Cryptocurrencies entrusted to an exchange provider: Shielded from the provider's bankruptcy?

KOJI TAKAHASHI*

Abstract

Cryptocurrency exchanges, *ie* online platforms where customers exchange their cryptocurrencies for other cryptocurrencies or fiat currencies, are routinely targeted by hackers, which often result in a massive drain of cryptocurrencies. The heists can be large enough to bring down the exchanges to their knees. The customers of an exchange who have entrusted it with cryptocurrencies would have a contractual right to claim their return. If the exchange is wound up, however, personal claims (such as a contractual claim) brought in bankruptcy proceedings would not yield to them a full recovery. It is, therefore, practically important to examine whether the cryptocurrencies entrusted to an exchange are shielded from the bankruptcy of the exchange provider, so that the customers can obtain a full recovery. Under most, if not all, legal systems, the answer to this question would be unclear because cryptocurrencies are a novel asset and because the legal relationships between an exchange provider and its customers have not been sufficiently scrutinised. This article will seek to improve legal clarity by presenting an analytical framework, identifying issues, and pointing to possible solutions.

It will begin by examining the law of Japan, possibly the only country in the world where the matter has been litigated. Following a hacking attack, Mt Gox, the world's biggest operator of a Bitcoin exchange at that time, became insolvent. After the opening of bankruptcy proceedings, one of its former customers filed a suit against the bankruptcy trustee in Japan, seeking a full recovery of the Bitcoins he had entrusted to the exchange. Rather than relying on a personal claim, the plaintiff asserted ownership over what he saw as "his Bitcoins". His claim was, however, dismissed by the Tokyo District Court for reasons to be examined in this article. More recently, other customers filed a suit in Japan by trying another legal avenue to obtain a full recovery. They are arguing that their Bitcoins had been held by the exchange on trust for them.

After presenting an analysis under Japanese law, this article will explore its relevance to other legal systems. Since Japanese law belongs to the family of civil law systems, the analysis concerning the ownership of cryptocurrencies would have direct relevance to other civil law systems in the context of *rei vindicatio* (vindication of property). It would also inform the debate whether cryptocurrencies are "property" in terms of the tort of conversion in common law systems. The analysis concerning whether an exchange holds cryptocurrencies on trust for its customers would be useful to all the common law systems of which the law of trusts forms an integral part as well as any civil law systems which, like Japanese law, have introduced the concept of trusts.

* * * * *

* Professor at the Doshisha University Law School (Kyoto, Japan).

1 Introduction

Cryptocurrency exchanges, *ie* online platforms where customers exchange their cryptocurrencies[1] for other cryptocurrencies or fiat currencies, are routinely targeted by hackers, which often result in a massive drain of cryptocurrencies. The exchanges which came under biggest hacking attacks include Mt Gox (losing Bitcoins[2] worth $473 million in 2014), Bitfinex (losing Bitcoins worth $72 million in 2016), Coincheck (losing Nems worth $523 million in 2018) and BitGrail (losing Nanos worth $170 million in 2018). The heists can be large enough to bring down the exchanges to their knees.

The customers of a cryptocurrency exchange usually entrust their cryptocurrencies to the exchange provider[3] prior to placing an order, so that their order can be swiftly executed. After the execution of transactions, the cryptocurrencies remain entrusted to the provider until such time that customers who have a positive balance on the provider's books request transfers. If, in the meantime, the exchange provider goes into bankruptcy, the customers would have a contractual right to claim the return of the cryptocurrencies they have entrusted. But a contractual claim would only allow recovery *pari passu* ("in equal steps") from the bankrupt's estate. The customers may wish to claim a full recovery as they often see such cryptocurrencies as their own. The merit of their claim will depend on the question whether the cryptocurrencies entrusted to an exchange provider are shielded from the latter's bankruptcy.

Under most, if not all, legal systems, the answer to this question would be unclear because cryptocurrencies are a novel asset and because the legal relationships between an exchange provider and its customers have not been sufficiently scrutinised. This article will consider this question under the law of Japan, perhaps the only country in the world where the matter has been litigated. Two legal weapons likely to be deployed by the customers - ownership-based restitution and trusts – will be examined in turn. After presenting an analysis under Japanese law, this article will explore its relevance to other legal systems.

2 Proprietary restitution under Japanese law

2.1 *Proprietary restitution based on ownership*

When the customers of a cryptocurrency exchange contend that the cryptocurrencies they have entrusted to the exchange provider are shielded from the latter's bankruptcy, they may seek proprietary restitution by asserting ownership over those cryptocurrencies.

[1] In this article the word "cryptocurrencies" refers to either different kinds of cryptocurrencies or units of a specific cryptocurrency, depending on the context.

[2] In this article the word "Bitcoins" is used to refer to units of the Bitcoin cryptocurrency.

[3] This article will focus on centralised exchanges, a type of exchange to which customers can entrust their cryptocurrencies. Towards the future, more use may be made of DEXs (decentralised exchanges) which enable trading without cryptocurrencies being entrusted to them and hence do not attract hacking attacks. But DEXs will not completely replace centralised exchanges since they do not enable trading with fiat currencies.

Such relief was sought in a suit against Mt Gox, which was once the world's biggest provider of a cryptocurrency exchange. In 2014, it became insolvent and bankruptcy proceedings were opened in Japan. Most of the creditors were its former customers who had entrusted it with Bitcoins and fiat currencies and had a contractual right to recover them. Conscious that filing a contractual claim in the bankruptcy proceedings would only yield a partial recovery, one of the former customers filed a suit before the Tokyo District Court against the bankruptcy administrator (hereafter "the Mt Gox case"), seeking a full recovery of what he saw as "his Bitcoins" by asserting ownership over them. Filing such a suit is permissible because a right of proprietary restitution is unaffected by the commencement of bankruptcy proceedings under Article 62 of the Japanese Bankruptcy Act, which provides:[4]

> "The commencement of bankruptcy proceedings shall not affect the right to recover, from the bankruptcy estate, assets that do not belong to the bankrupt."

The Court dismissed the claim[5] by denying that Bitcoins could be an object of *shoyûken,* that is the concept of ownership in Japanese law. In so holding, it relied on the provisions of the Japanese Civil Code which indicate that the objects of *shoyûken* are limited to tangible assets. The relevant provisions read:

> "Article 85: The term '*butsu*' (things) as used in this Code shall mean tangible assets.
>
> Article 206: The *shoyûken* holder of *butsu* shall have the right to freely use, profit from and dispose of them, subject to the restrictions prescribed by law."

In fact, Japan's first modern civil code, the Civil Code of 1890, did not limit the objects of *shoyûken* to tangible assets.[6] The limitation was introduced by the Civil Code of 1896 which replaced the 1890 Code and remains in force to this day. The 1896 Code adopted a two-tier scheme separating the law of property (contained in Part II) and the law of obligations (contained in Part III). It was feared that in this scheme, the notion of "ownership of personal rights" would invite a conceptual confusion. This, among other reasons, lead to limiting the objects of ownership to tangible assets.[7]

On a literal interpretation, "tangible assets" would be limited to solids, liquids and gas, excluding such assets as electricity, heat and light. In the course of the last century, various scholarly opinions were put forward to overcome this statutory limitation. One such opinion says that the words "tangible assets" should be interpreted broadly to cover the types of intangible assets which are amenable to exclusive control in a legal as opposed to factual sense.[8] This interpretation

[4] There is no official English translation of Japanese law. All the translation of Japanese legislation in this article is the work of the present author.

