Opening Statement for the House Financial Services Committee's Subcommittee on Terrorism and Illicit Finance

Written Testimony by Jonathan Levin, June 8th 2017

Introductory remarks

Thank you very much for the opportunity to speak to you this morning.

My name is Jonathan Levin and I am one of the Co-Founders of Chainalysis. Chainalysis is the leading provider of investigation software and risk management software for virtual currencies. In this field, we identify illicit use of virtual currencies, including terrorist financing. We provide tools to private industry and law enforcement to mitigate the risks that this activity poses to our society. Prior to my work at Chainalysis, I performed some of the first economic analysis of the incentives that power and secure Bitcoin, the most popular virtual currency.

I wish to prepare my briefing into three significant sections that I believe are worth considering in light of the potential risks that are posed by virtual currencies:

- **First, the potential of virtual currencies**
- **Second, the nature of the technology**
- **And finally, The current use of virtual currencies**

The potential of virtual currencies

The Internet has become the transport layer for all of our communications. It has fundamentally transformed how consumers, producers, friends, families and governments transfer information. The Internet started in the early 1960s but it did not enter the mainstream until the creation of an easy to use consumer layer with the Web and the availability of developer tools in the mid 1990s. Today, we probably almost all used the internet just prior to entering this room and will use it when this analogue session is concluded.

Many of the protocols and infrastructure that we use are now decades old and were pioneered mainly by academia and the government. The US government played an instrumental role in providing these essential layers for private industry to develop business models and products for us as consumers to use. The adoption of the internet by private industry required the use of payments, but these were not baked into the protocol layer of the internet and needed to be built on top.

Famously, value transfer and video streaming over the internet was pioneered by the adult entertainment industry and quickly criminals also saw this venue as a lucrative target for their criminal enterprises. The emergence of PayPal and other internet payment companies have built solutions on top of the internet, but nothing comes close to the native ability to move hypertext seamlessly between two machines anywhere in the world. This motivated the emergence of Bitcoin, which was released to the public in 2009.

Since 2009, the Bitcoin network has bootstrapped itself, and attracting over $1 billion in venture capital for applications being built on top of it. The current value of all virtual currencies exceeds $100 billion with daily liquidity across all the exchanges totaling approximately $4 billion a day. The main driver behind this trade activity is price discovery and speculation that virtual currencies present an opportunity to open completely new markets on the internet that disrupt the incumbent tech giants.

Decentralized internet protocols do not preclude the formation of centralized institutions over the top of them, think of decentralized protocols as providing interoperability between these institutions. It is possible to architect the existing web on top of these protocols and fundamentally new ways of sharing information and data between institutions. As such, we also need to recognize the new institutions that lie on top of these protocols and give them the appropriate regulatory framework and protections to operate within.

The history of virtual currencies is longer than simply Bitcoin, in the years before Bitcoin, there were centralized virtual currencies, such as Linden Dollars, the currency of second life or e-gold. With money laundering risk and financial stabilization concerns, some of these systems have come under regulatory scrutiny. These efforts can be ineffective at curbing demand and may serve to drive the activity underground. In 2007, in China, Tencent came under pressure from the

People's Bank of China to stop conversion between goods and services and Q Coin, a virtual currency issued by Tencent.

In February 2017, the People's Bank of China put pressure on the virtual currency exchanges to stop trading. This led to an uptick in Peer to Peer Bitcoin transactions that are out of the purview of the State. Trading on Local Bitcoins, which is just one of these sites, rose from ¥2.5m a week to over ¥100m. These peer to peer transactions cannot be regulated and diminishes the oversight that can be obtained by the state.

This technology has the potential to create a fundamental new layer for how we interact online where many of the existing institutions have similar roles to play and may benefit from new efficiencies. There is also the space for massively new applications that we haven't yet considered.

The nature of the technology

Bitcoin and other virtual currencies are decentralized and as such are censorship resistant. Receiving Bitcoin can be done by anyone with access to basic computing equipment anywhere in the world. There is no need to register or supply anyone with any identifying information. There is no ability to freeze assets or seize someone's virtual currencies without obtaining access to their private keys, which are their secret keys that only they have access to.

The same benefit that this affords entrepreneurs and software developers around the world to bring revolutionary new business models, it also offers nefarious actors the ability to abuse this technology. Transferring virtual currencies between people is done on a ledger that transcends national borders and current conceptions of identity. Virtual currency are ultimately bearer instruments. The person in control of a private key is the ultimate owner of the virtual currency.

In order to facilitate this system, Bitcoin makes every transaction public. These transactions are recorded in a single transaction ledger, the blockchain. However all of the entries in the ledger are pseudonymous and do not relate to any real world identities. The public broadcast of transactions permits third parties to be able to see certain aspects of these transactions and allow law enforcement armed with the right tools to patrol the virtual currency highways.

The current use of virtual currencies

Chainalysis analyzes the blockchain, to identify which transactions have been performed by the same entity and links these entities to real world services such as exchangers, merchant processors or underground marketplaces. This blockchain analysis can identify the underlying activity behind virtual currency transactions and the on-ramps and off-ramps to the existing financial system.

