**Manhattan District Attorney Cyrus R. Vance, Jr.**

**Testimony Before the Department of Financial Services**

Hearing on Digital Currency – Remarks as Prepared

January 29, 2014

Good morning Superintendent Lawsky and members of the Department of Financial Services. I am New York County District Attorney Cyrus R. Vance, Jr. Thank you for the opportunity today to discuss the criminal implications surrounding digital currencies.

As a young ADA, I prosecuted cases that had yellow tape blocking off a physical crime scene in Manhattan. While many Assistant District Attorneys in my office continue to prosecute these kinds of cases, we also face a newer and still emerging threat, as the internet becomes a global, boundary-free crime scene of the 21st Century. The internet provides cybercriminals with anonymity, which makes the task of investigating and prosecuting crime that is committed using cyber techniques more difficult.

Exploiting digital currency payment systems is no different. The anonymity offered by these payment systems attracts criminals who can now more easily move, conceal, and launder their illicit profits. My Office has investigated and prosecuted these kinds of cases, and I will highlight two momentarily. While we have and will continue to aggressively prosecute individuals who use digital currency to facilitate their criminal activities, we need stronger tools to combat new emerging threats derived from these payment systems.

Without stronger government oversight, we are allowing cybercriminals, identity thieves, traffickers of child pornography, and other malevolent actors to operate in a digital Wild West. Therefore, it is my position that digital currency exchanges should be required to obtain licenses as money transmitters in order to do business in New York State, and therefore, come under this regulatory framework.

This action by itself, however, would not be enough. I also ask that digital currency exchanges be required to perform enhanced due diligence with regard to the identification of their customers.

Let me give you two concrete examples of cases from my Office where digital currency was used to facilitate criminal activity:

Last year, my Office secured convictions against 14 members of a major cybercrime ring that crisscrossed the globe, from Russia, Ukraine, and Moldova, to the Czech Republic to California to Brooklyn. The ring trafficked nearly 100,000 stolen credit card numbers, resulting in more than $5 million in credit card fraud. One of the top defendants in this case was sentenced to 22-to-44 years in prison – just one example of how seriously the criminal justice system is now taking these types of crimes.

At the center of this international criminal organization was a corporation based in Manhattan called Western Express. The company served as the principal digital currency exchanger for the trafficking ring, allowing the buyers and sellers of stolen credit card information to move money anonymously using two types of digital currencies, E-Gold and WebMoney.

Briefly, this is how the trafficking operation worked:

- The buyers of stolen credit card information used Western Express to exchange U.S. Currency (in the form of cash or money orders or other structured payments) into E-Gold or WebMoney.
- The buyers then took this digital currency and used it to buy stolen credit card information from the vendors. They used this stolen information to manufacture forged credits cards, which they used to purchase merchandise online and in stores, and then fenced those products online or on the street for profit.
- The vendors needed to convert all the E-Gold and WebMoney they received as payment for stolen data either into a different digital currency, or into conventional currency. They used Western Express for this purpose.
- Western Express also facilitated the global flow of digital currency for criminal activity,

to the tune of $15 million dollars, and sent bank wires around the world.

- Western Express charged a fee for every transaction that it facilitated.

Similarly, in 2006, my Office prosecuted a company called Goldage, a digital currency exchanger operated by two men who moved millions of dollars for their customers.

Here, individuals used Goldage to exchange Egold digital currency. When purchasing Egold, customers could choose their method of payment to Goldage. Specifically, they could wire money, make cash deposits, or mail postal money orders and checks. When selling Egold to Goldage, customers could obtain payments through wire transfers to accounts anywhere in the world or have checks sent to individuals anywhere in the world. Goldage's owners charged customers a fee on both ends of the transactions and maintained various bank accounts under the guise of different subsidiary companies.

In both of these cases, the fact that the defendants ultimately converted digital currency back into cash helped investigators to trace the money. But now that retailers, both large and small, are starting to accept digital currency as payment, criminals might not have to convert their illegal proceeds back into cash. For example, criminals can use digital currency to buy high-end merchandise from major online retailers, and then sell those products for cash. Or they can simply refrain from ever converting their digital currency to cash, simply continuing to finance criminal conduct and engage in business, whether criminal or legitimate, using such currency. This makes it even more difficult for law enforcement to trace their transactions.

An even greater challenge to law enforcement may be the emergence of Bitcoin ATMs, in which individuals can insert dollars and get Bitcoins in return. Unlike users of debit or credit cards, the identification of Bitcoin ATM users can remain untraceable.

I want to note that I am not taking a position on the legitimacy of digital currency as a method of payment for goods and services. Additionally, I recognize that many digital currencies are not specifically designed to attract illicit activity.

But in this ever changing technological landscape, our laws have to keep up with reality. Digital currency is quickly becoming a part of our mainstream economy, bringing along with it criminals who exploit the gaps in our regulatory and criminal justice system. Law enforcement must be given appropriate updated tools to address criminal behavior as it actually exists today.

Under current law, money transmitters must comply with anti-money laundering requirements. Financial institutions facilitating deposits and withdrawals of large amounts of cash must file Currency Transaction Reports with FinCEN. Cross-border movements of large amounts cash also require governmental reporting. These valuable filings allow law enforcement to identify and investigate potential suspicious activity.

There should be no ambiguity that digital currency exchanges that transmit value act as "money transmitters," and are therefore required to comply with the same licensing, reporting, and anti-money laundering regulations imposed on banks and other money exchangers. This is consistent with numerous prior prosecutions conducted by my Office.

And there is no question that digital currency providers act as a medium of exchange in the sale and purchase of goods and services. Therefore, it is my opinion that the nature of a transaction in which digital currency is purchased is indeed a form of money transmission, no different than where a buyer directs a bank to send money to a vendor.

Furthermore, digital currency exchanges should be required to perform enhanced due diligence with respect to their customers' identification.

Digital currency exchangers, at minimum, should be required to do the following:

- Maintain records relating to transactions.
- Obtain customers' identifying information. This includes requiring a customer to provide his real name, his physical address, the name of his business, and the nature of that business. The customer should also be required to confirm that the "digital wallet" in which the currency is being sent is actually owned and controlled by the customer.
- Implement procedures to ensure the accuracy of this information – for example, that the

address is actually owned and controlled by the customer. This would help with the chain of custody in establishing who is receiving the digital currency.

- File periodic applications in order to do business. These filings should identity the owners and mangers of the exchange, and those principals should make sworn affirmations as to the accuracy and truth of the filings.

As we have seen in so many cases, digital currency is being used by bad actors to commit very serious crimes – multi-million dollar identity theft rings, child pornography, underground markets for drugs, guns, and other contraband.

The federal government is starting to bring digital currency exchangers under their regulatory umbrella. New York State should also recognize the dangers of these payment systems. It should be made clear that digital currency exchanges must be licensed as money transmitters in order to do business our state. We must also adequately supervise the exchanges to ensure that their customers are providing proper identification and are not using the exchanges for criminal activities. And we must also act to ensure that unlicensed digital currency exchangers are identified and prosecuted.

Thank you. I'm happy to take your questions.