ALLEN & OVERY

11 Aug 2016

Bitcoin theft highlights cryptocurrency regulatory uncertainty

Speed read

The recent suspension of trading on Hong Kong based Bitcoin exchange Bitfinex following the apparent theft of approximately US$60m worth of bitcoins is the latest in a series of Bitcoin thefts. With Bitcoin still in its relative infancy, some jurisdictions have taken steps to integrate Bitcoin into their financial regulatory system, while regulators in Hong Kong have not yet done so. With Bitcoin increasingly having real-world impact on everyday citizens, the question of how Bitcoin regulation should be approached becomes increasingly pressing.

CONTENTS

Background

On Tuesday 2 August 2016, Bitfinex announced that hackers had stolen 119,756 of clients' bitcoins (worth approximately US$60m at the time of the theft). Hong Kong based Bitfinex was the largest US dollar-denominated Bitcoin exchange globally. Bitfinex suspended all trading, withdrawals and deposits on the exchange pending further investigation – no further detail concerning the cause of the incident is available at the time of writing. The US dollar value of bitcoins fell over 20% in the immediate aftermath of the announcement, as the market processed the significance of the theft to the on-going development of Bitcoin.

The theft is the latest in a series of hacking and theft incidents globally that have affected Bitcoin wallets and exchanges. The most notable incident of this type occurred in early 2014, when Tokyo based Bitcoin exchange Mt. Gox suspended trading and entered bankruptcy protection, following the theft of approximately US$450m worth of bitcoins. In Hong Kong, the March 2015 collapse of Bitcoin exchange MyCoin resulted in losses of over HK$150m to investors in Hong Kong and Guangdong.

How can a theft occur if the technology is supposedly 'un-hackable'?

A key feature of Bitcoin is the assertion that the technology is 'un-hackable'. So how can thefts such as those described above occur if Bitcoin is 'un-hackable'? It is helpful to look more closely at how Bitcoin transactions work to better understand how Bitcoin thefts occur.

SECURITY OF PRIVATE KEYS AS THE WEAK-POINT IN BITCOIN SYSTEM

Bitcoin uses a form of cryptography known as public key cryptography, employing key pairs comprising a public key (which can be disseminated widely) paired with a private key (which are known only to the owner). Each bitcoin is associated with its owner's public key. To effect a transaction, the owner creates a message specifying the public key of the transferee and the number of bitcoins to transfer, and the message is then signed using the owner's private key. It is said to be impossible with current technology for a private key to be derived from a public key or a signed message. As such, the transaction can be broadcast to the Bitcoin network for all to see while remaining secure.

Bitcoin wallets, which may be software on a physical device such as a computer or mobile phone, or a service provided by an online platform, generate, store and manage public private key pairs. A Bitcoin wallet is loosely likened to a bank account in a traditional banking setting. Bitfinex operates a Bitcoin exchange, where users can trade their bitcoins for real-world currency.

To keep the private keys secure, access to Bitcoin wallets is usually restricted (i.e. by a password or PIN) and the private keys themselves encrypted. Therefore, in practice, a Bitcoin transaction usually requires:

1. a Bitcoin wallet password, to gain access to the wallet;
2. one or more public keys with bitcoins associated with it; and
3. corresponding private key(s).

The security of the private key is vitally important, and hackers have exploited this weakness to access the account and carry out transactions as if they were the owner.

To further bolster private key security, Bitfinex required two private keys for any Bitcoin transaction. This is theoretically more secure as the private keys can be stored separately. It is unclear at this stage how the Bitfinex theft was carried out given this multi-signature technology.

Mandated Sharing of Loss

On 6 August 2016 Bitfinex announced that losses sustained in the hacking attack would not be restricted to the wallets of users that had been affected, but a generalised loss of 36.067% would be distributed equally among all users of the platform. Users will also receive a 'token' that will be transferrable and in time repaid by Bitfinex or exchanged for shares in its parent company. This development raises further questions about the legal characterisation of Bitcoin property rights, and issues of segregation of users' assets.