There are over approximately 10 million virtual currency users in the world today. These users are primarily interested in the long term potential of the technology and are holding on to virtual currency in the hope that it appreciates over time. There are also users who send virtual currencies cross border to avoid high fees associated with traditional money transmitters and banks.

Terrorist organizations are not in the business of speculating on the price of virtual currencies, but rather may be interested to use virtual currencies for the following three cases:

1. **Using virtual currencies in cybercriminal activities to fund operations**
2. **Crowdfunding operations from sympathizers around the world**
3. **Paying for everyday items and internet infrastructure**

Cybercriminals have mainly used Bitcoin to buy and sell capabilities to launch cyber attacks and also to extort their victims. Their use of Bitcoin cannot be attributed to anonymity but rather the speed and finality of payment, its ability to transcend borders and its protection against seizure.

There is some evidence that some terrorist organizations have begun to resort to cybercriminal enterprises to fund activity. In the United Kingdom, in the case against Younis Tsouli, there was evidence of money laundering from stolen credit cards through e-gold online payment accounts. The funds were used both to fund the registration of 180 websites hosting Al-Qaeda propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity.

There has not been any evidence yet of terrorist organizations running any of the criminal enterprises that are based in virtual currencies. However, I have seen some Ransomware campaigns be associated with high risk jurisdictions in terms of terrorism hotbeds. Recent high profile Ransomware campaigns such as "WannaCry", raise the profile of this type of criminal enterprise but executing in the virtual currency domain successfully requires a level of sophistication. WannaCry despite its massive media presence and disruption to companies, only made $92,000 in victim payments calculated at the time of transaction. Despite lower distribution levels, other Ransomware families have raised over $15 million due to providing better customer service to their victims and gaining better reputation of decrypting files quickly and reliably.

In July 2016, the only verifiable public case of crowdfunding by a known terrorist organization occurred. The campaign itself was not very successful and has only raised a total of $1,000 to date. The nature of virtual currencies meant that Chainalysis was able to size the potential threat and find the ultimate source and destination of funds.

The July 2016 campaign was initiated by an Ibn Taymiyya Media Center (ITMC) online campaign, called Jahezona or "Equip us" in Arabic. The organization started in July 2015 arguing that Muslims donating funds to equip jihadists was equivalent to fulfilling a religious obligation to fight. In late June 2016, the campaign added the option to pay in bitcoin. ITMC began posting infographics on Twitter with QR codes that linked to a Bitcoin address. Due to the lack of success of the campaign, we have not seen any other Bitcoin addresses emerge on the internet to raise funds from sympathizers.

However, even in the ITMC case there is evidence in this case that there are other sources of Bitcoin that are being used to send money around the world. At Chainalysis, we have been able to identify some of the services that the ITMC has been using to purchase anonymity tools and the exchanges used to convert the virtual currency into regular currencies.

Terrorists, like any other person, may use Bitcoin to pay for internet infrastructure or everyday goods and services. There are many merchants around the world that accept virtual currency, some blue chip companies, such as Overstock, as well as internet service providers who offer popular anonymization tools. Using tools these purchases can be useful leads in investigations to

uncover the goods and services purchased and may provide leads to attribution of the individuals involved.

There are still no goods priced in Bitcoin or any other virtual currency. Hence, merchants that accept virtual currencies require Intermediaries to link virtual currencies to the existing financial system. The United States has done a great job at giving clear guidance to these companies about the need to register with FinCEN, as Money Service Businesses, in cases where their businesses facilitates the connection between virtual currencies and US dollars or where they are holding virtual currencies in custody on behalf of their customers. As a result, the Suspicious Activity Reports filed by virtual currency businesses has already led to many successful criminal investigations. Due to the permanence and transparency of Bitcoin transactions many of these cases are solved quickly as evidence of profiting from criminal enterprise is often indisputable.

Concluding remarks

The potential for this virtual currencies to bring radical new business models and ways of organizing social and economic relations around the world remains large. The pace of change in this domain is rapid and the eventual outcomes unpredictable.

The current use of virtual currencies is mainly financial speculation on their eventual impact. The use of virtual currencies by terrorist organizations is still very limited due to the lack of awareness and trust placed in virtual currencies. The use of Bitcoin and other virtual currencies require a level of sophistication that is not often found in terrorist organizations or their supporters. Due to the price volatility, even the use of virtual currencies requires connectivity to the existing financial system to purchase goods and services. The ease by which terrorists access the existing financial system undermines the potential benefits that virtual currencies would afford their organizations.

There is growing awareness among companies and government agencies about the potential threats and their topologies. Outright bans and over-burdening regulation on legitimate businesses pose a large risk to the visibility that we currently have into virtual currencies. Ensuring the financial sector, as a whole, is aware of the technology and has the adequate controls necessary to thwart the potential threat will help realize the potential for this technology.

Virtual currencies continue to evolve rapidly. Private businesses, like Chainalysis, and the public sector should endeavour to mitigate current threats but be cognizant of the future potential of this technology.