Paper on Staking Services on Proof-of-Stake Protocols

The following members of the CVA Regulatory Working Group have contributed to this paper:
Fabio Andreotti, Julien Binder, Dominik Hofmann, Katharina Lasota Heller, Dongliang Liang, Reto Luthiger, Christine McAteer, Timea Nagy, Alexander Smith, Joshua Taucher

The Swiss crypto industry is currently at a pivotal juncture regarding the regulatory treatment of crypto staking. This process enables crypto holders to support the operational functionality of blockchain networks and, in return for providing validation services with correct and system-compliant behavior, to receive a reward. Within this context, there is a central concern of CVA based on various feedback from the crypto industry about FINMA's proposition that entities offering staking services may require a banking license because staked assets shall not be deemed to be kept available for clients at all times in view of the slashing risk and the unstaking period.

The primary aim of this paper from the CVA on behalf of the crypto industry is to demonstrate, by looking at the technological design of staking structures and networks as well as further potential specific technical measures, that many custodial staking services are not in scope of the Banking Act and therefore do not need a banking license, and thus do not trigger the prohibitive capital adequacy requirements. The main argument hinges on the fact that, in most staking agreements, the holders of staked crypto assets or their custodians maintain the direct power over their staked assets at all times; however, this depends strongly on the technological design of the specific staking service. This paper will show technological designs and technical measures that ensure this control, arguing against the need for a banking license for staking services for most staking arrangements.

1 About Staking

1.1 Staking as a Protocol

As an alternative to Proof-of-Work (PoW) networks that use mining to validate transactions, Proof-of-Stake (PoS) is a consensus mechanism in blockchain networks where participants lock up a certain amount of cryptocurrency as collateral to support the validation of transactions and the creation of new blocks based on the specific rules of the PoS protocol.[1] This ensures that all transactions are verified and secured without a central operator or intermediary.

In this paper, the following actors are of relevance:

- **Staker**: A person who participates in the blockchain consensus mechanism, including the *client* of a Non-Custodial or Custodial Staking Service Provider;
- **Self-Staker**: A person who stores the private keys and operates a validator node;
- **Validator**: A person who runs the infrastructure and software to conduct attestations or validations of blocks on the blockchain network;

[1] SWISS BLOCKCHAIN FEDERATION (SBF), Zirkular Staking 2023/1, 29 August 2023, p. 5 f. See also IRRESBERGER FELIX/KOSE JOHN/MUELLER PETER/SALEH FAHAD, The Public Blockchain Ecosystem: An Empirical Analysis, NYU Stern School of Business, 2021, p. 5.

- **(Non-Custodial) Staking Service Provider**: A person who operates a validator node on behalf of the Staker or has delegated the operation of a validator node to a Validator, but carries out the Staker's staking order;
- **Custodial Staking Service Provider**: A Staking Service Provider that securely stores the private keys for the Staker.

Depending on the rules of the protocol, the staked tokens may be locked during the staking, i.e. the tokens become immobilized. By participating in staking, users can *earn rewards* as a compensation for providing validation services in a protocol-compliant manner.

In case a Validator or a Staking Service Provider that operates validator nodes itself engages in malicious behavior or violates the network rules when providing validation services, they risk being penalized (*Slashing*)[2]. Such Slashing penalties[3] can result in the partial or – in extreme and very rare cases – complete loss of the staked amount, acting as a strong incentive against violating the protocol rules. In simple terms, staking in validation services is a key component of PoS, providing a way for participants to actively engage in the security and operation of the blockchain network while earning rewards for their contributed services in a protocol-compliant manner.[4]

Once a Staker decides to terminate the staking, the staked tokens can remain locked up for a certain amount of time as pre-defined by the rules of the protocol (*Unstaking Period*).

