Cybersecurity Challenges in Japan's Cryptocurrency Market

In December 2017, the price of a bitcoin was more than USD 19,000 – nearly fifteen times the price for an ounce of gold. But while gold is a physical object that can be held, traded and used to make products and jewelry, bitcoin and other cryptocurrencies exist only digitally and derive their volatile prices from their perceived value in a still-forming market. With bitcoin and other crypto-currencies much in the news recently, we provide this introduction to cryptocurrency issues in Japan.

What are Cryptocurrencies?

History of Bitcoin

According to Bitcoin.org, "Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen."

Bitcoin was launched in 2009 – the year after the 2008 Financial Crisis – but gained widespread popularity from 2011 onwards. Essentially, bitcoin is a digital currency not backed by the promise of a government. There are no people or entities in the middle brokering deals, controlling or policing the money, or setting exchange rates. At the risk of broad generalization, early adaptors of Bitcoin tended to have anti-establishment, libertarian mindset; recently, however, Bitcoin adoption has become much more widespread, if not yet mainstream.

The earliest known reference to "cryptocurrency" – in other words, a digital currency that uses cryptography to secure its transactions – is a note authored by Wei Dai in 1998 on a cypherpunks[1] mailing list suggesting the idea of a currency that uses cryptography instead of a central authority to control its creation and transactions. However, the starting point for bitcoin is a paper authored by an individual or group using the pen name Satoshi Nakamoto. In the paper, Nakamoto proposed the use of a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

The main attraction of bitcoin was that users would not be subject to unwanted or unnoticed charges common with other payment methods. In addition, bitcoin does not give personal information to sellers in the event of a transaction, reducing the risk of identity theft.

Rise of Alternative Cryptocurrencies

The popularity and increasing difficulty of acquiring bitcoin has led to a rise in alternative cryptocurrencies, or "altcoins." In addition to bitcoin, the website CryptoCoinCharts lists 4,599 different cryptocurrencies. However, the space is extremely dynamic and it is unclear which of these cryptocurrencies have undergone initial coin offerings or are still active.

While bitcoin has the image of being an anonymous form of currency – hence its use as the currency of choice on defunct online black-market Silk Road – all transactions are publically available on the bitcoin blockchain's ledger. For this reason individuals dealing in illicit drugs and child pornography have instead turned to more secretive cryptocurrencies such as Monero, which hide everything from transaction origin addresses to transaction amounts.

blackpeak

The Rise and Fall of Mt. Gox

One of the first bitcoin exchanges was Mt. Gox, which was founded by Jed McCaleb, an American software developer. Originally the website name was short for "Magic: The Gathering Online eXchange," a platform for a popular trading card game developed more than 20 years ago. McCaleb soon transitioned Mt. Gox into a bitcoin exchange in July 2010, implementing balances, deposits and withdrawals using the order-matching system that was already in place from the card exchange business. The revamped website allowed trading between bitcoin and local currencies and was the first of its kind, according to investigative journalist Jake Adelstein's book "Pay the Devil in Bitcoin: The Creation of a Cryptocurrency and How Half a Billion Dollars of It Vanished from Japan," which he co-authored with Swiss-Japanese journalist Nathalie Stucky. McCaleb sold the exchange to Frenchman Mark Karpelès.

In February 2014, Mt. Gox filed for bankruptcy protection in Tokyo. According to a crisis management strategy document that was leaked to the public, the company had lost 744,408 bitcoins, a shortage that went unnoticed for several years.[2] Shortly before his arrest, Karpelès somehow "found" 200,000 bitcoins in a "cold wallet," slightly lessening the amount of total damages in losses.[3]

A "cold wallet" is a hardware or even a USB stick not connected to the internet. It can technically be stored in a safe or locked in a desk and is considered virtually impossible to hack. The opposite of a "cold wallet" is a "hot wallet" which is a digital account connected to the internet. Most knowledgeable cryptocurrency investors choose to store a small amount of funds in a hot wallet for day-to-day use, and the remaining majority in a cold wallet.

Adelstein notes in his book that when Karpelès purchased Mt. Gox from McCaleb, the website had already suffered frequent thefts. According to some sources Adelstein spoke to, a bitcoin theft occurred the day Karpelès acquired the site. McCaleb wanted the matter "kept under wraps" and convinced Karpelès to sign a nondisclosure agreement. While it is possible that more details will be released as the police investigation continues, according to Adelstein and Stucky's book, sources close to the Japanese police believe that more than 80,000 bitcoins may have already been stolen by the time McCaleb sold Mt. Gox.

