STATEMENT OF

BITS PRESIDENT PAUL SMOCER

ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

THE UNITED STATES SENATE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE AND
SUBCOMMITTEE ON ECONOMIC POLICY

NOVEMBER 19, 2013

TESTIMONY OF PAUL SMOCER, BITS PRESIDENT

Thank you Chairmen Warner and Merkley, Ranking Members Kirk and Heller and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am the President of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the US financial system.

The financial services market constantly evolves and matures to reflect the explosive growth of technological capacity, entrepreneurial innovation and consumer needs and preferences. The topic of today's hearing, "Virtual Currency," has been and continues to be an area of focus for our member companies and within the industry. As virtual or digital currencies have evolved, our members discuss the potential benefits as well as potential drawbacks – particularly drawbacks related to security, fraud and consumer impact. My testimony today will cover the evolution of digital currency, as well as opportunities and risks.

Digital Currency Evolution

Since the commercialization of the Internet, the concept of digital money has held intrigue. The terms "virtual currencies" and "digital currencies" are the generally accepted vernacular terminology used to identify forms of electronic currency that can be used to effect transactions involving true goods and services.

Attempts to develop digital currencies, and the methodologies used to exchange them for value, have existed for several decades. For example, in the 1990s, we saw attempts such as NatWest's Mondex card, which was an attempt at creating an electronic cash card that acted as alternative to coins and banknotes, and DigiCash Inc., which was an electronic money corporation founded by David Chaum. The regulatory community has also been thinking about this subject for some time. For example, in September 1996, the United States Department of the Treasury held a conference entitled "Toward Electronic Money and Banking: The Role of Government" that explored this issue. Until recently, however, attempts to launch digital currencies have been unsuccessful. What makes today's environment different and enhances the probability of success in launching digital currencies? The answers to that question include:

- Consumers are much more comfortable in transacting online through traditional financial systems as well as other vehicles such as online games that leads consumers to an increasing overall comfort with the online world.
- Computer systems are more powerful and less expensive thus facilitating some of the processing intensive techniques associated with emergent digital currencies.
- A growing interest in having an international currency free of some of the factors such as exchange rate considerations, inter-currency transactional fees, etc.
- The increasing desire for privacy.
- The general cache that some attach to the concept and to innovative developments on the Internet.
- And sadly, but realistically, a desire to facilitate illegal activities such as money laundering, fraud, and terrorism financing.

This has allowed a market for, though still on a limited basis, digital currency and the development of some infrastructures to support the exchange of digital currency.

Bitcoin is often the focus of digital currency discussions as it is the largest independent digital currency. Bitcoins are created through a digital process, "mining", which involves computer programs working on the same set of data to solve a puzzle. Across the Internet, a Bitcoin is mined every 10 minutes through this process with allegedly a maximum of 21 million allowed in circulation. Once mined, the owner is able to use his or her Bitcoins at any participating merchant and the transactions are tracked through a public ledger known as a block chain, which identifies users by a unique code. Bitcoin users review these ledgers to validate transactions and to ensure that users are spending existing Bitcoins. These transactions operate outside of the traditional payments system. Thus, they would not intersect with credit card, ACH or other trusted financial services networks. The system is not run by any one entity or company, but rather is supported by participants in the Bitcoin environment.

Unlike depository accounts held in traditional financial institutions, Bitcoin ownership is not associated with any named individuals. Owners of individual accounts are recognized by unique codes intended to assure their anonymity. Even the creator of Bitcoin is considered anonymous. Its creation is often attributed to a Satoshi Nakamoto, though it is speculated that this is actually a pseudonym for an anonymous individual or group of anonymous web developers. In general, Bitcoin provides a decentralized system, using peer-to-peer networking, digital signatures and cryptographic proofing to enable funds transfers between participants.

Other entities in the digital marketplace, such as Ripple, rely on the efficiencies of the Internet by developing an open source digital transaction protocol. Ripple uses existing currencies or valuable items (e.g., airline miles), which are converted into its internal currency called XRP. Users can then quickly transact within XRP. Individuals can convert funds back to a monetary value by selling the

XRP. Similar to Bitcoin, Ripple includes an open ledger to allow all participants to see the activity of the system and validate transactions, again with individual accounts recognized by a unique code. These transactions also would not cross the traditional payments, but could leverage the existing funds in a financial institution consumer's account as an individual could directly transfer dollars into their Ripple account. A unique feature of Ripple is to allow individuals to provide loans to others within the network. Individuals establish their own ability to trust different users and decide how much they would like to loan the individual. In addition, a trust score can be assessed to different users.

