Commissioner Wetjen and other members of the GMAC, my name is Jerry Brito and I am the Executive Director of Coin Center, a recently launched non-profit research and advocacy center focused on the public policy issues facing digital currencies. Thank you for inviting me to participate in this forum.

I would like to provide some background on the technology we are discussing, explain some of the demand for derivative products, and answer any technical questions you might have.

Bitcoin is frequently described as a “digital currency.” While that description is accurate, it can be misleading because it is at once too broad and too narrow. It is too broad because Bitcoin is a very particular kind of digital currency--a cryptography based currency (indeed, it is the first of its kind). It is too narrow because although currency is one aspect of the Bitcoin system, Bitcoin is more broadly an Internet protocol with many applications beyond payments or money transfer. Think of it like email or the Web--an open network to which anyone can connect without permission from a central authority, anyone can send a message to anyone else, and on top of which you can freely build many different kinds of applications.

Online virtual currencies are nothing new. They have existed for decades. From World of Warcraft Gold to Facebook Credits. Neither are online payments systems new. PayPal, Visa, and Western Union Pay are all examples. So what is it about Bitcoin, and similar cryptography based currencies, that make them unique?

Bitcoin is the world's first completely decentralized digital currency, and it's the "decentralized" part that makes it unique. Prior to Bitcoin's invention in 2009, online currencies or payments

systems had to be managed by a central authority. For example, Facebook issuing Facebook Points, or PayPal ensuring that transactions between its customers are reconciled. However, by solving a longstanding conundrum in computer science known as the "double spending" problem, Bitcoin for the first time makes possible transactions online that are person to person, without the need for an intermediary between them, just like cash.

Comparing Bitcoin to traditional payments and money transfer systems helps explain the distinction. Before Bitcoin's invention in 2008, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or Bank of America. Intermediaries like PayPal keep a ledger of account holders' balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob's account.

Without such intermediaries, digital money could be spent twice.Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a perfect copy of the money file after she had sent it. She could then easily send the same $100 to Charlie.

Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the Bitcoin network is registered in this distributed **public** ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bitcoins have not been previously spent, thus eliminating the double-spending problem. The global

peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact online without a third party intermediary.

And how is this possible? With Bitcoin, transactions are verified, and double-spending is prevented, through the clever use of public-key cryptography. Public-key cryptography requires that each user be assigned two “keys,” one private key that is kept secret like a password, and one public key that can be shared with the world. When Alice decides to transfer bitcoins to Bob, she creates a message, called a “transaction,” which contains Bob’s public key and how many coins she is sending. She then “signs” it with her private key and broadcasts the message over the network. By looking at Alice’s **public** key, anyone can verify that the transaction was indeed signed with her **private** key, that it is an authentic exchange, and that Bob is the new owner of the funds. The transaction—and thus the transfer of ownership of the bitcoins—is recorded, time-stamped, and displayed in one “block” of the block chain. Public-key cryptography ensures that all computers in the network have a constantly updated and verified record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

Out of technical necessity, transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes bitcoin a virtual currency in addition to a decentralized public ledger. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies. The total number of bitcoins that will ever be issued, as well as the rate at which they are algorithmically released into the ecosystem, is not determined by any person,

company, or central bank, but has instead been predetermined at the time the protocol was established.

To date, bitcoins have represented money at a floating exchange rate, and the Bitcoin network has been employed as a fast and inexpensive payments or money transfer system. But there is no reason why particular bitcoins could not represent something besides money. If we conceive of bitcoins simply as tokens, then other applications become apparent. For example, we could agree that a particular bitcoin (or, indeed, an infinitesimally small fraction of a bitcoin so as to allow for many tokens) represents a house, a car, a share of stock, a futures contract, or an ounce of gold. Conceived of in this way, the Bitcoin block chain then becomes more than just a payment system. It can be a completely decentralized and perfectly reconciled property registry.

Bitcoin is therefore an open platform for innovation, just like the Internet itself. In fact, Bitcoin looks today very much like the Internet did in 1995. Some dismissed the Internet then as a curiosity, but many could see that such an open platform for innovation would allow for world-changing applications to be built on top of it. Few in 1995 could have foreseen Facebook or Skype or Netflix, but they could see that all the building blocks were there for some amazing innovations. Bitcoin is like that today. We can't conceive yet what will be the killer applications, but it's pretty obvious that they will come.

Bitcoin faces some challenges, however, and chief among them is regulatory uncertainty. If we think back again to the early Internet, it was not until the government made it clear that it would pursue a light-touch regulatory approach, that Internet innovation really took off. Bitcoin today is in need of a similar commitment from government.

In the case of financial regulation specifically, Bitcoin would benefit from the development of hedging instruments. As I explained earlier, Bitcoin's value is determined on an open market. That market is still developing, and it is not very liquid. As a result, it has been historically volatile. Merchants, merchant processing services, exchanges, and many other businesses who want to build on top of the Bitcoin platform are in search of good hedging instruments.

Additionally, as Bitcoin matures, its root technology--a cryptographically verifiable distributed ledger system--could be employed as a clearing mechanism in financial markets and other applications. While unprecedented, such a use of the technology could lead to important new efficiencies and innovations. As regulators begin to consider these developments, they should do so with an open mind avoid undue restrictions that could have unintended consequences, including limiting innovation.

Thank you for your time and I look forward to your questions.