



# CYBERCRIMES AND CYBERSECURITY

ATTY. EMILIO B. AQUINO, CPA  
Supervising Commissioner  
for Enforcement and Investor Protection  
Securities and Exchange Commission

*PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018 : The Mansion, Iloilo City*

*“Technology is a queer thing; it gives you great gifts with one hand and it stabs you in the back with the other”* – Charles Percy Snow (Future Crimes by Marc Goodman)

Is it a Friend or a Foe?

It's like fire...

# PAUSE BEFORE YOU POST



WAR HISTORY ONLINE

## How 4 U.S. Attack Helicopters Were Destroyed Because of Geotagged Pictures

FEATURED NEWS

Jan 11, 2016 George Winston



Stock photo of Apache Helicopter in Iraq. U.S. Army photo/Sgt. Brandon Little

### Finding robbery victims through Instagram

While Hadnagy demonstrates to raise awareness, others may have more sinister intentions.

Arturo Galvan of California is accused of finding his 33 robbery victims through pictures they posted on Instagram. He used the GPS coordinates in the pictures to track where victims live and then came by to steal electronics, wallets and more, according to the Orange County District Attorney's Office. Galvan pleaded not guilty and is awaiting trial.

It's not just personal information at stake, and businesses need to be alert.

### Think Twice Before Using This Wildly Popular Facebook App



Elizabeth Renstrom for TIME

Some people say it wants too much of your personal data

JOHN PATRICK PULLEN @JPPULLEN  
NOV 26, 2015 7:29 AM EST



CNBC Business News and Finance  
NBCUniversal Media, LLC  
Get the App Now!

View

PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018 : The Mansion, Iloilo City

# OBJECTIVE

TO SHARE THE BASICS OF CYBERCRIMES AND CYBERSECURITY BASED ON SEC EXPERIENCE IN ORDER TO HELP PROTECT FELLOW PAGBANS, THEIR PROPERTY AND/OR THEIR ORGANIZATIONS FROM THE DISASTROUS EFFECTS THEREOF.

# OUTLINE

- What is a Cybercrime?
- Types of Cybercrimes
- State of Cybersecurity in the Philippines
- Cyber Attacks
- Crypto: Friend or Foe
- Bitcoins
- Blockchain
- What are Cryptocurrencies?
- What is an ICO?
- How Governments React to Crypto
- SEC/BSP Regulations
- Enforcement Actions against illegal ICOs
- Some Take Aways

# What is a Cybercrime?

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

# Types of Cybercrimes

Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:

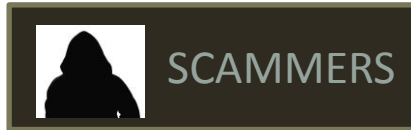
- **Cyber-enabled crime** – many ‘traditional’ crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism.
- **Advanced cybercrime** (or high-tech crime) – sophisticated attacks against computer hardware and software;

# CYBER-ENABLED CRIMES

TRADITIONAL CRIMES DONE ONLINE



# ADVANCE FEE SCHEME

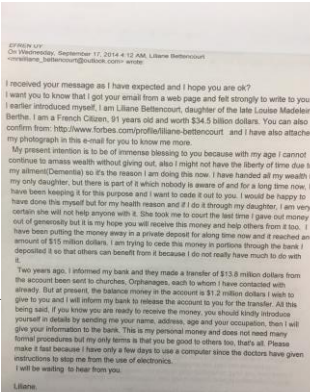


LILIANE  
BETTENCOURT

L'ORÉAL  
PARIS

- One of the principal shareholders of L'Oréal
- The richest French person with net worth at USD 36.1 Billion

Fake email: mrsLiliane\_bettencourt@outlook.com



Received your message as I have expected and I hope you are ok? I want you to know that I got your email from a web page and felt strongly to write to you. As I earlier introduced myself, I am Liliane Bettencourt, daughter of the late Louise Madeleine Berthe. I am a French Citizen, 91 years old and worth \$34.5 billion dollars. You can also confirm from: [http://www.forbes.com/profile/liliane\\_bettencourt](http://www.forbes.com/profile/liliane_bettencourt) and I have also attached my photograph in this e-mail for you to know me more.

My present intention is to be of immense blessing to you because with my age I cannot continue to amass wealth without going out, also I might not have the liberty of time due to my illness (Dementia) so it's the reason I am doing this now. I have handed all my wealth to my only daughter, but there is part of it which nobody is aware of and for a long time now, I have been keeping it for this purpose and I want to pass it on to you. I would be happy to have done this myself but for my health reason and if I do it through my daughter, I am very out of generosity but it is my hope you will receive this money and help others from it too. I have been putting the money away in a private deposit for a long time now and it reached an amount of \$15 million dollars. I am trying to pass this money in portions through the bank I deposited it so that others can benefit from it because I do not really have much to do with it.

Two years ago, I informed my bank and they made a transfer of \$13.8 million dollars from the account been sent to churches, orphanages, each to whom I have contacted with ahead. But at present, the balance money in the account is \$1.2 million dollars I want to give to you and I will inform my bank to release the account to you for the transfer. All this yourself in detail by sending me your name, address, age and your occupation, then I will give your information to the bank. This is my personal money and does not need many formal procedures but my only terms is that you be good to others too. That's all. Please make it fast because I have only a few days to use a computer since the doctors have given instructions to stop me from the use of electronics.

Liliane

Scammers sent an email to MR. X

VICTIM

Mr. X is a Filipino Citizen residing in the Philippines

(1)

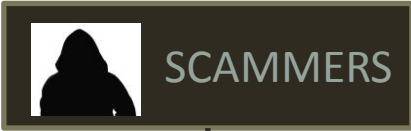
Ms. Bettencourt has decided to share her wealth to different persons around the world. MR. X was one of the lucky recipients thereof in the amount of USD 1.2 Million.

(2)

Ms. Bettencourt already transferred the amount to the name of MR. X and all that is required of MR. X in order to get the ATM Card and the money, is to pay GBP2,450 to Credit Suisse Securities (UK) LLC as transfer fee.

(3)

The scammers, representing to be Ms. Bettencourt, aggressively pressured MR. X to pay the processing fee. The scammers informed MR. X that Ms. Bettencourt will forward the emails of the bank, and advised him to strictly follow the instructions therein because they can expedite the release of the funds.



