SO & SATO
INNOVATIVE LAWYERS

28 August 2019
So Saito
Joerg Schmidt

CRYPTOCURRENCY EXCHANGE REGULATIONS IN JAPAN

Hot wallets, non-custodian exchanges and smart solutions

Cryptocurrency regulation in Japan is closely linked to the hack of the Japanese cryptocurrency exchange Mt. Gox in 2014 and Coincheck in 2018. As such, it is no surprise that the latest revision of the Payment Services Act (PSA) introduces detailed regulations on the safekeeping of crypto assets stored in hot wallets.

The impact of the new regulations depends on the exact business model of the cryptocurrency exchange. Before diving into the regulatory changes, their impact on the industry and potential solutions, we will therefore analyze the different business models in more detail.

1. Business models

Broadly speaking, cryptocurrency exchanges are centralized or decentralized. At present, all registered exchanges in Japan are centralized exchanges.

1.1. Centralized exchanges

An estimated 99 percent of trading volume occurs on centralized exchanges.[1] Centralized exchanges require users to transfer funds to an address controlled by the exchange. Until a user withdraws his funds from the exchange, he does not control the funds even though they are shown on his account.

Centralized exchanges host their own order books. Orders are matched and executed off-chain via proprietary matching and settlement systems.

1.2. Decentralized exchanges

Decentralized exchanges (DEX) allow users to trade crypto assets while remaining in full control over their funds throughout the transaction. Depending on the degree of decentralization DEX may further deploy on-chain order books and require users to manually identify and fill orders. To improve user experience and to overcome technological limitations related to full decentralization (e.g. latency of most public blockchains) most DEX use hybrid models. Typically, these models combine off-chain order books – and in some cases order matching – with on-chain settlement.

For the matching – in case of automatic order matching – and settlement users are required to transfer funds to a smart contract deployed by the DEX. The funds will only be used when orders are matched. Until then a user remains in full control and can withdraw his funds any

[1] *CircleResearch,* Decentralized Exchanges (DEX), retrieved from http://research.circle.com/wp-content/uploads/2019/02/circle-research-decentralized-exchanges.pdf (accessed 19 July 2019).

time. At no point a DEX has control over the funds sent to the smart contract.[2]

While the architecture of DEX may vary considerably, DEX typically enable users to transact crypto assets without losing control over their funds.

2. Cryptocurrency exchange regulations

Japanese crypto regulations do not distinguish between centralized and decentralized models. Of legal relevance are only the actual activities, but not how they are structured.

Crypto exchange services under the Payment Services Act (PSA) include

i. the purchase and sale of crypto assets (i.e. exchange between crypto assets and fiat currency) or the exchange with another crypto asset; and
ii. intermediary, brokerage or agency services for acts described under item (i).

Custody services are currently not regulated under the PSA. This will change under the new regulations which will enter into force early 2020. While the definition of custody services is somewhat unclear, we understand that only businesses managing their customers' funds or controlling their customers' private keys will be covered.

3. New requirements

Under the PSA both cryptocurrency exchanges and custodians must register with the Financial Services Agency (FSA).

In addition to the existing requirements the following additional compliance and reporting requirements will be introduced for registered exchanges:

- to establish and publish an incident report policy concerning the theft of crypto assets
- to hold crypto assets that are not less than the value of the customers' crypto assets in hot wallets (if any) as the exchange's own assets
- to put customers' fiat into a trust
- to disclose financial statements publicly
- to publish OTC deals with customers (if any) as well as bid prices, ask prices, and bid-ask spreads for such OTC deals
- to refrain from making excessive advertisement, misrepresentations, cold calls, inadequate solicitations considering the customer's knowledge, or advertisement and solicitations to induce speculative trading
- to notify the FSA of the intention to list new crypto assets for trading prior to such change taking place in order to exclude problematic crypto assets form listing

3.1. Exchanges

For exchanges that provide custody services, one must distinguish between funds stored in

[2] As can be seen from other decentralized apps (DApps) owners of DApps often exercise a certain degree of control over their smart contracts (e.g. pause of transfer, upgrade capabilities). For DEX, this type of control might directly translate into being subject to additional compliance requirements under the PSA and should therefore be analyzed carefully.

a hot wallet und such being stored in a cold wallet.

3.1.1. Hot wallet

Exchanges that hold parts of their customers' funds in a hot wallet are required to hold the same amount of crypto assets as their own assets. By way of example, an exchange holding BTC 5 of its customers' funds in a hot wallet must have BTC 5 as its own assets in a cold wallet. Maintaining an insurance policy that covers the crypto assets in the hot wallet is not sufficient under Japanese regulations.