Opportunities

As we think about the opportunities associated with digital currencies, I believe we need to think of them in two distinct areas – the concept of the currency itself and the infrastructure mechanisms being created to exchange them.

We have witnessed the concepts of new, emerging currencies before. Some have noted that even within our country, the creation of new currencies was an early part of our history as the states, regions, and even merchant exchanges established currencies. What makes digital currencies different is that they allow the concept of cash or a cash equivalent to be used over the Internet. That fact, in turn, essentially makes them a global form of currency.

One measure of a currency's success is its acceptability. An emergent trend is that institutions such as international and large retailers are beginning to accept select digital currencies as payment for goods and services. For example, in November 2012, the web publishing service WordPress announced they would accept Bitcoin as a form of payment for WordPress upgrades. Interestingly

too, just last week, we all became aware that the Federal Election Commission is seriously considering letting candidates and committees accept Bitcoins as in-kind contributions. Given digital currencies today rely neither on government-sponsored central banks nor have the backing of any national currency, merchant acceptance and certainly acceptance by government agencies tends to help these currencies establish their legitimacy and increase the trust parties have in them and their stability in the marketplace. At this point, however, the established financial services industry still does not generally recognize these currencies as broadly accepted.

One important aspect to recognize is that, as digital currencies become more internationally accepted, there is a growing recognition of their ability to increase international sales opportunities and their ability to facilitate simpler international funds transfers. Returning to the WordPress example of retailer acceptance, WordPress found the acceptance of digital currencies allowed it access to new consumers in countries where traditional payment systems do not permit access for financial, security or international sanction reasons.

Because of the ability to work internationally and outside of existing markets, some suggest digital currencies also have the ability to provide affordable access to the unbanked on a global scale. For example, a mobile phone based money transfer and microfinancing service in Kenya backed by Kenya's largest two mobile network operators called M-Pesa, recently added a Bitcoin payment option for customers in Kenya.

In addition, digital currencies can assist individuals in countries with repressive regimes to support causes or efforts that they might otherwise not be able to support. For example, in certain countries where citizens fall under strict government control, individuals can often not donate to or purchase from sites that are banned by their country's traditional payments providers. These transactions are

made easier using decentralized, unaffiliated, anonymous currencies with their own payment infrastructures. Because of this, often times digital currencies are referred to as a "censorship-resistant" currency.

If digital currencies reach a state where their economic stability is more assured, they can also function as an outside currency that can provide additional economic security for individuals living in a country whose own currency is under financial distress. For example, during the recent Cyprus and Argentina financial crises, citizens transferred funds to digital currencies, mostly Bitcoin, to provide a more steady assurance for the security of their funds.

The infrastructure supporting digital currency payments has some appealing quality to merchants also due to the lack of interchange fees. For many, digital currencies can provide a lower transaction cost to the benefit of both merchants and consumers. Digital currencies may be more attractive to merchants as many do not allow the payments to be reversed, so there is no opportunity for chargebacks.

Another interesting aspect related to certain digital currencies is their cryptographic protections. Ostensibly, the cryptography is intended to provide a level of security that both helps limit the amount of a currency in circulation and to bolster their providers' claims that their currencies cannot be duplicated or counterfeited. The currency providers also claim that the financial information about any particular user's wallet (e.g., their identity, their balance) is anonymous and, therefore, more secure than in other Internet-based financial transaction environments. If these claims hold true, which is questionable, this could be very significant for the future of monetary security.

In summary then, digital currencies and their supporting infrastructure do indeed present opportunities that we are closely watching. They could provide a model for how to facilitate real-time payments – particularly those involving international parties and those involving micropayments. They offer some opportunity to explore deeper cryptographic options for Internet-based transactions and they may offer opportunities to serve more effectively the under-banked and those who are truly politically repressed.

Risks

While the opportunities noted above have piqued the interest of the financial services industry in digital currencies, we also have to recognize a plethora of potential risks.

