# ‘It is a global problem’

Cyber-security expert **Aditya K Sood** explains to **Suman Guha Mozumder** the dangers digital currency poses to governments and people across the world

Aditya K Sood, senior security consultant, IOActive, says online currency transfer business companies like Liberty Reserve, which was indicted in the United States in a $6 billion money-laundering scheme, are becoming an alternative to the global banking system.

The basic concept, he adds, is to start with a fiat currency — an established national currency — like the US dollar or the Euro and convert it to an intermediate digital currency until the transaction is over, at which point the currency is converted back into  fiat currency.

“It is true that according to the terms of use digital currencies are not to be converted by recipients for use of criminal activities or money laundering,” he says. “But these restrictions are essentially unenforceable and that is how money laundering is taking place.”

Sood is a PhD candidate studying underground economy at Michigan State University, and has worked in the security domain for Armorize, COSEINC and KPMG.

**How big is the problem of underground economy in the United States?**

I won’t say that it is a problem related only to the US. It is a global problem. If you talk about e-currency, the question is where does this come from and where does it go? Where are the organizations that actually perform e-currency transactions? The Liberty Reserve was based somewhere in Costa Rica.

And WebMoney, another e-currency company, is based somewhere in Russia. The problem is big for those countries where actually the money is being extracted from, including the US.

The problem persists at the point where cyber attackers actually steal critical or sensitive information of different users and use that information to carry out monetary transactions. To do that they use what we call e-currency. So from the country perspective it is a big problem for the US, but it is also a big problem for countries all around the world.

## The Business Interview
## Aditya K Sood

**Can governments play a role in preventing this?**

Yes, governments can play a role. But we have to understand two points. Why did e-currency come to exist? The major idea behind e-currency is that these organizations do not actually want to pay huge taxes and transaction fee that is levied by different credit cards companies, or for banking transactions.

It is a big problem that the government is facing because all the money in these kinds of transactions is not reported to the financial intuitions or the regulatory bodies like the Internal Revenue Service.

So it is easy money or black money that is going in and out of the system. The government has to play a critical role. In the US, the laws are pretty strict. Still, it took seven to eight years to prosecute Liberty. The problem is that these organizations, which perform e-currency transactions, are actually private institutions residing outside the US, in countries where cyber laws are not that strict.

So there is a time lag here. The US government has to work with other governments around the world to actually come to a point where they can prosecute these criminals. But still they will have to wait a couple of years because they need to get all that information before they can prosecute these criminals.

In the Liberty Reserve case, they have taken down the system and that is only because the government has taken steps and has worked with foreign governments. The US has lost a huge amount of money not because of e-currency but for the kind of money and goods that have been transacted without being reported to the IRS or government regulatory authorities.

**You just mentioned cyber lag. All you need is an e-mail address, fake or original, to transfer the money. How does it work?**

There are two actors in this. The first are the exchange-makers who actually exchange your currency for e-currency. And then we have e-currency providers who have a particular set of exchange-makers, who are actually legitimate bodies, exchanging money at the current rate.

When you need to send money you have to register or have to go in person to these exchange-makers and have to register an account. Or maybe you can talk with them on the phone to initiate the process. They will say $1, for example, equal to one WebMoney dollar or one Liberty Reserve dollar and charge you some percentage of the money being sent.

Only recognized exchange-makers are allowed to perform e-currency transactions. From a cyber attacker’s perspective it is not hard to fake their identities and provide all the information and credentials to initiate transactions.

**But even cyber attackers need to have an account with exchange-makers for e-currency. How would they do that?**

As I said, once they have accessed information from a legit institution about a guy and validate that you are the same guy, you will be allocated an account number, which is used for storing money.

Remember until and unless an exchange-maker takes a step and converts e-currency into fiat currency, it is useless. E-currency can be stored and the recipient can take out any amount at any time. But if it is not converted to fiat money, if the system is taken down the stored money is gone.

Until and unless an exchange-maker goes to take out the money, or the government takes rigorous steps to move forward and force exchange-makers to convert money, the money is usually gone.

