The impact of the Bitfinex hack on cryptocurrencies

On 2 August 2016, Bitfinex - one of the world's largest digital currency exchanges - was subjected to a hack that resulted in the theft of nearly £60m worth of bitcoin. Adrian Shedden and Lucy Pegler of Burges Salmon explain the impact of the hack on cryptocurrencies.

Cryptocurrencies are alternative currencies that employ cryptography to encrypt the ownership (and transfer) of their digital value, and thus secure financial transactions made using them. Taking the example of Bitcoin, these are 'coins' that are earned (or 'mined') through the solving of 'blocks' of algorithm, achieved through software performing computations to decipher these algorithms and discover new bitcoins. Encryption is then attained through a pairing of a set of public and private 'keys,' which are used by the owner to transfer currency from their online wallet to another user's wallet.

Cryptocurrencies (also known as 'virtual' or 'digital' currencies) hold a value, and this value can fluctuate according to market demand. They can also be used in return for other items of value, originally only via the internet, but now increasingly they are being accepted for goods and services in bricks and mortar locations.

Unlike traditional, or 'fiat' currency, cryptocurrencies are not generally held centrally and their value is not attributable to, or 'backed,' by anything. They are stored on a distributed ledger, (such as a blockchain) and their ownership and transfer thereof is authenticated by multiple sources, being other users on a blockchain (a multi-validated distributed ledger, to secure and validate transactions). These transactions, in particular the process of performing the necessary mathematical solutions to 'mine' for currency, require computer software and a certain (large) degree of computer power. As a result of this distributed network of validation and security, the necessary computer power required to forge or hack the transfer of cryptocurrencies is significant.

The increasing popularity of cryptocurrencies is partly being attributed to a growing generation of innovative and technology-savvy consumers. Due to their decentralised nature, cryptocurrencies have also gained a following from those distrustful of traditional financial institutions, driven by a desire to retain some privacy over their daily activities and transactions. Though not fully anonymous, cryptocurrencies are pseudonymous in their ownership, providing users with increased levels of privacy. This has in itself been subject to much discussion, particularly in the context of the 'dark web' where cryptocurrencies have facilitated the covert acquisition of various illegal goods and services. Cryptocurrencies are yet to be widely regulated (with limited exceptions of, for example, Bitcoin licensing). Transfers from wallet to wallet are secured by the encryption discussed above, and payments are made and received based upon this process, which ultimately has its foundation in trust in the system and process - not only as to the value of the currency, but also to its ownership and legitimacy. When things go wrong, the support to assist with trouble is currently more limited than with fiat currency, as was discovered last month with the Bitfinex hack.

The Bitfinex hack

Bitfinex is a cryptocurrency exchange based in Hong Kong. Dubbed 'the world's largest and most advanced cryptocurrencies exchange,' it facilitates the trade of Bitcoin and other cryptocurrencies to and from US dollars. On 2 August 2016, 119,756 bitcoins were stolen during a hack that targeted portions of random users' online wallets. The amount represented 0.8% of all bitcoins and equated to nearly £60m.

Following the hack, the structure of Bitfinex accounts' wallets has been called into question. The structure combines a multi-signatory (or Multi-Sig) system with BitGo (a Bitcoin wallet provider), whereby Bitfinex holds two of the three keys necessary to authorise a transaction relating to each user account (one online, one offline), with BitGo holding the third (an online key). Automatic limits dictated that BitGo had to sign off transactions that were irregular or excessive in size. For reasons unknown, this structure was circumvented, enabling large quantities of bitcoins to be transferred freely.

In an attempt to calm its customers and manage the burden of the attack, Bitfinex opted to distribute the cost of the attack across users' accounts, to take a share of the 36% of losses, and provide a 'BFX Token' of credit equal to each user's personal loss, which will ultimately be exchanged for repayment or for shares. Commentators have already questioned this move, both in terms of its legality but also in commercial terms by enforcing a likely unpopular fine on their users. At a period of less than favourable press for this exchange, with many other exchanges more than willing to seize the opportunity of marketshare, Bitfinex might be treading a fine line in terms of retaining its users.