There are several types of staking mechanisms beyond the commonly known validation services in a PoS network. Each staking model has its own set of rules, requirements, and economic incentives. This paper only focuses on the staking for validation of transaction services and does not delve into the different types of PoS consensus mechanisms, such as delegated PoS, liquid PoS, Masternodes, Proof-of Burn, NFT staking, etc. Under these circumstances, it remains crucial to underline a key difference between staking as validation service and staking in the context of, e.g., pure lock-up without validation services, crypto lending or NFT staking.[5] The purpose of the latter type of staking is to incentivize users to purely earn rewards and realize potential profits, whereas the rewards received under the former type is compensation for the operational validation services provided in a protocol-compliant manner.

1.2 Staking as a Service

Depending on how Stakers choose to participate in staking, one can differentiate between three main approaches, namely: Self-staking, non-custodial staking, and custodial staking.

Self-staking refers to the ability of a Staker to independently participate in the staking process of the protocol (having own hardware and possessing the necessary know-how).

---

2 How does slashing in Ethereum actually work? To trigger the slashing procedure, it is necessary for other participants in the network to identify the validator in violation. This task falls upon another validator who acts as a "whistleblower." The whistleblower is required to generate and circulate a precise message detailing the infringement, which is subsequently included in a block by a proposer. The reward for this action by the proposer is intentionally modest, emphasizing that these efforts are intended to be altruistic rather than a pursuit of personal gain. Importantly, the whistleblower does not receive any reward for their contribution. (Source: https://www.blocknative.com/blog/an-ethereum-stakers-guide-to-slashing-other-penalties, visited on 22 Nov. 2023).

3 Slashing penalties in Ethereum can be: (1) exit the network during a 36-day epoch; (2) receive a penalty when the proposer adds the whistleblowing message to the block; (3) receive a penalty at each missed epoch; (4) receive a correlation penalty (Source: https://www.blocknative.com/blog/an-ethereum-stakers-guide-to-slashing-other-penalties, visited on 22 Nov. 2023). See also SWISS BLOCKCHAIN FEDERATION & BITCOIN SUISSE, FIND Staking Workshop, 8 Nov. 2023, Bern, p. 13.

4 BITCOIN SUISSE, What is staking?, 27 October 2020, https://www.bitcoinsuisse.com/de/fundamentals/was-ist- staking.

5 ZETZSCHE DIRK A./BUCKLEY ROSS B./ARNER DOUGLAS W./VAN EK MAURITS, Remaining regulatory challenges in digital finance and crypto assets after MiCA, ECON Committee, May 2023, p. 66 ff.

Similar to self-staking, *non-custodial staking* is also a method which does not involve a third-party custodian to manage and hold the private keys of the assets of the Staker while staking. In both scenarios, the Stakers maintain ownership of their private keys and have full control over their staked assets, with the one caveat that the Staker usually relies on the technical infrastructure of a third-party including validator nodes, i.e., a Non-Custodial Staking Service Provider and a Validator. Since Stakers manage their staking activities independently, they can reduce the risk associated with trusting third-party services. However, it would still not reduce the operational risk of Slashing or Unstaking Periods.

Regarding custodial staking, the Staker does not only use the infrastructure and node validating services of a third party, the *Custodial Staking Service Provider* and *Validator*, but also uses such a Custodial Staking Service Provider to securely store its private keys. Stakers opt for this solution mainly because they have neither the necessary know-how nor the hardware and software to operate the validator nodes. Moreover, to become a Validator, it may be required to commit an initial amount of tokens of the specific blockchain for staking. As example, the Ethereum blockchain requires a minimum of 32 ETH. Being a considerable amount, individual Stakers with insufficient capital turn to Staking Service Providers who have the capacity to link multiple Stakers together to enable participation in a network's consensus mechanism.

1.3 The View Expressed by FINMA

During the FinTech Roundtable on June 7, 2023, and the EIZ seminar on August 28, 2023, FINMA communicated their point of view regarding the regulatory qualification of staking (incl. staking for validation services). The main concerns of FINMA seem to relate to Slashing risk and (lengthy) Unstaking Periods which may question the requirement to "keep the assets available at all times" in accordance with the Federal Act on Debt Enforcement and Bankruptcy (DEBA) and the Banking Act (BankA).

