Digital Assets: Risk Mitigation

FIRMA

32nd
National Risk Management Training Conference

San Diego, California
April 22 – 26, 2018

John L. Shepherd, PMC
Principal
Condado Consulting, LLC
4-23-2018

Digital Asset Risk Mitigation
FIRMA 32nd National Risk Management Training Conference
San Diego, CA
April 22 – 26, 2018

Contents

Digital Asset Risk Mitigation
FIRMA 32nd National Risk Management Training Conference
San Diego, CA
April 22 – 26, 2018

I. Introduction

Good afternoon ladies and gentlemen. Welcome to today's session – Digital Assets: Risk Mitigation. This session is intended to identify some of the risks associated with digital assets and will focus on cryptocurrencies such as Bitcoin. Risks will be identified by reviewing and comparing the current trading, settlement and custody processes for assets such as cash, stocks, bonds and mutual funds to similar processes that apply to cryptocurrencies.

My career has been split almost equally between software development firms servicing the financial services industry and trust / custody. The software development experience included 12 years as Product Manager. A major part of that role was to provide solutions to clients that would enable them to effectively manage risk. The banking experience included trust examiner for the OCC, Trust Audit and Trust Operations. Those roles focused on identifying and managing risk. I am sure there are some of you in the audience today who may know more about risk management and cryptocurrencies. I am not an expert in those fields instead I have a proven track record of providing solutions and solving business issues that mitigate risk. This was accomplished by listening to experts like you.

The objective of the session is to provide risk managers and attendees background on the nature of digital assets, the potential risks (trading, market and regulatory) and recommendations for managing those risks. The wisdom of investing in cryptocurrencies will be left to experts in that field and is not covered in today's session.

We will cover the following material:

- An overview of cryptocurrencies including definitions of common terms.
- A comparison of the trading processes stocks and cryptocurrencies.
- Risks associated with Cryptocurrencies
- Risk mitigation recommendations

At the end of the session I will provide a brief recap of what has been learned will be provided. Please ask your questions as we go through the session. I will do my best to provide answers. You are invited to share your own experience with digital asset risk mitigation.

II. Cryptocurrency Overview and Definitions

A. Cryptocurrency Overview

All cryptocurrencies are decentralized. An important attribute is the rate of each cryptocurrency is publicly known at time of issue. Governments like the United States employ agencies similar to the Federal Reserve Bank to issue coins and paper money (flat currency) as well as to make additions to digital banking ledgers. On the other hand, cryptocurrencies cannot be added to by companies or governments. Currently cryptocurrencies do not provide backing.

The following are some definitions for commonly used cryptocurrency terms obtained from Wikipedia.org and Investopedia.com that seem appropriate for today's session.

B. Definitions

"A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.[1][2][3] Cryptocurrencies are a form of digital currencies, alternative currencies and virtual currencies. Cryptocurrencies use decentralized control[4] as opposed to centralized electronic money and central banking systems.[5] The decentralized control of each cryptocurrency works through a blockchain, which is a public transaction database, functioning as a distributed ledger.[6] "
Bitcoin, created in 2009, was the first decentralized cryptocurrency.[7] Since then, numerous other cryptocurrencies have been created.[8]"

Wallets - The wallet is used to buy, store and sell cryptocurrencies. It can be digital or offline. The wallet can also be personal or institutional.

"Cryptocurrency wallet stores the public and private "keys" or "addresses" which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. [14] With the public key, it is possible for others to send currency to the wallet." [15]

Blockchain – "A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

Think of a blockchain as being similar to the transaction history in your firms accounting book of record.

Blockchains were originally developed as the accounting method for the virtual currency Bitcoin. Blockchains – which use what's known as distributed ledger technology (DLT) – are appearing in a variety of commercial applications today. Currently, the technology is primarily used to verify transactions, within digital currencies though it is possible to digitize, code and insert practically any document into the blockchain. Doing so creates an indelible record that cannot be changed; furthermore, the record's authenticity can be verified by the entire community using the blockchain instead of a single centralized authority." [8]

Mining – "In cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGA's and ASICs running complex algorithms like SHA-256 and Scrypt. [9,13]

Timestamping – There are two primary timestamping methods: Proof-of-work schemes and proof-of-stake schemes. These schemes are used to eliminate the need for third party.

> "***Proof-of-work*** - The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and Scrypt.[10] The latter now dominates over the world of cryptocurrencies, with at least 480 confirmed implementations.[11]
>
> Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11."[9]
>
> "***Proof-of-stake and combined*** - Some cryptocurrencies use a combined proof-of-work/proof-of-stake scheme.[10,12] The proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it." [9]

Anonymity – "Cryptocurrency is pseudonymous rather than anonymous in that the cryptocurrency within a wallet is not tied to people, but rather to one or more specific keys (or "addresses").[16] Thereby, cryptocurrency owners are not identifiable, but all transactions are publicly available in the blockchain.[16] Still, cryptocurrency exchanges are often required by law to collect the personal information of their users."[16,17]

C. U.S. Dollar is a Flat Currency

U.S. Dollar – is a flat currency that is it is not backed by a physical asset. Since the U.S. Dollar is not backed by a physical asset does that make it a cryptocurrency? An interesting question that we should consider before we continue our discussion.

