Risks, Safeguards, and Regulation in a Changing Cryptoasset Landscape

Ken Katayama

10 October 2025

Iakyara vol.405

Nomura Research Institute, Ltd.

Executive Summary

With cryptoassets gaining recognition as an investment vehicle, Japanese regulatory authorities are discussing reclassifying them as a subclass of financial products. Retail investors count on crypto exchanges to protect them against cryptoassets' risks but it is advisable to devise risk mitigation measures in anticipation of growing use of noncustodial wallets.

Ken Katayama
Senior Chief Researcher
Financial Market & Innovation Research Department

Changes in regulatory landscape in wake of growing cryptoasset ownership

Cryptoasset ownership is growing in Japan. Japan's Financial Services Agency (FSA) reported[1] that cryptoasset exchanges in Japan collectively had 12mn customer accounts[2] and over ¥5trn of customer assets under custody as of January 31, 2025. Meanwhile, in March 2025, SBI VC Trade registered with the FSA as a trading venue for the US dollar-pegged stablecoin USDC[3] pursuant to the recently amended Payment Services Act. In August, JPYC Inc. registered as a money transmitter authorized to issue a yen-pegged stable coin.

Outside of Japan, the US has recently turned decidedly pro-crypto, with the new Trump Administration voicing support for various cryptoasset initiatives. Most notably, the US Securities and Exchange Commission (SEC) has abandoned a raft of crypto-related litigation and Congress passed the GENIUS (Guiding and Establishing National Innovation for US Stablecoins) Act, which was signed into law by President Trump on July 18. Congress is now deliberating on a proposed Digital Market Access Clarity Act that would clarify the SEC and Commodity Futures Trading Commission's respective regulatory authority over various digital financial instruments. After previously lagging behind Europe and Japan in terms of regulating cryptoassets with federal legislation, the US now appears intent on catching up posthaste.

In Japan, discussions of cryptoasset regulatory reforms were underway prior to the US's pro-crypto policy shift. Cryptoassets in Japan have long been regulated under the Payment Services Act, but growing recognition of cryptoassets as a mass-market investment vehicle has prompted Japanese regulatory authorities to address a number of urgent issues, including (1) augmenting information

NOTE

1) FSA, *Discussion Paper: Examination of the Regulatory Systems Related to Cryptoassets* (April 2025).
2) Including both individual and corporate accounts, where accounts owned by single party at multiple exchanges are each counted separately (see footnote 9 in above-referenced FSA discussion paper).
3) USDC is treated as a foreign electronic payment instrument in Japan.

disclosure, (2) dealing with unregistered dealers/exchanges, (3) dealing with misconduct by investment fiduciaries and (4) ensuring fair pricing and fair trading[4].

4) Per above-referenced FSA discussion paper.

Risks inherent in cryptoasset dealings

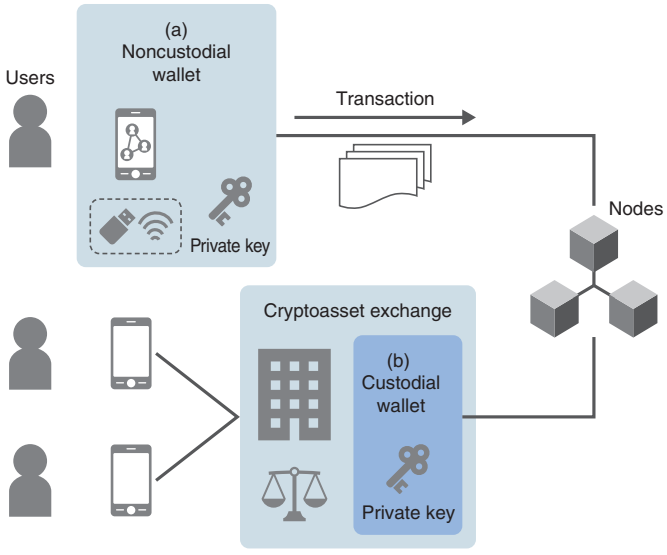
The following provides an overview of the basic mechanics of digital asset transactions, using Bitcoin as an example. To transfer Bitcoin, the sender composes a message specifying her blockchain address[5], the recipient's blockchain address and the quantity of Bitcoin to be transferred[6]. The sender signs the message (transaction) with her private key and sends it to the Bitcoin network, where it is validated by nodes of the network[7].