According to our understanding, FINMA is likely to deem the criterion of "keeping the assets available at all times" fulfilled only if the crypto based assets can be promptly delivered to the client on demand. This paper challenges such approach.

As the Slashing risk and the Unstaking Period have already been widely discussed between the industry and FINMA, this paper will mainly focus on the aspect of "keeping the assets available at all times". However, for the sake of completeness, staked tokens are exposed to risks, irrespective of the chosen staking method. In the below table, we created an overview of the technical and operational risks that Stakers may face and accept when participating in staking protocols in general:

Risks	**Self-staking**	**Non-custodial staking**	**Custodial staking**
Security (hacking)	Yes	Yes	Yes
Third-party mismanagement	No	No	Yes
Technological risks (forks, updates, software bugs, server outages, etc.)	Yes	Yes	Yes, but can be contractually minimized
Loss of private keys	Yes	Yes	No (Staker) / Yes (Custodial Staking Service Provider)
Slashing and penalties	Depends on the blockchain protocol	Depends on the blockchain protocol	Depends on the blockchain protocol

Unstaking Period	Depends on the blockchain protocol	Depends on the blockchain protocol	Depends on the blockchain protocol

2 Technology: Private Key Management in the Staking Lifecycle

In this section, we briefly delve into the essential distinctions between staking and custody mechanisms by taking the Ethereum (ETH) and Cardano (ADA) blockchain ecosystems as examples. We explore how the control of assets is maintained throughout the staking lifecycle, with a particular focus on technical innovations that allow a Staker and a Staking Service Provider to maintain control over the Staking Principal (see definition below) throughout the staking lifecycle, in particular the potential technical measure of obtaining a *pre-signed exit message* from the Validator.

2.1 Control of Assets and Technical Solution

The complete staking lifecycle can be understood by examining the control of the private key for the staked ETH assets (Staking Principal) at any point in time. The Staker or the Custodial Staking Service Provider controls the private keys related to the Staking Principal. Whereas in many protocols the Staking Principal is locked up within the Staker's or the Custodial Staking Service Provider's wallet, in staking on the Ethereum network, the 32 ETH used as Staking Principal are deposited into the Ethereum network's staking smart contract, which is not owned by any single entity but operated by the collective network of computer resources on the Ethereum network. A withdrawal address is included in the deposit transaction data, which is the public key of an address under the control of the Staker or the Custodial Staking Service Provider, respectively. Once this withdrawal address is submitted with the deposit transaction data, it cannot be changed. The Staking Principal of 32 ETH and any rewards accrued by the consensus layer are returned to the withdrawal address on exit.

The four relevant addresses on Ethereum may be defined as follows:

Name	Description	Private key control
Principal staking address	This is the address that needs to sign the Staking deposit transaction.	Staker or Custodial Staking Service Provider on behalf of the Staker
Withdrawal address	Consensus layer rewards and Staking Principal are returned to this address. The withdrawal address cannot be changed once submitted to the network.	Staker or Custodial Staking Service Provider on behalf of the Staker
Fee recipient address	Execution layer priority fees are transferred to this address.	Staker or Custodial Staking Service Provider on behalf of the Staker
Validator node	The Validator is responsible for signing the exit message with his validator private key (also referred to as "signing key") to release the Staking Principal.	Validator private key: Validator

