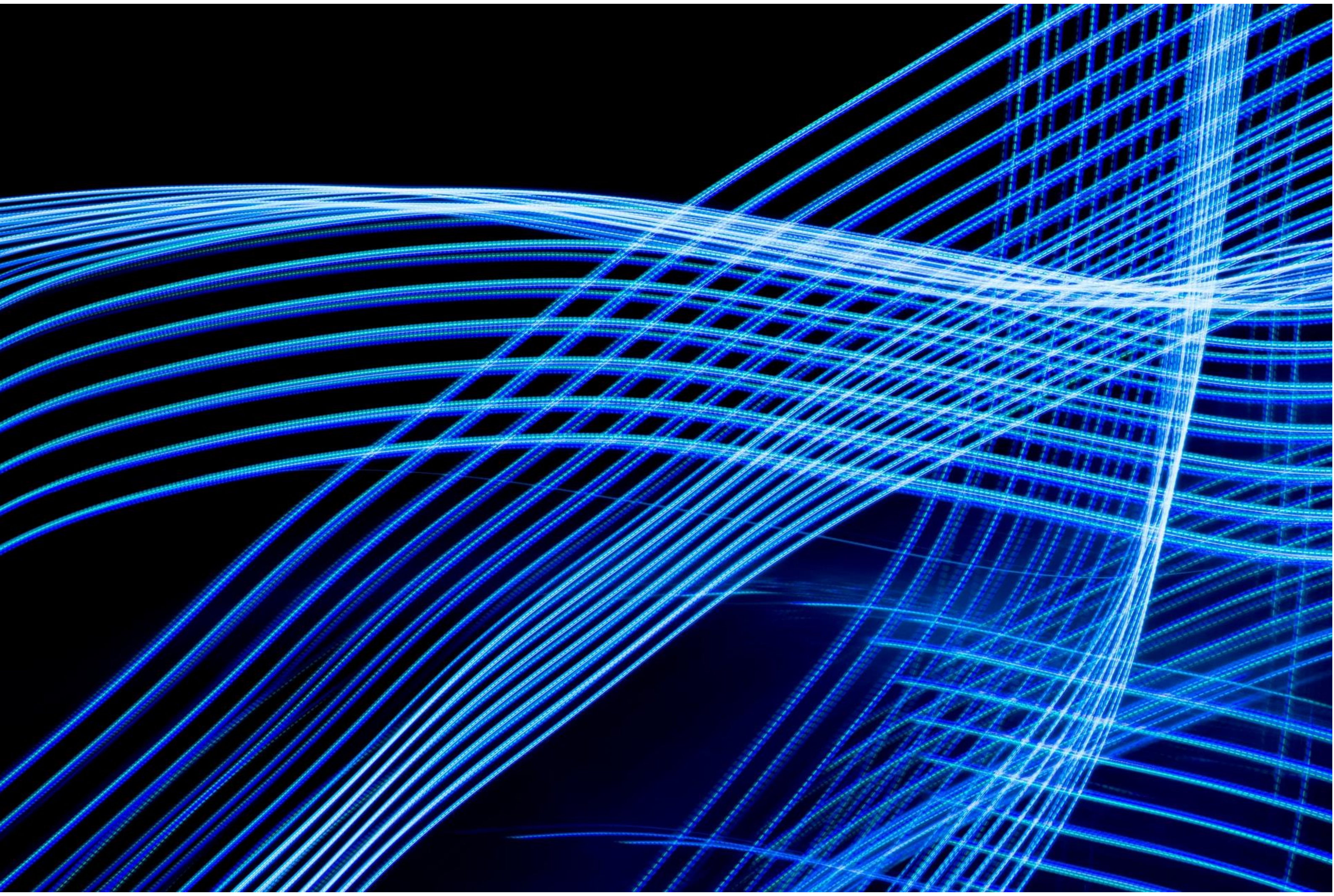

POS AND YIELD FARMING

A new revenue stream for Japanese crypto exchanges

06/08/2020

By So Saito & Joerg Schmidt

POS AND YIELD FARMING

With 24 registered crypto asset exchanges, the Japanese market has become increasingly competitive over the last few years. Constrained by regulations, Japanese exchanges have further only been able to list a fraction of the tokens traded elsewhere. At the same time, new restrictions on margin trading and additional license requirements for crypto derivatives have made it increasingly difficult to compete internationally.

The latest market developments, namely the shift from proof-of-work to proof-of-stake consensus mechanisms and the increasing popularity of yield farming, provide an excellent opportunity to exchanges, however, to add further services and to exploit additional revenue streams.

In this article, we analyze the regulatory environment for exchanges that want to use their customers' funds for staking and yield farming services, highlight potential pitfalls, and provide some legal considerations for implementing these services.

For more information on the regulatory environment for DeFi lending platforms, please visit our previous article.