Since the terms *hot wallet* and *cold wallet* are not defined in the PSA, we expect that subsidiary regulations and guidelines of the Japan Virtual Currency Exchange Association (JVCEA) – a self-regulatory body recognized under the PSA – will discuss the terms in more detail. It can be assumed, that the term *cold wallet* is interpreted in line with the general understanding that cold wallets are not connected to the Internet. Wallets that do not fall under this or a similar definition are likely to be considered *hot wallets.*

DEX are generally not affected by the new regulations, as they do not manage their users' funds.[3] Instead, users remain in full control of their funds at all times. This also applies to funds which were transferred to smart contracts deployed by DEX for the execution of orders. Unlike funds in a hot wallet, these funds cannot be accessed or transferred by the DEX deploying the smart contract. Users, however, can withdraw their funds at any time. The fact that the use of smart contracts introduces new risks, including the risk of total loss due to the exploitation of bugs, does not lead to a different assessment. While the result of vulnerabilities, i.e the total loss of funds, is the same, the risks are fundamentally different from the risks stemming from the use of hot wallets. As such it is highly unlikely that smart contracts will be deemed hot wallets. Slight changes to the design of the smart contract may lead to different results however and should therefore be considered carefully.

3.1.2. Cold wallet

The new regulations require exchanges to hold most customers' assets in a cold wallet. To ensure that all funds are readily available if an exchange fails, the funds stored in a cold wallet must be managed separately from the exchange's own crypto assets.

Smart contracts deployed by DEX will most likely not be considered cold wallets. In fact, they are unlikely to be classified as wallets for regulatory purposes at all, unless they allow an exchange to access and control the funds stored in the contract address.

3.1.3. Fiat currencies

Unlike bank deposits, funds deposited at exchanges are not protected. To ensure similar results, exchanges in Japan are required to put fiat currencies of their customers in a trust.

Until today, all exchanges in Japan are centralized exchanges. To the best of our knowledge

[3] Something different might only apply if DEX exercise control over the smart contract to which the funds are sent. Depending on the circumstances of the individual case, a smart contract might then be considered a hot wallet.

none of the DEX globally, provides a fiat gateway so far, so that applicants would not be affected by the new regulations.

3.2. Custodian Wallets

Other service providers such as custodian wallets that manage customers' funds are also affected by the new regulations. This applies in particular with regard to funds stored in hot wallets. Where wallet service providers do not control their customers' funds or private keys, it can be assumed that these providers are not subject to additional requirements.

4. Alternative structures

From our point of view, the most onerous burden for exchanges and custodians is most likely the one related to funds stored in a hot wallet. DEX provide clear advantages in that respect, but face challenges in other areas (e.g. scalability).

So, what are the alternatives for centralized exchanges? Shifting to a decentralized business model? Unlikely given the tradeoffs. Sacrificing customer experience for security and storing all funds in a cold wallet? Possible. Multisig or other solutions?

4.1. Multisig

While Multisig obviously provides enhanced security, it does not render a hot wallet a cold wallet. Something different might apply however, where the majority of keys is stored offline. It is our understanding that for a 2-of-3 Multisig at least two keys must be stored offline to be classified as a cold wallet. Except from enhancing security by eliminating unauthorized transactions through the misuse of a single key, Multisig does therefore not provide advantages over pure cold wallet solutions. In fact, it might even deteriorate customer experience by slowing down the transfer of funds in case a customer wishes to cash out.

4.2. Multiparty computation

Depending on the exact definition of hot wallets and cold wallets, multiparty computation (MPC) might provide a solution to the hot wallet problem. MPC ensures that the private key controlling the funds never exists in complete form in a single place. Instead, anyone participating in the MPC holds a fraction of the key which is constantly refreshed. If the promise that private keys never exist in complete form holds true, MPC might not even be considered a wallet. This would however only apply if the future definition of a wallet exclusively draws on the existence of a private key. It is much more likely that the subsidiary regulations and guidelines of the JVCEA ultimately draw on the control of funds. Where an exchange is effectively able to authorize transactions – irrespective of whether the keys exist in complete form or only as key shares – the provisions concerning custody services are triggered.

If the key shares are stored on devices permanently connected to the internet, it is likely that an MPC solution is considered a hot wallet. Where some of the key shares required for

authorizing a transaction are stored on devices permanently disconnected from the internet an MPC solution is likely to be considered a cold wallet solution. Insofar reference is made to the explanations in respect to the Multisig solution in the previous paragraph.

In summary, MPC offers a smart and much-needed solution for cryptocurrency exchanges to increase both customer experience and security. Yet, it is unlikely be considered a cold wallet solution by design.

5. Conclusion

With the new regulations entering into force in April 2020, investors will see higher levels of protection in Japan. The improvements will most likely come at a price – higher compliance costs for exchanges or a deterioration of customer experience.

In an increasingly competitive environment smart solutions are much needed and likely to make a difference. MPC could be one of them. While much is still unclear, providers of MPC should therefore carefully assess how their solutions fit into the new regulatory environment. After all Japan is still one of the biggest markets for crypto assets worldwide.

We are going to update you, once the subsidiary legislation and guidelines from the JVCEA are published.

Follow us on LinkedIn to stay up to date.

CONTACT

So Saito[4] (Partner)
s.saito@innovationlaw.jp

Joerg Schmidt[5] (Foreign Associate)
j.schmidt@innovationlaw.jp

DISCLAIMER

[4] Admitted in Japan and New York.

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