2.2 Validator Exit

On the Ethereum network, when the Staker or the Custodial Staking Service Provider wishes to withdraw the Staking Principal of 32 ETH (and any remaining excess balance), an exit message needs to be published to the network. This so-called "Voluntary Exit Message" (VEM) is generated by the validator node

and must be signed by the Validator with the validator private key, which is also referred to as “signing key”. It is usually the Staking Service Provider or the separate Validator that controls the validator private keys and thus becomes a controller of the exit message and therefore the exit of the Staking Principal (and any remaining excess balance). Regarding the Staking Principal, the Validator has at no time control over the Staking Principal itself, i.e., the Validator can in particular not dispose over the Staking Principal at will (unless the Validator could also change the withdrawal address, which is not possible if the Staker or Custodial Staking Service Provider has submitted the withdrawal address with the deposit transaction). However, the Validator has control over whether the exit from staking is being executed or not to the predetermined withdrawal address. This remaining control can be addressed technically: The Validator can give up the remaining control by *pre-signing* the VEM and transmitting it to the Staker or the Custodial Staking Service Provider. With such pre-signed VEM, the Staker or Custodial Staking Service Provider will be able to terminate the staking at any time without the involvement of the Validator.

Conclusion: In order to keep control over the Staking Principal at all times, including with respect to Validator exits, the termination of the staking by the Staker or the Custodial Staking Service Provider must be possible without the involvement of or the reliance on the Validator. As *one* of the possible technical solution in the Ethereum network to re-establish control over the staking exit process by the Staker or the Custodial Staking Service Provider, respectively, the Custodial Staking Service Provider or the separate Validator can, prior to staking, pre-sign and transmit the pertinent VEM to the Staker or the Custodial Staking Service Provider, respectively. This allows the Staker or the Custodial Staking Service Provider to remain in full control of their staked assets by being able to publish the VEM without any involvement of or reliance on the Validator at any time.

2.3 Variations in Staking: Cardano Blockchain

The mechanics of staking can differ significantly between different PoS protocols. *As an example:* Cardano’s approach to staking is defined as a delegation mechanism. Stakers of ADA can delegate their tokens to a stake pool of choice through a network transaction to the same address as their wallets, whilst stating their delegation. Delegated tokens never leave the Staker’s wallet, ensuring they maintain full custody while participating in the network’s consensus mechanism. Stakers of ADA can transfer their ADA even while on staking. However, in this case, the transferred ADA will be removed from the delegated staking pool, and the receiver may delegate them to the same or another staking pool again. Furthermore, the Cardano protocol does not have a Slashing or penalty mechanism. Incorrect validations and bad behaviors are limited to stake pools missing out on the respective rewards they would have received if they had conducted the validations correctly.

However, the short Unstaking Periods in Cardano also present inherent risks as they can cause swift and significant fluctuations in staking pools, potentially destabilizing the network during market downturns. Such instability might compromise network security and increase susceptibility to attacks. Furthermore, the lack of a Slashing and penalty mechanism reduces the network's capacity to deter malicious behavior, potentially impacting the security and integrity of staked assets.

3 Economic Aspects of Staking

3.1 General Considerations

In recent years, staking services have attracted the eyes of the crypto industry. To date, there is a market cap of $454B of stakable cryptocurrency[6], with Ethereum strongly keeping the lead.[7] The trend of staking is continuing to increase even taking on different forms such as liquid staking which basically addresses the issue of the unutilized locked up staking tokens.[8] Therefore, it is essential to discuss the economic aspect of staking itself. Relevant for financial regulators is to understand the prominent role of staking and its importance within both centralized and decentralized finance in order to avoid potential implications for systemic risk.

As we already established above that one of the main properties that distinguishes PoW from PoS is the consensus mechanism, it is also necessary to reiterate that Validators have to deposit a number of coins as stake, which is locked up for some time to incentivize the Validators to behave honestly since they stand to lose the locked value should they compromise the blockchain. Therefore, by design, staking provides the necessary security for public blockchains to have their utilities. As part of the staking "*ecosystem*", rewards, penalties, slashing as well as custody play an important role.