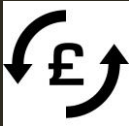
Mr. **IAN GREY**, representing to be connected with Credit Suisse:  
**FAKE EMAIL:**  
creditsuisse.actdept@outlook.com

(1)  
Confirmed that Ms. Bettencourt transferred an amount to his name evidenced by an email of acknowledgement; and

(2)  
Provided him with instructions and conditions on the transfer

**VICTIM**  
Mr. X, a Filipino from the Philippines

**VICTIM** transmits his money to the **SCAMMERS** in the amount of USD 4,206.00 (approx. PhP210,000)

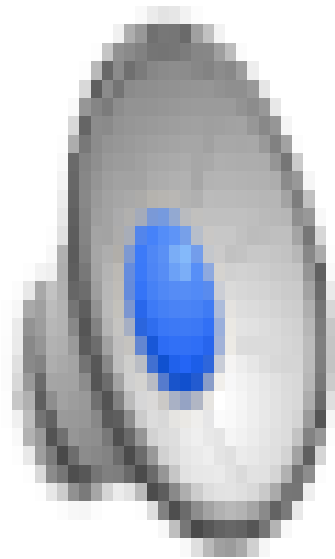
 Exchange of Money and Documents

**Scammer sends Evidence of Transfer**

The image shows three documents from Credit Suisse. On the left is an acknowledgment email from Mr. Efron Martinez to Mr. IAN GREY, dated 17/10/2014, stating that a payment of USD 4,206.00 has been made. In the middle is a credit memo showing a deposit of USD 4,206.00 on 17/10/2014. On the right is a Certificate of Deposit for USD 4,206.00, dated 17/10/2014, issued to Mr. IAN GREY.

- a. Acknowledgement email from Credit Suisse
- b. Credit Memo from Credit Suisse
- c. C. Certificate of Deposit

# Online Lending Scam (Advance Fee Scheme)



# ADVANCED CYBERCRIMES

ATTACKS ON COMPUTER HARDWARE OR SOFTWARE

# ILOVEYOU or Lovebug Virus

- The malware originated in the Pandacan neighborhood of Manila in the Philippines on May 5, 2000, thereafter following daybreak westward across the world as employees began their workday that Friday morning, moving first to Hong Kong, then to Europe, and finally the United States.
- The outbreak was later estimated to have caused **US\$5.5-8.7 billion** in damages worldwide, and estimated to cost **US\$15 billion** to remove the worm. Within ten days, over fifty million infections had been reported, and it is estimated that 10% of internet-connected computers in the world had been affected. Damage cited was mostly the time and effort spent getting rid of the infection and recovering files from backups.
- To protect themselves, The Pentagon, CIA, the British Parliament and most large corporations decided to completely shut down their mail systems. **At that time, the ILOVEYOU virus was one of the world's most destructive computer related disasters ever.**

# Business Email Compromise

- Pervasive and increasingly sophisticated
- Typically involve use of compromised or “lookalike” email accounts to induce firms to transfer their own or customer funds to unauthorized recipients ([robert@abcde.com](mailto:robert@abcde.com) vs. [robert@abcde.co](mailto:robert@abcde.co))
- 2015 FBI report that firms lost \$1.2B worldwide to BEC schemes from October 2013-August 2015
- Losses to individual firms can be substantial: 2015 disclosure by Ubiquiti Networks of \$39M loss from BEC scheme involving fraudulent payments to nonexistent vendors

# Denial of Service Attacks

- June 2015: Extortion attempts by DD4BC group threatening DDOS attacks on securities firms and others unless recipients paid them money in bitcoin
- January 2016: Arrests of DD4BC group members in Europe
- 2012-13 attacks on U.S. banks by al-Qassam Cyber Fighters
- Some attacks used to mask fraud and IP theft
- Attack bandwidth increasing: 2012-12 al-Qassam attacks involved @60-65 gigabytes per second; fall 2016 attack on Dyn domain name service involved reported volumes of 1.2 terabytes per second

----- Forwarded message -----

From: **DD4BC TEAM** <[REDACTED]>

Date: Sat, Nov 1, 2014 at 4:57 AM

Subject: DDOS ATTACK!

To: [REDACTED]

Hello

Your site is extremely vulnerable to ddos attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed!

My price is 1 Bitcoin only.

Right now I will star small (very small) attack which will not crash your server, but you should notice it in logs.

Just check it.

I want to offer you info on how I did it and what you have to do to prevent it. If interested pay me 1 BTC to

17aLGgw8AwJdqIBtMMG1QtQJgNQQkiyEsp

Thank you.



# SWIFT System Attacks

- Targeted malware enabled hackers to obtain banks' SWIFT network user credentials
- February 2016 attack on Central Bank of Bangladesh: hackers transferred \$100M to accts in Philippines and Sri Lanka; attempted to move \$1B. Loss of \$81M
- Anomalous transactions not detected and blocked by NY Fed
- Attacks on other banks subsequently became known:
- TP Bank in Vietnam – Blocked attempt to transfer \$1.4M in December 2015
- Ecuadorian Banco del Austro – \$12M in fraudulent transfers in January 2015
- October 2017 - \$60M illegally transferred from Far Eastern International Bank in Taiwan

# Ransomware

- South Asian and Middle Eastern Bank Attacks - 2016
- Data purportedly belonging to three Bangladeshi banks, two Nepalese banks, a Qatari bank, and UAE's Invest Bank was posted online in April and May 2016
- Data appears to include customer information and account credentials, scans of identity documents, transaction records, and other sensitive information
- Malware locks or encrypts data on servers, or spreads through networks to many computers. Can shut down entire organizations
- Series of ransomware attacks on U.S. hospitals in early 2016 caused significant disruptions until ransom paid or systems restored from backups
- May 2017 – Worldwide cyber attack by ransomware WannaCry cryptoworm demanding ransom payments in bitcoin. North Korea behind the attacks.

# Digital Currency Thefts

- 2014: Mt. Gox, then the world's largest Bitcoin exchange, based in Tokyo, declares bankruptcy after the theft of \$450M from digital wallets
- 2015: BitStamp, a London-based Bitcoin exchange, loses \$5.2M through compromise of Bitcoin wallets
- 2015: Chinese Bitcoin exchange Bter loses \$1.75M in attack on digital wallets
- June 2016: Decentralized Autonomous Organization loses \$53M in Ethereum digital currency theft
- August 2016: Bitfinex, based in Hong Kong, loses \$65M in Bitcoin theft by hackers
- 2018: Coincheck \$530M worth of NEM coins stolen. North Korea suspected to be the perpetrator.

# Morgan Stanley Data Breach

- Galen Marsh, a financial advisor employed by Morgan Stanley stole confidential information relating to 730,000 accounts and transferred it to his personal server
- Third party hacked Marsh's personal server, stole the customer information, and offered it for sale online in December 2014
- Incident resulted in criminal conviction and industry bar for Marsh, \$1M SEC penalty against firm

# SEC Cybersecurity Regulations

- 28.1.2.4.18. **Comprehensive Information Technology Plan, to include** among others: a) a list and brief description of the software and hardware to be primarily used in its functions and their location; **b) a back-up system or subsystem and their location; c) security system and procedures to be employed;** d) procedures to check sufficiency of system's capacity and expansion program, if necessary; and e) IT system maintenance schedule; and
- 28.1.2.5.2(p). The Commission may **require Broker Dealers to subject their information technology, trading, business continuity, disaster recovery and risk management systems to a regular review and audit by independent firm at least once every three (3) years** and such other frequency that the Commission may deem necessary. The Commission may also require that the results of said review and audit shall be submitted to the Commission

# PH, US, other govs. unprepared to fight hackers

Published February 2, 2018

By Emmie V. Abadilla

Governments the world over, from the Philippines to the United States, are not prepared to fight hackers, cybersecurity expert Marc Goodman declared last Jan. 31, during the PilipinasCon 2018, a Forum on Cybersecurity and the Internet of Things in Taguig City.

