by a trusted third party. First, it will perform fraud verification with the following checks.

- the country received as input in the incoming request is correct by running fraud-detection algorithms.
- The KYC/AML proofs are valid.

If any of these checks fail, the compliance service returns to the wallet indicating the error on the input data.

Then, this step analyzes the KYC/AML presented proofs with global reach, if there are any. For example, user location based on location technologies, proof-of-address based on decentralized social trust [11], token-based computation [10], etc. The global risk assessment will be part of a bigger return of this service, called compliance_level (CL).

Note 1: since the country information can be faked by the edge, there is a risk of doing the calculation using the wrong country, so it is better to consider as much analysis as possible at the global level, but it may demand a common agreement among different countries' regulations.

Step 4. Send info to country-specific risk assessment

[10] This text will discuss the concept of compliance level linked to compliance analysis service in Section 4, but the concept can also be applied to a VASP analyzing a user during its KYC/AML internal processes.

The compliance analysis service will send any relevant information to the country-specific risk assessment service.

Step 5. Country-specific risk assessment

Calculate country_risk_assement considering data received. The default calculation will focus on the KYC/AML proofs sent by the user. Additional proofs may lead to improved analysis and eventually to a different risk value.

Note 1: in the case of custodial wallets, this service may decide to trust the existing KYC/AML practices and sign it without doing another reevaluation of the user information.

Note 2: this step may include contact with the user for example to do a liveness check or to ask for additional KYC/AML proofs.

Defining standardized measures for risks with associated thresholds and KYC/AML standardized format at least country-level help to simplify the overall KYC/AML analysis done on this step.

Step 6. Generate proof of compliance analysis

The service must generate a proof that enables any interested party to verify that the legal analysis was done in the entity in a timely manner. This text proposes to use as compliance proof a non-transferable NFT token like proposed by Vitalik [10] and recently announced for future support by Binance, as previously discussed. Since the proof is saved on-chain, it will enable on-chain verification for DeFi services. After sending the DLT/blockchain transaction, the service should recover the identification of this transaction to the wallet (or even to the NFT directly). We will call this transaction Tc.

It is important to link the public key of the asymmetric key pair belonging to the compliance analysis service to a real-world identification, since some DeFi services may want to base their compliance decisions considering this identification, as explained in Section 4.

Note 1: there are pros and contras of linking the compliance proof to a specific country. The country information may be considered PII (personally identifiable information), but it may also be a relevant piece of information for some verifiers. So, the user may inform if he/she wants to make the country info public on-chain in the analysis of the compliance proof even by including this info in step 1 or by configuring it as a parameter in the wallet (and the wallet includes it in step 2).

Note 2: one could argue that other PII could also follow a similar approach, for example, if the user is bigger than 18 years etc. We understand that this kind of proof should be achieved using another solution, for example, a verifiable credential [9]. Actually, the entity offering compliance analysis services will be well-placed to provide additional services as credential issuers.

Note 3: it is important to make compliance_level, current_analysis_time[11] and an identification of the compliance analysis service provider public on the NFT so any external party will be able to check the compliance proof is valid, even without going off-chain.

Step 7. Store necessary additional info

The compliance analysis service should store in private repository information for possible future risk analysis and compliance verification. The persisted info includes at least chainId, identification of the DLT/blockchain transaction used to save the compliance proof, compliance_level, the country considered for regulation, KYC/AML proofs. Also, some information about the incoming request, namely IP address and device id.

Step 8. Return to Wallet

Return values to the wallet, including the identification of the DLT/blockchain transaction used to save the NFT.

Step 9. Wallet decision

In this step, the wallet should store the identification of the DLT/blockchain transaction used to save the compliance proof (Tc) and any additional relevant information to enable the user to select the most appropriate compliance proof when sending further transactions using the wallet. One relevant information is the on-chain address of the NFT (which may be more than one number, depending on the NFT standard used), because this information will be used later to link the Originator transaction with the NFT.

