Pandora's box opened by Bitcoin, threats of new types of crimes

Itsuro Nishimoto, Director and Chief Technology Officer (CTO) of LAC

Jan 22, 2014 7:00

A virtual currency of Bitcoin is becoming a breeding ground for crimes. Bitcoin spread rapidly as it can also be exchanged for Dollars and Yen through exchange offices on the internet. There are increasing crimes committed by cyber-criminals who have noticed that, such as mining or theft of Bitcoin by abusing other persons' computers. While the next-generation currency, which does not need to be bound by financial institutions such as central banks, provides consumers with new convenience, it also exposes risk of troubles that would not have occurred in the past.

*Speculative money inflows, transactions heat up

The virtual currency of “Bitcoin”, which spread rapidly.

With fluctuations in prices.

A short time ago, a computer virus became a hot topic among specialists. It's a virus called "ransomware", and requires a ransom. Computers can get infected with this virus when clicking a file attached to an e-mail or accessing a manipulated website. It viciously makes the computers unusable by encrypting the stored data without permission, and requires a ransom for clearing the encryption. The ransomware itself previously had been existing, but specialists were amazed at the fact that Bitcoin was specified as a method for paying a ransom of 100 Dollars.

Bitcoin can be briefly explained as a currency created by making full use of digitization. Unlike the existing currencies for which banknotes

have been issued, Bitcoin can be "mined" by solving a certain numerical formula. The more the amount of Bitcoin issued is increased, the more the numerical formula becomes complex so that it becomes more difficult to mine. This is a measure implemented to prevent Bitcoin from exceeding a certain amount for stabilizing the value of the currency. The unit of this currency is BTC.

The number of the stores that accept Bitcoin is increasing. (Vancouver, Canada) = Reuters

Bitcoin also has a characteristic that it has exchange rates for currencies including Dollars. Bitcoin had had almost no value when it had come into the world in around 2009, but at the beginning of last year, 1 BTC had risen to 14 Dollars, and the transactions heated up after that. The Cyprus financial crisis in March served as a trigger for generating a lot of attention toward Bitcoin. The Cyprus government decided to impose a tax on bank deposits, and there was a rush of behaviors of choosing Bitcoin as an escape for assets. The concerns about Euro also helped boost the price of BTC to around 240 Dollars.

After the beginning of November, a flurry of news reports saying that the FRB approved Bitcoin as a currency and the speculation that Bitcoin would be useful for protecting assets in China, where exchanges for foreign currencies have been limited, caused an outbreak of the "Bitcoin bubble". The price of Bitcoin jumped up to 1,200 Dollars during the bubble. After that, China's central bank prohibited exchanging Bitcoin for Renminbi, and the U.S. Department of Commerce submitted a warning statement that Bitcoin would be included in the list of items subject to restrictions to Bitcoin dealers. Then, the Bitcoin dropped down until its price reached around 500 Dollars at the end of the year, but has been soaring again since the start of the New Year. The situation where nobody can predict the

future rates of Bitcoin, has been continuing due to inflows of speculative money caused by the repeated rises and falls in the price.

It is surmised that the creator of the ransomware specified Bitcoin as a method of payment because it allows transactions of money to be accomplished without leaving a trace such as a banking record. The issue is that, with cross-remittance through Bitcoin, money laundering is not difficult.

*Illegal acquisition of coins using viruses.

Neither a government nor a central bank is an issuer of Bitcoin.

It can be a target for criminals. = AP

One of the current attempts of cyber-gangs, who are sensitive to smell of money, is trying to acquire Bitcoin illegally by infecting a large number of computers with a virus for mining it. The mechanism of acquisition of Bitcoin is that it can be obtained as an asset by solving a certain numerical formula, and the numerical formulas used to be simple enough to be computed on computers that were available for ordinary people. However, as the numerical formulas have been getting complicated as the quantity of Bitcoin in circulation has increased, and currently, it is difficult to acquire without massive amounts of computational resources. Recently, it is considered that it takes a computer one year or more to mine Bitcoin.

Then, a method of having a virus solve numerical formulas on other people's computers without their permission and sending all of the results to the criminal side has been devised. If 400 computers are infected with the virus at once, one BTC can be earned in one day, and 10 BTC can be obtained on 4,000 computers. By converting the amount at the current rate of 1 BTC = 976 Dollars, the effectiveness of this method in making money quickly can be imagined.

According to a survey conducted by Trend Micro, which sells anti-virus software, in Japan, computers that have been infected with viruses for illegal mining account for 24.02% of the total. This is the highest level in the world, ahead of the U.S., in which 21.34% of computers are infected. It is well conceivable that in the future, a criminal will take control of a supercomputer in a research institute for a short period of time for earning Bitcoin.

Another method devised by criminals is theft of Bitcoin. A computer that has been using Bitcoin from a long time ago may have a large reserve of Bitcoin. It should be easy to take an opportunity to search for Bitcoin possessed by a computer when infecting it, and steal the Bitcoin when found. This is because in Bitcoin transactions, when a "wallet is replaced", the later wallet is recognized as an authorized one. Also, the mechanism does not allow it to be returned to the original wallet. Like cash, the ownership of Bitcoin belongs to the person who currently possesses it.

*The stance to defend ourselves has been important.

Recently cyber robberies, boldly, targeted at exchange offices, have also occurred. More vicious cases are that Bitcoin exchange offices aimed at fraud have been established. They are, so to speak, vicious exchange offices, where the customers collected under the advertisement that their Bitcoin can be exchanged for Dollars or Yen are exploited. In the future, if authorized exchange offices are excluded by governments, which watch out the circulation of Bitcoin, that may raise the possibility that false exchange offices will be increasingly widespread.

It is more appropriate to call Bitcoin "virtual gold coins" rather than the expression of the virtual currency or virtual notes. To say a little roughly, the circulation of Bitcoin is like the appearance of a mine where a gold coin supported by a certain numeric formula has been buried, on the internet. This mine came into the world by a paper released by a person who introduced himself as "Satoshi Nakamoto" in 2008. Characteristics, such as its theory, the strength of its cryptography, and the mechanism of ensuring its reliability by all participants, have contributed describing Bitcoin as a product of the digital society.

The crucial point is that Bitcoin has proven the possibilities of being able to discover a "mine" where an enormous asset is buried, and control the world with the availability of a "reliable numeric formula". Pandora's box may have been opened. When the second and third Bitcoin is generated respectively, we will be forced to fight with crafty cyber criminals. But we can never lose. As we protect our wallets by ourselves, each of the consumers needs to take a stance of protecting the wallets on the internet at their own responsibilities.