[5] The judgement of the Tokyo District Court on 5 August 2015 (in Japanese), 2015 WLJPCA 08058001 (accessible by the subscribers of Westlaw Japan).

[6] Article 6(1) provided: "*Butsu* are tangible or intangible."

[7] Stenographic Records of the Proceedings of the Meetings of the Chief Examiners of the Investigative Committee of Codes (Division of Civil Code) (1893) vol 1 64 [Masaaki Tomii].

[8] Sakae Wagatsuma *Shintei Minpô Sôsoku* (Revised Edition on the General Rules of the Civil Code) (1965) 201 *et seq* (in Japanese).

would allow *shoyûken* to be extended to such intangible assets as electricity. Another opinion respects the literary meaning of the words "tangible assets" but suggests that the rules applicable to *shoyûken* should, where warranted, be extended by way of *mutatis mutandis* application to intangible assets.[9]

In the Mt Gox case, the plaintiff argued that Bitcoins were "tangible assets" on the interpretation that this expression covered intangible assets amenable to exclusive control. But the Court rejected this argument in view of the two-tier scheme of the Civil Code and favoured the literal reading.

2.2 *Proprietary restitution with respect to intangible assets*

Proprietary restitution under Article 62 of the Bankruptcy Act (above) is typically based on *shoyûken* and accordingly relate to tangible assets. It is, however, generally accepted that proprietary restitution may be granted under the same provision with respect to such intangible assets as intellectual property rights and receivables.[10] What should matter is, as indicated in that provision, whether the asset belongs to the claimant. The asset would have to be amenable to exclusive control for it to belong to somebody and for it to be recovered by way of proprietary restitution.

On this reasoning, the customers of a cryptocurrency exchange who have entrusted their cryptocurrencies to the exchange provider should, in the event of the provider's bankruptcy, be able to obtain proprietary restitution of their cryptocurrencies from the bankruptcy estate on the fulfilment of two requisites, namely: (i) that cryptocurrencies are amenable to exclusive control; and (ii) the cryptocurrencies entrusted to an exchange provider by its customers belong to the latter. These two requisites will be examined in turn below.

Amenability of cryptocurrencies to exclusive control

In the Mt Gox case, the Tokyo District Court did not merely rule that Bitcoins were not "tangible assets". It went on to consider whether Bitcoins were amenable to exclusive control. The Court answered this question in the negative for the reasons that (i) the transactions of Bitcoins need to be propagated to the network and confirmed by mining, a process which necessarily involves third parties and (ii) an address on the Bitcoin blockchain exhibits no electronic record showing the balance of the Bitcoins therein.

Are these good reasons? The observation made in (i) is factually correct. The miners who validate blocks of transactions could, if they so wish, decide not to process transactions from a specific Bitcoin address. But as long as there are other miners willing to process them, they will be processed sooner or later. More importantly, Bitcoins exist invincibly unlike the digital assets of the pre-

[9] Kazuo Shinomiya *Minpô Sôsoku* (General Rules of the Civil Code) (3 ed 1983) 132 (in Japanese).

[10] *eg* Makoto Ito *et al Jokai Hasan Hô* (Commentary on the Bankruptcy Act) (2 ed 2014) 474 (in Japanese). It does not explain how its proposition is reconciled with the restriction of *shoyûken* to tangible assets.

existing type which are recorded in a centralized registry. While the record of pre-existing digital assets is at the mercy of the administrator of the registry, the transactional record of Bitcoins is unassailable as it is contained in the blockchain and distributed across the network. Furthermore, the transfer of Bitcoins is only possible at the behest of the person who has the knowledge of the private key corresponding to the blockchain address in which they are held. It would, therefore, seem possible to say that Bitcoins and other similarly engineered cryptocurrencies are amenable to exclusive control.

The observation made in (ii) is also factually correct. The balance of Bitcoins in a blockchain address merely represents UTXOs (unspent transaction outputs), which is worked out by referring to all the previous transactions associated with that address. An address on the Bitcoin blockchain, therefore, only conceptually contains Bitcoins and, unlike a bank account, exhibits no electronic record showing their balance.[11] It is, however, no good reason to deny the amenability of Bitcoins to exclusive control because it should suffice to consider the amenability to control of a balance of Bitcoins rather than specific units of the Bitcoin.

To whom do the entrusted cryptocurrencies belong?

In Japanese law, there are currently no specific rules for the assignment of cryptocurrencies. There are, however, rules for the assignment of tangible assets and certain intangible assets. With respect to tangible assets, an assignment takes effect upon an agreement between the assignor and the assignee without any formalities required.[12] With respect to certain intangible assets which are registrable such as carbon emissions allowances and dematerialised book-entry securities, an assignment requires the transfer of registration on the relevant registry in addition to a valid agreement between the assignor and the assignee.[13] With respect to such registrable intangible assets, an account holder is presumed to be in lawful possession of the assets recorded in the account.[14]

[11] It should be noted that the Bitcoin's UTXO architecture is not the only record-keeping model for blockchains. The Ethereum blockchain, for example, keeps the record of each user account showing the most recent balance, as does a bank account.

[12] Article 176 of the Civil Code provides: "The creation and assignment of proprietary rights shall take effect solely by the manifestation of intent by the relevant parties."

[13] Article 50 of the Act to Promote Measures to Counter Global Warming provides in the relevant part: "An assignment of carbon emissions allowances shall not take effect unless the assignee has had an increase in carbon emissions allowances recorded in its account as a result of the transfer of registration … ." Article 140 of the Act on Book-Entry Transfer of Corporate Bonds and Shares provides: "An assignment of book-entry shares shall not take effect unless, upon an application for book-entry transfer, the assignee has had an entry recorded in the holdings column … of its account, showing an increase in the number of book-entry shares in accordance with the assignment."

[14] Article 53 of the Act to Promote Measures to Counter Global Warming provides: "It shall be presumed that the national government and account holders are in lawful possession of the carbon emissions allowances recorded in their accounts." Article 143 of the Act on Book-Entry Transfer of Corporate Bonds and Shares provides: "It shall be presumed that participants are in lawful possession of the rights in book-entry shares recorded in their accounts … ."

The presumption is rebutted where there is no valid agreement to assign the assets to the account holder.

Since the rules for registrable intangible assets promote transparency and transactional certainty, it would be reasonable to suggest that those rules should be applied *mutatis mutandis* to an assignment of cryptocurrencies. On this proposition, an assignment of cryptocurrencies would require the transfer of registration on the blockchain in addition to a valid agreement between the assignor and the assignee. The person who controls the blockchain address[15] in which cryptocurrencies are held would be presumed to be in lawful possession of them. This presumption would be rebutted where there is no valid agreement to assign the cryptocurrencies to that person. The agreement does not have to be expressed but can be inferred from the circumstances including any related contractual terms between the parties.