Step 10. Originator sends a transaction to DLT/Blockchain network

In a further moment, the Originator decides to send a transaction to the DLT/blockchain network and informs that he/she wants to reuse an existing KYC/AML compliance proof. We will call this transaction Tx.

Step 11. Include reference to compliance proof

The Originator selects the most appropriate compliance proof to be linked with Tx. Because the wallet will link the on-chain address of the NFT in Tx, any DeFi service will be able to find the compliance proof without going off-chain.

Note 1: We confirmed that it is possible to include extra bytes of information on the Ethereum network keeping backward compatibility both in a transaction sending only ETH (Ethereum native cryptoasset) as well as in a transaction invoking a smart contract (by including

[11] One could argue that the DLT/blockchain is already time-based, but this info may not be available on the smart contract.

them after the last argument of the smart contract function). For simplicity, we are not covering the case of networks which this backward compatibility is not possible.

Step 12. Sign and send Tx transaction

The wallet then signs the transaction Tx and sends it to the financial network.

Additional comments:

- When sending Tx to the network, the compliance wallet may also offer a new compliance analysis to check KYC/AML linked to the user transaction, e.g., KYT risks. We did not cover this case for simplicity.

3.2. Analyzing KYC/AML of a Transaction in the Edge

The overall model to do the compliance analysis of a transaction is depicted in Figure 2. This flow should be selected when the user wants to create uncorrelated transactions, perhaps using different blockchain addresses or even blockchain networks, without reusing the compliance proof. The remainder of this subsection will describe the steps of Figure 2.

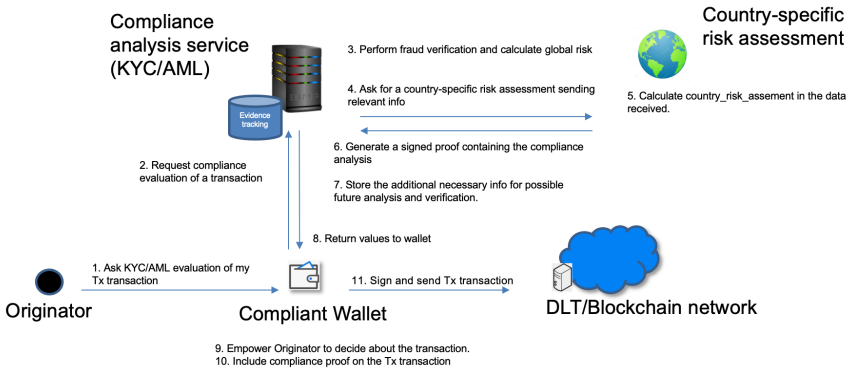

Figure 2: Analyzing KYC/AML compliance of a transaction to be sent a compliance proof.

Step 1: Ask KYC/AML evaluation of a transaction

In addition to the information in step 1/3.1, the Originator should also send transaction data to be signed by the wallet - the transaction can be a simple value transaction or a complex smart contract transaction involving many transfers at the same time.

Step 2. Request compliance evaluation of a transaction

Similar to step 2/3.1 but invoking the compliance analysis service for a transaction (in opposition to an entity).

Step 3. Perform fraud verification and manage global risks

In terms of fraud verification, this step will verify the same topics of step 3/3.1 plus the transaction format. The transaction should have a valid format considering the chainID DLT/blockchain network indicated.

When estimating the global risks in this step, besides analyses in the entity detailed in Section 3.1, new analyses can focus on the transaction itself. An important example is KYT to determine the transaction risk in the specific blockchain network.

Two additional notes in addition to the ones in step 3/3.1 are:

Note 2: Since the same transaction can involve many internal value exchanges, the global analysis should consider the entire transaction, not only the Originator, the Beneficiary (ies) and the amount involved.