> **Key Findings**
>
> **Registered exchanges can generally provide staking and yield farming services in Japan if they remain in control over the staked funds and do not transfer the economic risk resulting from the new services to their users.**

DEFINITIONS

Proof-of-Stake (PoS)

Blockchains depend on some form of consensus mechanism. The mechanism ensures that all nodes in the network agree on a single state and that the transaction history becomes immutable. The proof-of-work (**PoW**) consensus mechanism was the first successfully deployed. Given its high energy consumption and low transaction throughput, new consensus mechanisms have evolved. The most prominent is the proof-of-stake (**PoS**) consensus mechanism.

PoS generally uses a pseudo-random selection process to select a node as a validator. Selection criteria vary from platform to platform and include, among others, a node’s wealth, staking age, or other factors.

The validator of a block generally receives a block reward together with transaction fees paid by the users of a network. According to stakingrewards.com, the staking rewards for the bigger platforms are typically between 3-9 percent of the staked amount.[1]

While the Ethereum community has discussed the transition from a PoW to a PoS consensus mechanism for some time, other platforms have pressed ahead. Current forms range from pure PoS to different types of delegated PoS (**DPoS**). For the latter, a user does not directly participate in the validation of transactions but delegates this activity to others, the delegates.

Table 1: Overview of different consensus mechanisms using some form of PoS

	consensus mechanism		**funds controlled by user**	**direct distribution to user**	**penalties**
Ethereum 2.0	PoS		yes, but temporarily locked in a smart contract	yes	yes
tezos	liquid PoS	baking (PoS)	yes, but locked in a smart contract as a bond	yes	yes
		delegating (DPoS)	yes, different keys for transactions and staking	no	no

[1] *Staking Rewards,* Trusted Data. Stakeable Assets., retrieved from https://www.stakingrewards.com/proof-of-stake (accessed on 03/08/2020).

EOS	DPoS	yes, but temporarily locked in a smart contract	not necessarily any distribution to delegators	no
Algorand	pure PoS	yes	yes	no
LISK	DPoS	yes, but temporarily locked	no	only lock-up for an extended period

Yield Farming

Yield farming allows token holders to generate passive income from their crypto holdings as well. Instead of participating in staking, yield farming requires users to lock their funds into a lending protocol such as Compound or MakerDAO, which in turn allows others to borrow from the pooled funds at a certain interest rate.

Many of the lending protocols currently involve an additional type of token, which is used as an incentive for both lenders and borrowers. Together with these incentives, annual yields of up to 100 percent were possible until last month. More recently, the price of most governance tokens dropped, however, and brought the yield for lenders down to more realistic levels.

Currently, most DeFi lending activities focus on the Ethereum blockchain. Since Ethereum still uses the PoW, yield farming and staking do not compete directly. However, this will change with the roll-out of Ethereum 2.0 over the next five to ten years.

LEGAL CONSIDERATIONS

Registered exchanges in Japan can engage in the exchange of crypto assets and the management of their users' funds – all, of course, within the boundaries set by the Payment Services Act (**PSA**) and subsidiary legislation.

Crypto Asset Exchange Services

The definition of crypto asset exchange services in the PSA does not only lay out the services subject to registration. It also determines the scope of regulated services a registered exchange may provide.

According to Section 2(5) PSA, the following services are considered crypto asset exchange services:

(1) the purchase and sale of crypto assets or exchange of crypto assets
(2) intermediary, brokerage, or agency services for the purchase, sale, and exchange of crypto assets
(3) the management of a user's funds in relation to the purchase, sale, and exchange of crypto assets
(4) the management of crypto assets on behalf of another person

Since all exchanges in Japan are centralized exchanges, they provide exchange and custody services.[2] Accordingly, they must also follow the rules for crypto custodians when providing staking or yield farming services.

Custody Services

Under the new regulations, exchanges are generally required to hold 95 percent of their users' funds in a cold wallet or secure them by means which provide a similar level of security. The remaining 5 percent can be stored in a hot wallet but must be fully backed by an exchange's own funds.

It should be noted that in both cases, the exchange remains in full control over its users' funds. A user is, therefore, generally able to withdraw his funds at any time. This even applies in cases similar to a bank run and must be borne in mind when preparing the terms and conditions for yield farming and staking services.

POS UNDER THE PSA

As shown above, PoS mechanisms come in different shapes and sizes. It is, therefore, necessary to analyze the design carefully when assessing the admissibility of staking services.

As much as the admissibility depends on the design of the respective consensus mechanism, it depends on the contractual arrangements in

[2] Unlike decentralized exchanges, centralized exchanges require users to transfer their funds to an address controlled by the exchange. The user does not have any control over the funds until he instructs the exchange to transfer the funds to an address specified by him.

place. Both components and their interaction with each other must, therefore, be analyzed comprehensively. This applies in particular because the right contractual arrangements may neutralize some of the negative effects resulting from design choices.