3.2 Rewards

Rewards play a crucial role in supporting the staking of assets on networks, reducing opportunity costs and operational expenses associated with Validator infrastructure. Staking large amounts of assets enhances the security of the network by discouraging malicious activities. The Ethereum network currently boasts over $67 billion worth of staked assets.[9]

Validators engage in attestation, performing validation activities that yield rewards. For a 32 ETH validator, attestation rewards typically range from 0.00001 to 0.00225 ETH per 24 hours. These rewards are added to the 32 ETH Staked Principal and held in the staking smart contract until exit.

Execution rewards, in the form of block proposal fees, are random and occur every two to three months on average. During periods of heavy network activity, these fees can be substantial, encompassing transaction priority fees. A noteworthy component of execution rewards is the whistleblower reward, incentivizing Validators to address and finalize bad behavior on the blockchain, amounting to around 0.06 ETH divided by 512 of the offender's balance.

The total reward in Ethereum, encompassing attestation and execution rewards, is extrapolated by service providers and currently amounts to 3.75% of the Staking Principal p.a. It is crucial to note that Annual Percentage Yields (APYs) are often used incorrectly in this context, as staking reward calculations do not compound, and only the initial 32 ETH Staking Principal is considered in the reward calculations. Therefore, it is better to apply Annual Percentage Rates (APRs) to reward calculations. Also, APR indications should

---

6 Cf. inter alia, https://www.stakingrewards.com/assets/proof-of-stake?sort=staking_marketcap&timeframe=7d&order=desc, page visited on 9 Dec. 2023.

7 Cf. https://www.stakingrewards.com/assets/proof-of-stake?sort=staking_marketcap&timeframe=7d&order=desc, page visited on 22 Nov. 2023.

8 SCHARNOWSKI STEFAN/JAHANSHAHLOO HOSSEIN, The economics of liquid staking derivatives: Basis determinants and price discovery, February 17, 2023, p. 5, available at https://ssrn.com/abstract=4180341.

9 Cf. inter alia, https://www.stakingrewards.com/assets/proof-of-stake?sort=staking_marketcap&timeframe=7d&order=desc, page visited on 8 Dec. 2023.

ideally take into consideration the specific token emission inflation in order not to overstate the APR in real terms.

3.3 Penalties and Slashing

The economic landscape of staking encompasses penalties and slashing mechanisms to deter malicious activities and protect the network's integrity. Penalties act as a deterrent for small mistakes, while slashing serves as a more severe consequence for significant offenses, whether intentional or not, emphasizing the importance of maintaining the system's security.

The amount of penalty is equal to the reward the Validator would have received if they conducted their assigned tasks correctly. This equates to about 5 USD per 24 hours[10]. These are slashable events and are punished by automatic reduction of the Staked Principal of the Validator at fault. Slashing is concerned with more significant mistakes and non-compliant behavior, such as when multiple Validators are used with the same validator key or a Validator signs blocks that contradict previous finalized blocks. Historically, most slashing occurred when Validators have built a redundant setup to prevent that Validators become offline and there was a misconfiguration within the setup.[11]

3.4 Economic Relationship between Staking, Custody, and Trading

In the industry, it is a necessity for Custody service providers to provide staking capabilities to reduce opportunity cost of the clients and be competitive in the global market. Only with assets under custody will trading activities be considered commercially viable and thus reduce triggering severe instability of the crypto industry in Switzerland, but not just. It is important to note that, without commercially viable staking, the majority of commercial value in cryptocurrency services will most likely migrate out of Switzerland.

Conclusion: The economic importance of staking in the cryptocurrency ecosystem extends across various dimensions. In essence, the economic importance of staking lies not only in its role as a security mechanism and essential part of the infrastructure for the PoS network but also as a fundamental driver for market competitiveness and regional commercial viability within the dynamic landscape of the cryptocurrency industry in Switzerland. Therefore, when analyzing the role of staking within the crypto ecosystem, a holistic view including its economics should be applied.

4 Civil Law Treatment of Custodial Staking Services

The following section analyses custodial staking services under civil law, focusing on the segregation of staked assets in Swiss bankruptcy procedures.