When the United States ended the ability to convert dollars (Demand Notes) to gold in 1971 under then President Nixon. The process of converting the US Dollar and other currencies pegged to the Dollar to a flat currency (not backed by physical assets) was completed.

A brief history of the US Dollar is in order:

- Demand Note was the first paper money issued by the United States Government that achieved wide circulation. The original issuance was $50,000,000 (August 1861 and April 1862). They were convertible to specie (bullion coin struck in precious metal) "on demand".
- United States Note (1862 – 1971). The first issuance was $150,000,000 then expanded in 1863 to $450,000,000 (1862 – 1971).
- Federal Reserve Note (1914 to current).

Demand Notes, United States Notes and Federal Reserve Notes, with a brief gap between 1863 and 1879, were convertible to specie. The circulation was limited in 1879 at $346,681,016 for almost 100 years. In 1933 private ownership of gold was banned and then circulating currency could only be redeemed for silver. Silver redemption stopped in 1968. Circulation of Demand Notes ceased January 1971. Thereby ending the ability to convert US Dollars to gold. In 1963 the words "Payable to the Bearer on Demand" were removed from the Federal Reserve Note. [20]

Interestingly the Demand Note can be considered as the first flat currency (unbacked by physical asset) issued by the United States as it was never intended to be redeemed to specie, even though federal officials were authorized at times to exchange if requested. Since 1971, the US Dollar like most other currencies is a flat currency.

As of September 2017, there is approximately $3.85 trillion is circulation - $2.27 trillion in digital banking ledgers and $1.58 trillion in physical currency ($1.53 trillion in Federal Reserve Notes and $50 billion in coins). The amount of currency is determined by the size of the National Debt which is determined by Congress. The Federal Reserve via Open market operations determines the money supply. Can we say the $2.27 trillion in digital banking issues is really a cryptocurrency? Some might say yes if you consider how rapidly the cryptocurrency is evolving. By definition though the U.S. Dollar is not a cryptocurrency as it is backed by the U. S. Government.

D. Do Governments Issue Cryptocurrencies?

Let's examine why the answer to that question might be yes.

As previously mentioned current cryptocurrencies such as Bitcoin are not backed by companies or governments. That began to change when Venezuela's President, Nicolas Maduro urged 10 other countries to adopt his plan for an oil-backed cryptocurrency, the petro. President Maduro made this announcement at the Bolivarian Alliance for the Peoples of our America – Treaty of Commerce of the Peoples (Alba – TCP). Alba is made up of Antiqua and Barbuda, Bolivia, Cuba, Dominica, Ecuador, Nicaragua, Saint Lucia, Saint Vincent and the Grenadines, Saint Kitts and Nevis, Grenada and Venezuela on January 12, 2018. The ICO would consist of 100 million petros backed by 5 billion barrels of crude oil. There is a major obstacle to this ICO as Venezuelan Constituent National Assembly declared the cryptocurrency illegal. [7] As reported by the Washington Post on February 20, 2018 those obstacles appear to have been overcome as Venezuela began. "The pre-sale of the "petro," which will represent a barrel of crude from a specific division in the country's Orinoco oil belt, started Tuesday morning. Investors were offered $60 "tokens" at discounted rates that they can exchange for petros during what is being dubbed an "initial coin offering," or ICO, in March." [18] Per Reuters as of February 20, 2018 the ICO for petro has allegedly raised $735 million on the first day of presale. [19]

Other recent announcements by governments include:

- Switzerland - February 28, 2018 Robert Lacher, chairman of the Swiss Stock Exchange has come out in favor of a Swiss backed cryptocurrency. However, this is in conflict with the stated opinion of the Swiss National Bank. As previously seen with the petro this may change.
- Marshall Islands – Bitcoin News - March 1, 2018, written by Avi Mizrahi - "Offshore Tax Haven Marshall Islands to Issue National Cryptocurrency" concerning the Marshall Islands announcement of their intent to issue a cryptocurrency 'Govcoin' late r in 2018.

The question "Do governments issue cryptocurrencies/" can be answered with a maybe today but soon that answer will most likely change to yes as countries like Venezuela, Marshall Islands and others consider issuing their own cryptocurrencies.

E. Comparing US Dollar and Cryptocurrencies

When comparing cryptocurrencies to the US Dollar there are similarities as well as differences. The amount of both the US Dollar and cryptocurrencies are limited and publicly known.

- Control of the US Dollar is centralized. Cryptocurrencies use decentralized control through the use of blockchains.

- While US Dollars can take on a physical form they also exist in digital banking ledgers. Whereas cryptocurrencies only exist in digital form.

- US Dollars are backed by the US Government and have value based on the economy. Cryptocurrencies currently have no backing but that may change as previously mentioned.

- Sophisticated mechanisms exist to ensure US Dollars for individual and institutional accounting records are accurate. Similarly, sophisticated mechanisms exist for individuals holding cryptocurrencies.

- The US Dollar is a flat currency issued in both physical form and digital entries whereas cryptocurrencies digital entries only.

- The US Dollar is the official currency of the United States and is used to conduct financial transactions in the United States and around the world. It is also used by the British Virgin Islands and Turks and Caicos Islands as their currency. Cryptocurrencies are not used as currencies by governments (yet).

