Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 08/2023

Staking

20 December 2023

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Contents

1 Introduction

The entry into force of the DLT Act (Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology) established a legal basis for the custody of cryptoassets that protects customers in the event of the custodian going bankrupt. Due to the growing importance of staking services, FINMA has increasingly had to respond to questions about how these custody rules apply to staking. Depending on the nature of the staking service, it is possible that the requirements of the DLT Act may not be met and the assets would therefore not be protected in the event of the custodian's bankruptcy.

The adoption of a proof-of-stake consensus mechanism by the Ethereum blockchain, the change in the macroeconomic situation and rising interest rates has made enquiries about this issue even more current, which accentuates the need to take action. To raise awareness of the issues surrounding staking among market participants, FINMA has held roundtable discussions with industry representatives. In addition, FINMA conducted a survey among supervised institutions about their staking services.

This guidance sets out the result of the discussions surrounding the supervisory treatment of staking services for customers. It aims to provide guidance on how FINMA will interpret financial market law with regard to distinguishing between custody assets that are protected in the event of bankruptcy and deposits exposed to insolvency risk, the associated bank licensing obligations and the impact on capital requirements for authorised institutions.

2 Staking

2.1 Description

There is currently no single definition of staking. FINMA regards staking as the process of blocking native cryptoassets at the staking address of a validator node in order to participate in a blockchain validation process based on a proof-of-stake consensus mechanism. Participants earn rewards for staking cryptoassets.

Proof-of-stake blockchains differ in that in some cases the inverse process of unstaking involves a variable lock-up/exit period, which means there is a delay in returning blocked cryptoassets. Moreover, blockchains sometimes create negative incentives for maintaining compliant validation activity, in that in the event of a validator node behaving improperly cryptoassets that

have been locked by staking can be subject to partial or complete deletion ("slashing").

2.2 Variants

Various variants of staking have developed in practice. For the purposes of this guidance there will be differentiated between the following types:

- **Custodial staking:** In custodial staking, the customer transfers the cryptoassets to a third party. Custodial staking comprises the two variants of *direct staking* and the *staking chain*:
  - **Direct staking**: in direct staking, the service provider operates the validator node itself or outsources its operation to a technical service provider, but retains the withdrawal keys to return the customer's staked cryptoassets itself.
  - **Staking chain**: in a staking chain, the cryptoassets being staked are passed on by the institution with the customer relationship to one or more other institutions who operate the validator node and hold the withdrawal keys.
- **Non-custodial staking:** In non-custodial staking the customers maintain exclusive control over the withdrawal keys and therefore there is no custody or acceptance of assets by third parties.

2.3 Risks

The use of staking services entails a number of risks:

- Technical risk of a malfunction of the staking process; in addition there is a risk of the cryptoassets being slashed due to misconduct by the validator node; penalties may also be imposed automatically, for example if the validator node goes offline due to technical problems or a lack of adequate business continuity management.
- Counterparty risk due to the unclear legal position in the event of bankruptcy; in Switzerland there is currently legal uncertainty about the treatment of staked cryptoassets in bankruptcies in certain situations (see section 3.2). This legal uncertainty is even greater if the custody or staking is delegated to foreign institutions, as there are often no specific regulations on the treatment of cryptoassets in bankruptcies in many foreign countries.
- Market risk, as it may not be possible to sell staked cryptoassets at the right time in a volatile period if the unstaking process includes a lock-up/exit, creating a delay in returning blocked cryptoassets. In certain blockchains such as Ethereum, the lock-up period is longer if the number of unstaking orders rises, which can lead to very long lock-up periods in a crisis and temporarily make it technically impossible to sell