The providers of a cryptocurrency exchange usually prepare terms of service which the customers must accept before using their service. Under usual terms, exchange providers do not undertake to act as a counter-party to exchange transactions with their customers but provide a multilateral trading facility,[16] that is a facility that brings together multiple third-party offers of selling and buying and facilitates their matching. Thus, for example, the terms of service of Mt Gox which were applicable shortly before it became insolvent stated:[17]

> "Members acknowledge and agree that, when completing Transactions, they are trading with other Members, and Members accept that MtGox acts only as an intermediary in such Transactions and not as a counterparty to any trade."

Under other terms, exchange providers undertake to act as a counter-party to exchange transactions with their customers. Thus, the terms of use of Coincheck provide in the relevant parts:[18]

> "ARTICLE 10-2 SPOT TRANSACTIONS AT SHOP
>
> 1 … (1) Each Registered User shall be allowed to perform spot transactions at the virtual currency shop being operated by the Company, by placing orders to purchase or sell virtual currency through the procedure as specified by the Company. The counterparty in such transactions will be the Company."

[15] by means of the private key associated with that address. This rule would require further elaboration where the private key is intentionally or accidentally disclosed to other persons.

[16] A terminology drawn from the MiFID II (Directive 2014/65/EU on markets in financial instruments) of the European Union.

[17] Terms as of 20 January 2012 (available at http://web.archive.org/web/20140122203409/https://www.mtgox.com/terms_of_service).

[18] The terms applicable as of the time of writing (June 2018) (available on the website of Coincheck: https://coincheck.com). The terms also offer an alternative service whereby the provider undertakes to provide a multilateral trading facility in the following language:

> "ARTICLE 10-1 SPOT TRANSACTIONS AT EXCHANGE
>
> 1. … (2) The Company's responsibility shall be to provide an exchange where virtual currency can be bought and sold based on the orders placed ... . Therefore, the Company shall not become a party that is directly involved in virtual currency purchase and sales transactions, unless in exceptional cases... ."

When a customer of a cryptocurrency exchange entrusts the exchange provider with his or her cryptocurrencies, the provider will keep those cryptocurrencies in the blockchain addresses it controls.[19] It will also record those cryptocurrencies in its off-chain books, that is a ledger outside of the blockchain. When an order placed by the customer is executed, the balances on the provider's off-chain books will be adjusted accordingly. But the transaction will not immediately be broadcast to the blockchain network since it takes time and cost to have the transaction inscribed in the blockchain. Where the provider has acted as the counter-party to the transaction, the cryptocurrencies used to fulfil the transaction will eventually be transferred to a separate blockchain address controlled by the provider where it keeps the cryptocurrencies it owns. Where, on the other hand, the provider has merely provided a multilateral trading facility, the cryptocurrencies may be kept in the blockchain address controlled by the provider until such time when customers who have a positive balance on the provider's books request transfers to the blockchain addresses they control.

If the rules for registrable intangible assets are to be applied *mutatis mutandis* to the assignment of cryptocurrencies, the exchange provider to which cryptocurrencies are entrusted would be presumed to be in lawful possession of them while they remain held in the blockchain address controlled by the provider. This presumption would be rebutted if there is no valid agreement to assign those cryptocurrencies to the provider. Is there such an agreement?

Where an exchange provider merely provides a multilateral trading facility, it will not be acting as a counter-party to exchange transactions with its customers. This might lead one to think that no agreement could be inferred to assign the entrusted cryptocurrencies to the provider. If that were the case, however, the assignment of cryptocurrencies would have to take place directly between customers. And it is hard to see how it works because it is often impossible to identify a specific customer with whom specific cryptocurrencies have been exchanged. As stated above, an exchange provider may not transfer cryptocurrencies to blockchain addresses controlled by its customers until such time that customers who have a positive balance on the provider's books make a request for transfer. In these circumstances, it is not possible to infer an agreement between specific customers directly to assign specific cryptocurrencies between themselves. It would be more reasonable to consider that cryptocurrencies are assigned first to the exchange provider when they are entrusted to the latter, which the latter re-assigns to its customers when requests for transfer are made.

Where, on the other hand, an exchange provider acts as a counter-party to exchange transactions with its customers, it would not be difficult to infer an

[19] It may be contrasted with the holding patterns of online wallet providers. Some of them, like exchange providers, control the blockchain addresses in which the cryptocurrencies entrusted by their customers are held while others, unlike exchange providers, merely provide software allowing their customers to possess private keys to control the blockchain addresses in which their cryptocurrencies are held. See Raskin, "Realm of the coin: Bitcoin and civil procedure" 2015 *Fordham Journal of Corporate and Financial Law* 969 996.

agreement to assign the traded cryptocurrencies to the provider at the time when the customer's order is executed. But would it be more reasonable to infer an assignment agreement at an earlier point in time when the customer entrusts their cryptocurrencies to the exchange provider? Suppose that before the customer's order is executed, the blockchain for the entrusted cryptocurrency is hard forked and has yielded cryptocurrencies of a new breed. If it is the customer to whom the entrusted cryptocurrencies belong, the exchange provider would be obliged to extract the cryptocurrencies of the new breed and deliver them to the customer. It is a task involving risky operations which an exchange provider would not undertake without charging a sufficient level of fees. In view of the current practice of an exchange provider charging no fees for keeping custody of entrusted cryptocurrencies, it seems reasonable to infer an agreement for customers to assign their cryptocurrencies to the exchange provider at the time when they entrust them to the latter.

From the foregoing analysis, it follows that regardless of whether an exchange provider acts as a counter-party to exchange transactions with its customers or merely provides a multilateral trading facility, the presumption that the cryptocurrencies entrusted to an exchange provider by its customers belong to the provider is not rebutted. It must accordingly be concluded that the customers of a cryptocurrency exchange have no right to obtain proprietary restitution with respect to the cryptocurrencies they have entrusted to the exchange provider.

3 Trusts under Japanese law

When the customers of a cryptocurrency exchange contend that the cryptocurrencies they have entrusted to the exchange provider are shielded from the provider's bankruptcy, they may base their contention on the principle that trust property is shielded from the trustee's bankruptcy,[20] arguing that the provider holds the cryptocurrencies on trust for them. This argument envisages that the provider is acting as a trustee and the customers are acting simultaneously as settlors and beneficiaries.[21]

[20] This principle is enshrined in article 25(1) of the Trusts Act (*Shintaku Hô*), which provides: "Where an order for the commencement of bankruptcy proceedings is made against a trustee, no asset forming part of trust property shall be included in the bankruptcy estate." Procedurally, when a trustee goes into bankruptcy, its duties come to an end (article 56(1)) and the bankruptcy administrator steps in to preserve the trust property until a new trustee is appointed and becomes ready to administer the trust (article 60(4)). Article 56(1) of the Trusts Act provides: "The duties of a trustee shall be terminated on the following grounds ... However, in the case of subparagraph (iii) below, if the terms of trust otherwise provide, such terms shall prevail. … (iii) an order for the commencement of bankruptcy proceedings has been made against the trustee … ." Article 60(4) of the Trusts Act provides: "Where the duties of a trustee have been terminated on the ground stipulated in Article 56(1)(iii), the bankruptcy administrator shall, until a new trustee is ready to carry out the administration of the trust, preserve the assets forming part of trust property and take the necessary steps to hand over the administration of the trust."