**Elections worldwide are being hacked by those who want to cling to power and these incidents have skyrocketed because of automation**, according to Goodman, author of the best-selling book Future Crimes, founder of Future Crimes Institute, and chairman of Policy, Law and Ethics at Silicon Valley's Singularity University.

At the Def Con, the world's longest running and largest underground hacking conference, he said, "They were able to break into 25 different vote counting machines remotely and directly – which means that every single counting device is hackable."

In the Philippines, the susceptibility of its elections to hacking was established when Filipino hackers committed the biggest government data breach in history in April, 2016, one month after the national elections.

***"The Commission on Elections was taken over by the Philippine group of Anonymous to show how hackable the elections were. Over 55 million voter's data were leaked, 200,000 emails leaked, 2.3 million passport details leaked, and 15.7 million fingerprints are now available in the dark web. That was the largest government data breach in the world so far and it was carried out by a 23-year-old Filipino."***

said.

PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018, The Mansions, Iloilo City

# Philippines top victim of cyber attacks

By Edu Punay (The Philippine Star)

| Updated January 15, 2018

MANILA, Philippines — The Philippines, **considered as the social networking capital of the world**, is the **most susceptible nation in Southeast Asia to cyber attacks**, according to an expert.

Digital technology expert Reynaldo Lugtu, a member of the advisory board of Global Chamber Manila, said the country also **ranks 10th in the world in terms of falling prey to cyber attacks**, citing data released recently by the US Federal Bureau of Investigation (FBI). Canada topped the list, followed by India, United Kingdom, Australia, Brazil, Mexico, China, Japan and Germany. Two of the country's neighbors in Southeast Asia – Malaysia and Singapore – also placed in the Top 20.

Lugtu stressed that cyber security in the Philippines remains weak considering such vulnerability to attacks in cyberspace and despite several laws enacted for this purpose.

The Philippines **ranks 37th out of 193 countries in terms of cyber security preparedness** based on the recent global security index report.

“In the legal aspect, we are **ahead of other countries** because we have already passed the **Data Privacy Act, the E-Commerce Law and the Anti-Wiretapping Law**. However, **we are low in the cultural aspect because we are not well-informed of the dangers lurking online so that we easily open emails or click links without knowing the risks,**” Lugtu explained in a forum on Friday.

Lugtu attributed this to lack of information among Filipino cyberspace users on the different schemes of cyber attacks, including hacking, phishing and malware.

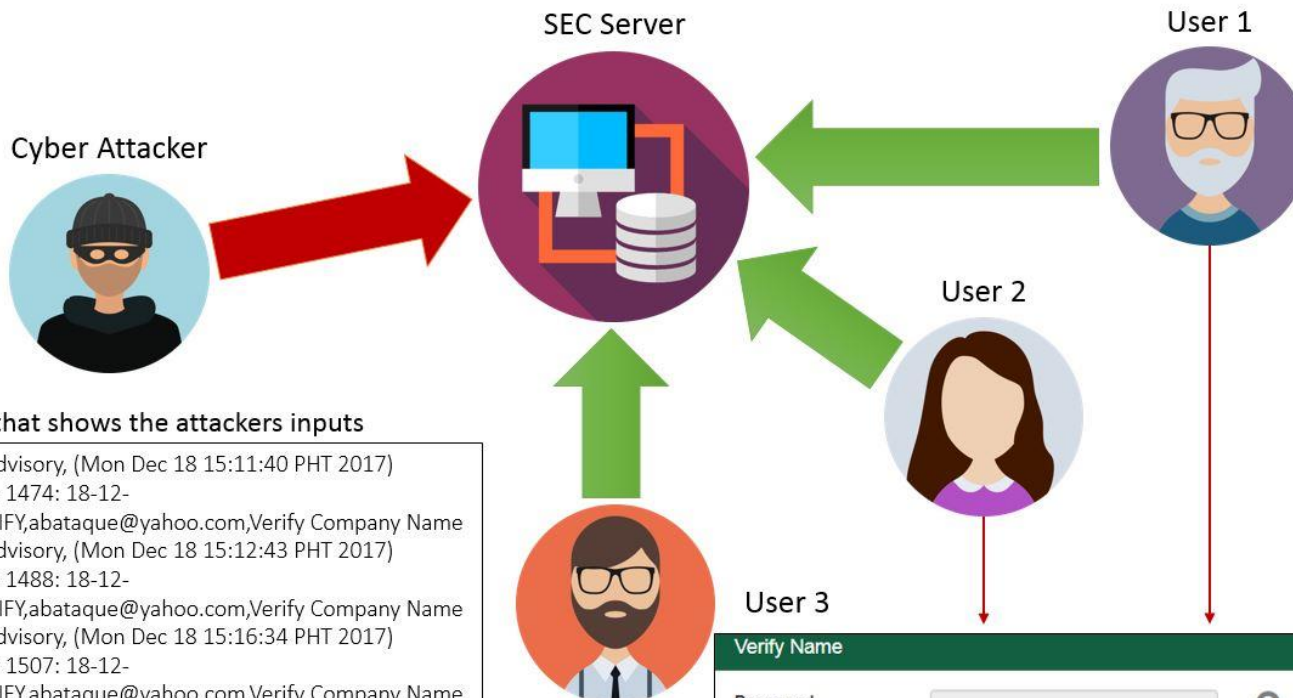
A report of social media management platform Hootsuite and United Kingdom-based consultancy We Are Social Ltd. showed that **Filipinos spent an average of four hours and 17 minutes per day on social media sites such as Facebook, Instagram, Snapchat and Twitter in 2017.**

*PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018: The Mansion, Iloilo City*

# SEC CRS Denial of Service Attack

- From December 15 – 18, 2017 the Developers of the CRS have detected high incidence of hacking attempts
- Unidentified users have flooded the server with false attempts of name verification causing other users to experience high traffic in verifying their company names





### Logs that shows the attackers inputs

```

= SME Business Advisory, (Mon Dec 18 15:11:40 PHT 2017)
  Line 1474: 18-12-
17:15:12:671,VERIFY,abataque@yahoo.com,Verify Company Name
= SME Business Advisory, (Mon Dec 18 15:12:43 PHT 2017)
  Line 1488: 18-12-
17:15:16:656,VERIFY,abataque@yahoo.com,Verify Company Name
= SME Business Advisory, (Mon Dec 18 15:16:34 PHT 2017)
  Line 1507: 18-12-
17:15:21:779,VERIFY,abataque@yahoo.com,Verify Company Name
= Assurance Delivery Philippines, (Mon Dec 18 15:21:26 PHT 2017)
  Line 1523: 18-12-
17:15:24:218,VERIFY,abataque@yahoo.com,Verify Company Name
= SUM-TING-WONG ADVISORS, (Mon Dec 18 15:24:54 PHT 2017)
  Line 1538: 18-12-
17:15:30:319,VERIFY,abataque@yahoo.com,Verify Company Name
  
```

**Verify Name**

Proposed Company Name: \*  ?  ?