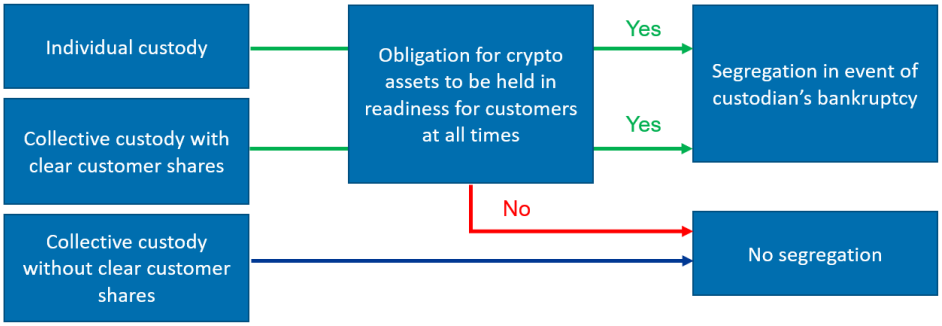
the cryptoassets. The duration of the lock-up may sometimes be non-transparent and unpredictable for customers due to a continuously changing withdrawal queue and number of validators.

3 Supervisory treatment

3.1 Legal basis for custody of cryptoassets

The DLT Act entered fully into force with effect from 1 August 2021. The new Article 242*a* of the Debt Enforcement and Bankruptcy Act (SchKG) created a legal basis for the bankruptcy-protected custody of cryptoassets. The chart below shows the requirements that must be met to segregate assets in the event of the custodian's bankruptcy.

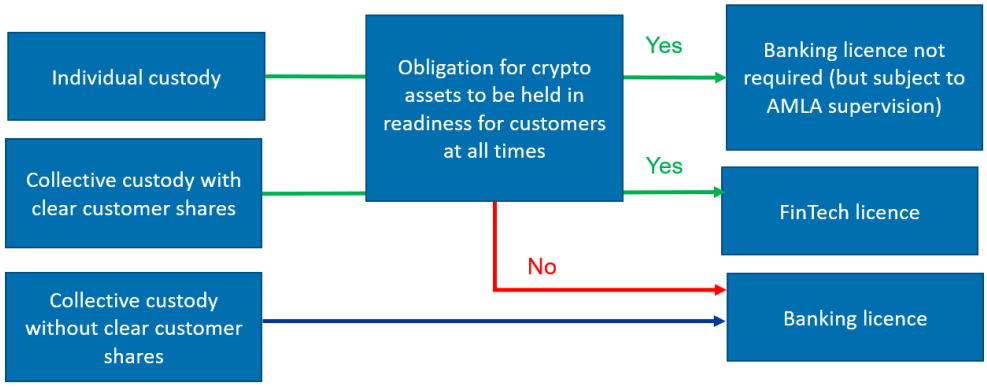
Treatment under bankruptcy law (Art. 242*a* para. 2 SchKG):



In line with this new regulation in bankruptcy law, an equivalent provision was added in Article 16 no. 1bis of the Banking Act (BA) for institutions covered by banking law. Article 16 BA lists the custody assets that are segregated from the estate in the event of bankruptcy and returned to custody account holders in accordance with Article 37*d* BA. The segregation is designed to give preferential treatment to instruments that appear in the custody account holders' custody statements and are not held on the bank's own books.

These provisions are also relevant for determining whether there is an obligation to obtain a banking licence. For example, since the entry into force of the DLT Act, accepting cryptobased payment tokens in collective custody on a commercial basis has, in addition to commercial acceptance of public deposits, been explicitly subject to authorisation within the meaning of Article 5*a* of the Banking Ordinance (BO).