Since the downfall of Mt. Gox, much has changed in Japan's bitcoin scene. On 25 July 2017, Russian citizen and bitcoin exchange operator Alexander Vinnick was captured in Greece and was accused by the United States of obtaining funds stolen in the Mt. Gox hack. In addition, the Japanese police who handed Karpelès's case were forced to admit to the judge that they had not even bothered to investigate the cause of the Mt. Gox hack and only investigated charges that they felt would "stick," such as embezzlement – which, even then, were "dubious" charges, according to Adelstein. Adelstein adds, "This case took two years to go to court and was dragged out for months because it was such as poor case."

Recent High-Profile Hacks

The Mt. Gox heist, which was the biggest of its time, hasn't stopped other exchanges from popping up to fill the void – or hackers from seeking vulnerabilities to make quick cash. In August 2016 hackers managed to obtain access to private keys held by Hong Kong-based Bitfinex to steal 119,756 bitcoins (USD 75 million based on August 2016 prices). In 2017, South Korean exchange Bithumb lost USD 6.99 million in funds in a hack suspected to have originated from North Korea; in the same year, North Korean hackers used malware to target popular cryptocurrency exchange YouBit and stole 4,000 bitcoins. As of December 2017, YouBit had filed for bankruptcy in South Korea.

However, the most recent – and notable – hack in Japan was the January 2018 heist of Coincheck, a Tokyo-based cryptocurrency exchange, which lost over USD 500 million in NEM – another cryptocurrency built on blockchain technology – coins. This loss topped the Mt. Gox hack, making it the largest cryptocurrency heist in history. Although the investigation into the hack is ongoing, according to experts from Israeli cybersecurity firm Cyberess S&T, it appears that the hackers exploited two missing features in Coincheck's security system that a reputable cryptocurrency exchange should have had in place: multi-signature security and the use of a "cold wallet" rather than a "hot wallet" to store large amounts of funds.

Multi-signature security is a measure that requires multiple sign-offs before funds can be moved. The technology requires more than one cryptographic key to execute a transaction, a process similar to the multifactor authentication used to access a secure e-mail account.

Cryptocurrency environment in Japan

Promotion by the Japanese government

Prior to Mt. Gox's bankruptcy filing, the Japanese government exercised essentially no oversight over virtual currencies. The Mt. Gox scandal spurred the Japanese government into introducing regulations into the cryptocurrency industry, but instead of outright banning it, the Japanese government, normally known for being a slow decision-maker, embraced digital

currencies, setting itself up as the world's de facto cryptocurrency capital. In 2017 Japan became the first country to regulate cryptocurrency exchanges on a national level. As of 7 March 2018, there are 16 companies officially recognized by the Japan Financial Services Agency as virtual currency exchanges.[4]

"Japan has wanted to be the cryptocapital of the world since 2014, and one of the reasons why is because Abenomics has failed. Inflation hasn't gone up, wages haven't increased and Japanese people aren't investing in the stock market – though I do note that foreign investors are," according to Adelstein. "However, cryptocurrencies have young and old, men and women investing, and because Japan has a surprisingly lax and tolerant policy towards cryptocurrency, it is becoming a center for cryptocurrency and for people who want to talk about cryptocurrency."

Recent crackdown by the Financial Services Agency ("FSA")

Despite the recent Coincheck hack, it doesn't appear that the Japanese government will change its stance when it comes to promoting the use of bitcoin, according to Adelstein.

Prior to the hack, Coincheck was a "quasi-virtual currency exchange". In other words, it had not yet technically received a license from the FSA to operate a cryptocurrency exchange, but was taking money from customers and conducting transactions. This was allowed as long as Coincheck did not state on its website and marketing materials that it was a licensed exchange. As of February 2018, there were 15 so-called quasi-virtual currency exchanges in Japan, not including Coincheck, whose operations were suspended during that period.[5]

For now, it appears that Coincheck is safe from outright collapse. It has reimbursed victims of the stolen NEM funds and has partially resumed trading. The Japanese government wants to keep the site running – and for a good reason, according to Adelstein: "It distracts people from the failure of Abenomics. If people are interested in Japan, they will invest in Japan. If Coincheck goes under, everyone will flee the Japanese cryptocurrency market for a while. The Japanese government seems to be keeping Coincheck from collapsing."

Cybersecurity Challenges in Japan

Regulatory Issues

While being the first country in the world to recognize cryptocurrency exchanges on a national level may offer some first-mover advantages, the challenge for the Japanese government is that they have no precedent to follow when it comes to accrediting cryptocurrency exchanges. They can't regulate them the same way they treat banks, or "they might as well start issuing Morgan Stanley Coin," joked Adelstein.

