TFR position paper

Version 1.1 - 22-jun-2022

Bert & Peter Slagter

In this document we would like to outline our concerns on the draft of the proposal for the 'Regulation on information accompanying transfers of funds and certain crypto-assets (TFR)' as reported on april 6 2022[1].

On certain aspects the current proposal is incompatible with the nature of crypto-assets, which causes the proposal to contain concepts that don't actually exist and make no sense technically. These aspects could potentially cripple legitimate use of the technology without actually improving security or prevention of crime.

Wallets don't have addresses

Crypto-assets are fundamentally different from traditional digital assets, like bank money, that are managed by a central party like a commercial bank, tech company or government institution. The same words (e.g. wallet, address, transaction) are used for fundamentally different concepts.

Let's start with 'wallet'. Unfortunately, in the context of crypto-assets '**wallet**' is not a rigorously defined term, on the contrary, it's an abstract and vague concept that is used in many fundamentally different ways.

Basically a wallet is software in the form of a mobile or desktop app that manages information needed to view and transfer crypto-assets. A wallet does not contain any assets, as the metaphor suggests. Assets are registered on a blockchain together with spending conditions that can only be satisfied by proving the possession of certain information.

[1] https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.html

There is no such thing as ‘your assets’ or ‘my assets’, in the sense that assets are explicitly linked to an individual. Someone can possess or know certain information that enables him to transfer crypto-assets. This information includes (but is not limited to) seed phrases, passwords, private keys, public keys and redeem scripts.

Wallets manage this information for the user, and help the user construct a valid transaction, i.e. a transaction that meets the spending conditions recorded in the blockchain. This unlocking process sometimes requires multiple parties to sign off; multiple wallets need to provide information to meet the spending conditions.

The term ‘wallet’ is also used for hardware devices that contain keys and are used by wallet software to construct a transaction. ‘Signing device’ would probably have been a better name than ‘hardware wallet’. It is common practice to require multiple signing devices for valuable transactions.

So, to summarize:

- Crypto-assets are digital property registered in a blockchain together with the conditions that need to be met to transfer these assets.

- A wallet is software that manages keys and other information that enables a user to construct a transaction.

- A transaction is an instruction to transfer crypto-assets, which means record new spending conditions in the blockchain. Constructing a transaction may involve multiple wallets and/or signing devices.

- There is no explicit concept for person, entity or ownership. Just possessing or knowing certain information (words, numbers) implies (shared) ownership.

These wallets are called ‘**unhosted wallets**’ in the TFR proposal.

The term ‘wallet’ is also used by service providers. This can mean two things: (1) the service provider manages the keys on behalf of the user or (2) the service provider manages a pool of assets and the user only has a claim on a fraction of that pool.

These are called ‘**crypto-asset accounts**’ in the TFR proposal.

So in TFR the term ‘wallet’ refers to ‘unhosted wallets’ or ‘non-custodial wallets’ that are not an account at a service provider.

The term ‘**wallet address**’ is used in the TFR proposal as a way to identify wallets. However, there is no such thing as a ‘wallet address’. They do not exist. Wallets don’t have addresses.

Many blockchains use the term address for either the spending conditions (utxo-based[2], e.g. bitcoin), a derivative of a public key (account-based, e.g. ethereum) or even a route/path to a node (lightning network[3]).

It might very well be the biggest mistake in the entire technology that the term ‘address’ was used for this, as it wrongly evokes the image of a bank account number or e-mail address.

A wallet contains keys and other information that can be used to generate many addresses. For example, for utxo-based blockchains it is advised to never re-use the exact same spending conditions (address) twice, and generate a new address for every utxo.

It is useful for service providers to register the origin and destination addresses (or just the transaction ID) for future (criminal) investigation purposes.

It makes no sense to treat addresses as a proxy to a person or wallet, comparable with bank account numbers or e-mail addresses. There is no way to ‘verify an unhosted wallet’ that technically means anything.