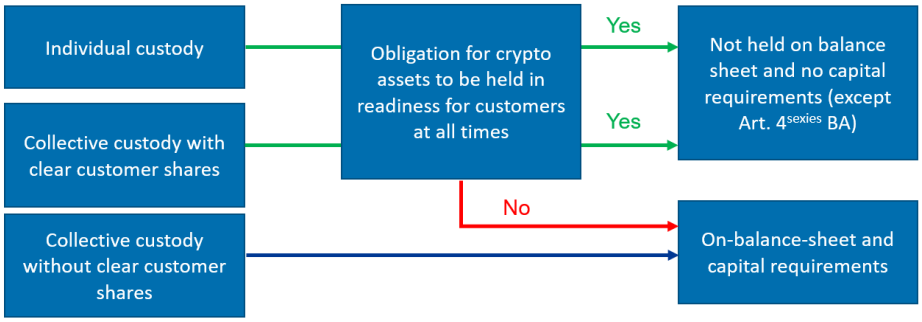
Treatment under banking law (Art. 1*a* and 1*b* BA in conjunction with Art. 5 and 5*a* BO):



Holding payment tokens in a collective account with clear customer shares requires a banking licence. A FinTech licence in accordance with Article 1*b* BA is sufficient for this kind of custody, provided the payment tokens are held in readiness at all times. But a banking licence is not required for individual custody of payment tokens held in readiness at all times. However, such custodians are subject to the AMLA as financial intermediaries and must join a self-regulatory organisation for the purposes of money laundering supervision.

For banks there is also the question of which cryptoassets held in custody must be booked as deposits and which can be held off-balance sheet as custody assets. This is an important question, as prudential requirements need to be met for assets held on the balance sheet.

Accounting treatment and prudential requirements:



A prerequisite for qualifying cryptoassets as off-balance sheet custody assets is that they are *held in readiness for the customer at all times*. If the cryptoassets are not held in readiness for the customer at all times, in the case of payment tokens they are public deposits that need to be held on the balance sheet, which triggers further capital requirements. In the case of collective custody of cryptoassets, a further requirement for qualification as a

custody asset is that custody account holders' shares in the collective assets are clear (e.g. by means of an internal register that clearly allocates the cryptoassets to each customer and enables them to be segregated and returned to customers in the event of bankruptcy).

3.2 Applicability to staking

There are a range of questions about how the custody provisions set out above should be interpreted in relation to staking services. These mainly revolve around the central criterion for bankruptcy protection, which is that the cryptoassets are held in readiness for the customer at all times.

This criterion is not met if the custodian carries out staking on its own account. In these situations, this can be viewed as business on the institution's own account, as defined by Article 1*a* para. b BA. Consequently, cryptoassets that are staked on the custodian's own account cannot be segregated in the event of bankruptcy and attract capital requirements.

But when the staking is carried out on behalf of the customer for the customer's account, the legal position is uncertain. In these situations, the exact staking mechanism of the blockchain concerned needs to be analysed on a case-by-case basis.

From a bankruptcy protection perspective, blockchains that do not have a lock-up period or sanctions mechanism (slashing) for staking are unproblematic. Without lock-up periods, slashing or similar restrictions on access, the cryptoassets are available to the customer at all times and can thus be segregated if necessary.

The dispatch on the new Article 242*a* SchKG states: "This means that from the point at which power of disposal over the assets is transferred by the third party to the insolvent company, or it acquires ownership of the assets on behalf of the third party, the insolvent company is obliged to have uninterrupted power of disposal (as defined by para. 1) over the assets, although it is sufficient if the obligation is limited to keeping custody of the number of units held for third parties on an uninterrupted basis. In other words, the insolvent company is permitted to replace individual tokens, provided the total number of tokens is not reduced, so that the tokens can be returned to the beneficial owner at all times."[1]

If the staking service involves a risk of slashing and/or a delay in unstaking (lock-up/exit period) for the cryptoassets held in custody, while the provider retains the power of disposal over the withdrawal keys, it is unclear whether, in accordance with the Federal Council's dispatch, it is ensured that the

[1] Dispatch of 27 November 2019 on the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, Federal Gazette **2020** 233, available at: https://www.fedlex.admin.ch/eli/fga/2020/16/de (not available in English).

cryptoassets can be returned to the beneficial owner at any time. It is therefore doubtful whether the requirement of being held in readiness at all times within the meaning of Article 242*a* para. 2 SchKG and Article 16 no. 1bis BA is met. Under the current legislation there is a legal ambiguity here.

