KEY POINTS

- Segregated wallets protected by private keys are a popular method of holding cryptocurrency, often with multiple parties holding keys including the exchange. This makes analysis of legal title complex, especially when users engage in margin trading and funding.
- The recipient of financing for trading obtains legal title to the cryptocurrency, subject to a lien in favour of the funding provider, enforced by the exchange retaining control of one private key.
- Users with cryptocurrency in segregated wallets will only have certainty should a hack occur if remedies are adequately understood. Proprietary restitution is the optimal remedy, but remedies against the exchange and third party service providers must be explored.

Feature

Author Lucy Chambers

The keepers of the keys: remedies and legal obligations following misappropriations of cryptocurrency

This article addresses two important legal issues arising from the recent misappropriation of Bitcoin following the hack of the Bitfinex exchange. First, how is legal ownership of Bitcoin determined when the keys to access Bitcoin wallets are spread across a number of parties, and what is the impact of Bitcoin trading? Second, what remedies exist for the misappropriation of Bitcoin in such segregated wallets? It is only if these two questions can be answered with certainty that users of Bitcoin markets can be assured of the security of their cryptocurrency.

INTRODUCTION: THE IMPORTANCE OF THE KEYS

On 2 August 2016, nearly 120,000 Bitcoins, worth about US$72m and representing 75% of the total Bitcoin supply, were misappropriated from the exchange platform Bitfinex in Hong Kong. Bitfinex immediately suspended trading and conducted an investigation into the circumstances surrounding the hack. Although the misappropriation of the Bitcoin is much smaller than the scale of the Mt. Gox KK losses, it is still the second biggest security breach of such an exchange and its ramifications were felt across the market. Bitfinex is the world's largest dollar-based exchange for Bitcoin, allowing both exchanging and trading in cryptocurrency, and is known in the cryptocurrency market for having deep liquidity in the US dollar/Bitcoin currency pair.

Around one year before the hack, Bitfinex adopted a new system for securing the wallets of Bitcoin held by each investor. On all exchanges, Bitcoin and other forms of cryptocurrency are held in wallets. Each wallet is protected by one or more private keys, which are secret numbers unique to and only known by the owner of the Bitcoin wallet, and which enable the Bitcoin in the wallet to be spent. The private keys are mathematically related to all Bitcoin addresses generated for the wallet, and are used to release the Bitcoin and update the blockchain with the appropriate transaction details.

It is important that the private keys are kept secure, as it is the keys that enable the Bitcoin to be spent or exchanged. Often keys are kept on computer files, commonly referred to as "hot storage", as the keys can only be accessed through a computer or the Internet. An alternative to this method is so-called "cold storage", where the keys are kept offline such as on a USB drive or written on paper. It was once thought that cold storage minimised the risk of a security breach because the key to the Bitcoin wallet could not be obtained by a hacker.

Following an investigation by the US Commodity Futures Trading Commission (CFTC), Bitfinex implemented a new system involving multi-signature segregated wallets. Bitfinex CEO Giancarlo Devasini said that this system would make it 'impossible for our users to lose their Bitcoins due to [Bitfinex] being hacked or [hackers] stealing them'.[1] The system involved each wallet having three signatures. Users who were lending or borrowing Bitcoin for the purposes of margin trading had three keys distributed, with one to Bitfinex, one to BitGo, a third party service provider, and one to the user. Users who were trading with Bitcoin had a different arrangement, where two out of three parties needed to sign to release the funds. BitGo had one of the keys and Bitfinex had two.

Although at the time of writing the exact cause of the hack is unknown, it appears that the multi-signature system was hacked and individual private keys were compromised, enabling the Bitcoin to be stolen. This raises a number of interesting questions for the application of the law of obligations to cryptocurrency: how does legal ownership get divided when keys are separated, especially in the context of Bitcoin trading, and what remedies do the owners of the Bitcoin wallets have when their Bitcoin are misappropriated?

LENDING THE KEYS: TRADING WITH CRYPTOCURRENCY

The Bitfinex platform, similar to other cryptocurrency platforms, allows users to both trade and lend cryptocurrency, including Bitcoin. Bitfinex's Exchange Trading feature permits users to exchange dollars for Bitcoins, and *vice-versa*, as well as to trade cryptocurrencies for other cryptocurrencies. Another of Bitfinex's services is its Margin Trading feature. Through this feature,

Bitfinex permits traders to borrow dollars and Bitcoins from other users on the platform in order to open leveraged positions on Bitfinex's exchange. Users ("Funding Providers") are permitted to enter an offer for their Bitcoin including their own set terms (duration, rate of return and amount), and the recipients are permitted to trade with the Bitcoin. Recipients ("Financing Recipients") are then responsible for paying interest and any fees to the users providing the financing. The role of Bitfinex in the lending is solely as the enforcer of the contracts established between the Funding Providers and the Financing Recipients.