**Can you elaborate on exchange-makers?**

Exchange-makers have their policies and they present themselves as trading companies, saying that they just exchange money. There is actually one system out there that makes this happen. Unless and until you want to exchange the money, there is no way you can get the money out.

It is a game of ping-pong where everybody is trying to push the ball to another person’s court. They have set up policies in such a way that you have just exchanged money and the money has gone into another system. The big problem is that all these transactions are irreversible in nature. And you do not know who to prosecute.

**There are many money transfer companies here, say, for India. How safe it is for people to send money that would be converted from dollars to rupees?**

You need to use an authentication system. If you use legitimate banks like the State Bank of India, it will get into your account one way or the other. There is a possibility that whatever interest you earn on that they

▸ Page A17

◂ Page A16

are going to report it to the government.

Similarly, for PayPal, you need to have an account and you need to have a proper checking account in your bank.

But in other cases, you send money and they will give the money only in cash. They do not send the money to a person's bank account. So there is no record and even if there is one it could be deleted. So that is the problem. There is no authentication when you register with e-currency. It is actually black money because it is not reported to the government. That is why the government is worried.

**How do then people send money to Swiss banks, black or white money?**

Swiss banks work in a different way. There you hold your currency in fiat currency, which is declared by a government to be legal tender. You can actually make exchanges, for example Indian rupees into Swiss currency, but there is no intermediate currency in between like e-currency.

Also there is a different way an account in a Swiss bank can be opened. The only thing is that they do not divulge account holders' information because of compliance rules.

**So are you actually transferring money when you talk about e-currency? Suppose one has an account with a recognized bank, the bank will ask the sender about where the money is being sent, right?**

That is a pretty good question. Yes you actually transfer money. But a sender can evade surveillance because the exchange-makers have legitimate bank accounts and so you can transfer inter bank.

Exchange-makers have usually different bank accounts. When you send money to an exchange-maker, banks do not want to know anything except whether the exchange-maker has an account with them or not.

Since exchange-makers have accounts with banks, they would not question the sender about anything else. Exchange-makers would admit that they have got the money from another legitimate account holder in a bank.

The problem starts after hackers have compromised the account, because banks would not know who the actual actor is. So it is basically open to hackers who can reset notification, passwords sitting in another part of the globe.

**Can't something be done about it technologically?**

Yes. Actually there are various organizations that are building some production mechanism to disrupt the flow. In computer parlance, one has to stop the error at the top; if we are not able to do that, it will keep on increasing.

We have to detect those kinds of malicious codes before they can extract all the information.

Solutions are being built but it is a kind of arms race. They (*cyber attackers*) know how the Internet works and that is why it has become a potential problem.

**But many companies provide Internet security against virus attacks, etc.**

The problem is that the companies that are building defense mechanisms do not know about malicious codes until and unless they are discovered.

Banks too are trying hard to build different policies and have fraud-detection teams or fraud-prevention teams, given that the underground economy in the US is a multi-billion-dollar and lucrative industry for criminals all over the world.

There are parallel systems like Liberty out there.

Cyber attackers have already built a market place and have built systems, which are completely automated using Botnet, a collection of Internet-connected programs communicating with other similar programs in order to perform tasks.

This use can be as mundane as keeping control of an Internet Relay Chat channel, or it could be used to send spam e-mail.