[10] Unless a larger penalty called inactivity leak applies when more than one third of all Validators are offline, a scenario very unlikely with over 800,000 Validators on the Ethereum network.

[11] An example event of Slashing occurred with a service provider on February 2, 2021: 75 validators were slashed due to a faulty technical setup to improve performance. At the time, there were 660,000 validators in total on the Ethereum network, the total amount slashed per validator was approximately 1.072 ETH. Another example of a rare case of Slashing was when a validator ran the same validator key in two instances. As a consequence, the validator was exited from the network.

4.1 Legal Qualification of Custodial Arrangements

Custody of crypto based assets for a client, due to lack of a depositable object, is qualified by legal doctrine as a mandate contract (art. 394 seq. CO) with strong deposit contract characteristics (art. 472 seq. CO). In case the crypto based assets under custody are staked, the contractual relation still qualifies as a mandate contract, blending custody and staking elements. Such a staking mandate supplements but does not replace the initial (deposit-like) custody mandate. In case the validator nodes are operated by the Custodial Staking Service Provider, the contractual relationship is extended to include work contract elements (art. 363 seq. CO). In summary, custodial staking setups form an innominate contract.[12]

4.2 Segregation of Staked Tokens in Swiss Bankruptcy Procedures

The question whether tokens that are being staked within a custodial staking agreement can be segregated (*ausgesondert*) according to art. 242a DEBA is – although being also decisive for the regulatory treatment of staking services – primarily a civil law question.

Art. 242a DEBA states the requirements for the segregation of crypto based assets (*kryptobasierte Vermögenswerte*) which may apply in the event of bankruptcy of a Custodial Staking Service Provider. These requirements are:

- The debtor having sole power of disposal over crypto based assets by the time of the bankruptcy declaration (*Konkurseröffnung*).
- The debtor undertakes to keep the crypto based assets available for the claiming third party, i.e. its client, at all times (*Verpflichtung die kryptobasierten Vermögenswerte für den Dritten jederzeit bereitzuhalten*).
- The debtor ensures that the crypto based assets either are individually allocated to the respective third party (on-chain segregation within individual wallets) or to a community and it is clear what share of the community assets the third party is entitled to (off-chain segregation of pooled assets).

The recent discussion regarding the regulatory treatment of custodial staking services also highlighted that there is not yet an established practice of the Swiss bankruptcy authorities (*Konkursämter*) and courts for how to apply art. 242a DEBA. The exact scope of this still rather novel provision therefore needs to be interpretated according to the established principles of Swiss law.[13]

a. Literal Interpretation

Art. 242a DEBA stipulates that the debtor undertakes (*sich verpflichten*) to keep the crypto based assets available for his client at all times (*jederzeit bereitzuhalten*). This implies that the control over the assets must be upheld at any time, but not that the assets can be transferred at any time (see also systematic interpretation). Therefore, Unstaking Periods have no influence on the segregation of crypto based assets in bankruptcy procedures.[14]

---

[12] Cf. ANDREOTTI FABIO/ZIMMERMANN STEPHAN/PRANTL FLORIAN, Custodial Staking, GesKR 2023, p. 333 ff., 338 f.; SBF, Zirkular 2023/1, section 3.3.

[13] Cf. BGE 145 III 324, E. 6.6.

[14] Cf. ANDREOTTI FABIO/ZIMMERMANN STEPHAN/PRANTL FLORIAN, Custodial Staking, GesKR 2023, p. 339; SBF, Zirkular 2023/1, section 4.2.1.

b. Historical Interpretation

The obligation to keep the crypto based assets available for the client at all times has been introduced to clarify that the debtor shall not conduct any active business (*Aktivgeschäft*) by using the assets of its clients in its own name and for its own account. Further, according to the message of the Federal Council regarding the introduction of the DLT Framework Act[15], also cold storage solutions would comply with the requirements of Art. 242a DEBA. Hence, constant access and control over the assets is the decisive factor, not their immediate transferability.