From 2016, Bitcoin settled in both the Exchange Trading feature and the Margin Trading feature is held in individually enumerated wallets under the multi-signature system. Bitfinex retains control over the keys to the wallets, as its key is required to release any funds from the wallets in addition to the key of the user or the third party. Such a system is common to many cryptocurrency platforms offering trading functions.

The CFTC investigated Bitfinex's cryptocurrency business during the period April 2013 to February 2016 for violation of the Commodity Exchange Act 1936, as amended.[2] However, the more important legal question arising from this part of Bitfinex's business is the operation of legal title during the trading of cryptocurrency, which has broad application to all cryptocurrency trading platforms.

In each situation of lending for the purposes of trading with cryptocurrency, the Funding Provider intends for legal title to transfer to the Financing Recipient, however through the multi-signature wallet system, the individual Bitcoin are not released until the exchange allows its key to be used to release the funds. As the exchange operates as the enforcer of the contract between the Funding Provider and the Financing Recipient, the exchange uses its key to enforce the payment of fees and interest to the Funding Provider. This operates to create a lien over the cryptocurrency in favour of the Funding Provider, so the Financing Recipient will not receive the funds until the amounts owed to the Funding Provider are fully settled. At all times the cryptocurrency remains individually identifiable through the keys to each separate wallet and the blockchain.

Therefore, an analogy can be drawn under English law between cryptocurrency trading and trading shares as cryptocurrency is also an individually identifiable form of pure intangible.[3] This enables both the Funding Providers and the Financing Recipients to have certainty over both the nature of the legal title in their cryptocurrency trades and the appropriate remedies that can be exercised if the Financing Recipient does not perform the contract, including the enforcement of the Funding Provider's lien, so long as the understanding of the operation of legal rights in securities trading is extended to cryptocurrencies.

Furthermore, the technology underpinning cryptocurrency trading, the blockchain, may be extended to bond trading in the near future in order to increase security in trades.[4] Although the blockchain is not yet close to mass adoption, the ability to individually identify each digital trade can aid in the remedies available should such a trade go wrong. Therefore, trading with cryptocurrencies can be considered as legally certain as securities trading, as long as the operation of legal title and remedies for digital intangibles are properly understood by both market actors and the courts.[5]

LOSING THE KEYS: APPROPRIATE REMEDIES

Following the misappropriation of the Bitcoin, Bitfinex announced that the impact of the losses would be shared across the site's users,[6] regardless of whether or not they had lost or even held any Bitcoin. Each user suffered a generalised loss of 36.067%, which was said to match what Bitfinex expected to transpire in a liquidation context. In place of the losses, Bitfinex credited each customer's account with tokens labelled "BFXs", which are contingent on the recovery of the misappropriated Bitcoin and remain outstanding, pending redemption for US$1 per token by Bitfinex or pending exchange for shares of the capital stock in Bitfinex's parent company. On 13 October 2016 Bitfinex announced that it would redeem 1.1812% and 1.3152% of outstanding BFX tokens. Redemptions were applied pro rata to all settled wallet balances and opportunities were given for customers to exchange tokens for capital stock.[7]

This form of remedy for the misappropriation of the Bitcoin is inappropriate in the context of cryptocurrency. Not only is it a potential breach of Bitfinex's terms of service and may attract attention from securities regulators[8] but loss sharing as a remedy also demonstrates a fundamental misunderstanding of the legal nature of cryptocurrency as property.

An analogy may be made between Bitfinex's loss sharing arrangement and the "bail in" arrangements for certain European banks during the banking crisis where depositors and bondholders were forced to have the liabilities owed to them by the bank reduced in order to allow the bank rescue to continue. However, an important distinction may be made between the losses imposed on bank depositors and those imposed on Bitfinex investors. Cryptocurrency is a different form of legal property to money in a bank account: As a pure intangible, cryptocurrency may be enforced by action since it confers an immunity, is individually identifiable and it exists only in electronic form. Recognising that cryptocurrency is a form of pure intangible means that an analogy can be made with shares, thereby aiding the understanding of transfer of title when cryptocurrency is misappropriated.[9] As each Bitcoin is individually identifiable, it is not akin to money in a bank account, which is not individually identifiable by each depositor and exists as a form of liability owed by the bank.[10] Indeed, it was recently recognised by the 11th Circuit in Miami, Florida that, although Bitcoin is a means of exchange in a similar way to money, Bitcoin is not legally akin to money.[11] Moreover, even if an exchange such as Bitfinex controls a key to the individually segregated wallets of cryptocurrency, there is constructive delivery of the cryptocurrency to each user in a way that does not exist in a bank account.