[21] In a separate move, a trust bank is planning to offer a scheme whereby an exchange provider (acting as a settlor) assigns the cryptocurrencies entrusted by its customer to the trust bank who

Such an argument was made in a fresh action against the bankruptcy administrator of Mt Gox filed on 19 February 2018 in the Tokyo District Court.[22] Instead of asserting ownership over the Bitcoins they had entrusted to Mt Gox, the former customers argued that Mt Gox had held them on trust for them. As of the time of writing (June 2018), the court has yet to hand down a decision.

The following analysis will consider the merit of such an argument and examine the duties of a trustee to see whether they are compatible with the *modus operandi* of exchange providers.

3.1 *Creation of a trust*

A trust is an arrangement pursuant to which a specific person manages or disposes of an asset in accordance with a specific purpose.[23] The asset can be tangible or intangible since there is no good reason to restrict it to tangibles.[24] It would, therefore, be safe to assume that cryptocurrencies can comprise trust property.

A trust is created by a trust agreement, a will or a unilateral manifestation of intent.[25] Among those methods, the one most relevant to the present discussion is a trust agreement. Thus, a trust is created where there is an agreement between A and B whereby A will assign an asset to B and B will keep it in custody or

is to hold them (as a trustee) for the customer (as a beneficiary) with the aim of shielding the cryptocurrencies from the bankruptcy of exchange provider. See *Nihon Keizai Shimbun* (Nikkei Newspaper), the morning edition of 7 Feb 2018, 7 (in Japanese).

22 *Nihon Keizai Shimbun* (Nikkei Newspaper), the morning edition of 20 Feb 2018, 38 (in Japanese).

23 Article 2(1) of the Trusts Act provides: "The term 'trust' within the meaning of this Act refers to an arrangement created by any of the methods set out in the following Article, pursuant to which a specific person is to manage or dispose of an asset in accordance with a specific purpose (other than the purpose of exclusively promoting his own interests …) and take any other steps necessary to achieve that purpose."

24 The Trusts Business Act (*Shintaku Gyô Hô*) previously provided for an exhaustive list of assets capable of comprising trust property. The list included tangible movables and certain intangible assets such as receivables. By the 2004 amendment of the Act, the list was abolished, paving the way for a trust to be created with respect to other intangible assets such as intellectual property and carbon emissions allowances.

25 Article 3 of the Trusts Act provides: "A trust shall be created by any of the following means: (i) by concluding an agreement with a specific person to the effect that an asset shall be assigned to the latter or encumbered with a security right or otherwise disposed of in favour of the latter and that the latter shall manage or dispose of the asset for a specific purpose and take any other steps necessary to achieve that purpose (hereinafter referred to as a 'trust agreement'); (ii) by making a will to the effect that an asset shall be assigned to a specific person or encumbered with a security right or otherwise disposed of in favour of a specific person and that the latter shall manage or dispose of that asset in accordance with a specific purpose and take any other steps necessary to achieve that purpose; or (iii) by a manifestation of intent by a specific person to manage or dispose of a specific asset he holds in accordance with a certain purpose and take any other steps necessary to achieve that purpose, with the manifestation being evidenced by a notarial deed or any other document or electronic or magnetic record … stating or recording that purpose, the particulars necessary to specify the asset, and other particulars specified by the ordinances of the Ministry of Justice."

dispose of it for a specific purpose.[26] The agreement need not be expressed or use the word "trust." It can be inferred from the circumstances.

It follows that a trust is created between an exchange provider and its customer in favour of the latter (i) when the customer entrusts cryptocurrencies to the provider if there are circumstances which make it possible to infer an agreement between them that the customer will assign the cryptocurrencies to the provider and that the latter will keep them in custody and dispose of them for the purpose of executing the customer's order for exchanging them for other cryptocurrencies or fiat currencies and delivering the latter to the customer; or (ii) when the customer entrusts the provider with fiat currencies if there are circumstances which make it possible to infer an agreement between them that the customer will assign the fiat currencies to the provider and that the latter will keep them in custody and dispose of them for the specific purpose of executing the customer's order for exchanging them for cryptocurrencies and delivering the latter to the customer. If a trust as described above is created, the cryptocurrencies or fiat currencies obtained in the course of the transaction will form part of the trust property until they are delivered to the customers.

There is, however, uncertainty as to what circumstances make it possible to infer a trust agreement. In a leading case, a construction company held in its bank account a sum of money paid by a local municipality as an advance for the building work for which the municipality had engaged the company. The Supreme Court ruled[27] that the money was shielded from the bankruptcy of the company, reasoning that the company held it on trust for the municipality. To reach that ruling, the Court found that there was a trust agreement between the company and the municipality whereby the company was to use the money for the purpose of defraying the cost of the building work. The Court so found notwithstanding that the parties had not used the word "trust" in the construction contract. The Court observed that the construction contract only stipulated that the company could not use the advance for purposes other than to defray the cost of the building work. But it noted that the contract additionally laid down, by way of incorporation of the terms of another contract, (i) that the advance must be deposited in a dedicated bank account, (ii) that the company could only make a withdrawal from the account after submitting documents showing the proper use of the fund to the bank and receiving its verification, (iii) that the proper use of the fund must be inspected by an external auditor, and (iv) that the auditor could demand the bank to suspend withdrawals should it find that the advance was not properly used. It is not clear from the Court's reasoning whether any of such additional elements are indispensable to infer a trust agreement.

In this regard, it is interesting that under the Japanese regulatory rules in force as from 1 April 2017,[28] the providers of a cryptocurrency exchange

[26] *ibid* article 3(i) of the Trusts Act.

[27] The judgment of the Supreme Court on 17 Jan 2002 (56-1 Minshû 20).

[28] These rules are contained in the Payment Services Act (*Shikin Kessai Nikansuru Hôritsu*) which devotes one chapter to "virtual currencies". The words "virtual currencies" are defined in article 2(5) in the following terms. It is a technologically neutral definition but the chapter is

soliciting business in Japan must be registered with the Prime Minister.[29] To be registered, the providers must comply with certain requirements.[30] Among those requirements are (a) to establish a system necessary to ensure the segregation of the fiat currency and cryptocurrencies received from its customers from its own fiat or virtual currencies and (b) to have the status of segregation periodically inspected by an external auditor.[31] Furthermore, (c) the Prime Minister may through his or her officials inspect the business operation of the provider,[32] and, (d) where necessary, order improvement.[33] Among the additional elements mentioned by the Supreme Court, (i) corresponds to (a), (iii) to (b) and (c), and (iv) to (d). To that extent, it would be easier to infer a trust agreement with the exchange providers who have been registered in Japan by complying with the relevant regulations.

primarily aimed at cryptocurrencies. "The 'virtual currencies' within the meaning of this Act are anything described in either of the following subparagraphs. (i) anything having financial value (but only those recorded electronically in electronic devices or other items, excluding the Japanese or foreign currencies and assets denominated in such currencies), which can be used to pay to unspecified persons for goods bought or rented or for services received, which can be sold to or bought from unspecified persons, and which can be transferred by means of electronic data processing systems. (ii) anything having financial value which can be exchanged with unspecified persons for anything described in the preceding subparagraph, and which can be transferred by means of electronic data processing systems."