Company name for registration

**▲ Please Validate Company Name**

**✘ There is a high traffic in name verification. Please try again after a few minutes.**

**Error message users will get from the server because of high traffic cause by the attacker.**

# Crypto: Friend or Foe

# Facebook bans crypto ads

- Facebook has said it will block any advertising promoting crypto-currency products and services.
- The company said it was open to emerging technologies but many companies were not acting in "good faith" when extolling the virtues buying into virtual currencies.
- Recently, a wave of new currencies have emerged, seeking to piggyback Bitcoin's huge increase in value.
- Facebook urged users to report any ads the company's security measures missed.
- It admitted it would not always catch every ad for a crypto-currency.
- "We want people to continue to discover and learn about new products and services through Facebook ads without fear of scams or deception," wrote Rob Leathern, product management director for Facebook Business.

# Banks ban Bitcoin Purchases

- JPMorgan, Bank of America, and Citigroup are all putting a stop to Bitcoin purchases made using their cards, citing high risk due to extreme price volatility.

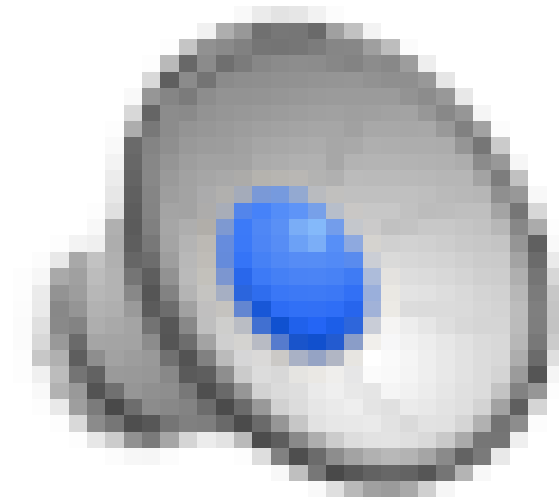
## CREDIT CARDS DECLINED

- With Bitcoin suffering one of its worst weeks since 2013, major US banks are putting a stop to Bitcoin and other cryptocurrency purchases made using their credit cards. According to reports, JP Morgan Chase, Bank of America, and Citigroup are all banning cryptocurrency purchases using their credit cards, leaving some investors eager to “buy the dip” out in the cold.
- “At this time, we are not processing cryptocurrency purchases using credit cards, due to the volatility and risk involved,” a J.P. Morgan Chase spokesperson said in [a statement to CNBC](#). [“We will review the issue as the market evolves.”](#)

## A HARD FALL

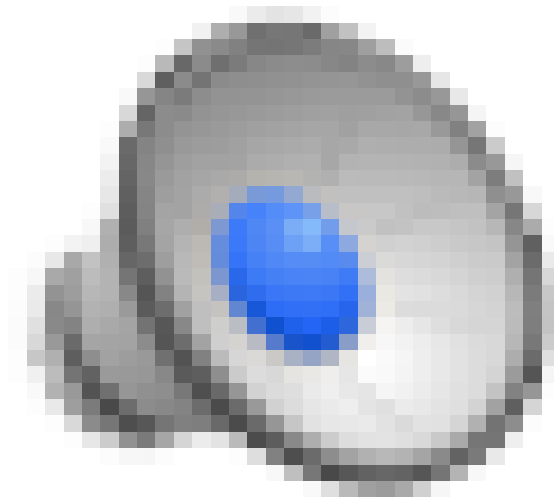
- The decision to ban Bitcoin purchases with certain credit cards comes after a steep and unprecedented run-up at the end of 2017, which has since been followed by a sharp decline.
- Over the past year, Bitcoin has surged more than 700%, reaching highs of \$20,000. On February 2, however, [Bitcoin reached lows of under \\$8,000 – and some inexperienced investors who FOMO’d \(Fear of Missing Out\) into the cryptocurrency market at its all-time high using credit may have already panic sold.](#)