First, digital currencies pose significant market risk. Without government funding or support, digital currencies may be subject to extreme market volatility. The participants in the market itself have to decide the worth of each currency. Given the immaturity of the market, slight changes in the market can produce significant swings in value. In addition, the value of items purchased could change drastically and there would not be a single arbitrator to provide final decisions as to the value of the currency. Bitcoin is the best example of market volatility. Since its creation four years ago, the market has gone through several significant swings in value, including in 2011 when the value fell 90 percent from $30 to $3. Recently, its value took a steep dive again when the use of Bitcoins was associated with the alleged operations of the drug ring known as "Silk Road." While its value has bounced back, broad swings in value create significant risk to both holders of the currency and to merchants and others who accept the currency as payment. With an established currency, merchants can generally be assured that the payment they receive will be of equal value to the service or merchandise purchased. With a currency that can fluctuate wildly, there is significantly more risk and

little to no recourse for the merchant if the payment currency's value falls significantly. If the transaction happens to be international, the payment settlement methods used with established currencies do not apply. If, for example, one makes a purchase with a credit card issued in the US from a UK-based merchant, the payment infrastructure will convert the purchase price from British pounds to US dollars at a market rate and post that amount to the purchaser's account. The infrastructure to support this type of conversion is only in its infancy with the digital currency world. As well, we simply do not yet have enough experience to know if these currencies will even continue to exist. Many factors including broader acceptability will influence whether we see an increase or collapse in value of these currencies.

On the consumer side, the use of these currencies and the infrastructure exchange mechanisms they utilize are currently subject to few of the consumer protections we have come to expect in the traditional world of currency and payments. In addition, since these currencies do not carry clear and effective disclosures, even the most sophisticated consumers are unlikely to be aware of and understand the risks associated with them.

At this point, in the US, the Financial Crimes Enforcement Network (FinCEN) has taken the regulatory lead by creating its formal statement on digital currencies. This March 2013 guidance clarified the responsibilities of participants in the digital currency marketplace to register as money services businesses and money transmitters. Given the decentralized approach of the currencies, this requires registration by many individuals who previously did not consider themselves part of this network. Beyond this March guidance of FinCEN, digital currency providers have virtually no existing regulatory oversight. This is even more meaningful for currency providers and users operating outside regulated countries. Without regulations, these digital currencies are not providing

appropriate consumer protections to ensure individuals understand the risks much less are protected in ways we now take for granted. As examples:

- If the value in an individual's digital currency account is fraudulently stolen, the victim has no recourse to recover the funds. In fact, within the last two months there have been multiple reports of Bitcoin currency disappearances from various Bitcoin trading platforms. Some allegedly involved hacks into Bitcoin repositories. At least one allegedly involved the creation of an "unlicensed" repository into which Bitcoin owners deposited their funds only to have the repository suddenly disappear. In none of these cases is it expected that the owners will recover a single Bitcoin. Contrast that to the recourse available to a consumer who is a bank customer. If funds are fraudulently taken from the consumer's deposit account, the bank will make that customer whole. If an entire institution that is an FDIC-insured depository institution were to fail due to a major cyber-attack, consumers would generally be afforded protections that would allow them to recover a significant balance of their deposit accounts.
- If a consumer's digital currency account were used to make an unauthorized payment, laws that limit the amount of consumer financial responsibility and require investigation by the financial institution holding the consumer's transaction or credit card would not apply. The consumer would simply lose the value of the fraudulent payment.
- While there is an emerging trend in the regulatory community, led by FinCEN at the federal level, to consider the classification of certain parties in the digital currency world as money transmitters, laws and regulations that apply to funds transfers occurring through traditional financial institutions currently have little relevance in the digital currency world. There is no method for attrition or preemptively stopping the transfer of digital currency funds.

These types of fraud protections provided by the financial services industry have developed into an essential part of overall consumer protection. Without some level of parity, today's digital currency consumers are essentially unprotected.

It is important to note however, that while the digital currency market seems ripe for further oversight and regulation, the act of regulating it, in and of itself, adds legitimacy to the market.

Another risk related to digital currencies involves the fact that most digital currencies are stored in digital wallets that are associated with personal computers or devices. Once these devices are compromised, there are no additional ways for the consumer to access their funds. In addition to the fraud risks noted above, there have been several recent cases of hacks on digital wallets that hold digital currencies. These hacks use similar techniques to traditional hacking efforts we have seen in the financial services industry. For example, phishing techniques are used to gain access to a user's information needed for authentication.