c. Teleological Interpretation

The main goal of including the obligation to keep the crypto based assets available for the client at all times was to avoid an increased risk of the custodian conducting an active business with the client's assets as well as to avoid the impression in the market that these assets actually belong to the debtor, which would – incorrectly – increase its creditworthiness. Based on a pure civil law perspective, in particular the latter element is decisive. Whether a custodian keeps the crypto based assets in wallets for its clients (which are not publicly identifiable as such) or whether the custodian stakes these assets, does not lead to a different perception of the solvency of the custodian as a debtor. Hence, a differentiation in this regard is not justified.

d. Systematic Interpretation

Art. 242a DEBA has been drafted on the basis of art. 242 DEBA which applies to physical objects. While art. 242 DEBA also requires the sole power of disposal (i.e. control) being with the debtor, it neither requires that such object can be returned immediately, nor does the segregability cease to exist if the object is damaged. Hence, the same should apply also to crypto based assets if an Unstaking Period exists or Slashing has occurred. Finally, it needs to be kept in mind that the control over the private keys of the wallet is decisive for the question whether crypto based assets fall into the bankruptcy estate of a custodian in the first place. Hence, the control over such private keys should be decisive for the question whether a crypto based asset is kept available for the client at all times.

The interpretation of art. 242a DEBA leads to the conclusion that crypto based assets, which are staked in a custodial staking setup are segregable, irrespective of the existence of an Unstaking Period and/or a potential Slashing risk, which are purely operational elements.[16]

4.3 Pre-signing as a Possible Technical Solution in Ethereum Custodial Staking

As described above in section 2.2 in connection with staking on the Ethereum network, the pre-signing of a VEM by the Validator with its validator private key offers a possible technical solution to ensure that a Custodial Staking Service Provider can meet the requirement to keep crypto based assets available for clients at all times. This approach involves the Custodial Staking Service Provider obtaining a pre-signed VEM from the Validator. The pre-signed message is an off-chain commitment, ensuring that the Custodial Staking Service Provider retains the ability to un-stake and access the Staked Principal at any time later on, without the need for further actions from the Validator.

[15] Cf. BBl 2020, p. 247.
[16] Cf. ANDREOTTI FABIO/ZIMMERMANN STEPHAN/PRANTL FLORIAN, Custodial Staking, GesKR 2023, p. 332 ff.

4.4 Conclusion

Conclusion: It was shown that crypto based assets locked up in a custodial staking setup are kept available for the client at all times and can be segregated in the event of bankruptcy of the Custodial Staking Service Provider. Furthermore, in the context of Ethereum custodial staking, a possible technical solution was proposed on how the client's position in the event of bankruptcy of the Custodial Staking Service Provider can be further improved by pre-signing and transmitting a VEM by the Validator and thereby ensuring the Custodial Staking Service Provider's control over the Staked Principal without the need for further actions from the Validator.

5 Financial Market Regulatory Treatment of Custodial Staking Services

The following section analyses custodial staking services under financial market regulations, focusing on the segregation of staked assets as deposit values (*Depotwerte*) in accordance with art. 16 (1bis) BankA.

As of August 2021, the term crypto based assets (*kryptobasierte Vermögenswerte*) was introduced by the DLT Framework Act. Such crypto based assets are assets that were issued with the primary intention to serve either as a payment instrument for the acquisition of goods and services or as an instrument for money or value transfer. As stated in the dispatch and in the explanatory report on the associated ordinances of the DLT Framework Act, crypto based assets are referred to in particular as payment tokens. Due to their compatibility with fiat money, the professional acceptance of payment tokens could trigger a banking or fintech license requirement (art. 1 (2) and art. 1b BankA), unless one of the exceptions in art. 5 (1) and (3) of the Banking Ordinance (BankO), art. 5a or art. 6 BankO (*sandbox regime*) applies.

