

How cyber security is failing cryptocurrencies

Investor Daily
23rd August 2016

On 2 August 2016, a hack of cryptocurrency exchange platform Bitfinex resulted in the theft of somewhere between 120,000 and 200,000 bitcoins with a total estimated value of up to US\$70 million.

The attack followed two smaller scale thefts from other bitcoin exchanges earlier this year, and the largest reported hack, of the Tokyo-based Mt. Gox exchange, in 2014.

In the immediate wake of the latest hacking attack, the value of bitcoin plummeted by 20 per cent, recovering almost 18 per cent two days later.

However, Bitfinex evidently intends to 'generalise' losses among its users by charging them approximately 36 per cent of their account balances.

Think for a moment of the likely reaction if a bank reacted to a theft from one of its branches by charging its entire depositor base a fee of 36 per cent of their account balances.

This highlights a stark difference in the level of customer protection between the cryptocurrency world and the traditional currency world.

Depositors with digital accounts have losses that are seemingly arbitrary and patently unfair imposed on them, while those with traditional accounts have their deposits protected by guarantee.

A rapid pace of innovation, often referred to as disruption, is an increasingly common feature of the modern business world.

No area has been left untouched, with disruption becoming pervasive to the extent that it is impacting the world's exchange-of-value mechanism, namely money.

Professor David Yermack of the New York University Stern School of Business, and a presenter at a recent Centre for International Finance and Regulation (CIFR) seminar on blockchain and the future of finance, has observed that throughout history money has been an ever-changing concept.

However, there remain three characteristics that are essential to any form of money.

Firstly, it must facilitate a ready comparison of the relative prices of different goods (ie, it must serve as a unit of account).

Secondly, it must be universally accepted as a medium of exchange.

Thirdly, money must be a reasonably stable store of value. People will only accept money if they are confident of the purchasing value it will provide them over a reasonable period of time.

Rapid advances in technology in recent years have led to plastic cards complementing paper as a form of money.

Since World War II, credit and debit cards have gone from being non-existent to arguably the most widely used form of commercial exchange.

Notice how contactless payWave technology is advertised as the smart and efficient way to pay, with traditional currency exchange portrayed as being archaic.

Digital technology in the payments system has now taken a further step, with the introduction of so-called cryptocurrencies.

However, recent events may mean that predictions that cryptocurrencies herald the imminent demise of traditional forms of currency may be unduly hasty.

The Bitfinex case undermines the merits of cryptocurrency as a form of money.

A precipitous loss of value and excess short-term volatility in value mean that bitcoin fails two of the three essential characteristic tests of money.

With regard to money being a readily accepted medium of exchange, it appears that bitcoin again records a fail.

Despite its apparently fashionable appeal, bitcoin has attained only a niche acceptance and continues to be regarded with scepticism more broadly.

It is essential that a well-functioning payments system, and a broader financial system, be characterised by integrity, efficiency, confidence and stability.

In this context, we as Australians should be justifiably proud of our financial system.

Nevertheless, our sound situation should not be a cause for complacency. We must remain alert to the potential emergence of risk.

To sustain confidence in our system, we should be asking whether our banks have been the target of attacks similar to that on Bitfinex, and if so, how have they responded.

The banks, in common with many large companies, run sophisticated security operations centres, designed to safeguard the integrity of transactions and customers' details.

It would be reassuring to see evidence of the banks' ability to counter hacking attacks such as that on US retailer Target in late 2013, when the credit card and personal details of up to one in three US consumers were stolen.

The misadventure of the 2016 Australian national census further highlighted the vulnerability of digitally-based systems to hacking attacks.

Amid acrimony over who was responsible for the system failure, one salient point becomes patently clear: providers of online services, whether financial or otherwise, need to ensure that system integrity remains a key priority if they are to retain the faith and trust of the using public.

David Gallagher is the chief executive of the Centre for International Finance and Regulation.