- US Dollar is easily exchanged for other currencies and vice versa at a variety of locations worldwide and US Dollar based accounts can be easily accessed via ATM's throughout the United States and worldwide. Cryptocurrencies can be bought / sold with / for other currencies over the internet via crypto exchanges. Cryptocurrencies have limited ATM access and there are a limited number of merchants willing to accept them as payment.

When comparing the US Dollar to cryptocurrencies while there are many similarities the most striking difference is their nature. Cryptocurrencies are more like stocks as they are speculative in nature and as a result the price can vary dramatically. Cryptocurrencies do not have intrinsic value, whereas the US Dollar does and has the backing of the U. S. Government.

III. Compare and Contrast Trading Processes

Now let's look at the process for buying and selling cryptocurrencies as compared to tradeable assets like stocks, bonds and mutual funds.

A. The Trading Process for Stocks

We all know the trade life cycle for stocks but a quick reminder may be in order. As a reminder the trade settles 2 business days after trade date. The following summarizes the trade life cycle for stocks.

1. On trade date a decision is made to buy or sell a stock that translates to an order.
2. The order is routed to the trader where the order is placed with a broker.
3. The broker places the order with an exchange.
4. The order is executed and becomes a trade.
5. The exchange notifies the broker.
6. The broker provides execution details to the buyer / seller.
7. Buyer / seller notifies the custodian of the trade.
8. A confirmation is sent to the buyer / seller.
9. The buyer / seller matches the confirmation to the trade execution details and affirms the trade.
10. On settlement date monies and shares exchange hands and ledgers are updated.

As we all know this life cycle is highly automated and will settle provided all control points are satisfied. In the vast majority of cases once the order has been submitted human intervention is not required and the ledgers for all participants are programmatically updated. When we look at how the trade life cycle has advanced since the 60's where every step was paper and required human intervention this is an amazing accomplishment. Especially considering the settlement period at that time was 5 business days after trade date.

B. The Trading Process for Cryptocurrencies

The trade life cycle for cryptocurrencies is much more streamlined than the life cycle for stocks. The following summarizes the trade life cycle for cryptocurrencies.

1. A wallet has to be established. The wallet can be virtual or offline. The wallet must be linked to existing bank account.
2. The user requests a transaction.
3. The network validates the user's status.
4. The transaction is verified through mining.
5. The new block is added to the existing blockchain.
6. The transaction is complete.

This process does not have any intermediaries and is completed real time. The technology for wallets, mining and blockchains is current and every evolving but not without risk which we will discuss in a few minutes. First let's compare the two trade life cycles.

C. Comparing Stock and Cryptocurrency Trade Life Cycles

When comparing trade life cycles for stocks and cryptocurrencies there are similarities and some important differences. The following summarizes those similarities and differences.

- Both trade life cycles are highly automated with sophisticated controls for validating information.

- The stock trade life cycle is Trade date plus 2 business days. The cryptocurrency life cycle is immediate.

- The stock trade life cycle employs a number of intermediaries required to complete the transaction. The cryptocurrency trade lifecycle does not.

- Post trade, the stock trade life cycle offers sophisticated mechanisms for reconciling disparate ledgers to ensure data integrity is maintained for all affected ledgers. Cryptocurrencies do not offer a post trade automated mechanism for reconciling ledgers.

As early as 2014 the distinction between stock and cryptocurrency trade life cycles began to blur to the point where today they are close to merging. The following firms are actively evaluating or are in the process of implementing solutions that are based on blockchains and cryptocurrencies. Other firms such as TD Ameritrade are offering expanded after hours trading in an attempt to compete with blockchain solutions for stock, bond, cash and cash equivalent trading. The firms listed below are examples of activities that are in process.

- TD Ameritrade announced earlier this year expanded after hours trading 24 x 5 for selected securities.

- The U.S. Patent and Trademark Office announced July 17, 2017 that Goldman Sachs has was granted a copywrite for their own cryptocurrency, SETLcoin. The SETLcoin would be based on blockchain technology and be used to for trading stocks, bonds, cash, cryptocurrencies and cash equivalents. [21] Multiple asset type wallets would be employed. The use of SETLcoin will offer immediate settlement same as cryptocurrency without the need for intermediaries. Theoretically this should reduce transaction costs.

- UBS, Deutsche Bank, Santander and BNY Mellon began promoting a solution in 2016 with usage targeted in 2018. [22]

- As reported in Fortune by Robert Hackett – October 4, 2016 J.P. Morgan is developing a blockchain based on Ethereum called Quorum.

We can see that the efforts underway with the firms listed above as well as others including players like IBM, that the technology behind cryptocurrencies, specifically blockchains, have the potential to transform our industry. These firms are actively working to make the technology industrial strength to satisfy the needs of the financial services industry. The potential cost savings resulting from a streamlined trade life cycle are enormous. The implications and opportunities for the financial services industry as well as other industries are enormous.

IV. Risk

Cryptocurrencies like any other asset class have risks. The following will discuss some the risks associated with trading, market, accounting and government regulations. We will also review measures to mitigate risk. The risks associated with investments nor the prudence of investing in cryptocurrencies will not be discussed.

A. Trading Risk

For the purposes of this discussion we will define Trading Risk as the ability to buy or sell cryptocurrencies. I realize some you may feel this a narrow definition but I believe there is more than enough to discuss given our time constraints. Before we discuss Trading Risk let's look at some of the headlines over the last several months.