With regard to the staking of crypto based assets, one must assess whether the staking of crypto based assets by use of a Custodial Staking Service Provider and, in some cases, a separate Validator would be considered a public deposit or could fall under the provisions of deposit values according to art. 16 (1bis) BankA. Deposit values are crypto based assets that are individually allocated and kept available at all times for the client.

Based on the latest developments, FINMA has challenged the "available at all times" requirement in staking structures and announced that Custodial Staking Service Providers therefore would require a banking license. In other words, staked assets would not qualify as deposit values but as public deposits. This would not only trigger a banking license for Custodial Staking Service Providers, but also prohibitive capital adequacy requirements for banks of today 800% and 1'250% upon the implementation of the Basel standards because such staked assets would have to be treated on-balance sheet. Further, such staked assets would not qualify as privileged public deposit in scope of the deposit insurance scheme in the event of bankruptcy of the Custodial Staking Service Provider according to the clear wording of art. 42a (1)(a)(1.) BankO.

Overall, based on FINMA's recent announcements, everyone would be worse off than with a segregation as deposit value: unregulated or AML-only supervised Custodial Staking Service Providers would require a banking license, banks would be subject to prohibitive capital adequacy requirements making custodial staking services unattractive or even factually impossible and the client would not be protected by the deposit insurance scheme in the event of bankruptcy of the Custodial Staking Service Provider.

In view of the above explanations in sections 2.2 and 4, the wordings and principles of art. 242a DEBA and art. 16 (1bis) BankA have explicitly been aligned by the legislator. Therefore, also from a regulatory

perspective, staking can, depending on the specific technological design of the different networks and specifically implemented technical measures, in principle, be operated by a Custodial Staking Service Provider and separate Validators (if any) without the need for a banking or fintech license and thus without affecting the segregation rights of the client. Generally, even during staking, the private keys are held by the Staker respectively the Custody Staking Service Provider who can always terminate the staking. In particular on the Ethereum network, where the Validator is required to sign the VEM and therefore exercise some control over the unstaking process, further technical measures can be implemented to avoid this: The pre-signing of the VEM by the Validator and transferring it to the Staker or Custody Staking Service Provider enables the Staker or Custody Staking Service Provider on behalf of the Staker to terminate the staking at any point of time without any involvement of the Validator. Therefore, it is possible based on the technological design of the specific network in combination with further technical measures to have full control over the assets at any moment of time with the Staker or the Custody Staking Service Provider, in which case neither a banking nor a fintech license is needed.

Conclusion: Based on the explanations in sections 2.2 and 4 above, which can also be applied from a financial market regulatory perspective in particular in view of the fully aligned wordings of art. 242a DEBA and art. 16 (1^{bis}) BankA, which was the intention of the legislator, we are also from a financial market regulatory perspective of the strong view that, based on the specific technological design of the different networks and specifically implemented technical measures, staking can, in principle, be operated by a Custodial Staking Service Provider and separate Validators (if any) without the need of a banking or fintech license and thus without affecting the segregation rights of the client.[17] The control over the private keys of the Staked Principal at all times is the decisive factor, which is already given in certain networks and which can sometimes be achieved by specific technical measures in other blockchains, such as pre-signing VEM on the Ethereum network by the Validator and transmitting such message to the Custodial Staking Service Provider prior to staking. However, this also means that, e.g., custodial staking on the Ethereum network might become subject to a banking license if the termination of staking cannot be triggered by the Custodial Staking Service Provider on behalf of the client without the involvement of the Validator (if separate).

[17] Cf. also SBF, Zirkular Staking 2023/1, p. 9; ANDREOTTI FABIO/ZIMMERMANN STEPHAN/PRANTL FLORIAN, Custodial Staking, GesKR 2023, p. 333, 338 ff.; SCHÄRLI KILLIAN/MEISSER LUZIUS/LUTHIGER RETO, Classification of staking of cryptocurrencies under Financial Market Law, Juspaper IT, 30 Sept. 2021, p. 11.