# Bitcoins Simplified

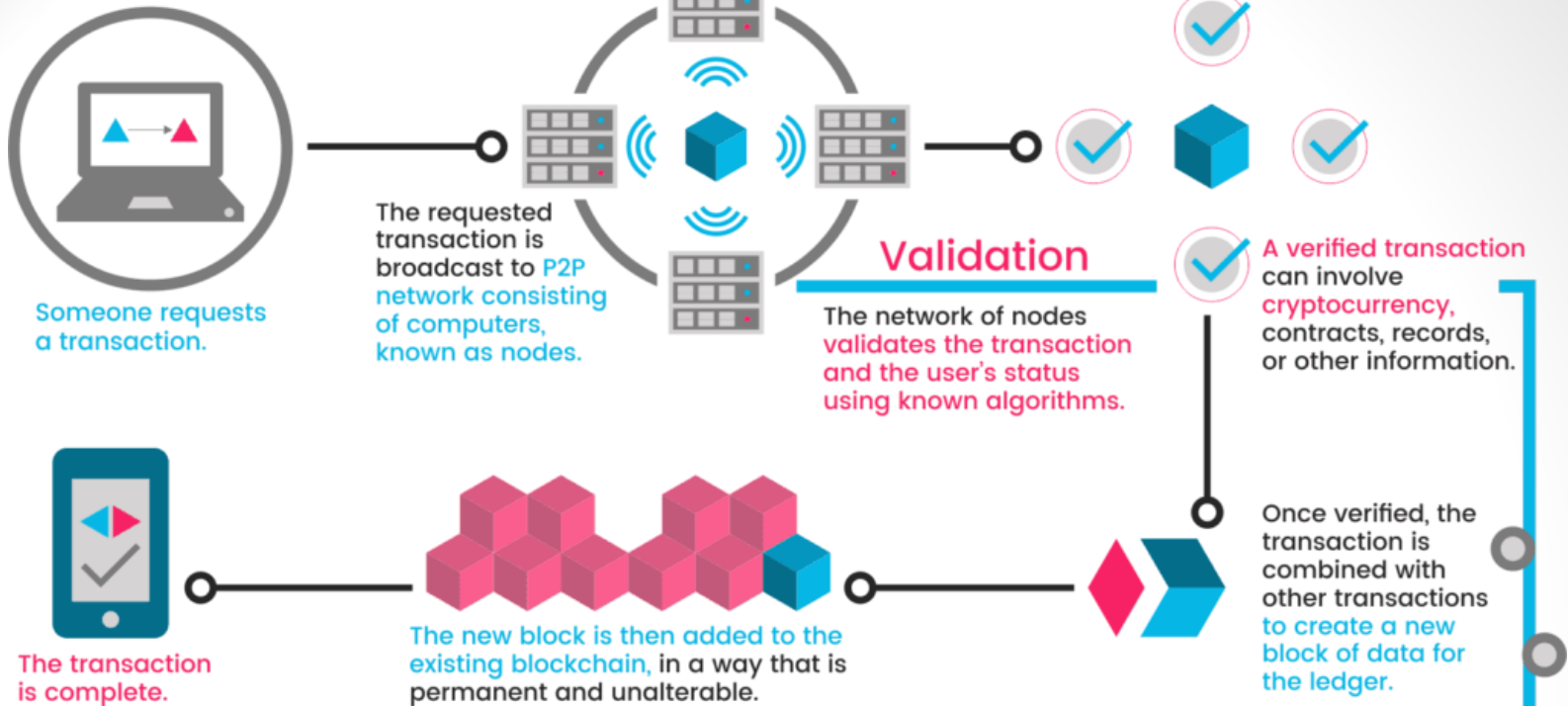


# Blockchain

(Underlying Technology of Bitcoin and other cryptocurrencies)



# How it works:



## Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.



Has no **intrinsic value** in that it is not redeemable for another commodity, such as gold.



Has no **physical form** and exists only in the network.



Its supply is not determined by a central bank and the network is completely decentralized.

PAGBA 1st Quarterly Seminar and Meeting  
February 2018: The Mansion, Iloilo City

# What are Cryptocurrencies?

- Cryptocurrencies are digital or virtual currencies that are encrypted (secured) using cryptography. Cryptography refers to the use of encryption techniques to secure and verify the transfer of transactions. Bitcoin represents the first decentralized cryptocurrency, which is powered by a public ledger that records and validates all transactions chronologically, called the Blockchain.
- It is important to note that all coins or tokens are regarded as cryptocurrencies, even if most of the coins do not function as a currency or medium of exchange. *The term cryptocurrency is a misnomer* since a currency technically represents a unit of account, a store of value and a medium of exchange. All these characteristics are inherent within Bitcoin, and since the cryptocurrency space was kickstarted by Bitcoin's creation, any other coins conceived after Bitcoin is generally considered as a cryptocurrency.



# Crypto: Altcoins

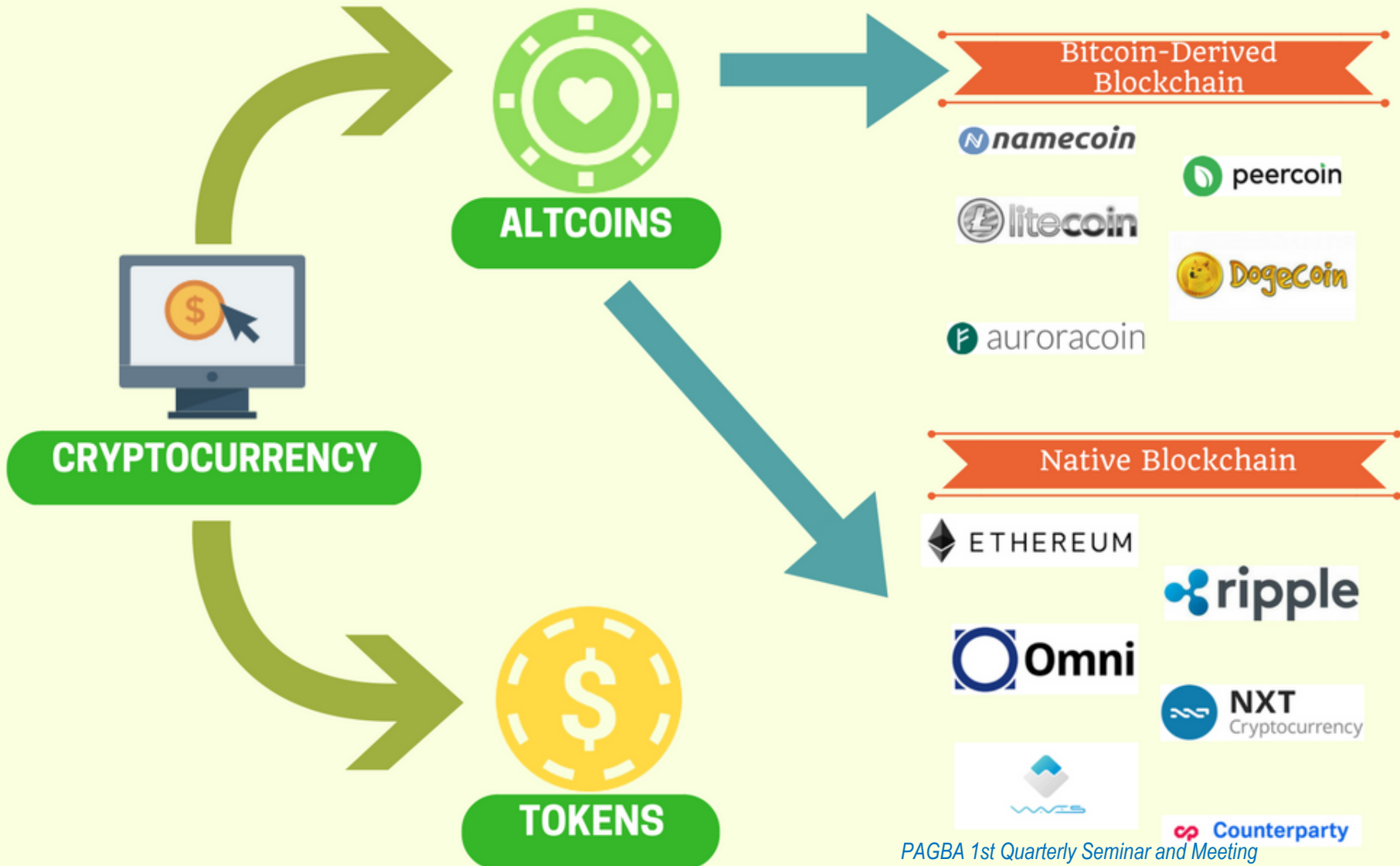
- Alternative cryptocurrency coins are also called altcoins or simply “coins”. They’re often used interchangeably. Altcoins simply refers to coins that are an alternative to Bitcoin. The majority of altcoins are a variant (fork) of Bitcoin, built using Bitcoin’s open-sourced, original protocol with changes to its underlying codes, therefore conceiving an entirely new coin with a different set of features.
- There are other altcoins that aren’t derived from Bitcoin’s open-source protocol. Rather, they have created their own Blockchain and protocol that supports their native currency. Examples of these coins include [Ethereum, Ripple, Omni, Nxt, Waves and Counterparty.](#)
- A commonality of all altcoins is that they each *possess their own independent blockchain*, where transactions relating to their native coins occur in.