29 Article 63-2 of the Payment Services Act provides: "Unless registered with the Prime Minister, no person may engage in the business of exchanging virtual currencies." Article 63-22 of the same Act provides: "Unless registered pursuant to Article 63-2, no foreign provider of a virtual currencies exchange may solicit from persons in Japan the business activities listed in Article 2(7)" [note by the present author: this refers to the business activities related to the exchange of virtual currencies].

30 Article 63-5 of the Payment Services Act provides: "(1) The Prime Minister shall refuse to grant registration where the applicant is any of the following persons … (v) A corporation which has not established a system necessary to ensure compliance with the provisions of this Chapter". Article 63-17 of the same Act provides: "(1) In any of the following circumstances, the Prime Minister may rescind the registration granted under Article 63-2 … (i) where the provider has become any of the persons described by the subparagraphs of Article 63-5(1)".

31 Article 63-11 of the Payment Services Act provides: "(1) The provider of a virtual currencies exchange shall, in connection with its business, segregate the fiat or virtual currencies entrusted by its customers from its own fiat or virtual currencies pursuant to the Ordinance of the Cabinet Office. (2) The provider of a virtual currencies exchange shall, pursuant to the Ordinance of the Cabinet Office, periodically undergo an audit by a certified public accountant … or by an auditing firm as regards the status of the segregation laid down in the preceding provision."

32 Article 63-15 of the Payment Services Act provides: "When the Prime Minister finds it necessary for the proper and secure business operations of a virtual currencies exchange, he or she may order the exchange provider to submit reports or materials concerning its business operations or financial conditions and may have his or her officials enter its place of business or other premises, ask questions about its business operation or financial conditions and inspect its books and other items."

33 The Payment Services Act provides in article 63-16: "When the Prime Minister finds it necessary for the proper and secure business operation of a virtual currencies exchange, he or she may, to the extent necessary, order the provider to take measures necessary to improve its business operation or financial conditions or any other measures necessary for the purposes of supervision."

3.2 *Compatibility with trustee's duties*

Once a trust is created, the trustee is subject to a range of duties including the duty to avoid conflicts of interest and the duty of segregating trust property from his own property. If an exchange provider holds the fiat currencies and cryptocurrencies entrusted to it by its customers on trust for the latter, it would be subject to such duties. The following analysis will examine whether such duties are compatible with the exchange providers' *modus operandi*.

Acting as a counter-party to exchange transactions

It has been seen earlier that an exchange provider may, depending on the terms of service, undertake to act as a counter-party to exchange transactions with its customers. If the exchange provider is acting as a trustee for its customers, it raises doubt whether such conduct involves the type of conflict of interest which the provider is obliged to avoid. Japanese law indeed prohibits a trustee from acting as a counter-party to the sale or purchase of the trust property.[34] As an exception, however, the trustee can so conduct itself if the beneficiary has given an informed consent.[35]

When a customer of a cryptocurrency exchange places an order in response to the price quoted by the exchange provider, the customer may be deemed to have consented on an informed basis to the provider acting as the counter-party to the exchange transaction. It would, therefore, be safe to conclude that an exchange provider can act as a counter-party to exchange transactions with its customers without failing in its duty as a trustee to avoid conflicts of interest.

Commingling cryptocurrencies in a blockchain address

There are two models for the way in which the providers of a cryptocurrency exchange hold the cryptocurrencies entrusted to them by their customers on the blockchain.

In one model, the cryptocurrencies of each customer are held in a blockchain address which is associated with that specific customer. To avoid delay in executing the customers' orders, the private keys would need to be kept in an online wallet ("hot storage"), though it makes the cryptocurrencies vulnerable

[34] The Trusts Act provides in article 31(1): "A Trustee shall not carry out the following conducts: (i) causing assets forming part of trust property … to be included in the trustee's own property or causing assets forming part of the trustee's own property … to be included in trust property;".

[35] The Trusts Act provides in article 31(2): "Notwithstanding the contrary provisions in the preceding paragraph, a trustee may carry out the conducts listed therein in any of the following circumstances. However, sup-paragraph (ii) shall not apply where the terms of the trust provide that the conduct in question shall not be carried out even in the circumstances set forth in that sub-paragraph … (ii) The trustee has disclosed facts material to the conduct in question and obtained the beneficiary's consent ...".

to hacking attacks. This was the model apparently adopted by Bitfinex,[36] prior to receiving a major hacking attack in August 2016.[37]

In another model, the exchange provider commingles the cryptocurrencies entrusted to it by its customers in blockchain addresses which are not associated with any specific customers. The holdings of each customer are only recorded in the provider's off-chain books. This model allows the provider to leave the private keys in an online wallet ("hot storage") for only so much of the cryptocurrencies as would be sufficient to cover the volume of transactions instructed in normal circumstances. For a bulk of the entrusted cryptocurrencies, the provider can keep the private keys in an off-line wallet ("cold storage"). This arrangement enhances security, which presumably is the reason behind the prevailing adoption of this model. Thus, Mt Gox indiscriminately distributed the Bitcoins entrusted to it by its customers in a number of blockchain addresses and randomly moved them around different addresses to avoid hacking attacks.[38] This model is permissible under the Japanese regulations applicable to the providers of a virtual currencies exchange,[39] which require the providers to segregate the cryptocurrencies entrusted to them by their customers as a whole from their own cryptocurrencies but do not go to the extent of requiring them to segregate the cryptocurrencies of each customer on the blockchain. This model is also permissible under the regulations of other jurisdictions such as New York.[40]

The second model, however, begs the question whether commingling the cryptocurrencies entrusted by different customers in the same blockchain addresses is compatible with the duty of the exchange provider as a trustee. Under Japanese law, a trustee has the duty to segregate trust property from his own property and any other trust property he administers. The required manner of segregation depends on the categories of assets.[41] Thus, to segregate

[36] See an announcement by Bitfinex on 4 June 2015 (https://www.bitfinex.com/posts), which stated, "[s]tarting today we … will separate each user's funds on the public blockchain".

[37] Bitfinex adopted multi-signatures as a measure to limit vulnerability to hacking attacks (In the Matter of BFXNA Inc. d/b/a BITFINEX, CFTC No 16-19, 2016 WL 3137612 (June 2 2016) 3). But it failed to ward off the attack.

[38] This is based on a finding made by the Tokyo District Court in its judgement in the Mt Gox case.

[39] article 63-11 of the Payment Services Act (see note 31 *supra* for the text) and article 20 of the Cabinet Office Ordinance on the Providers of a Virtual Currencies Exchange, read in conjunction with II-2-2-2 of the Operational Guidelines (May 2017) of the Financial Services Agency.

[40] 23 CRR-NY 200.9, which provides for the rules on the custody and protection of customers' assets, does not require the segregation of the cryptocurrencies of each customer on the blockchain. It reads in the relevant part: "(b) To the extent a licensee stores, holds, or maintains custody or control of virtual currency on behalf of another person, such licensee shall hold virtual currency of the same type and amount as that which is owed or obligated to such other person. (c) Each licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering assets, including virtual currency, stored, held, or maintained by, or under the custody or control of, such licensee on behalf of another person except for the sale, transfer, or assignment of such assets at the direction of such other person."