Biog box

Lucy Chambers is a trainee solicitor at Slaughter and May. Lucy's personal research interests centre on economic analysis of law, with specific application to the laws of contract and restitution and the legal treatment of money. The views expressed in this article are the personal views of the author and do not represent the views of Slaughter and May.
Email: lucy.chambers@slaughterandmay.com

Therefore, loss sharing is inappropriate when cryptocurrency is individually identifiable and it can be determined which users suffered loss and which users did not. Moreover, a misunderstanding of the nature of cryptocurrency as property leads to incorrect application of the appropriate remedies when cryptocurrency is misappropriated. The preferable remedy for misappropriation of cryptocurrency, especially in the context of the Bitfinex hack, is using a claim in proprietary restitution. The hacker may be described as a constructive trustee because the subject matter of that trust is his possessory title to the stolen Bitcoin rather than the claimant's retained, and superior, interest as legal owner.[12]

More recently, third party service providers, similar to brokers, have also become a popular way of holding cryptocurrency such as Bitcoin on exchanges such as Bitfinex. In such arrangements users are instead provided with accounts that track their cryptocurrency balances but wherein the underlying cryptocurrency is controlled and managed by the third party in question, as the third party holds the private key to the cryptocurrency wallet. In effect, users of these sorts of services do not hold the cryptocurrency directly but rather the liabilities of the third party agents. This raises interesting questions of what happens when the cryptocurrency is misappropriated from the exchange. Since the users do not hold the cryptocurrency directly, but the third party agents are responsible for the management of the keys, proprietary restitution is not possible but there is the possibility for a claim against the third party for pure economic loss. This claim could also be possible against the exchange even in a situation where no third party service is used, as a way of attempting to obtain a remedy where the hacker cannot be traced. However, given the strict interpretation applied to claims for pure economic loss in English law, it is very unlikely that the relevant assumption of responsibility would be found to lie with the broker. It was not the negligent act or omission of the broker or the exchange that led to the misappropriation in the case of a hack, similar to the Bitfinex situation.[13]

Therefore, the most effective remedy remains a proprietary restitution claim, or a possible contract claim against the exchange for breach of terms and conditions depending on the circumstances of the misappropriation.

PROTECTING THE KEYS FOR THE FUTURE

In the wake of the Bitfinex hack and the large scale misappropriation of cryptocurrency, the legal analysis of the legal title in cryptocurrency and the appropriate remedies following misappropriation are even more important. It is paramount that the English courts adopt the correct analysis of the nature of cryptocurrency as individually identifiable pure intangibles, thereby enabling both the cryptocurrency lending market to function with certainty.

Individually enumerated multi-signature wallets with keys controlled by different parties, such as those used by Bitfinex, may continue to be popular in the cryptocurrency market, especially when trading or lending to fund trading. This way of holding cryptocurrency requires a careful analysis of the location of legal title, constructive delivery of the cryptocurrency and any liens that might exist over the wallet. Without such an analysis, trading and lending to fund trading in cryptocurrency will become too legally uncertain for users of each exchange, even if it is regulated by the appropriate securities laws.

Moreover, as the risk of online hacking increases, it is particularly important to understand the remedies available to users who have lost cryptocurrency as a result of a hack. Loss sharing is not appropriate in these situations, unless it is clearly written into the terms and conditions of the exchange. Since cryptocurrency is individually identifiable and not analogous to money in an online bank account, losses should only be suffered where they fall and not imposed on all users. Proprietary restitution remains the best remedy against those that misappropriated the cryptocurrency, although it is important to consider potential alternative remedies against the exchange and third party service providers especially when those that misappropriated the cryptocurrency cannot be traced.

Overall, the hack of Bitfinex leading to the misappropriation of 120,000 Bitcoins provides many lessons for the cryptocurrency market and its legal foundations, including the understanding of the proper remedies users can avail of in the situation of misappropriation. It is also likely to encourage the market to price risk more realistically when trading cryptocurrency, increase the usage of "cold storage" for private keys and improve understanding of what impact multiple private keys have on the ownership rights for one wallet of cryptocurrency. ■

1 G Devasini statement to The Whale Club, 4 August 2016.
2 BFXNA INC. d/b/a BITFINEX, CFTC Docket No 16–19.
3 See eg Goymour & Watterson [2012] LMCLQ 204.
4 CNBC, 40 banks test Bitcoin tech for trading bonds 3 March 2016.
5 See further Lucy Chambers [2016] 5 JIBFL 263 and Peter Susman QC [2016] 3 JIBFL 150.
6 Bitfinex Announcement, August 6, 2016.
7 Bitfinex Announcement, October 13, 2016.
8 See Reuters, Can Bitfinex Really Impose a $72 Million Theft on Its Customers? August 15, 2016.
9 See *Armstrong DLW GmBH v Winnington Networks* [2012] Bus LR 1199 and Lucy Chambers [2016] 5 JIBFL 263.
10 See eg Goymour & Watterson [2012] LMCLQ 204.
11 *State of Florida v Michell Abner Espinoza* No.F14- 2923, 651 Fed. Appx. 898 (11th Cir.2016).
12 See *Westdeutsche Landesbank Girozentrale v Islington London Borough Council* [1996] AC 669).
13 *White v Jones* [1995] 1 All ER 691, 716.

Further Reading:

- The legal aspect of virtual currencies [2016] 11 JIBFL 569.
- Misappropriation of cryptocurrency: propelling English private law into the digital age? [2016] 5 JIBFL 263.
- LexisPSL: Banking & Finance: Blockchain: mitigating or aggravating regulatory risk?