# Crypto: Tokens

Tokens are a representation of a particular asset or utility, that usually resides on top of another blockchain. Tokens can represent basically any assets that are fungible and tradeable, from commodities to loyalty points to even other cryptocurrencies!

Creating tokens is a much easier process as you do not have to modify the codes from a particular protocol or create a blockchain from scratch. All you have to do is follow a standard template on the blockchain – such as on the Ethereum or Waves platform – that allows you to create your own tokens. This functionality of creating your own tokens is made possible through the use of smart contracts; programmable computer codes that are self-executing and do not need any third-parties to operate.

# CRYPTOCURRENCY TYPES



# BITCOIN

Bitcoin is the original cryptocurrency, and was released as open-source software in 2009.

Using a new digital ledger known as the blockchain, the Bitcoin protocol allows users to transact peer-to-peer transactions using digital currency while avoiding the "double spending" problem.

No central authority or server controls transactions, and instead the legitimacy of a payment is determined by the decentralized network itself.

## KEY FEATURES

- Blockchain - Foundational Technology
- Fast P2P Payments Worldwide
- No Double Spend Problem
- Low Processing Fees
- Decentralized
- Available To Anyone
- Anonymity (Partial)
- Transparent

## INTERESTING FACT

In 2010, a programmer bought two pizzas for 10,000 BTC in what is the first real-world Bitcoin transaction. Today, 10,000 BTC is equal to roughly \$28.1 million - a big price to pay for satisfying hunger pangs.

While regrettable, it is also forgivable. No one knew Bitcoin would be around by the time the first real-world Bitcoin transaction occurred.

New cryptocurrency enthusiasts around the world celebrate "Bitcoin Pizza Day" every year on May 22nd, the date the transaction took place.

### 1 10,000

## BOTTOM LINE FOR BITCOIN

Bitcoin is the original cryptocurrency with the most liquidity and significant network effects. It also has the most name recognition around the world, with an eight-year track record.

# LITECOIN

Litecoin was launched in 2011 as an early alternative to Bitcoin.

Around this time, increasingly specialized and expensive hardware was needed to mine bitcoins, making it hard for regular people to get in on the action. Litecoin's algorithm was an attempt to open the playing field so that anyone with a regular computer could take part in the network.

## KEY DIFFERENTIATIONS FROM BITCOIN

- A Simpler Cryptographic Algorithm
- 4x Faster Block Generation
- Faster Transaction Processing
- 84 Million Coins Max (Bitcoin: 21 million)

## INTERESTING FACT

Litecoin's creator is a former Google employee, and MIT grad named Charlie Lee, the scientist who made cryptocurrency more accessible - and for Litecoin to be the "silver" to Bitcoin's "gold".

## BOTTOM LINE FOR LITECOIN

Other altcoins have taken away some of Litecoin's market share, but it still has an early mover advantage and some strong network effects.

# RIPPLE

Ripple is considerably different from Bitcoin. That's because Ripple is essentially a global settlement network for other currencies such as USD, Bitcoin, EUR, GBP, or any other units of value (i.e. "fiat" or real money, commodities).

To make any such settlement, however, a tiny fee must be paid in XRP (Ripple's native token) - and these are what trade on cryptocurrency markets.

## KEY DIFFERENTIATIONS FROM BITCOIN

- Global Settlement Network
- Works With Any Store of Value
- Backed By Many Banking Institutions
- No Mining Involved

## INTERESTING FACT

Because Ripple is intended as a new global settlement system for the exchange of currencies and other assets, many banks are experimenting with the technology. Banks' earliest supporters include Royal Bank of Canada, Citicorp, UBS, and Citigroup.

There is no "mining" on the Ripple network - instead, there is an existing supply of 100 billion ripples, with only half being held by the company. In mid-2015 the company announced that it had up-ripples in dollars worth of ripples in escrow smart contracts to decrease any fears of the market being "floored".

## BOTTOM LINE FOR RIPPLE

Ripple runs on many of the same principles as Bitcoin, but for a different purpose: to serve as the middle man for all global P2P transactions. It can successfully capture that market, the potential is high.

# THE CRYPTO UNIVERSE

## COMPARING SIX MAJOR CURRENCIES

Timeline: Bitcoin (2009), Litecoin (2011), Ripple (2012), Dash (2014), Ethereum / Ethereum Classic (2015)

## % OF THE CRYPTO UNIVERSE VALUE

Year	Bitcoin	Litecoin	Ripple	Dash	Ethereum	Ethereum Classic	Other
2013	93%	3%	3%	0%	0%	0%	0%
2015	84%	7%	3%	2%	2%	0%	0%
2017	47%	1%	2%	6%	19%	2%	23%

## MARKET CAPITALIZATION

Year	Bitcoin	Litecoin	Ripple	Dash	Ethereum	Ethereum Classic
2013	\$76.1B	\$4.15B	\$8.6B	\$2.4B	\$31B	\$1.7B
2015	\$9.6B	\$8.1M	\$43.6M*	\$140M	\$5.8B	\$53M
2017	251K	24K	600K*	7K	373K	37K

## ALL-TIME PEAK PRICE USD

Date	Bitcoin	Litecoin	Ripple	Dash	Ethereum	Ethereum Classic
Sep. 1, 2017	\$4,935					
Jun. 12, 2017			\$412.93			
Aug. 26, 2017			\$409.77			
Jun. 16, 2017			\$22.22			
May 17, 2017			\$0.43			
Sep. 2, 2017			\$1.32			

## Metrics by Coin

- Market Capitalization: Bitcoin (\$76.1B), Litecoin (\$4.15B), Ripple (\$8.6B), Dash (\$2.4B), Ethereum (\$31B), Ethereum Classic (\$1.7B)
- Daily Volume (30 day moving avg): Bitcoin (\$9.6B), Litecoin (\$8.1M), Ripple (\$43.6M\*), Dash (\$140M), Ethereum (\$5.8B), Ethereum Classic (\$53M)
- Daily Transactions (30 day moving avg): Bitcoin (251K), Litecoin (24K), Ripple (600K\*), Dash (7K), Ethereum (373K), Ethereum Classic (37K)

\*Source: coinmarketcap.com as of Sept. 12, 2017

# DASH

Dash is an attempt to improve on Bitcoin in two main areas: speed of transactions, and anonymity.