It is important to recognize too that while FinCEN has taken some action and others at the federal and state levels are considering regulatory actions, currently none of the digital currency operators or infrastructure providers are subject to the intense level of regulatory oversight applied to regulated and chartered financial providers. They are not subject to any required regulatory standards regarding, for example, cyber security and data breach notification requirements that grew out of the Gramm Leach Bliley Act. They are not subject to the regulatory and best practices guidance issued by the Federal Financial Institutions Examination Council and its member agencies that they have developed over the last 20 years. Likewise, they are not subject to independent examination of their controls environments by any regulatory authority. Because digital currency transactions typically

occur within privately operated, unregulated networks, financial and security risk determination and mitigation is left up to the currency or infrastructure provider.

In addition, while many digital currencies tout that they are anonymous, they rely on a unique identifier for each account. Through analysis of transactions or confirmation by an individual, these identifiers could be connected with an individual. Given that digital currencies rely on a public ledger, the individual's transaction could become knowledgeable to individuals who have been identified.

Earlier I noted in the "Opportunities" section the ability for individuals to provide funds to legitimate organizations that their native country might inappropriately ban. This can also work in the reverse. Using digital currencies, individuals may also be able to donate to illegal organizations that would otherwise be legitimately banned by one or more governments. The ability for governments to ban payments to sites, for example, is a useful technique in thwarting illegal activity and terrorist funding.

Allowing digital currencies, particularly ones that by design are intended to provide full anonymity to the currency holders, has also invited their use for illicit activities. In fact, some recent studies suggest that the anonymous nature of digital currencies has made them a haven for illegal activity. The most notable recent example is the FBI case that resulted in the take down of Silk Road – an operation that allegedly was used to anonymously buy or sell illegal drugs, offer guns and assassins for sale, and provide tutorials on hacking ATM machines. The operation was completely reliant on digital currency for transactions. When this site was taken down, law enforcement had numerous challenges in seizing the funds of the site and those of Silk Road's alleged operators and customers.

The digital currency environment is also being used as a new way to launder money. A recent major example would be the situation involving the May 2013 indictment of Liberty Reserve. Liberty Reserve was a global currency exchange that allegedly ran a $6 billion money-laundering operation online ostensibly serving as an exchange for criminals engaged in various illegal activities. According to the prosecutors who presented the charges, Liberty Reserve was responsible for laundering billions of dollars, conducting 55 million transactions that involved millions of customers around the world, including about 200,000 in the United States. It is also important to note that all a user need to do to use the system was to provide a name, address and date of birth. However, unlike the Know Your Customer requirements that apply to traditional financial institutions, Liberty Reserve, being unregulated and incorporated outside the US, was not required to validate customers' identities. As the indictment stated, "Accounts could therefore be opened easily using fictitious or anonymous identities."

While the Silk Road and Liberty Reserve situations serve as examples, the point here is that digital currencies are being used to assist a broad array of criminal activities including illegal drug sales, stolen identities, child pornography, prostitution, human trafficking, and illegal weapons sales. It is also being used as a favorite of cyber criminals to pay for services such as developing and distributing malicious software to the movement of stolen funds resulting from account take overs.

One additional consideration is the level of clarity that currently exists regarding how virtual currencies will be treated within the tax code and whether virtual currencies offer an ability to evade taxes. In May 2013, the United States Government Accountability Office issued a report to the US Senate's Committee on Finance entitled, "Virtual Economies and Currencies, Additional IRS Guidance Could Reduce Tax Compliance Risks." The report suggests that the IRS should determine and subsequently address the need for additional tax guidance and additional taxpayer education.

The lack of regulatory oversight, the risks to consumers and the market risks associated with digital currency provide a continuing challenge to its overall legitimacy, usage and endorsement by the financial services industry.

Conclusion

In conclusion, there is no denying that the use of digital currencies will continue to evolve. Consequently, we will continue to discuss that growth and the associated opportunities and risks. As with the Internet and electronic commerce in general, we have seen innovations grow from early concepts where the risks outweighed the advantages to, over time, becoming an accepted norm. For now, I would opine we are not yet there with digital currencies. They do provide opportunities – or more accurately perhaps suggest areas of opportunity, but we will need to address the threats to consumers and society, the need for appropriate regulation and the effectiveness of risk mitigations. As the discussion continues, we would be happy to continue to participate, particularly where it would be advantaged by public-private collaborations such as through the Federal Reserve Banks study of the future of the payments system.

Thank you for your invitation to testify to the Subcommittees this afternoon. We look forward to continuing to work with you relative to this emerging technology.

#####