[41] article 34(1) of the Trusts Act provides: "A Trustee shall segregate assets forming part of trust property from assets forming part of his own property or any other trust property he

fiat currencies, it is sufficient to account for their quantity by keeping books.[42] On the other hand, the assets which can be registered as forming part of trust property, such as carbon emissions allowances and dematerialised book-entry securities, must be segregated by means of effecting such registration.[43] It has been suggested earlier in this article that the rules for registrable intangible assets should be applied *mutatis mutandis* to determine the owner of cryptocurrencies. However, the registration of cryptocurrencies as forming part of trust property is not possible unless and until the blockchain is so configured as to make it technically possible and the law recognises it as a valid registration. Consequently, cryptocurrencies would fall within the same category as fiat currencies for the purpose of segregation[44] and accordingly, it will be sufficient to account for their quantity by keeping books. It follows that an exchange provider would not be failing in its duty of segregation if it uses off-chain books to account for the quantity of each customer's holdings.

It should be noted that to tolerate commingling cryptocurrencies entrusted by different customers in the same blockchain addresses would not harm the interests of the customers. The law will treat the bulk of cryptocurrencies as being subject to shared interests and deem those interests to belong to each trust property which the exchange provider administers for each customer.[45] Each customer may divide the bulk in consultation with other customers or, failing all other statutorily prescribed manners of division, submit a petition for division to the court.[46]

administers in the manners specified by the following subparagraphs for each category of assets. If, however, the terms of the trust provide for other manners of segregation, such terms shall prevail. (i) the assets which may be registered as forming part of trust property … (excluding the assets mentioned in subparagraph (iii)): by the said registration; (ii) the assets which may not be registered as forming part of trust property … (excluding the assets mentioned in subparagraph (iii)): the manners specified in (a) or (b) below for each category of assets: (a) tangible movables (excluding fiat currencies): by holding the assets in custody in a condition that allows them to be distinguished by appearance from his own property and any other trust properties he administers; or (b) fiat currencies and any assets other than those mentioned in (a): by accounting for their quantity; or (iii) the assets specified by the Ordinance of the Ministry of Justice: in the manners specified by the Ordinance as the appropriate manners of segregation."

42 article 34(1)(ii)(b) of the Trusts Act (see n 41 *supra*).

43 article 34(1)(i) of the Trusts Act (see n 41 *supra*).

44 article 34(1)(ii)(b) of the Trusts Act (see n 41 *supra*).

45 This is derived from article 18 of the Trusts Act, which provides: "(1) Where an asset forming part of trust property becomes indistinguishable from an asset forming part of the trustee's own property …, it shall be deemed that shared interests in those assets belong to the trust property and the trustee's own property. In this case, the shares of the interests shall be proportionate to the values of the respective assets as of the time when they became indistinguishable from each other. (2) … (3) The two preceding paragraphs shall apply *mutatis mutandis* to the cases where the same person acts as a trustee for two or more trusts and an asset forming part of the trust property of one trust becomes indistinguishable from an asset forming part of the trust property of another trust …. In such a case, the words 'the trust property and the trustee's own property' shall be read as referring to 'the trust property of each trust'."

46 This follows from article 19 of the Trusts Act, which provides: "(3) Where shared interests in an asset in the possession of a trustee belong to the trust properties of two or more trusts administered by the same trustee, the asset may be divided in the following manners: (i) in

4 The relevance of the analysis under Japanese law to other legal systems

Different legal systems will apply different legal principles to address whether cryptocurrencies entrusted to an exchange provider are shielded from the provider's bankruptcy. This article will focus on the principles related to *rei vindicatio*, tort of conversion and trusts, to see what relevance the foregoing analysis under Japanese law has for these principles.

4.1 *Rei vindicatio*

The legal systems which have inherited the Roman law concept of ownership, *dominium*, would allow a suit to be filed for *rei vindicatio* (vindication of property: an owner's claim against the possessor for the return of the property). Those are typically the legal systems of the civil law tradition.[47] But legal systems of mixed traditions may also recognise this form of relief.[48] The modern Japanese law is rooted in the civil law tradition and the ownership-based restitutionary claim made in the Mt Gox case was the Japanese-law version of *rei vindicatio*. The foregoing analysis under Japanese law concerning proprietary restitution would, therefore, have direct relevance to other legal systems in which this principle may be invoked. Thus, the same issues as examined under Japanese law will confront such legal systems when addressing whether the cryptocurrencies entrusted to an exchange provider by its customers are shielded from the provider's bankruptcy.

The first issue which will be confronted is whether cryptocurrencies can be an object of ownership. The concepts of ownership are different from one legal system to another reflecting the precedents and doctrines behind them. Some legal systems limit the objects of ownership to tangible assets while others extend it to intangible assets.[49] The legal systems of the former type would encounter the same difficulties as experienced under Japanese law. The foregoing

accordance with the terms of the trusts; (ii) in consultation among the beneficiaries of the trusts … ; and (iii) by a decision of the trustee where it is reasonable to consider that the division is necessary in order to achieve the purpose of each trust and it is clear that the division will not harm the interest of the beneficiaries or where there are justifiable grounds for the division in the light of, *inter alia*, the impact it may have on the trust properties, the purpose and manner of the division, and the actual relationships of the trustee with the beneficiaries. (4) In the case falling within the preceding paragraph, if no agreement is reached through consultation under subparagraph (ii) and in no other manners provided by the other subparagraphs is the division possible, the beneficiary of each trust … may submit a petition to the court for the division of the asset subject to the shared interests."

47 *eg* an *action en revendication* in French law, *Herausgabeanspruch* in German law (par 985 of the German *BGB* (Civil Code)) and *Eigenthumsklage* in Austrian law (par 366 of the Austrian *ABGB* (General Civil Code)).

48 *eg* the law of South Africa. See Van der Merwe & Du Plessis (eds) *Introduction to the Law of South Africa* (2004) 218 [CG der Merwe].

49 Akkermans classifies German and Dutch law into the former category, and French law into the latter ("Property law" in Hage & Akkermans (eds) *Introduction to Law* (2014) 71 78). Von Bar and Drobnig add Greek law to the former camp and the law of Portugal, Italy, Austria, Belgium, Spain, and Sweden to the latter (*The Interaction of Contract Law and Tort and Property Law in Europe A Comparative Study* (2004) 317).

analysis under Japanese law would accordingly be of particular relevance to such legal systems. Even in the legal systems which do not limit the objects of ownership to tangible assets,[50] not all intangible assets will qualify as an object. So it will be necessary to consider whether cryptocurrencies can be an object of ownership. Under Austrian law, for example, the General Civil Code defines *Sachen* (things) broadly[51] but it is understood that assets must have the attribute of controllability (*Beherrschbarkeit*) to qualify as *Sachen*. It has been observed that the controllability of cryptocurrencies is evident because the transfer of cryptocurrencies to another address would be impossible without the knowledge of the private key. On that reasoning, it has been suggested that cryptocurrencies can be classified as *Sachen.*[52] This reasoning has a familiar ring to it as a similar question, whether cryptocurrencies are amenable to exclusive control, has been considered in the foregoing analysis under Japanese law.