To do this, Dash has been their architecture with miners and also "masternodes" that help the network perform advanced functions such as near-instant transactions and coin-mixing to provide additional privacy.

## KEY DIFFERENTIATIONS FROM BITCOIN

- Two-Tier Architecture
- Advanced Transactions
- Decentralized Autonomous Organization (DAO)
- Improved Anonymity

## INTERESTING FACT

For each block mined, a 1% reward goes to the treasury to help fund improvements and projects around Dash.

Dash is the first ever Decentralized Autonomous Organization (DAO), a type of organization run through rules encoded in computer programs and smart contracts.

## BOTTOM LINE FOR DASH

The innovations behind Dash are interesting, and could help to make the coin more consumer-friendly than other alternatives.

# ETHEREUM

Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

In the Ethereum blockchain, instead of mining for bitcoins, miners work to earn ether, a type of crypto token that fuels the network. Beyond a tradable cryptocurrency, ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

## KEY DIFFERENTIATIONS FROM BITCOIN

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

## INTERESTING FACT

Ethereum has had a rocky adoption from its introduction in 2015, and to date its total market value is approximately the market cap of Bitcoin.

It's increased in value by 2,200% in just the last year - a huge boon for early investors.

## BOTTOM LINE FOR ETHEREUM

Ethereum serves a different purpose than other cryptocurrencies, but it has quickly grown to replace all but Bitcoin in value. Some experts are so bullish on Ethereum that they even see it becoming the world's top cryptocurrency in just a short span of time - but only time will tell.

# ETHEREUM CLASSIC

In 2016, the Ethereum community faced a difficult decision. The DAO, a venture capital firm built on top of the Ethereum platform, had \$50 million in ether stolen from it through a security vulnerability.

The majority of the Ethereum community decided to help the DAO by "hard forking" the currency, and then changing the blockchain to return the stolen proceeds back to the DAO. The minority thought this idea violated the key foundation of immutability that the blockchain was designed around, and kept the original Ethereum blockchain the way it was. Hence, the "Classic" fork.

## KEY DIFFERENTIATIONS FROM BITCOIN

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

## INTERESTING FACT

Because Ethereum and Ethereum Classic stem from the same code, they run in parallel, using virtually the same thing.

The DAO hacker still holds over 3 million of Ethereum Classic, which could be "burned" somewhere along the line - a baked in risk that could drag on price.

## BOTTOM LINE FOR ETHEREUM CLASSIC

As time goes on, Ethereum Classic has been carving out a separate identity from its bigger sibling. With similar capabilities and a different set of principles, Ethereum Classic could still have upside.

etoro.com - etoro is the first global market place for people to trade currencies, commodities, indices and CFD stocks online in a simple, transparent and more enjoyable way.

VISUAL CAPITALIST

Facebook: /visualcapitalist, Twitter: @visualcap, LinkedIn: /visualcapitalist, Instagram: /visualcapitalist

# What is an ICO?

An ICO stands for **Initial Coin Offering**, it is a fundraising procedure wherein a company entice capitalists who are looking for the next big thing in crypto by releasing its digital currency for bitcoin and ether in return. As of November 2017, there were **around 50 offerings per month**. There's a new ICO web browser named "Brave" which generated \$35 million in just under 30 seconds. As of October 2017, there were ICO coin sales worth \$2.3 billion had been executed during the year and it is more than 10 times as much as in all ICO coin sales in 2016.

The initial coin offering can be of use for a wide range of activities, it is from **corporate finance** to a **charitable fundraising** and to a **complete trickery or fraud**. Many ICOs could give luck to an investor. One good example is ETH, it was sold at 0.0005 BTC and today, it is worth almost 0.05 BTC. If you bought the coin on its lowest price let's say that was 0.0005 BTC per 1 ETH and you have hold it until now, eventually, you will have a **10,000% gain**.

# Useless Ethereum Token Crowdsale Netted \$300K

[JP Buntinx January 11, 2018 Crypto, News](#)

- A few months ago, an individual announced he was creating the Useless Ethereum Token. As the name suggests, this new asset serves no real purpose, will not necessarily appreciate in value, and shouldn't even be listed across exchanges. Despite the lack of appeal to investors, the Useless Ethereum Token's creator raised over US\$300,000 through his initial coin offering. It is evident a lot of people didn't pay attention to what this project was about.
- Although no one really expected anything to come of the Useless Ethereum Token, it did confirm that the entire initial coin offering industry is in a very bad place. Anything that is labeled an ICO, blockchain, or cryptocurrency will attract a lot of attention at some point. In some cases, projects might even raise several thousands of dollars even though they blatantly state their currencies will never achieve any goals. Even so, investors are still too blind to read the obvious and they keep throwing money at pretty much everything.
- Such was the case for the Useless Ethereum Token. Although its website was designed in a clever manner, the creator never shied away from mentioning how this token would never amount to anything. In fact, he made it clear no one should buy into this ICO or expect to use the token in the future. No one should be particularly surprised to learn there are some people who actually bought into this ICO, allowing the "inventor" of the Useless Ethereum Token to raise over US\$300,000.
- It is obvious that people should never invest in offerings such as this one. Why some people eventually decided to ignore all of these warnings is hardly understandable. The Etherscan address shows over 23,630 transactions, the last of which took place just three days ago. That's pretty problematic, for obvious reasons.

# How Governments React

Dec 3, 2017 at 15:00 UTC

*Dunny Medina is the head of capital markets and securities at Oziel Law, a business and technology law firm based in Toronto, Canada.*

- The message is far from clear. While many nations can stand united on challenges like melting ice caps, they're a bit more baffled with crypto.
- So, how does a government react when faced with this new class of disruption? We have identified at least five approaches by global governments to ICOs.
- The 'forbidden city' approach
- On one extreme, we have the “forbidden city” approach currently championed by the People’s Bank of China: a [blanket ban on ICOs and exchanges.](#)
- As many observers have noted, this approach is likely a stopgap measure that allows a government to be unequivocal (all token sales are illegal) until it can properly assess the situation and decide what to do.

# How Governments React

- 'in the works' approach
- Some governments, in the face of change, choose to be progressive and open to innovation. They come out and say: we recognize that this is different, so we need to have special legislation, and we are working on it.
- In some cases, this may be optics alone. Russia flip-flopped in the past few months on its stance on ICOs, but the latest comes right from the top: President Vladimir Putin has ordered that legislation be implemented on ICOs to bring them in line with traditional securities financings (e.g., initial public offerings of stock).
- In other cases, it may be an earnest attempt to put forth clear legislation. The governments of Isle of Man and Gibraltar seem to have a repurposing or revised framework of existing legislation in development.