Global Regulatory Approaches to Bitcoin

CHALLENGES IN BITCOIN REGULATION

The nature of Bitcoin presents considerable challenges to the traditional legal and financial regulatory system. Bitcoin operates on a decentralised, peer-to-peer basis. There is no central authority nor set of rules, nor any central record keeping system.

The anonymity of Bitcoin transactions and the lack of any central repository of transaction records present money laundering issues. The Securities and Futures Commission (**SFC**) issued a circular on 16 January 2014 highlighting the particular money laundering risks presented by cryptocurrencies, and requiring heightened money laundering compliance processes in transactions concerning cryptocurrencies[1]. The Hong Kong Monetary Authority (**HKMA**) also highlighted the money laundering risk in a 9 January 2016 circular[2].

Global regulatory focus to date has generally been at the point where cryptocurrencies and real-world currencies are exchanged. The European Union has raised the idea of a register of Bitcoin addresses linked to real world identities, with the possibility of a reporting obligation for exchanges and custodial wallet providers and self-reporting by users. Any such measures, however, are only in the early stages of discussion.

BEGINNINGS OF A REGULATORY REGIME

The United States Treasury regards Bitcoin as a 'convertible decentralised virtual currency', and has been actively enforcing United States law and regulation on that basis. A United States District Court Magistrate Judge has also recognised Bitcoin as a currency in a Securities and Exchange Commission enforcement action[3]. On the other hand, a Florida state court has recently concluded that Bitcoin is not money for the purposes of that state's legislation.

New York adopts a formal licensing and regulatory system for Bitcoin and related business activity. In September 2015, the United States Commodity Futures Trading Commission (**CFTC**) defined 'virtual currencies' as commodities covered by the Commodity Exchange Act, and therefore the trading of bitcoins in the United States is subject to CFTC regulation[4]. United States regulators are keen to regulate Bitcoin, though further legislative and judicial clarification is required before the legal position is settled.

In Japan, following the Mt. Gox collapse in early 2014, the Japan Financial Services Agency (**JFSA**) assumed regulation of 'virtual currencies' and their exchange. Virtual currency exchanges are required to register with the JFSA, and cryptocurrency specific regulation may be imposed.

Other major jurisdictions are at varying stages of recognition and regulation of cryptocurrencies. Two regulatory approaches appear to be emerging. One approach has been to define cryptocurrencies as a subject matter to which the existing regulatory framework applies. The second approach has been to introduce a new form of licensing and crytocurrency specific regulations.

Comment

At this stage, the HKMA has clarified that Bitcoin is not legal tender, but a 'virtual commodity'. Bitcoin and other similar virtual commodities are not currently regulated by the HKMA or SFC. So far, Hong Kong regulators have focused on AML risks, requiring financial institutions to assess the heightened risk associated with virtual commodities in complying with the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615).

This recent incident shows that cryptocurrencies present broader issues than AML risk. Users of cryptocurrencies suffering losses can file a criminal complaint and pursue civil remedies. Any such process may be complicated by the legal and regulatory uncertainty regarding cryptocurrencies, challenges in cross-border enforcement and, where relevant, insolvency.

As cryptocurrencies gain wider acceptance among the public in Hong Kong and elsewhere, future incidents may create increasing real world financial impact. We await with keen anticipation Hong Kong's answer to these challenging issues.

---

[1] www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC2

[2] www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20140109e1.pdf

[3] SEC v. Trendon T. Shavers and Bitcoin Savings and Trust, 416 (E.D. Tex. 2013).

[4] www.cftc.gov/PressRoom/PressReleases/pr7231-15

Contact information

Fai Hung Cheung
Partner, Hong Kong fai.hung.cheung@allenovery.com

Charlotte Robins
Partner, Hong Kong charlotte.robins@allenovery.com

Lian Chuan Yeoh

Counsel, Singapore lianchuan.yeoh@allenovery.com

Benjamin Crawford
Counsel, Hong Kong benjamin.crawford@allenovery.com

Ryan Middlemas
Associate, Hong Kong ryan.middlemas@allenovery.com