Recent Security Breaches

The flexibility of being able to trade cryptocurrencies comes with great security risks. The following security breaches provide us examples of risks associated with trading cryptocurrencies:

"Exchanges Suspend USDT Transactions After $30 Million Tether Treasury Wallet Hack". November 21, 2017 – Bitcoin News – Avi Misrahi.

"Two Weeks After Losing $60 Million in Bitcoin. Nicehash are Back". Previously the mining pool Nicehash had announced in early December that 4,450 BTC had been hacked. December 21, 2017 – Bitcoin News – Kai Sedgwick.

A man's bitcoins valued at $117,000 was stolen while he was logged into a public Wi-Fi in a restaurant in Vienna, Austria. - November 23, 2017 - The Palm Beach Post.

"Coingather Exchange Has Been Offline for Days and No One Knows Why". Since this was first reported the exchange remains offline impacting users tied to the exchange. November 25, 2017 – Bitcoin News - Kai Sedgwick.

"One Week On from the Etherdelta Hack, Funds Are Still Being Stolen" reported that a supposedly decentralized exchange that could not be hacked was hacked. 308 ETH were worth about $270,00 plus a number of tokens worth hundreds of thousands of dollars were also stolen. December 26, 2017 – Bitcoin News - Kai Sedgwick.

"Chinese Programmer Arrested Over 20 Million Japanese Yen Bitcoin Theft" – reported that by hacking a Bitcoin wallet the thief was able to transfer deposits from the account of the user to his own account. December 26, 2017- Bitcoin News - Cindy Wang.

"Man's Life Savings Stolen From Hardware Wallet Supplied by Reseller". A Nano Ledger hardware wallet purchased online was compromised by the seller prior to sale. The buyer did not reset the device to generate a new seed but instead used the one provided by the seller. January 6, 2018 – Bitcoin News - Kai Sedgwick.

"Bitconnect Shuts Down Its Exchange Citing a String of Excuses". Bitconnect had been widely accused of operating a Ponzi scheme. Subject to cease and desist orders they elected to shut down the exchange locking out its users. January 16, 2018 – Bitcoin News - Kai Sedgwick.

"Hackers Steal $400k from Users of Stellar Lumen (XLM) Web Wallet". Hackers were able to redirect the Domain Name System to point to servers they controlled. January 16, 2018 - Bitcoin News – Avir Mizrahi.

"Coincheck Faces Pressing Questions in the Wake of the World's Biggest hack. Coincheck was subject to a hack that resulted in the theft of NEM valued between $400 and $534 million. January 26, 2018 – Bitcoin News - Kai Sedgwick.

"$9 Million a Days Is Lost in Cryptocurrency Scams". In the first 59 days of 2018 $1.36 billion has been reported stolen by scammers. See the list of scams published in the referenced article. March 2, 2018 – Bitcoin News – Kai Sedgwick.

Article	Scam Type	Value $
Bitcoin Skeptic Dennis Gartman Duped by Dubious Blockchain Investment	Fraud	
The Bee Token Crowdsale Stung by Phishing Scam	Phishing	1,000,000
Vegetables on a Blockchain ICO Exit Scams After Paying People to Write On Their	Exit Scam	
Benebit ICO Does a Runner with $2.7 Million of Investor Funds	Exit Scam	2,700,000
CFTC Files Against 'My Big Coin' for Scamming $6 Million USD	Fraud	6,000,000
European Authorities Seek Arrests in Bitcoin Scam Investigation	Fraud	115,000,000
Russian Crypto Developer Beaten, Robbed Of 300 BTC On Moscow Streets	Theft	3,000,000
Moscow Man Mutilated And Mugged For $1 Million In Bitcoin, Local Sources Report	Theft	1,020,000
Texas Regulator Orders Another Crypto Scam To Stop Selling Fraudulent Securities	Fraud	177,000,000
Chicago Trader the First to Be Charged With Cryptocurrency-Related Fraud	Fraud	2,000,000
Impersonators Scam Seele ICO Investors out of $2 Million in Ethereum	Phishing	2,000,000
Coinhoarder $50 million phishing scam including $2m in four weeks	Phishing	2,000,000
A Bitcoin scam artist in the United Arab Emirates who fleeced a victim of $545,000	Theft	545,000
SEC Halts Alleged Initial Coin Offering 'Scam' Endorsed By Evander Holyfield (ARI	Fraud	200,000,000
Cryptocurrency startup LoopX pulls exit scam after raising $4.5M in ICO (LoopX)	Exit Scam	4,500,000
Bitconnect	Exit Scam	250,000,000
Investors Caught In Two Crypto 'Exit Scams' BITGRAIL	Hack	170,000,000
Coincheck Users Pull $373 Million in First Chance Since Hack	Hack	400,000,000
IOTA Wallet	Hack	4,000,000
Stellar Wallet	Hack	400,000

Some of 2018's more prominent scams

B. Best Practices for Risk Mitigation

With bad news like this be reported on a regular basis it would seem the risks of trading cryptocurrencies is insurmountable. However, there are a number of best practices that can be employed to mitigate risk. Interestingly those practices are available to the general public. For example: Bitcoin publishes best practices for mitigating the risks associated with wallets. The following are their recommendations as published on bitcoin.org/en/secure-your-wallet Bitcoin.com.