Note 3: The risk analysis is valid for a specific chainID. There may be cases in which the transaction has a valid format for different DLT networks. To minimize the risk of doing the analysis for one chainID and later sending the transaction to another chainID, a careful approach of including two chainIDs with similar transaction formats must be followed. A natural approach would be to always consider the riskiest chain, but this decision may lead to risks higher than necessary. Further analysis of this case should be done. To make the decision explicit in the transaction, the chainID will be considered in the generation of the compliance result returned to the wallet in step 8.

Note 4: This proposal does not completely handle the KYC/AML linked to the Beneficiary(ies) of the user transaction. This is especially important when dealing with transactions without smart contracts, when KYC/AML proofs of the Beneficiary(ies) can be an important input to measure the transaction risk. Although some analyses can consider the Beneficiary (like KYT for example), this topic deserves a more elaborated discussion. This is left to future work.

Step 4. Send info to country-specific risk assessment

Equals to step 4/3.1.

Step 5. Country-specific risk assessment

Similar to step 5/3.1. New analyses, if any, can focus on the transaction itself.

Step 6. Generate proof of compliance analysis

The service must generate a compliance proof that enables any interested party to verify that the legal analysis was done in a timely manner. We propose to use a compliance_check, generated by the following steps:

1. Recover the current time in seconds following UNIX standard and call it current_analysis_time.
2. Take the hash of {transaction_data + current_analysis_time + chainID } using SHA-3. This hash is called in this paper hash_to_sign.
3. Using the asymmetric key pair of the compliance analysis service, sign the hash_to_sign.

Comments about the link of the compliance analysis service to a real-world identification and notes 1 and 2 are equal to step 6/3.1.

Step 7. Store necessary additional info

The compliance analysis service should store in private repository information for possible future risk analysis and compliance verification. The persisted info includes at least transaction_data, current_analysis_time, chainId, compliance_check, compliance_level, the country considered for regulation, KYC/AML proofs (if any and if necessary). This step should also store some information about the incoming request, namely IP address and device id.

Step 8. Return to Wallet

Return values to the wallet, including compliance_check (that is the compliance proof), compliance_level (including global_risk_assement and country_risk_assessment) and current_analysis_time.

Step 9. Empower Originator to decide about Tx

In this step, the wallet will do some sanity checks and ask the user how to follow considering the response of the compliance analysis service.

For sanity checks, the wallet verifies that the current_analysis_time is still not expired. The wallet should also confirm that the compliance_check or similar proof is well-formed (i.e., the signature is valid and linked to the correct data).

The wallet will inform the user about the calculated risks and recommend sending or not the transaction based on it. The wallet may do additional tests to check if global_risk_assessment and country_risk_assessment are bigger than local thresholds. These thresholds may be configured by the Originator. One example here would be someone trying to send a transaction to a risky smart contract without the proper awareness. It is especially relevant considering that the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the virtual currency mixer Tornado Cash smart contract[12]. A compliant wallet would avoid sending transactions involving this new category of sanctioned smart contracts.

The compliant wallet advises the user about the risks linked to the transaction empowering a more informed user decision. The user will decide how to follow: send or cancel the transaction. In addition, the user may opt to store the compliance_proof for some use in the future.

Step 10. Transaction final bundling

Supposing the user decides to send the transaction, the wallet finishes transaction bundling considering the Originator transaction data and the data returned by the compliance analysis service.

The wallet will attach the compliance information in the Originator transaction keeping backward compatibility as explained in Note 1 of step 11/Section 3.1.

Note 1: it is important to make current_analysis_time, compliance_level and the identification of the compliance analysis service provider public on-chain so any external party

[12] https://home.treasury.gov/news/press-releases/jy0916

will be able to check on-chain the signature of the compliance_check was created for that chainID network in a timely manner and using an appropriated compliance level.

11. Sign and send Tx transaction

The wallet then signs the Tx transaction and sends it to the financial network.

4. Verification of the Compliance Information Produced in the Edge

This section describes how to make use of the information generated by the edge about KYC/AML compliance. The text is divided into possible verifiers, compliance level details and how to verify compliance proofs.