5) Addresses are lengthy alphanumeric strings.
6) Antonopoulos, Andreas M., *Mastering Bitcoin* (2016).
7) Once a sender's transaction has been validated (added to a block), other blocks are subsequently appended to the blockchain, reducing the likelihood of the transaction being reversed (making the transaction more certain).

In Bitcoin's early days following its invention in 2009, Bitcoin owners built or installed wallets on their computers to store their blockchain addresses and private keys. Such wallets are called noncustodial wallets ((a) in accompanying graphic) to distinguish them from custodial wallets hosted by a third-party custodian.

However, wallets are often difficult to use and differ considerably from one model to another. Setting one up requires significant technical skill. Additionally, wallet use poses several risks, most notably safekeeping risk, privacy risk and immaturity risk. Safekeeping risk is cryptoassets' vulnerability to theft. A blockchain can be likened to a traditional bank's core ledger exposed to the public. Cryptoassets are prone to disappear if their owner's private key is compromised. Privacy risk

Custodial vs. noncustodial wallets



Source: NRI, based on various information

stems from reporting of blockchain transactions to network nodes. Disclosure of transactions to nodes increases the risk of leaks of personal information or trade secrets and of crimes such as robbery, kidnapping and blackmail if a malicious third-party[8] is able to associate a wallet's address with the identity of the wallet owner[9]. Immaturity risk reflects the fact that blockchain technology and cryptoasset ecosystems are less than two decades old and remain in an experimental stage. Questions remain about issues such as concentration of influence and systemic resilience. Unproven technology may lead to problems like delayed or chronologically disordered transaction validation.

Most retail cryptoasset owners have been counting on exchanges to safeguard against these risks. As protection against safekeeping risk, customer assets under custody are segregated from the exchange's own assets in a custodial wallet ((b) in the graphic) and the customer uses the custodial wallet's private key to sign off on the transactions required to fully execute the customer's orders. Additionally, Japanese exchanges have so far reimbursed customers for all losses incurred as a result of domestic cybersecurity breaches.

In terms of privacy risk, as long as the customer places her order within her account at an exchange, neither the order's terms nor the customer's account balances are observable to outsiders. When cryptoassets are transferred to an account at another exchange, the transfer is aggregated with other transfers and batch-processed in accounts titled in the exchanges' names. Information specific to the involved customers would generally not be observable in such cases[10].

To mitigate immaturity risk, Japan subjects exchanges' applications to list a new cryptoasset to a more rigorous review process than other countries do[11]. How to classify different blockchains and assess their maturity is a topic of ongoing discussion in Japan as well as globally.

Growth in noncustodial wallet usage and user protections

Based on the above, some may conclude that there is not much need to worry about cryptoassets' risks anymore but I disagree for a couple reasons. First, ongoing institutional and regulatory reforms may lead to further growth in cryptoasset ownership. Second, if wallets become more user-friendly, noncustodial wallet usage may expand, potentially resulting in increased transaction traffic to nodes, including from use of Web3 services, as cryptoasset owners transfer

8) Technologies that enhance transaction privacy are being developed but ensuring transparency from the standpoint of law enforcement is an issue. A partial-disclosure approach has been proposed. There have been incidents of serious harm, albeit not directly related to a transaction. In France, the CEO of a wallet technology company was kidnapped for ransom.

9) The named individual or entity or the ultimate beneficiary.

10) However, transfers from an exchange's account to a someone's noncustodial wallet and vice-versa are observable as individual transactions.

11) Additionally, providers of new yield-generating services (e.g., staking) are also required to explain the various risks involved.

assets from exchanges to their own wallets[12].

Wallet user authentication will be simplified by integration of services into IT platforms. The hassle of correctly inputting the sender and recipient's long addresses (alphanumeric strings) is already being alleviated by use of QR codes. The aforementioned JPYC Inc. has adopted a service model that bypasses exchanges by issuing stable coins directly into purchasers' wallets.

If the changes outlined above accelerate a shift from a system in which exchanges protect cryptoasset owners to one in which owners bear full responsibility themselves, it will be essential to prepare for that reality. This includes identifying the risks inherent in cryptoasset transactions, determining how best to mitigate them, calling attention to ordinary users and clarifying which parties are best positioned to take on these roles.

12) Transactions such as secured loans and exchanges of one cryptoasset for different one require trading technology and a high degree of financial knowledge.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.1 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including Tokyo, New York, London, Beijing and Sydney, with over 16,700 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Innovation Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/list.html#lakyara