Securing your wallet

The ability to trade cryptocurrency is dependent on establishing a wallet. The wallet is like your own personal wallet that you use to carry credit cards, ID and cash. We all know that our wallets must be must be kept secure. The same is true for cryptocurrency wallets. A wallet can be online or physical.

Like in real life, your wallet must be secured. Bitcoin makes it possible to transfer value anywhere in a very easy way and it allows you to be in control of your money. Such great features also come with great security concerns. At the same time, Bitcoin can provide very high levels of security if used correctly. **Always remember that it is your responsibility to adopt good practices in order to protect your money**.

Be careful with online services

You should be wary of any service designed to store your money online. Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank. Accordingly, you might want to use other types of Bitcoin wallets. Otherwise, you should choose such services very carefully. Additionally, using two-factor authentication is recommended.

Small amounts for everyday uses

A Bitcoin wallet is like a wallet with cash. If you wouldn't keep a thousand dollars in your pocket, you might want to have the same consideration for your Bitcoin wallet. In general, it is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment.

Backup your wallet

Stored in a safe place, a backup of your wallet can protect you against computer failures and many human mistakes. It can also allow you to recover your wallet after your mobile or computer was stolen if you keep your wallet encrypted.

Backup your entire wallet
Some wallets use many hidden private keys internally. If you only have a backup of the private keys for your visible Bitcoin addresses, you might not be able to recover a great part of your funds with your backup.

Encrypt online backups
Any backup that is stored online is highly vulnerable to theft. Even a computer that is connected to the Internet is vulnerable to malicious software. As such, encrypting any backup that is exposed to the network is a good security practice.

Use many secure locations
Single points of failure are bad for security. If your backup is not dependent of a single location, it is less likely that any bad event will prevent you to recover your wallet. You might also want to consider using different medias like USB keys, papers and CDs.

Make regular backups
You need to back up your wallet on a regular basis to make sure that all recent Bitcoin change addresses and all new Bitcoin addresses you created are included in your backup. However, all applications will be soon using wallets that only need to be backed up once.

Encrypt your wallet
Encrypting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software.

Never forget your password
You should make sure you never forget the password or your funds will be permanently lost. Unlike your bank, there are very limited password recovery options with Bitcoin. In fact, you should be able to remember your password even after many years without using it. In doubt, you might want to keep a paper copy of your password in a safe place like a vault.

Use a strong password
Any password that contains only letters or recognizable words can be considered very weak and easy to break. A strong password must contain letters, numbers, punctuation marks and must be at least 16 characters long. The most secure passwords are those generated by programs designed specifically for that purpose. Strong passwords are usually harder to remember, so you should take care in memorizing it.

Offline wallet for savings

An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches.

Offline transaction signing

This approach involves having two computers sharing some parts of the same wallet. The first one must be disconnected from any network. It is the only one that holds the entire wallet and is able to sign transactions. The second computer is connected to the network and only has a watching wallet that can only create unsigned transactions. This way, you can securely issue new transactions with the following steps.

- *Create a new transaction on the online computer and save it on an USB key.*
- *Sign the transaction with the offline computer.*
- *Send the signed transaction with the online computer.*

Because the computer that is connected to the network cannot sign transactions, it cannot be used to withdraw any funds if it is compromised. Armory *can be used to do offline transaction signature.*

Hardware wallets

Hardware wallets are the best balance between very high security and ease of use. These are little devices that are designed from the root to be a wallet and nothing else. No software can be installed on them, making them very secure against computer vulnerabilities and online thieves. Because they can allow backup, you can recover your funds if you lose the device.

Keep your software up to date

Using the latest version of your Bitcoin software allows you to receive important stability and security fixes. Updates can prevent problems of various severity, include new useful features and help keep your wallet safe. Installing updates for all other software on your computer or mobile is also important to keep your wallet environment safer.

Multi-signature to protect against theft

Bitcoin includes a multi-signature feature that allows a transaction to require multiple independent approvals to be spent. This can be used by an organization to give its members access to its treasury while only allowing a withdrawal if 3 of 5 members sign the transaction. Some web wallets also provide multi-signature wallets, allowing the user to keep control over their money while preventing a thief from stealing funds by compromising a single device or server.

Think about your testament

Your bitcoins can be lost forever if you don't have a backup plan for your peers and family. If the location of your wallets or your passwords are not known by anyone when you are gone, there is no hope that your funds will ever be recovered. Taking a bit of time on these matters can make a huge difference.

E. Review of the Bitcoin Best Practices

1. Be Careful of Online Services – The recommendation is to not store online. This is a sound recommendation. The importance of establishing a wallet is important but do not store cryptocurrencies in the online wallet. A combination of online wallet for trading and a hardware wallet in my opinion is a best practice. We will discuss hardware wallets later in this document. The best practice recommends dual factor authentication which is strongly supported. When evaluating where to open an online wallet great care must be given to ensure the exchange selected is viable and can operate in your domicile. The exchange should offer institutional accounts that have multiple signers / approvers. The exchange should also offer segregated custody accounts that are stored offline. An example is Gemini Trust Company, LLC https://gemini.com

2. Small amounts for everyday use – absolutely limit the amount of currency held on the computer, mobile or server. The recommended best practice is only place in the trading wallet what is intended to be sold. Any purchases should be moved to a more secure offline account. For institutions use of mobile devices for trading is discouraged. As we have seen mobile devices is risky. Further, when establishing a wallet linking to a bank account is required. A separate bank account should be used for that purpose. One that is not used for client uninvested cash or trade settlement.