Possible Verifiers

This verifier we are originally interested are DeFi services. Smart contracts of DeFi services are able to read the information included by the edge because the compliance proof (either the NFT or the compliance_check) and all the necessary info to read the analysis were saved on-chain. New DeFi services can verify at the user or transaction level, that the minimum compliance_level was satisfied achieving what we called compliance by design.

Besides DeFi services, other possible verifiers of the compliance proof are:

- VASPs that may make business decisions based on compliant proofs. For example, to receive a transaction for non-custodial wallets only when it contains or it refers to a compliance proof with a minimum compliance level. This technical solution can be used to deal with the border of Travel Rule regulation;
- self-hosted wallets which may also want to verify the received transaction in similar ways VASPs do;
- gateways to DLT/blockchain networks that may distribute only transactions with a minimum compliance level;
- new KYT services which may, for example, create a new type of analysis considering the historical trace of KYC/AML compliance.

The mentioned sanction of Tornado Cash demonstrated how different crypto services, including DeFi services[13], stablecoin providers[14], gateways[15] and exchanges[16] avoided transactions linked to U.S. sanctions. Many DeFi services blocked transactions only in the front-

[13] https://cryptoslate-com.cdn.ampproject.org/c/s/cryptoslate.com/defi-protocols-aave-uniswap-balancer-ban-users-following-ofac-sanctions-on-tornado-cash/?amp=1
[14] https://cointelegraph.com/news/circle-freezes-blacklisted-tornado-cash-smart-contract-addresses
[15] https://cointelegraph.com/news/alchemy-and-infura-block-access-to-tornado-cash-as-vitalik-buterin-weighs-in-on-debate
[16] https://www.coinbase.com/institutional/research-insights/research/weekly-market-commentary/weekly-market-commentary-august-12-2022

end, due to the difficulty of acting at the smart contract level. Our proposed mechanism would help DeFi services to act at the smart contract level as well[17].

Following this approach, it would be possible for example to create a fork of Tornado Cash used only by KYC/AML-users and these users would have their identity protected by the compliance analysis service provider selected by themselves, creating thus a compliant service that we could call "Tornado Clean Cash".

Understanding the compliance level

Section 3 mentioned a few times the concept of levels of compliance. The compliance_level may assume different values for different types of proofs. The bigger the value, the bigger the expected level of compliance, from 0 to 100. Lower values of compliance may be used by those service providers who want to offer innovative KYC/AML services. The table below presents some fictitious levels for proof of identification with their respective required proof as an example.

Example of Compliance_level	Example of proof required
100	Physical presence on site + government-issued document authentication + message signature using private key of a blockchain address of a compliance service
80	Online presence using video + government-issued document authentication + message signature using private key of a blockchain address of a compliance service
50	Recorded video with the person + government-issued document authentication + message signature using private key of a blockchain address of a compliance service
30	Verifiable Credential issued by an entity called X1 to the blockchain address attesting full name, place and date of birth.

The necessary level of compliance varies for each DeFi use case, the amount of value in the user transaction, transaction history and maybe others. Since global standards for these compliance levels are hard to achieve, an additional solution is needed to map the service provider offers with the DeFi service needs. We imagine that service providers will need to publish the rules they adopt for calculating compliance levels while DeFi services will need to configure the minimum level for each compliance provider. For example, this process may be automated if the compliance provider publishes a smart contract containing a description of the compliance levels using a formal model. This formal model should be created as a standard to enable the comparability of compliance service providers.

[17] In this case, DeFi services could for example increase the compliance level of some compliance analysis services providers or even do nothing since existing mechanisms could already consider the new risks (e.g., KYT providers would be updated to consider the risks of the new sanctions). Blockchain-level decisions should still be taken in a decentralized way by using a multisig wallet or a DAO (Decentralized Autonomous Organization).