Whatever the technicality involved in each legal system, cryptocurrencies would be a latest addition to the list of new assets which challenge the conventional boundary of assets deemed to qualify as the objects of ownership. Other such assets include domain names, wireless networks, carbon emissions allowances and data. Such assets have been compelling the law makers of each State to consider *de lege ferenda* (with a view to the future law) whether and how their legal systems should embrace them. Broadening the qualifying assets would cause friction with *numerus clausus*, a principle which says that there shall be no property rights other than those prescribed by legislation.[53] Where necessary, however, the law will evolve to accommodate new assets. The law of Luxembourg, for example, has been amended to allow proprietary restitution of data stored in a cloud computing service in the event that the service provider goes into bankruptcy.[54]

The second issue which will be confronted is whether the cryptocurrencies entrusted to an exchange provider by its customers belong to the latter. Under many legal systems, the rules for the assignment of cryptocurrencies would be

[50] The English word "ownership" is fitting in this context as it covers both tangible and intangible assets. Thus, it is not uncommon to speak of the "ownership" of an intellectual property right.

[51] Par 285 of the *Allgemeines bürgerliches Gesetzbuch* (General Civil Code) provides: "Alles, was von der Person unterschieden ist, und zum Gebrauche der Menschen dient, wird im rechtlichen Sinne eine Sache genannt (Everything which is distinct from a human and serves the use of men is called a thing in the legal sense)."

[52] Völkel "Privatrechtliche Einordnung virtueller Währungen" (2017) 6 Österreichische Bankwissenschaftliche Gesellschaft 385 387.

[53] In Japanese law, it is enshrined in article 175 of the Civil Code, which provides: "No property rights may be created other than those prescribed by this Code or other legislation."

[54] This result would be derived from article 567(2) of the Luxembourg Commercial Code, which provides: "Les biens meubles incorporels non fongibles en possession du failli ou détenus par lui peuvent être revendiqués par celui qui les a confiés au failli ou par leur propriétaire, à condition qu'ils soient séparables de tous autres biens meubles incorporels non fongibles au moment de l'ouverture de la procedure … (Non-fungible intangible movable assets in the bankrupt's possession or detention may be recovered by the person who has entrusted them to the bankrupt or by their owner, provided that they are separable from all other non-fungible intangible movable asset at the time of opening of the proceedings …)." See also Avis du Conseil d'Etat, No 49.937 (12 March 2013).

unclear. As noted in the foregoing analysis under Japanese law, it will often be reasonable to draw an analogy with the rules for the assignment of tangible assets or other intangible assets. Thus, under Austrian law, it has been suggested, by drawing an analogy with the rules for tangible assets, that an assignment of cryptocurrencies would not take effect unless they have been transferred to a new blockchain address under the sole control of the assignee.[55]

The third issue which will be confronted is how the rules for assigning cryptocurrencies are to be applied to the cryptocurrencies entrusted to an exchange provider by its customers. Here, it will be essential to analyse the legal relationships between the exchange provider and its customers. This analysis must be no different from that conducted under Japanese law.

4.2 *Tort of conversion*

For a number of legal systems, notably those of the common law tradition, *rei vindicatio* is an alien concept.[56] In such legal systems, the gap of the missing *vindicatio* may be filled by the tort of conversion.[57] It protects the claimant's right to possession of property.[58] The courts have discretion to order the converted property to be returned to the claimant.[59] This discretion may be exercised, in the event of the defendant's bankruptcy, to allow recovery from the bankruptcy estate.[60]

It has been long debated what intangible assets can be classified as "property" subject to conversion.[61] A line of cases has dealt with assets like contractual rights,[62] information comprising a database,[63] domain names[64] and carbon emissions allowances.[65] In English law, an asset must "be definable, identifiable by third parties, capable in its nature of assumption by third parties and have some degree of permanence or stability"[66] before it can be admitted into the category of "property." In the United States, according to the Court of Appeals for the Ninth Circuit, "property" must be an interest capable of precise definition and of exclusive possession or control.[67]

55 Völkel (n 52) 388.

56 In the English common law, for example, a demand in court which consists in the direct assertion of ownership is not available: See Burrows (ed) *English Private Law* (3 ed 2013) par 17.304 [Donal Nolan & John Davies].

57 *ibid* par 17.309.

58 See Calnan *Proprietary Rights and Insolvency* (2 ed 2016) par 2.132.

59 subsections (2)(a) and (3)(b) of s 3 of the Torts (Interference with Goods) Act 1977.

60 See Calnan (n 58) par 2.108.

61 *eg* Palmer & Kohler "Information as property" in Palmer & McKendrick (eds) *Interests in Goods* (2 ed 1998) 3; Green "The subject matter of conversion" [2010] *JBL* 218 225.

62 *OBG v Allan* [2007] UKHL 21 (English House of Lords).

63 *Your Response Limited* [2014] EWCA Civ 281 (English Court of Appeal).

64 *Kremen v Cohen* 337 F 3d 1024 (2003) (US Court of Appeals for the Ninth Circuit).

65 *Armstrong DLW GmbH v Winnington Networks Ltd* [2013] Ch 156 (English High Court).

66 *National Provincial Bank v Ainsworth* [1965] 1 AC 1175, 1247 (English House of Lords).

67 *Kremen v Cohen* (n 64). The Court also required that the putative owner had established a legitimate claim to exclusivity. But this requirement seems more related to the question of who is the owner than to the question of what are the essential attributes of "property."

Whether cryptocurrencies are "property" has already been a subject of academic discourse for several years.[68] In applying the relevant tests for "property," the foregoing analysis under Japanese law on whether cryptocurrencies are amenable to exclusive control will be informative to the extent similar elements exist in the tests.

4.3 *Trusts*

Historically, the trust is an institution which has been developed in the legal systems of the common law tradition. But a similar institution has been embraced by Japanese law[69] and some other legal systems of the civil law tradition[70] as well as some legal systems of mixed traditions.[71]

The bottom line seems to be shared by all such legal systems: Assets belonging to trust property are shielded from the trustee's bankruptcy.[72] The foregoing analysis of trusts under Japanese law may, therefore, shed some light where trusts are invoked in other legal systems to address the question whether cryptocurrencies entrusted to an exchange provider by its customers are shielded from the provider's bankruptcy.

Care should, however, be taken not to underestimate the differences in the underlying theories of trusts law between the common law and civil law traditions. In the common law systems, where the claimant can show that he has an equitable proprietary interest in an asset that is in the possession of the defendant, the court may declare that the asset is held on trust for the claimant and order the defendant to transfer the asset in specie to the claimant.[73] Equitable proprietary interests are created by the maxim "equitable treats as done what ought to be done", whereas legal proprietary interests can only be derived from the owner. The distinction between equitable and legal proprietary interests is alien to Japanese law and other legal systems of the civil law tradition. These legal systems adopt a unitary concept of ownership, that is an ownership which cannot be divided between equitable and legal proprietary interests.