3. Backup your wallet – the wallet is like any other financial accounting software. The best practice employed for accounting books of record is to back up at least daily. The wallet is no different it is your book of record for cryptocurrencies.
    a. Backup the entire wallet – very sound advice especially for those of us new to cryptocurrencies
    b. Encrypt on line backups – as well as any backup exposed to the network - very good risk mitigation.
    c. Use many secure locations – a strong practice to ensure recovery
    d. Make regular backups – the best practice in the financial services industry is daily. This is no exception

4. Encrypt your wallet – this should be standard practice for any computer or device used by firms in the financial services industry. Wallets are no exception

a. Never forget your password – there is very limited ability to recover passwords for wallets. Historically writing down your password was never considered a best practice. In this instance recording and storing in a secure location like a vault is strongly recommended.
b. Use a strong password – this is a common best practice in this industry.

5. Offline wallet for savings – employing cold storage for custody is strongly recommended. The storage location should be isolated from the network. The best practice recommended includes use of offline wallet, backups and encryption. This while time consuming and without some expense is a solid recommendation.
    a. Offline transaction signing. A very secure method for transacting. There is expense involved but the security is worth it.
    b. Hardware wallets – A very good best practice and a cost-effective solution. More on hardware wallets is discussed later in this document.

6. Keep your software up to date – a common best practice for all applications employed by the institutions in the financial services industry

7. Multi-signature to protect against theft – as mentioned previously when evaluating exchanges some offer institutional wallets that require 3 to 5 members to sign. Given the vulnerability of wallets and exchanges it would seem very prudent to employ this best practice.

8. Think about your testament – sound advice for individuals. Not so pertinent for institutions.

D. Selling Cryptocurrencies

The ability to cash out of cryptocurrencies may not be as easy as it is to buy cryptocurrencies. There are failure points at every level, the exchange may cancel the sale, the receiving bank may freeze the account, regulators may monitor for money laundering and tax evasion. Tax withholding may be required. [28] The recommendation for institutions is to vet with the exchange and bank in advance as to the rules for selling cryptocurrencies. Make sure you know the requirements before you transact the sell.

F. Market and Regulatory Risk

As we have seen from the headlines mentioned above the risk associated with cryptocurrencies is not limited to trading. Markets shut down for no apparent reason either from fraud or by countries intent on limiting trading ability. Governments are grappling with how to draft and implement regulations to protect their citizens from fraud. The response has ranged from

attempting to shut down exchanges to approving specific exchanges to transact business in their countries to attempting to emulate existing regulations governing as tradeable assets and related markets. In an opinion piece written by Roy Keidar – January 30, 2018, Roy states:

"Distributed ledger technology ("DLT") has been pitched as a way to improve transactions transparency, mitigate systemic risk and strengthen financial stability. Experts of the regulatory technology industry have even described blockchain as having the potential effect to create compliance partnerships between regulators and market participants, by directly inputting compliance rules inside the blockchain (i.e. via a smart contract) and therefore facilitating an almost real-time access, analysis and processing of data.

Nevertheless, in reality, market abuse risks have not been eliminated by DLT, and, given the nature of unregulated ICOs or crypto-currencies investments, such risks are, in many ways, far greater. A lack of information on price formation and order execution, central order book manipulation, or price manipulations such as "pump and dump" and "spoofing" practices represent only some of the potential issues for investors in crypto-currencies." [23]

For the most part cryptocurrency markets are not regulated and are subject to market manipulation which would be very hard prove. Many European countries have the opinion that most cryptocurrencies do not meet the requirements of a financial instrument. [23]

Further, Mr. Keidar notes that while blockchains do register every transaction that proving mis conduct would be very difficult. Also, in his opinion, the lack of a central authority governing crypto market manipulation because cryptocurrencies are not registered as securities and the fact that trading occurs on various platforms worldwide making it difficult for regulators to claim responsibility. [23]

As with everything related to cryptocurrencies this lack of market regulation is changing rapidly. The Japanese government approved 16 cryptocurrency exchanges and are teaming up to form a self-regulatory group. [24] Australia is also set to introduce legislation for anti-money laundering with the goal of providing increased transparency. [25] Barely a day goes by without at least one announcement concerning a government attempting to provide some level of oversight. In addition to the two previous announcements the 6 days starting February 25 to March 3 the following announcements were published in Bitcoin News:

- Korea Investigate 20 public companies for using crypto related announcements to boost share prices - February 25, 2018.
- Georgia lawmakers propose tax amendment that allows Bitcoin payments - February 26, 2018.
- Uzbekistan to legalize Bitcoin and support developers - February 26, 2018.
- Israeli Supreme Court forbids bank form denying service to Bitcoin Exchange - February 27, 2018.

- 35 Countries and Financial Action Task Force (FATF) agree to revise global cryptocurrency standards - February 28, 2018.
- Court will not seize cryptos as debt payment form bankrupt citizens in Russia - March 1, 2018.
- Thai regulators in race with growing popularity of token sales - March 2, 2018.
- Ukraine's financial watchdog clarifies stance on cryptos - March 2, 2018.