**What drew you to cyber security?**

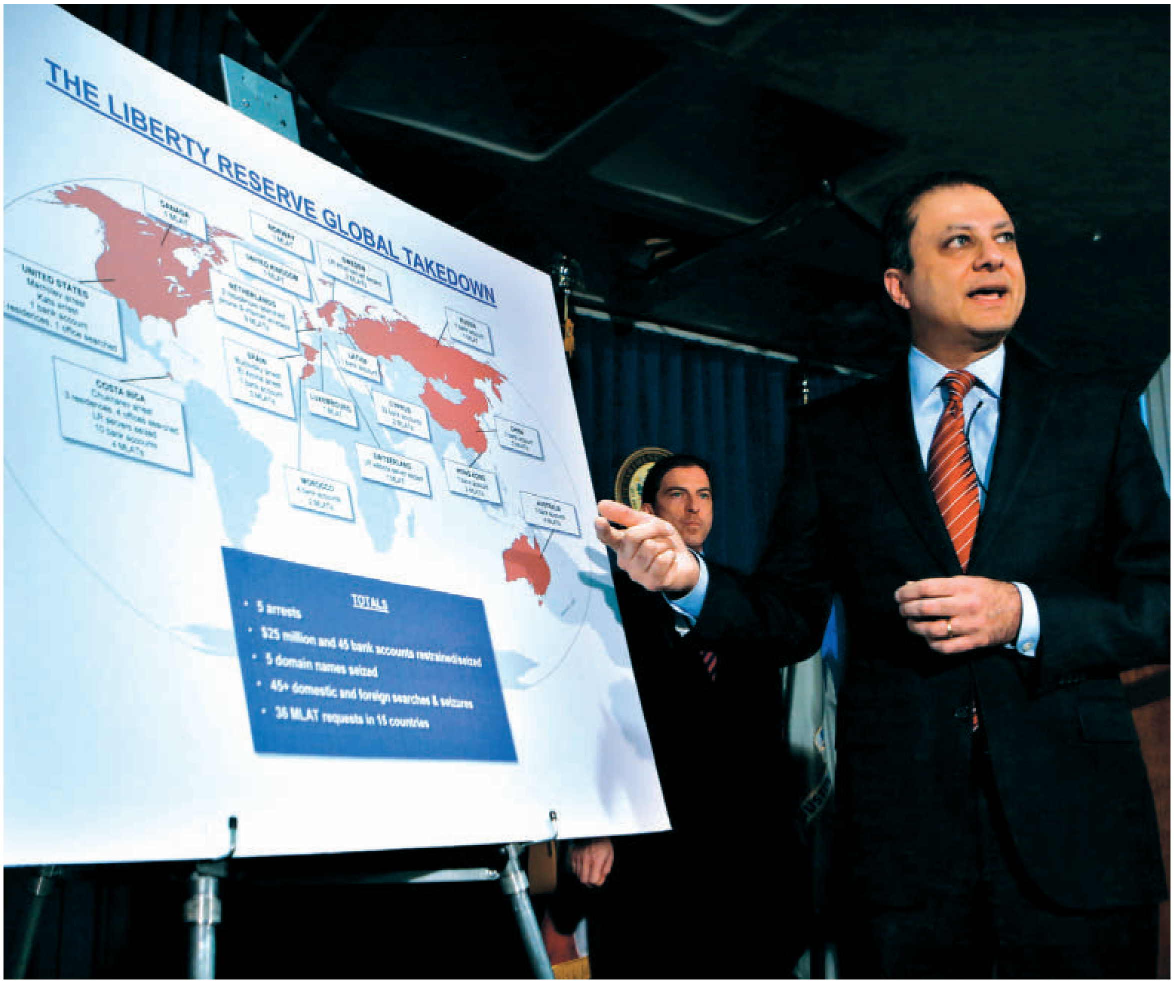
We are building technology but how many users understand the technology and its pros and cons? That is one big problem from the users' point of view. We take a step forward and start using technology right away without understanding the pros and cons.

You cannot expect every user to be technology savvy. That is why it is important to understand where people are sending their information and what could be the consequences of that.

Security is very important while using technology. There is a dearth of cyber-security professionals and we need to have cyber-security solutions.

To answer your question, security is something that motivates me and we have to build products. We need to take care of people's privacy and their security as more and more people are using technology these days.

We have to make sure that information does not fall into wrong hands. I want to be someone who will provide security to people who are using new technologies and to protect them from cyber criminals.


THE LIBERTY RESERVE GLOBAL TAKEDOWN
TOTALS
5 arrests
$25 million and 45 bank accounts restrained/seized
5 domain names seized
45+ domestic and foreign searches & seizures
36 MLAT requests in 15 countries

MIKE SEGAR/REUTERS

Preet Bharara, United States Attorney for the Southern District of New York, describes charges against Costa Rica-based Liberty Reserve, one of the world's largest digital currency companies, May 28. The company and seven of its principals employees were indicted in the US for allegedly running a $6 billion money laundering scheme.

# 'It is a global problem'