The requirement of being held in readiness at all times flows from the technology-specific provisions of Article 242*a* para. 2 SchKG and Article 16 no. 1bis BA, which, reflecting the circumstances at the time the legislation was drawn up, were designed with custody in mind rather than staking. To date there is no relevant case law or practice by the Swiss bankruptcy courts as to whether cryptoassets staked on blockchains with lock-up periods and/or slashing still meet the criterion of being held in readiness at all times. Nor are there any international recommendations on the treatment of staking.

4 Legal consequences

4.1 Staking by licensed institutions

4.1.1 Staking chain

If an institution delegates the operation of the validator node in a staking chain to a third party (e.g. other banks or staking pool operators), in accounting terms the institution has a claim on this counterparty from the authorised institution (hereafter referred to as the “third party provider”). This claim can either be recognised on the balance sheet as a claim on the third-party provider or, if certain conditions are met, as a fiduciary claim within the meaning of Article 16 no. 2 BA, which can thus be treated as a custody asset.

A prerequisite for qualification as a fiduciary claim is an analogous application of the Swiss Banking Directives on fiduciary investments, adapted to the risks of cryptoassets, to rule out gross negligence by custodians towards their customers. This adaptation of the directives is needed to take account of the specific risks of staking.

To assume a fiduciary relationship of this kind in relation to staking, there would thus at a minimum need to be a fiduciary agreement with a specific fiduciary mandate from the customer including the selection of the cryptoassets and the amount. The agreement would also have to contain a comprehensive risk disclosure to the customer in connection with the staking mandate (in particular with regard to slashing and any lock-up period), which is in keeping with the other duties set out in the directive.

The institution must in particular:

- limit counterparty risks by selecting an institution subject to prudential supervision with a good credit standing, or the subsidiary of a consolidated and prudentially supervised financial group with a good credit standing;
- ensure by means of specific due diligence that:
  - the third-party provider is not conducting business on an unauthorised basis;
  - the third-party provider holds the relevant withdrawal keys itself, which rules out long staking chains. If the third-party provider wishes to use another provider, the institution must verify that the mitigation measures (such as presigning the withdrawal transactions) have an equivalent effect;
  - the third-party provider records the validator addresses (e.g. by means of an internal register) on which it holds the custodians' cryptoassets and informs the custodian of these;
  - the third-party provider has taken all necessary measures to limit operational risks relating to the operation of the validator node, such as validation errors or offline status, rule out other penalties on the validator and ensure business continuity; and
  - if providers outside Switzerland are used, in addition to the abovementioned requirements, they must be subject to prudential supervision in a jurisdiction with equivalent regulation, in which there is the same legal certainty as in Switzerland regarding the treatment of cryptoassets held in custody under bankruptcy law and undergo specific due diligence which includes the requirements listed above for providers based within Switzerland;
- draw up a Digital Assets Resolution Package (DARP) to ensure adequate risk management. The DARP should be updated regularly and:
  - contain the most important information required to identify and secure the cryptoassets promptly (e.g. description of the custody type, details of contact persons with access to the private keys, information on third-party custodians etc.);
  - ensure that the liquidator can pay out the cryptoassets quickly to investors in the event of bankruptcy, limiting the administration and expense of an orderly return of the assets to a minimum.

4.1.2 Direct staking

In direct staking an institution usually performs the staking itself and also has power of disposal over the withdrawal keys to return the blocked

cryptoassets. Segregation in accordance with Article 16 no. 2 BA therefore does not apply.

As discussed in section 3.2 above, there is legal uncertainty about whether the requirement of being held in readiness at all times within the meaning of Article 242a para. 2 SchKG and Article 16 no. 1bis BA are met.