The climate in the United States for increasing regulation is no different than other countries. In a recent article by Carlos Terenzi – Coinstaker.com – "United States to Analyze Potential Cryptocurrency Regulations".

Different countries are trying to regulate cryptocurrencies and ICOs, but this is not an easy task. The United States Justice Department is working in a "comprehensive strategy," a specific approach towards regulation cryptocurrencies. It is important for governments not to kill the market by imposing very strict regulations but neither leave it unregulated. That's a difficult equilibrium to find.

United States Justice Department Crypto Regulations

Apparently, the US Justice Department is searching for new ways of regulating virtual currencies. As the cryptocurrency market is getting more and more interest from the media and the society, regulations must follow. There is not a clear path followed by different states about how to regulate this volatile market.

Regulations must be addressed as soon as the market shows signs of being mature. Regulations before it can completely destroy it or slowing it development by restricting its potentialities. If there's not a clear framework, it can also be a problem for individuals and investors that may lose their investments.

Cryptocurrencies cannot be compared to fiat money because it works in a completely different way. It also expresses a society that is tired about the old system and wants to change. It is a way to express how society sees the future of money and relationships between individuals and enterprises.

Most of the regulations should attack the illegal activities around cryptocurrencies, including money laundering, criminal fundraising and terrorism financing. This is a clear problem that sometimes is directly linked to cryptocurrencies, when in reality, the problem is wider. Drugs and criminals have always existed and they have always found a way to avoid regulations and operate.

For example, Singapore has expressed its intention not to regulate cryptocurrencies, but instead, all the criminal activities that may use virtual currencies. This is what the head of the Monetary Authority of Singapore, Ravi Menon, commented

> *"Our attitude is to keep an open mind about (cryptocurrencies and bitcoin). Very few jurisdictions regulate cryptocurrencies per se. The currency itself does not pose the kind of risk that require regulation. Our intention is to look at the activity around the*

cryptocurrency and then make an assessment about which regulation would be suitable."

What's Next?

At the moment there is not clear information about what the Justice Department is expected to do. It can also happen that the discussions that are taking place now may not find a clear solution in the months to come. The regulatory measures can wait; it is not something that should be treated as fast as possible.

Other experts believe that cryptocurrencies need to be regulated as soon as possible or before they become mainstream. There is no clear plan as of today. The G-20 will let us know better which the panorama in front of us regarding crypto regulations is.

G. Initial Coin Offerings and Market Risk

Initial Coin Offerings (ICOs) are proving to very risky. In an article published on February 23, 2018, it was noted that 46% of the ICOs in 2017 failed despite raising over $104 million. Of 902 ICOs 142 failed outright and another 276 subsequently failed due to fraud or lack of interest. Due diligence is required when subscribing to ICOs.

H. Threat of Violence

There is a growing risk of violence by thieves going after cryptocurrencies. As reported in the New York Times on February 18, 2018, thieves in Thailand, Ukraine, United States, Russia, Turkey and Britain are taking victims hostage and use the threat of violence to make victims transfer their cryptocurrencies to the thieves. Given the design of blockchains it is very difficult to trace the transaction and identify the perpetrators. [26]

To mitigate the risk investors are employing multi signature wallets, avoiding in person meetings for trading, avoiding countries where attacks are easier to pull off, installing video surveillance and in extreme cases going dark (moving to a new location and not providing the address to anyone). [26]

I. Wallets

As previously mentioned previously hardware wallets are one of the risk mitigation measures to address trading risk. In an article written by Kai Sedgwick the merits of several hardware wallets are discussed as well as best practices for their use. [27] A review of this article before purchasing a hardware wallet is strongly recommended.

J. Risk Mitigation

The recommendations listed above are all solid recommendations for best practices that mirror best practices employed today by most firms in the financial services industry. One mitigation measure not mentioned concerns the method of trading. Trades can be executed online are

arranged via a personal meet where details are exchanged. Covered in more detail later are the risks for personal meets. As rule avoid personal meets to conduct trades. Only trade online.

Risk mitigation measures have been employed as a standard for most firms and as such should be familiar to all of us. Some of the recommendations mentioned above would only apply to trading cryptocurrencies such as the use of offline transaction signing and hardware wallets. Most others have been employed in various degrees for many years and are sound business practices.

How do you mitigate market and risk in this currently unregulated market? A challenging question to answer given where we are today. One answer to emulate what is being done by institutions in other countries by forming self-regulating bodies, Japan for example, in concert with our regulators. Our various agencies are looking at the how regulate cryptocurrencies. Our opportunity is to be part of that conversation before regulations are created.

V. Conclusion

The objective of today's session was to provide risk managers and attendees background on digital assets, identify and discuss potential risks and recommendations for risk mitigation. Hopefully those objectives have been met.

During today's session definitions for commonly used cryptocurrency terms have been provided. Terms such as wallets, blockchain and mining are better understood.
A comparison between the U.S. Dollar and crypto currencies has been made and while some attributes are similar we can state the U.S Dollar is not a cryptocurrency and that cryptocurrencies are not flat currencies. We have also learned that some governments are currently issuing or contemplating the issue of cryptocurrencies some backed by physical assets such oil backing the Petro.