We imagine that a smart contract is needed for each service provider but in the longer run, some standards (de facto or formal ones) may simplify this matching process. Other examples of proofs that may compose the compliance level are proof-of-funds, proof-of-wealth, proof-of-address, proof-of-not-politically-exposed-person, etc.

How to verify the compliance proof

The verifier may need to determine the real identity of the compliance service provider as explained in step 6 of Sections 3.1 and 3.2. Since our proposal wants to enable on-chain verification, we propose to use an on-chain repository of trusted third-party identification like the one already described as Lacchain DNS.

To verify the compliance proof of an entity (generated by flow 3.1), it is necessary to first follow the reference inside the Originator transaction to find the NFT acting as compliance_proof. Then, check the attributes of the NFT to verify its integrity and if the compliance_level meets the necessary requirements of the use case. All of this can be done on-chain, enabling compliant-by-design DeFi services.

The verification aims to determine that the compliance proof was really signed by the expected compliance analysis service provider. The following steps are valid for one compliance_check (flow 3.2) saved together with the Originator transaction:

1. Recover the transaction_data without signature and without the compliance_check, current_analysis_time and compliance_level;
2. Recover the chainID (ID linked to the DLT network in use), the current_analysis_time and the compliance_level;
3. Calculate the hash_to_sign following what was described in step 6/Section 3.2;
4. Recover the identification of the compliance analysis service provider and verify that it really signed hash_to_sign generating the compliance_check.

In case of success, the verifier can check if the current_analysis_time is not expired, if the real identity of the signer is a trustworthy institution and if the compliance_level meets the necessary requirements of the use case. Again, all of this can be done on-chain, enabling compliant-by-design DeFi services.

5. Considerations for implementation

Some concerns in the implementation of this model are: (a) the possibility of censoring transactions that should be sent to the financial network; (b) increasing of surveillance state without a proper measure of the results in practice; (c) how to bootstrap this model and (d) increasing of cost and time to send a financial transaction to the network.

The possibility of censoring transactions is minimized because the compliance analysis is voluntary and the user is free to choose different service providers.

The concern of surveillance is also minimized because the analysis is voluntary, so the user may select to use it only when compliance analysis is already necessary. A relevant discussion is how to regulate DeFi services and how it will force use cases to ask users to prove KYC/AML information. As discussed, there are already institutional DeFi use cases requiring compliance verification. In the future, we foresee that the number of these use cases will increase

since regulation in crypto is becoming more mature. This regulation may increase the surveillance state and it is true that this proposal is a way to implement this at smart contract level. We understand this as a way to make the regulatory needs work together with the crypto ecosystem, at the same time that it preserves users' privacy and freedom of choice.

The bootstrap of this model is simplified because the transactions are backward-compatible. A famous regulated use case may be enough incentive to start using a model like that. A relevant difficulty will be the creation of trusted parties willing to provide this compliance service. Providers may ask for a fee, adding financial incentives to the equation. Still, some legal considerations must be taken since these service providers will manage PII and will sign the responsibility of correct KYC/AML checks.

The last concern is the fact that compliance analysis may increase the cost and time to send a user transaction. The first flow that generates an NFT token minimizes this concern because the compliance proof may be reused in many transactions. We foresee that this decision for reusing the NFT or generating new proofs for each transaction will vary depending on the DeFi use case, transaction amount, user preference and maybe other factors. In addition, both flows may be optimized with an authentication mechanism to reuse some saved info about the user during the compliance analysis service execution.

6. Conclusions

This paper proposes an approach to comply with KYC/AML regulations supporting self-hosted wallets, empowering users to voluntarily comply by selecting the most suitable compliance analysis provider when participating in regulated use cases and to take more informed decisions considering the intrinsic risks of their own transactions. This voluntary approach creates an infrastructure for DeFi services self-regulation and enables the development of new DeFi use cases compliant-by-design with KYC/AML requirements. By introducing innovative KYC/AML techniques based on dynamic computation, the approach supports financial inclusion and privacy-preserving techniques in regulated DeFi services, while respecting the risk-based FATF recommendations.