"The biggest problem is setting up a system to license exchanges that can do sufficient checks on the people who sign up on its platform, and that they make sure that the exchanges have a system in place that can do those checks," said Adelstein. He added, "The [FSA] also needs a system in which they can approve these exchanges on a regular basis."

Lack of talent

One major problem holding Japan's cybersecurity industry back is the lack of peer-to-peer and cryptocurrency engineers, in addition to PhD holders, which Japan is unable to generate locally. It is estimated that for every 10 job vacancies, only one qualified person is available to fill it.

That leaves Japan with no choice but to look abroad for its talent. Japan obtains most of its foreign talent from France, China, Poland and notably Israel – the latter is considered to be the world's cybersecurity hub. The immigration process is relatively smooth for engineers recruited from abroad, since the candidates tend to have a good educational background and job experience and the Japanese government is open to allowing more foreign engineers immigrate to the country.

Security Issues

One area where Japan lags behind other large markets is in security awareness. For example, in 2017 Japan Airlines was defrauded out of USD 3.7 million due to one of its employees failing to verify an e-mail claiming to be one of the companies it leases aircraft from and requesting that payments be directed to a U.S. account rather than the usual Hong Kong account.[6]

One Mt. Gox hack (there were several) carried out in 2011 was allegedly caused by a compromised computer belonging to a company auditor. Such issues can be prevented through regular IT training programs and company-wide phishing exercises to target employees who have clicked on links, opened files or leaked sensitive company information and require extra guidance. Additionally, background checks for entering employees and measures to prevent data theft for departing or even current employees should be put in place.

In addition, since cryptocurrency is a new industry, nearly all the companies in the field are startups lacking the infrastructure to identify and prevent hacks. In startups, bring-your-own-device (BYOD) policies or using generic, store-bought devices are popular trends. While convenient, these policies pose security risks. If employees can compromise the storage of private keys, or otherwise inject their own address into the company's withdrawal process, once the coins go out the door there's little hope of seeing them again, other than on the blockchain.

Adelstein and Stucky wrote in their book that when Karpelès came to Japan for the first time he was impressed by the efficiency of the country and the honesty of its people. He could leave a laptop on a park bench unattended and come back to it later to find it untouched – not a wise idea for the CEO of someone handling millions of dollars in client money. For bitcoin to be successful in Japan, its technology and financial sectors will have to be a little bit less trusting. Ronen Almog, the CEO of Cyberess S&T, stresses that "employees need to be vigilant and make sure that their employees will not fall victim to emails containing malware or phishing attacks that will trick them into downloading malicious script or scams."

References

[1] A cypherpunk is an activist who advocates the widespread use of cryptography and privacy-enhancing technology to promote social and political change.

[2] https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/

[3] https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on

[4] https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf

[5] https://www.fsa.go.jp/policy/virtual_currency/09.pdf

[6] https://www.japantimes.co.jp/news/2017/12/21/business/japan-airlines-bilked-%C2%A5384-million-getting-bogus-emails-seeking-lease-fees/#.WrtIGZNubBI

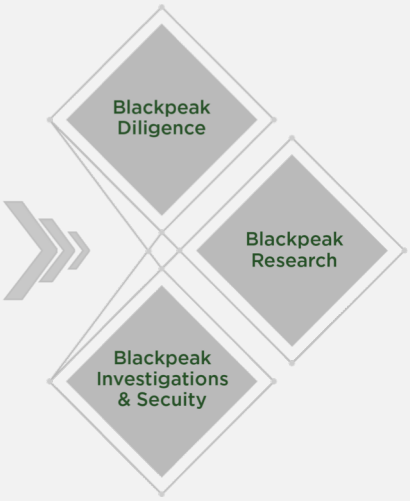
About Blackpeak

Blackpeak is an international investigative research firm.

Founded in Asia, the firm now operates from strategic locations in key financial and economic centers, including Hong Kong, Singapore, Tokyo, Shanghai, Beijing, Guangzhou, New York and Washington DC.

We handle highly complex research assignments, including integrity due diligence, internal and external investigations, asset searches, business intelligence for institutional and hedge fund investors, stakeholder mapping, political risk research and more.

Over 400 clients rely on Blackpeak's services, including the world's leading investment banks, corporations, law firms and asset managers.



Key Contacts

Tokyo

David Suzuki

dsuzuki@blackpeakgroup.com
+81 3 6455 5306

Washington DC

Thomas Pellman

tpellman@blackpeakgroup.com
+1 202 747 4947