Control Over Funds

The first thing to consider is who controls the staked funds. If it is the user, which is highly unlikely if not impossible in case of centralized exchanges, there are no concerns. The same is true if the funds are controlled and remain under the control of the exchange after being used for staking.

PoS

In most PoS models, a user must lock his tokens in a smart contract for staking. While the tokens are temporarily locked in the smart contract, i.e. the time they are used for staking and in some cases an additional period, they can generally be unlocked at any time.

The only one who can unlock the funds from the smart contract is the person controlling the private key corresponding to the address that was initially used to lock the funds in the smart contract. Except for slashing staked funds in case of misbehavior or excessive downtimes, the smart contract does not control the staked amount. In particular, it is not able to transfer the funds independently.

Since the funds remain under the control of an exchange, the situation is not different from any other situation where the funds are associated with an address controlled by an exchange.

DPoS

In the case of DPoS, the situation is generally not different from the situation described above. An exchange using funds for delegation services does not lose control over the funds at any time. This applies even if the funds are locked in a smart contract for delegation.

In some cases, namely the liquid PoS by tezos, the exchange must not even send a users’ funds to a smart contract. Instead, there are two keys – one for controlling the funds and another one for delegation. Unlike in other PoS models, it is therefore not even necessary to send the funds to a smart contract and withdraw them when a user wants to withdraw his funds from the exchange.

Hot Wallet VS Cold Wallet

Since the smart contracts used for staking do generally not control the locked funds, the situation is comparable to the situation where the funds are associated with an address controlled by the exchange. In both cases, the funds can only be transferred by the person controlling the private keys. If these keys are stored offline, the level of security is generally the same for funds locked in the smart contract and funds associated with an ordinary address. That being said, there is no reason to treat the two situations differently.

Liquidity Constraints

Most PoS consensus mechanisms require the user to lock funds into a smart contract. Even if the funds are unlocked, the holder of the private key may not receive the funds directly. An exchange staking its users' funds may, therefore, not be able to respond to a withdrawal request immediately.

An exchange may either counter the delay by using its own funds or provide in its terms and conditions that there may be delays if a user also wants to use the exchange’s staking services. The terms may further lay out different periods for different protocols or simply use the longest period as a standard.

Economic Risks (Slashing)

Some PoS consensus mechanisms provide for slashing in case of misbehavior, excessive downtimes, or other violations of the protocol's rules. In other words, the person violating the rules loses a certain amount of staked funds.

Where the economic risks and benefits are borne by the user, staking is more akin to investments than to deposits. Investment activities are, however, regulated under the Financial Instruments and Exchange Act (**FIEA**) and require a different license. A crypto asset exchange license is not sufficient.

Crypto asset exchanges that do not have the necessary licenses must, therefore, implement measures to prevent users from bearing the economic risk of staking. One way to do so is by reconciling losses with the exchange’s own funds.

Legal Considerations – Yield Farming

The legal considerations are generally the same for PoS and yield farming. In short, an exchange may not carry out activities where the users run the risk of making a loss.

Compared to staking, there is one fundamental difference, however. An exchange will lose control over the lent amount. The control over the asset is transferred to the lending protocol, which in turn lends the funds to other users.

In exchange for supplying the funds to the protocol, an exchange does, however, receive another token which represents an increasing share in the protocol’s funds. By transferring these tokens to the protocol, an exchange can generally redeem the locked funds from a lending protocol at any time. This applies at least if there is sufficient liquidity. In the case of illiquidity, an exchange may have to wait for a certain amount of time until the redemption may be completed. An exchange may bridge this time either by using its own funds or putting a contract in place that allows it to wait with the refund until there is sufficient liquidity on the respective market.

The private keys controlling the tokens issued by the protocol can be stored in a cold or hot wallet like any other key in possession of the exchange. Insofar, nothing different applies.

Conclusion

The PSA does not generally prohibit yield farming or staking services. This applies at least if the economic risks of staking or yield farming are not transferred to the user. It is also necessary to take a closer look at the respective PoS mechanism and adjust, where appropriate, the contractual documentation.

We expect that PoS and yield farming will gain more traction on the Japanese market in the next few months. If you want to discuss the technical and legal implementation of PoS and staking services with us, please feel free to contact us at any time.

CONTACT

So Saito[3]
Partner
s.saito@innovationlaw.jp

Joerg Schmidt[4]
Foreign Associate
j.schmidt@innovationlaw.jp

DISCLAIMER

The DeFi protocols and blockchain projects mentioned in this article are used for illustrative purposes only. Given the format of the article, not all details of the protocol or consensus mechanism have been considered comprehensively, so that the results of the assessment may deviate from the results by the regulator or a legal opinion prepared for the respective project. By no means, the explanations should be understood as a legal opinion regarding DeFi protocols and PoS consensus mechanisms mentioned in this article.

[3] Admitted in Japan and New York.

[4] Admitted in Germany (not registered in Japan).