---

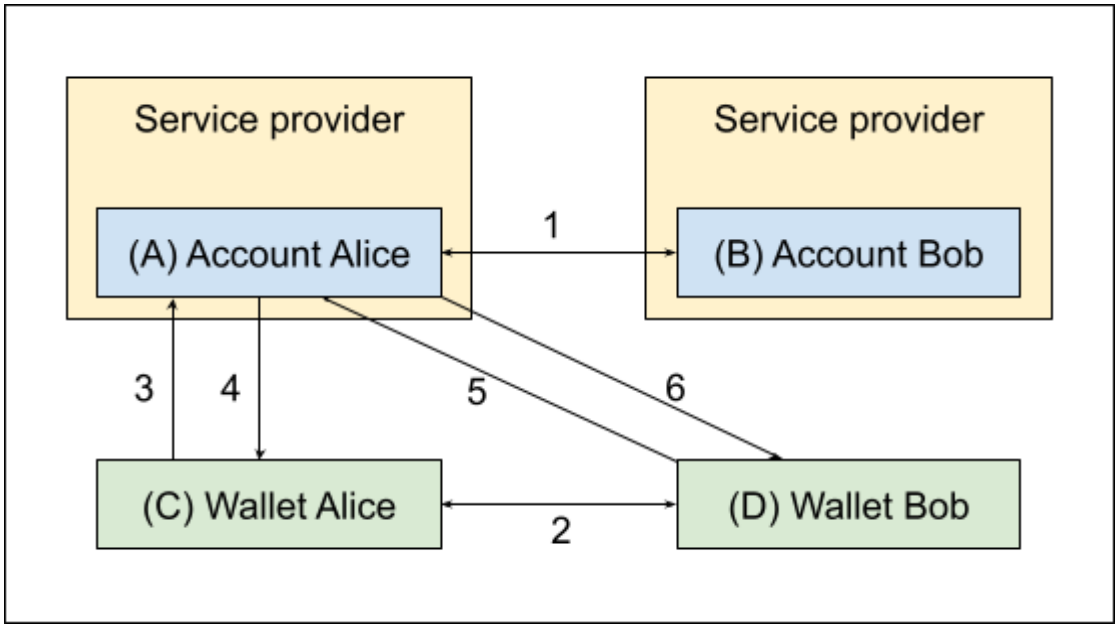
[2] UTXO stands for Unspent Transaction Output and represents some amount of digital currency which has been authorized by one account to be spent by another.
[3] The Lightning Network is a payment protocol layered on top of bitcoin, intended to enable fast transactions among participating nodes.

Similar to ‘security through obscurity is false security’, we could say ‘security through clarity is false security’. Both are forms of theater that give the uninitiated a feeling of security but don’t mean anything material for malicious actors.

Let’s look at an example. In some countries users are currently required to provide a screenshot of their software showing an address. It’s trivial to (a) generate a fake screenshot and (b) relay incoming and outgoing transactions from and to any other address.

Different kinds of transfers

Let’s explore the different kinds of transfers.



(1) Account to Account

This transfer can be regulated using the current TFR proposal by requiring the two involved service providers to comply.

(2) Wallet to Wallet

This transfer falls outside of the scope of the TFR proposal.

(3) My wallet to my account (deposit)

This is a transfer of assets between a wallet and account of the same person or entity, usually referred to as ‘deposit’.

This is where we need to pay attention, because this is where illicit assets can potentially enter the regulated system.

For both deposit (3) and withdraw (4) identification or verification of ownership of a wallet or address does not mean anything. In both cases the actual transaction connects an address to an account holder. Knowing the address (which is nothing more than spending conditions) beforehand does not provide extra benefits.

In both cases (3) and (4) bad actors can effortlessly relay assets from or to any address using (2). So even if it could be implemented, it not only wouldn’t provide any (extra) intelligence, it wouldn’t hinder bad actors either.

However, we can require the user to be identified (KYC/CDD) and require service providers to use risk based controls to identify illicit transactions or patterns of transactions (e.g. smurfing). In the Netherlands many service providers have already implemented advanced transaction monitoring tools (KYT[4]) and already screen their customers to comply with AML regulations.

Summary:

- The user is identified by signing in to their account, and all crypto-assets transferred into their account shall be considered theirs. The service provider is required to monitor the transactions to make sure they match the customer profile and are not connected to illicit activity.

- The ‘unhosted wallet’ will not be identified or verified, as this is just security theater (Article 16, 4a).

(4) My account to my wallet (withdraw)

[4] KYT stands for Know Your Transaction, which is a commonly used term that refers to the process of examining financial transactions for fraudulent or suspicious activities including money laundering.

This is a transfer of assets between an account and a wallet of the same person or entity, usually referred to as ‘withdraw’.

Under (3) we already argued that it wouldn’t provide any intelligence nor hinder bad actors to require unhosted wallets to be identified or verified for withdrawal.

Summary:

- The user is identified by signing in to their account, and all crypto-assets transferred out of their account shall be considered theirs. The service provider is required to monitor the transactions.

- The ‘unhosted wallet’ will not be identified or verified (Article 14, 5b).

(5) & (6) Other wallet to my account

Transfers (5) and (6) are between an account and a wallet of different persons or entities, it can be conceptualized as ‘to pay’ or ‘be paid’.

Technically (5) and (6) do not differ from (3) and (4). Practically they don’t either, since (5) is the same as (3) + (2) and (6) is the same as (4) + (2).

The TFR proposal requires Bob to identify Alice in case of (5) but not in case of (3) + (2). Similarly it requires Alice to identify Bob in case of (6) but not in case of (4) + (2).

This is inconsistent and introduces an impediment for service providers to interact with unhosted wallets on behalf of their customers, for example to interact with smart contracts, web3-enabled websites or pay with lightning.