The trading processes for stocks and cryptocurrencies were compared and contrasted. During this segment we covered plans in process to employ blockchains and cryptocurrencies for trading stocks, bonds, cash and cash equivalents.

Risks associated with cryptocurrency trading were identified and reviewed. Best practices for risk mitigation were discussed include the following topics:"

- Securing the wallet
- Online Services
- Having two wallets – Trading / Storage
- Backup Recommendations – Including encryption and frequency
- Encrypting the wallet and controls for passwords
- Offline wallets for storage
- Use of two computers to complete a transaction
- Hardware Wallets
- Software updates
- Multi signature features
- For individuals a backup plan for peers and family
- Withdrawing proceeds from sales
- Market and Regulatory risks
- Initial Coin Offering (ICO) risks
- Threat of violence
- Hardware wallet options.

Every aspect of cryptocurrencies is changing rapidly. Those changes have the potential to dramatically impact how information is processed and stored not only for cryptocurrencies but also other tradeable asset like stocks. There are opportunities for establishing focus groups with developers, consumers, institutions and regulators be part of conversation and influence

the evolution. Cryptocurrency is in its infancy. Cryptos have been with us for almost 10 years. During this period the industry, while ever evolving, has been geared toward the individual investor and not institutions like yours. To make wallets, blockchains and mining industrial strength will require cooperation by all parties, developers, consumers, institutions and regulators. Now is the time to become part of the conversation at all levels to ensure your business needs and requirements are heard and understood. Participation in the conversation also comes with responsibility. We must learn more about the technology, how to apply the technology, risks and how to mitigate those risks. Given the rapid pace of evolution surrounding cryptocurrencies this will be no small task but it should be one we welcome.

VI. Acknowledgements

I would like to thank everyone who has helped me understand the nature and benefits of cryptocurrencies and the associated risks. Especially helpful have been Simon Algar, Principal at Wealth-Reports a consultancy providing services to financial institutions and Walter Joyce, Managing Director – Investment Services TIAA. FSB. I would also like to acknowledge Wikipedia (Cryptocurrency, United States Dollar and Monetary Police of the United States), Daily Bitcoin News, The Evening Standard (London UK), New York Times, Washington Post, Palm Beach Post and Wall Street Journal as sources of information as well as specific references detailed in the next section.

VII. References

1. *Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com.*
2. Cryptocurrencies: A Brief Thematic Review. *Economics of Networks Journal.* Social Science Research Network (SSRN).
3. *Schuettel, Patrick (2017). The Concise Fintech Compendium. Fribourg: School of Management Fribourg/Switzerland.*
4. *McDonnell, Patrick "PK" (9 September 2015). "What Is the Difference Between Bitcoin, Forex, and Gold". News BTC.*
5. *Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless". News BTC.*
6. *Matteo D'Agnolo. "All you need to know about Bitcoin". Times of India – economic times.*
7. Bitcoin News – January 15, 2018
8. Investopedia.com Blockchain definition
9. Wikipedia.org Cryptocurrency/Architecture/timestamping
10. Wary of Bitcoin? A guide to some other cryptocurrencies
11. "CryptoCoinTalk.com – Discussing the World of Cryptocurrencies"
12. *Sunny King, Scott Nadal (19 August 2012). "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake"*
13. Krishnan, Hari; Saketh, Sai: Tej, Venkata (2015) "Cryptocurrency Mining – Transition to Cloud". International Journal of Advanced Computer Science and Applications. ***6*** *(9). doi:10.14569/IJACSA.2015.060915. ISSN 2156-5570.*
14. *Juchisth, Smith. "*Wat is cryptocurrency? Een introductie in de blockchain". *Cryptostart (in Dutch).*
15. Wikipedia.org Cryptocurrency/Architecture/mining.
16. "Bitcoin Basics Lesson 2: Essentials of Bitcoin". *Medium.com.*
17. Wikipedia.org Cryptocurrency/Architecture/anonymity.
18. Washington Post, February 20, 2018
19. Reuters, February 20, 2018
20. Wikipedia.org United States Dollar
21. Investopedia. Com - Shobhit Seth "Here's How the SETLcoin Trade System Will Work" (February 17, 2016)
22. Bitcoin News – August 24, 2016 – Jon Southurst - Four Big Banks to Create a New Bitcoin alternative
23. Bravenewcoin.com – January 30, 2018 – Roy Keidar – "Cryptocurrency Adoption, Opinion".
24. Bitcoin News – March 3, 2018 – Kevin Helms – "16 Government-Approved Cryptocurrency Exchanges Forming Self-Regulatory Body in Japan".
25. Bitcoin News – March 2, 2018 – Samuel Haig – "Aussie Crypto Traders Expect Tax Crackdown Ahead of New Regulations".
26. New York Times – February 18, 2018 – Nathaniel Popper – "Bitcoin Thieves Threaten Real Violence for Virtual Currencies".

27. Bitcoin News – January 19, 2018 – Kai Sedgwick – "Bitcoin for Beginners: Which Hardware Wallet to Use".
28. Bitcoin News – December 28, 2018 – Jamie Redman – "Dancing With the Devil: 'Cashing Out' Cryptos Into Fiat Not So Easy".