The impact of the hack

Value of Bitcoin

The value of Bitcoin dropped significantly (nearly 20%) following the theft and, curiously, in the days leading up to the attack. This prompted speculation about an information leak revealing the hackers' intentions. The reactive decline in market price was perhaps to be expected, as with a crisis in any market. However, such a major deterioration is perhaps also reflective of the lack of confidence in appropriate resolution mechanisms (such as regulation and enforcement) to guard against operational and counterparty risk in these embryonic monetary systems. There is an expectation (or hope) that events like this might act as catalysts to develop appropriate safeguards, build trust and confidence in cryptocurrencies, and ultimately settle Bitcoin's (and other cryptocurrencies') value, pegging it at a more realistic (and hopefully sustainable) level.

Trust in cryptocurrencies

Hacks damage confidence in the cryptocurrencies and stunt their growth and adoption in mainstream financial transactions. Conversely, it may be that this effect is ultimately felt less than is currently expected (and less than would be expected in the context of a traditional fiat currency exchange), due to the nature of the existing market of users. With Bitcoin in its infancy, it attracts a certain type of investor, and conceivably, they will be perhaps more open to the types of associated risks that manifest themselves in hacks - so this attack is perhaps just another in a series of many that make up the turbulent birth of an emerging technology, or indeed a promising alternative currency for the future, and the investors who traded before, will continue to trade again, in spite of this attack. Equally, increasingly damaging attacks will lead to increasing engagement by regulators and legislative bodies as well as attempts to regulate cryptocurrencies to ultimately decrease the attacks and their impact on consumers and the financial system.

If the Multi-Sig model is found to have contributed to the security weaknesses that allowed the hack, other Bitcoin exchanges using its technology may reconsider their preferred solutions

Trust in exchanges

The scrutiny that Bitfinex has come under in the wake of this attack may also lead to a more general scrutiny of cryptocurrency exchanges. There will be greater acknowledgement of the flaws in the concept of being 'trustless' (something upon which decentralised currencies rely heavily), given the serious effects when it goes wrong. There may well be greater demand for security and perhaps in return a greater willingness amongst users to comply with KYC requirements (with the price of reduced privacy of transactions perhaps being worth the increased capability to track misappropriated cryptocurrencies).

Though increased levels of security do pose threats to accessibility, models such as Multi-Sig, which is employed by Bitfinex and Bitgo, enable a balance of security and accessibility. However, by increasing one, the other may suffer - the rationale behind these multiple passwords, as well as the system of storing some online and some offline, is borne from the objective of facilitating password systems securely whilst maintaining accessibility.

Trust in security providers

The practices of Bitcoin security providers might too come under fire in light of this hack. If the Multi-Sig model is found to have contributed to the security weaknesses that allowed the hack, other Bitcoin exchanges using its technology may reconsider their preferred solutions.

What's next?

As there is no such thing as an unhackable system, it is likely that, even with tougher security, we will see more hacks akin to Bitfinex.

Cryptocurrency exchanges are not necessarily less secure than traditional banking but at the core of these hacks are unregulated and largely unsecured investments. Ultimately these investments are made at the investors' risk. As with Bitfinex, there is no statutory compensation scheme and any losses arising from a successful hack have to be recognised and absorbed by the investors themselves. The fact that the exchanges are typically under-capitalised means that avoiding bankruptcy means distributing the costs as with Bitfinex. However, this is unlikely to be an acceptable proposition for most mainstream investors looking to invest savings.

The practical implication of this is that it is unlikely that cryptocurrencies will form the basis of mainstream financial transactions for the time being. Whilst technological innovation will continue to march on at pace, it is likely that we will start to see more regulatory developments targeted at cryptocurrency exchanges (as is already the case with proposals to extend the application of AML frameworks to cryptocurrencies, for example). Only when this happens are cryptocurrencies likely to become a viable alternative for those looking to invest outside of mainstream banking.

Adrian Shedden Senior Associate
Lucy Pegler Associate
Burges Salmon LLP, UK
adrian.shedden@burges-salmon.com
lucy.pegler@burges-salmon.com