Due to the unclear legal position, FINMA will not at present require banks to meet the capital requirements for staked cryptoassets, provided all of the following conditions are met:

- the customer has given a specific instruction about the type and number of cryptoassets to be staked;
- appropriate steps have been taken to ensure that the cryptoassets placed on a particular validator address, and a particular withdrawal address after unstaking, can be allocated unambiguously to the customer;
- the customer is informed transparently and clearly of all risks (including slashing, lock-up periods and risks relating to the legal uncertainties in the event of bankruptcy);
- appropriate steps are taken to mitigate the operational risks of operating a validator node (including business continuity management), in order to avoid slashing and other penalties; and
- a Digital Assets Resolution Package (DARP) is prepared to ensure adequate risk management (see section 4.1.1 for details on the contents of a DARP).

If these requirements are met, FINMA's current assessment is that in the event of the bankruptcy of a supervised entity, the staked cryptoassets should be segregated from the estate and returned to the custody account holders in accordance with Article 37*d* in conjunction with Article 16 no. 1bis BA.

This practice only applies on an interim basis until the position is clarified by new legislation, a court decision or international developments, which would lead FINMA to re-evaluate its interpretation.

4.2 Direct staking by unlicensed market participants

Where unlicensed market participants engage in custodial direct staking commissioned by customers for their own account, FINMA will assume that there is no requirement to obtain a banking licence, subject to the same proviso that there are no court rulings, regulatory changes or international developments to the contrary. This assumes that the staked payment tokens continue to be held in individual custody in direct staking, i.e. there is a separate and assignable blockchain address for each customer (at the levels

of the original custody address, staking address and withdrawal address) and the provider holds the withdrawal keys itself. However, the custodian must join a self-regulatory organisation for anti-money laundering supervision.

It should be noted that a minimum amount of cryptoassets is sometimes required for staking (e.g. 32 ETH for Ethereum). This amount is often set at a high level to incentivise compliant behaviour by validators. Therefore the cryptoassets of various customers are often collected at a single staking address in order to reach this amount, particularly in the case of services for retail investors. Hence the offer of staking services often implies a collective custody of payment tokens, which requires a banking licence.

5 Glossary

Digital Assets Resolution Package (DARP)	Instruction to a liquidator informing them of responsibilities for and means of accessing assets in the event of the bankruptcy of a bank that holds cryptoassets in custody
Direct staking	Where an institution operates staking itself and therefore has power of disposal over the withdrawal keys
Individual custody	Segregated custody of cryptoassets at an individual blockchain address for each customer
Cryptoassets	Digital assets that are held on a blockchain and can only be accessed by means of a cryptographic procedure consisting of a public key and a private key
Lock-up/Exit period	Minimum duration of staking before the cryptoassets can be unblocked again, or the duration between the submission of the unstaking order and the actual return of the staked cryptoassets
Collective custody	Segregated custody of cryptoassets at a collective blockchain address
Slashing	Process by which the staked cryptoassets are usually partly or wholly burned due to misconduct by the validator
Staking (pool) operator	Where block validations are carried out with third party cryptoassets for the account of the third party. If the validator uses cryptoassets from various customers collectively, reference is made to a staking pool.
Staking chain	In a staking chain an institution delegates responsibility for staking to a third-party provider (e.g. other banks or staking pool operators), who takes control of the withdrawal keys
Technical service provider	Responsible for the technical setup of hardware and software components in order to operate the block production. The service provider only has a relationship with the validator, not the staking customers.
Validator node operator	Direct operator of a validator node on the blockchain – either as a staking (pool) operator or a technical service provider

Withdrawal keys	Cryptographic keys to control the return of staked cryptoassets. Losing these keys will result in losing the staked cryptoassets
Payment tokens / Cryptocurrencies	Cryptoassets that can be used, or are intended by the issuer or organiser to be used, as a means of payment to buy goods or services and for the transfer of money or assets (see Art. 5*a* para. 1 BO and the ICO guidelines of 16 February 2018)