Examples:

- Bob pays for bread at Alice’s Bakery. Bob uses his unhosted wallet, Alice uses a service provider (5)

- Alice pays for coffee at Bob's Coffee Shop. Alice uses her account at a service provider, Bob uses his unhosted wallet (6)
- Alice uses a service provider to deposit money at a decentralized finance smart contract, which is unhosted by nature (6)
- Alice uses a service provider to issue a decentralized identifier to an unhosted third party (self-sovereign identity) (6)
- Bob's car streams money to Alice's energy company for using energy while charging (5)

Some of these examples may use/involve:

- Real time payments, micropayments or streaming payments;
- Non-human participants (e.g. robotics, autonomous vehicles, smart contracts);
- Transactions of crypto-assets that do not have value (e.g. decentralized identity or certain NFT's).

For those examples identification/verification would be impossible or the sheer amount of data that it produces makes it practically infeasible.

To exclude these use cases from the TFR proposal, there should be a de minimis threshold based on the transaction value, in concordance with the FATF recommendation.

Furthermore, from the perspective of a service provider these examples can be treated the same as deposits and withdrawals with regard to transaction monitoring and compliance with AML regulations.

Note that though there's no technical distinction between (3) and (5), the semantics of a transaction (deposit/withdraw vs. pay/be paid) become clear at the level of the service that is provided:

- A service provider that facilitates custody, trading or brokerage should treat all transactions as deposits (3) and withdrawals (4), and belonging to the authenticated user (and monitor transactions accordingly).

- A service provider that facilitates point-of-sales solutions should treat all transactions as payments (5), and require the merchant to adhere to AML regulations that already require the merchant to verify customer identity for high risk transactions.

Summary:

- Consider a payment to an account (5) to be the same as a deposit (3) and a payment from an account (6) to be the same as a withdrawal (4).

- Remove the requirement to collect information about the owner of the unhosted wallet (Statement 29a) and inform authorities about these kinds of transactions (Statement 33a).

- Remove ‘no exemptions based on the value’ and re-introduce a threshold of 1000 euro per transaction (statement 20 and 22a).

Self-sovereign identity

In the future a universal self-sovereign identity (SSI) ecosystem might contribute to a user-friendly and secure way to verify the identity of users (human and non-human) of unhosted wallets. The necessary standards, protocols and applications are in early development. Notable organizations involved are the W3C, Microsoft, and TBD (Square). Some of them are working together[5] to establish an open ecosystem of decentralized identity.

As with cryptocurrencies, a future SSI ecosystem will be most useful if it is based on open and global standards to which people, organizations and governments can adhere. The developments have now passed the proof of concepts phase, but a lot of work is still being done on the basis of local, fenced-in initiatives. If MiCA and/or TFR provide a direction for these developments, our advice would be to steer stakeholders towards working with global and open (source) components.

[5] For example, dozens of organizations work on foundational components under the flag of the Decentralized Identity Foundation (DIF), see https://identity.foundation/.

This includes the following components:

- Decentralized identifiers (DID's). DID's are a W3C international standard[6] for identifiers created, owned, and controlled by individuals, without reliance on centralized entities.
- Decentralized web nodes. An implementation of DIF's emerging decentralized personal datastore standard.[7]
- Self-sovereign identity services[8]. A service that handles the full verifiable credentials lifecycle, including issuance, verification, revocation, and more.

Implementation and usage of these components puts users in control of their data and identity, as opposed to the third parties that now own and control their private data. This is beneficial for a wide range of applications, including the communication between a user and his crypto-asset service provider (CASP). Alice and Bob would be able to prove their identity without even revealing any of their personal information (using zero-knowledge proofs[9]), including at times when they interact with a CASP using their unhosted wallet.

Assuming a mature SSI ecosystem, MiCA and/or TFR could be amended to explicitly mention the usage of the involved ecosystem components. For example, a CASP could drop the threshold of 1000 euro per transaction if both actors are identifiable using SSI compatible services or software.

We estimate that it will take at least 10 years for these specifications and standards to be implemented in consumer level applications, smart phones, point-of-sales systems, etc.

Proposed changes to the TFR proposal

Statement 20 & 22a

Remove the statement about the exemption for low-value transactions and the de minimis threshold, since transaction monitoring is perfectly able to mitigate the risks.

---

[6] See Decentralized Identifiers (DIDs) v1.0.
[7] See Decentralized Web Node specification. This specification is in a draft state.
[8] See TBD's ssi-service for an example implementation (in development).
[9] In cryptography, a zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.

Statement 29a

Remove this statement, or change to consider all assets transferred from and to unhosted wallets to be owned by the account holder.

Statement 33a

Remove this statement, or change to explicitly rely on risk based monitoring by the service provider.

Article 14 - 5b

Remove the requirement to collect and verify information about the owner of the unhosted wallet. Just consider any crypto-assets transferred to any unhosted wallet to be a withdrawal of the account holder.

Article 16 - 4a

Remove the requirement to collect and verify information about the owner of the unhosted wallet. Just consider any crypto-assets transferred from any unhosted wallet to be a deposit (and therefore the responsibility) of the account holder.

Remove the requirement to notify the competent authority of any customer having received more than 1000 euro. A risk based approach using transaction monitoring and knowledge of the customer by the service provider is more proportionate.

Add the explicit responsibility of the service provider to monitor all incoming transactions and detect high risk transactions or patterns of transactions (e.g. smurfing).