[68] *eg* Bayern, "Dynamic common law and technological change: The classification of Bitcoin" 71 *Wash & Lee L Rev Online* (2014) 22; Fairfield, "BitProperty" 2015 *S Cal L Rev* 805; Lavy & Khoo, "Who owns blockchains? An English legal analysis" (http://sclbc.zehuti.co.uk/site.aspx?i=ed47875) (2016); Hurich "The virtual is real: An argument for characterizing bitcoins as private property" 2016 *BFLR* 573; Perkins & Enwezor, "The legal aspect of virtual currencies" 2016 *JIBFL* 569.

[69] The history goes back over a century to the enactment in 1905 of the Secured Corporate Bond Trusts Act (*Tanpo-tsuki Shasai Shintaku Hô*).

[70] *eg* France introduced in 2007 the concept of *fiducie* (Titre XIV of the Civil Code), which is structurally a trust.

[71] *eg* the law of South Africa. See Van der Merwe & Du Plessis (n 48) 187 [MJ de Waal].

[72] See, *eg,* s 283(3)(a) of the United Kingdom Insolvency Act 1986; article 2024 of the French Civil Code; article 25(1) of the Japanese Trusts Act (for the text, see n 20 *supra*).

[73] See, *eg, Boscawen v Bajwa* [1996] 1 WLR 328 335 (English Court of Appeal); *Giumelli v Giumelli* (1999) 196 CLR 101 par 3 (High Court of Australia).

In English law, equitable proprietary interests can be created over intangible assets[74] and, therefore, it is probable that cryptocurrencies can be held on trust.[75] Despite the difference in the underlying theories of trusts law, it has been seen in the foregoing analysis that cryptocurrencies can also constitute trust property under Japanese law.

In some legal systems of the common law tradition, an equitable proprietary interest may be imposed by law to create a constructive trust. It will be a difficult question whether the provider of a cryptocurrency exchange is deemed to hold the cryptocurrencies entrusted to it by its customers on trust for the customers. In Japanese law, there is no statutory basis for constructive trusts. That is why the foregoing analysis under Japanese law has focused on the creation of a trust by a trust agreement inferred from the circumstances. That analysis may be useful to other legal systems which allow a trust to be created by an agreement inferred from the circumstances. But its relevance to constructive trusts would be limited since imposing an equitable interest is not the same as inferring an agreement to create a trust.

5 Conclusion

Where the provider of a cryptocurrency exchange goes into bankruptcy, whether the cryptocurrencies entrusted to it by its customers should be shielded from the bankruptcy might be seen first and foremost as a policy question. But the policy hangs in the balance as it is a contest between the interests of two innocent groups of parties, namely the customers who have entrusted their cryptocurrencies and the general creditors of the exchange provider. On the one hand, the customers have a greater stake in the cryptocurrencies they have entrusted than do the general creditors. On the other hand, the customers may be deemed to have taken the risk of the exchange provider's bankruptcy since the custody of cryptocurrencies is a risky operation which attracts many hacking attacks.

Since the policy consideration is indecisive, this article has focused on the legal principles. It has first examined the law of Japan, a country in which the matter has been actually litigated. Where an exchange provider goes into bankruptcy, the most obvious remedy the customers would seek is proprietary restitution. The foregoing analysis has, however, revealed that this remedy is fraught with difficulties. Firstly, while proprietary restitution is typically based on ownership, there is a ruling of the Tokyo District Court holding that cryptocurrencies, being intangible, cannot be an object of *shoyûken*, the Japanese-law concept of ownership. In the foregoing analysis, it has been argued that proprietary restitution should still be possible with respect to the type of intangible assets which are amenable to exclusive control. The second hurdle is put up again by the same court which expressed the view that cryptocurrencies were not amenable to exclusive control. The foregoing analysis has sought to

[74] Calnan (n 58) par 2.69 and 5.42.
[75] For the same view, see Lavy & Khoo (n 68).

demonstrate that this view is not well founded. The third hurdle lies in arguing that the cryptocurrencies entrusted to an exchange provider by its customers belong to the customer rather than the provider. But the foregoing analysis has shown that this argument cannot be supported. It has accordingly been concluded, in the final analysis, that the customers would not be entitled to proprietary restitution.

A more promising avenue for the customers would be to rely on the principle of trusts, according to which trust property is shielded from the trustee's bankruptcy. If it can be argued that the provider of a cryptocurrency exchange holds the cryptocurrencies entrusted by its customers on trust for the latter, those cryptocurrencies will be shielded from the provider's bankruptcy. The fact that cryptocurrencies are intangible does not disqualify them as assets comprising trust property. It will, however, be difficult to figure out whether a trust agreement can be inferred from the relationships between an exchange provider and its customers. The foregoing analysis has suggested that where the exchange provider is registered in Japan, the regulatory requirements which must be complied with are conducive to inferring a trust agreement. Once a trust is created, the exchange provider would be subject to a range of duties as a trustee, such as the duty to avoid conflicts of interest and the duty to segregate trust property from his own property and any other trust property he administers. It has been observed above that those duties are not incompatible with the *modus operandi* of exchange providers even if they act as a counter-party to exchange transactions with their customers and even if, as is usually the case, they commingle cryptocurrencies entrusted by different customers in the same blockchain address.

After conducting an analysis under Japanese law, this article has proceeded to examine its relevance to other legal systems. It has focused on *rei vindicatio*, tort of conversion and trusts as these are likely to be invoked by the customers of a cryptocurrency exchange when they argue that the cryptocurrencies they have entrusted to the exchange provider are shielded from the provider's bankruptcy. Despite significant differences which exist among different legal systems, many similar issues will be encountered, on which the analysis under Japanese law will shed useful light. Thus, the tort of conversion may exist in legal systems to which *rei vindicatio* is not known. But they both give rise to similar issues, namely the issue whether cryptocurrencies can be classified as "property" subject to conversion and the issue whether cryptocurrencies can be an object of ownership. On these issues, the analysis under Japanese law on whether cryptocurrencies can be an object of *shoyûken* and whether they are amenable to exclusive control may be informative. Again, the analysis of trusts under Japanese law may be useful to other legal systems which have the institution of trusts. Under each such legal system, similar issues will arise such as whether cryptocurrencies can comprise trust property and in what circumstances an exchange provider holds the cryptocurrencies entrusted to it by its customers on trust for the latter. Care should, however, be taken not to transpose the conclusions under Japanese law unquestioningly to legal systems of the common law tradition because the underlying theories of trusts law are different.

Given the high frequency of hacking attacks to cryptocurrency exchanges and the large size of heists, the question whether the cryptocurrencies entrusted to an exchange provider by its customers are shielded from the provider's bankruptcy is a question of practical significance. Notwithstanding that, the answer seems unclear in most legal systems. This article has sought to improve legal clarity by presenting an analytical framework, identifying issues, and pointing to possible solutions. It has also highlighted the similarities and differences between different legal systems. It should, however, be noted that even if analysis and solution in each legal system have been clarified, as long as they differ from one legal system to another, the question of conflict of laws cannot be avoided. It is a question which is not addressed in this article but calls for discussions because here, too, there is much uncertainty.[76]

[76] For a discussion in a somewhat broader context, see Takahashi "Implications of the blockchain technology for the UNCITRAL works" in United Nations Commission on International Trade Law *(ed) Modernizing International Trade Law to Support Innovation and Sustainable Development* (United Nations 2017) 81 91.