The proposed approach can be implemented in a complementary way to existing intermediary-based regulations, like centralized KYC and AML and the Travel Rule. In fact, it can be applied to comply with the FATF recommendations to collect Travel Rule data from self-hosted wallets when interacting with virtual asset service providers (VASPs), which is an issue when implementing Travel Rule.

As presented during the text, the guidelines considered in the design of this proposal are: (a) working on all types of wallets, on-the-fly, without relying on intermediaries or on a single verifier; (b) enabling the user to select among a set of existing compliance analysis service provider(s); (c) backward-compatible with existing on-chain code and with existing DLT/blockchain networks; (d) preserving evidence that compliance analysis was done, verifiable for any external observer, while not exposing PII on-chain; (e) minimizing the disclosure of PII while respecting specific national regulations; (f) enabling the development of new use cases compliant-by-design with KYC/AML requirements with on-chain verification; (g) enabling the use of more than one blockchain address or the use of more than one DeFi service without additional user action; (h) not blocking any user transaction.

Some could argue that this proposal minimizes the crypto ethos of monetary liberty by creating built-in censorship. We do not believe this proposal should be applied to all use cases nor at protocol level. It is a tool to be applied when society understands it is appropriate, using the adequate compliance level. We hope that innovative KYC/AML techniques will enable meeting the compliance requirements while minimizing the disclosure of PII. We also expect that competition among compliance analysis service providers will incentivize these innovative KYC/AML techniques to flourish. In sum, this proposal enables DeFi services to meet the necessary regulatory needs while it preserves users' privacy and freedom of choice.

7. References

[1] UNODC, "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes," 2011. [Online]. Available: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

[2] FATF, "The FATF Recommendations." 2019. Accessed: Dec. 10, 2019. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[3] Notabene, "State of Crypto Travel Rule Compliance Report 2022," Jan. 2022. Accessed: Jul. 03, 2022. [Online]. Available: https://notabene.id/state-of-crypto-travel-rule-compliance-report

[4] Consensys, "DeFi for Institutions," Jul. 2021. Accessed: Jul. 03, 2022. [Online]. Available: https://pages.consensys.net/defi-for-institutions-report-2021

[5] "Aave - Open Source Liquidity Protocol." https://aave.com/ (accessed Jul. 03, 2022).

[6] "Alkemi Network - Compliant DeFi for Institutions & Individuals." https://alkemi.network/ (accessed Jul. 03, 2022).

[7] S. M. B. M. Moreno, J.-M. Seigneur, and G. Gotzev, "A Survey of KYC/AML for Cryptocurrencies Transactions," in *Handbook of Research on Cyber Crime and Information Privacy*, 2020. Accessed: Oct. 03, 2021. [Online]. Available: https://www.igi-global.com/chapter/a-survey-of-kycaml-for-cryptocurrencies-transactions/261722

[8] W3C, "Decentralized Identifiers (DIDs) v1.0." https://www.w3.org/TR/did-core/ (accessed Mar. 26, 2022).

[9] W3C, "Verifiable Credentials Data Model v1.1." https://www.w3.org/TR/vc-data-model/ (accessed Mar. 26, 2022).

[10] E. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized Society: Finding Web3's Soul." Rochester, NY, May 10, 2022. doi: 10.2139/ssrn.4105763.

[11] S. M. de Borba Maranhão Moreno and J.-M. Seigneur, "Towards a decentralized social trust solution to proof-of-address," in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, New York, NY, USA, Abril 2022, pp. 330–333. doi: 10.1145/3477314.3507186.

[12] European Blockchain Observatory and Forum, "Decentralised Finance (DeFI)." Accessed: Jul. 03, 2022. [Online]. Available: https://www.eublockchainforum.eu/reports

[13] S. Jean-Marc, "Trust, Security and Privacy in Global Computing," University of Dublin, 2005.