# How Governments React

- The 'warning' approach
- The U.S., Australia and Japan are all prime examples of reasonable democracies for which the “warning” approach is not an unreasonable reaction.
- When faced with a complicated and disruptive development, one should not be hasty. Don't crack down, but also don't go full-steam ahead. The safer approach is to fall back on existing legislation and issue statements which amount to warnings, rather than clear-cut guidelines.
- To paraphrase, here's the gist of these statements: *Be careful. ICOs are risky and dangerous. It's possible that a token, depending on the circumstances, might not be a security, but it probably is. If the token resembles a security, again on a case-by-case basis, then you need to follow existing securities regulation for an ICO.*

# How Governments React

- The 'sandbox' approach
- A regulatory "sandbox," in theory, invites companies to work with the regulators, with the promise of a temporary free pass on some of the more complex and costly aspects of securities regulations.
- The Canadian regulatory sandbox is one of the more active global sandboxes, and it has come out with some definitive results. It's a live laboratory currently running a few regulatory experiments with ICOs, token crowdfunding platforms and crypto investment funds.
- Most recently, the Canadian regulators put out a decision on the [TokenFunder ICO, which may win the award for the most clearly laid out guideline on how to run a compliant security ICO.](#)
- This latest guinea pig decision sets out how to offer tokens to both high-net-worth and retail investors under an ICO, the requirement for additional know-your-client (KYC) and other onboarding procedures, and the acceptability of a template form for a detailed white paper (by using an existing disclosure document in Canada known as an Offering Memorandum).

# How Governments React

- The 'jack-of-all-trades' approach
- And then there is Switzerland.
- A refreshing laissez-faire mentality to crypto seems to be in the Swiss mountain air, but the reality (as usual) is a bit murkier.
- At one point in the summer, some commentators had mentioned that the token vs. security debate was much more clear-cut under Swiss law, such that token sales were not regulated. Smells a little funky.
- The reality may be that it's only unregulated because the Swiss haven't regulated it yet; they're working on it.
- And then, on September 27, Switzerland's Financial Market Supervisory Authority (FINMA) announced that it is investigating ICO procedures, indicating that these transactions may come under existing regulatory legislation. The old "warnings" approach.

# Bangko Sentral Ng Pilipinas

Circular No. 944, Series of 2017 in relation to Circular No. 942 on Money Service Businesses

- Subject: Guidelines for Virtual Currency (VC) Exchanges
- The Monetary Board, in its Resolution No. 121 dated 19 January 2017, approved the following rules and regulations governing operations of VC exchanges in the Philippines, which shall be incorporated as Section 4512N of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).
- Section 1. Section 4512N shall read as follows:  
"Section 4512N Guidelines for Virtual Currency Exchanges; Statement of Policy.
- It is the policy of the Bangko Sentral to provide an environment that encourages financial innovation while at the same time ensure that the Philippines shall not be used for money laundering (ML) or terrorist financing (TF) activities and that the financial system and financial consumers are adequately protected. Thus, the Bangko Sentral recognizes that **Virtual Currency (VC) systems have the potential to revolutionize delivery of financial services, particularly for payments and remittance**, in view of their ability to provide **faster and more economical transfer of funds, both domestic and international, and may further support financial inclusion**. These benefits, however, should be considered along with the corresponding risks in VCs considering the higher degree of anonymity involved, the velocity of transactions, volatility of prices and global accessibility. In particular, VCs pose ML and TF risks, information technology risks, and consumer protection and financial stability concerns, among others.
- The **Bangko Sentral does not intend to endorse any VC, such as bitcoin, as a currency since it is neither issued or guaranteed by a central bank nor backed by any commodity**. Rather, the BSP aims to regulate VCs when used for delivery of financial services, particularly, for payments and remittances, which have material impact on anti-money laundering (AML) and combating the financing of terrorism (CFT), consumer protection and financial stability.

# Phil. SEC Advisory on ICOs

Published January 8, 2018

- The Commission has detected that certain companies, individuals or groups of persons are enticing the public, either through popular social media platforms or through their own independent website, to participate in so-called “initial coin offerings” and to purchase the corresponding “virtual currency”.
- Virtual currency refers to a digital representation of value issued and controlled by its developers and used and accepted among the members of a specific community or users. An Initial Coin Offering (ICO) is the first sale and issuance of a new virtual currency to the public usually for the purpose of raising capital for start-up companies or funding independent projects. In an ICO campaign, a percentage of the total available virtual currency is sold to interested buyers in exchange for (1) fiat currency; (2) another virtual currency; or (3) another asset or security.
- Based on the information gathered by the Commission, some of these new virtual currencies, based on the **facts and circumstances surrounding their issuance, follow the nature of a security as defined by Section 3.1 of the Securities Regulation Code (SRC)**. However, unlike ordinary securities, these virtual currencies are neither guaranteed by any Central Bank nor backed by any commodity. (Section 1 par. 2 of BSP Circular No. 944, Series of 2017)
- When a virtual currency is likewise analogous to any of the types of securities under Section 3.1 of the SRC, there is a strong possibility that the **said virtual currency is a security under the jurisdiction of the SEC and has to be registered and necessary disclosures have to be made for the protection of the investing public.**

# US SEC Action Against Plexcoin

Washington D.C., Nov. 11, 2017

- PlexCoin, a Canadian digital token startup, is flatly “a scam,” according to the US Securities and Exchange Commission.
- SEC filed for an emergency freeze of the US assets of the company and those of its founders, Quebecers Dominic Lacroix and Sabrina Paradis-Royer, on Friday. The US SEC said that PlexCoin has “all of the characteristics of a full-fledged cyber scam.” Lacroix’s assets in Quebec have already been frozen by the Autorité des marchés financiers (AMF).
- PlexCoin is a digital token on the Ethereum platform that launched with an ICO. During its fundraising round, which began in August, the SEC states that thousands of investors traded \$15M worth of cryptocurrency for PlexCoin tokens. But while tokens for some Ethereum apps are functional, PlexCoin tokens had no discernable purpose except to become more valuable as people buy and sell them while promising eye-popping returns.

# US SEC Enforcement Action on DAO

Washington D.C., July 25, 2017

- The US SEC issued an investigative report cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of securities laws. Such offers and sales, conducted by organizations using distributed ledger or blockchain technology, have been referred to as "Initial Coin Offerings" or "Token Sales." Whether a particular investment transaction involves the offer or sale of a security – regardless of the terminology or technology used – will depend on the facts and circumstances, including the economic realities of the transaction.
- SEC's report of Investigation found that tokens offered and sold by a "virtual" organization known as "The DAO" were securities and therefore subject to securities laws. The Report confirms that issuers of distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws. Additionally, securities exchanges providing for trading in these securities must register unless they are exempt. The purpose of the registration provisions is to ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for investors' protection.

# US SEC CDO on Munchee

Washington D.C., Dec. 11, 2017 —

A company selling digital tokens to investors to raise capital for its blockchain-based food review service halted its ICO after being contacted by the SEC, and agreed to an order which found that its conduct **constituted unregistered securities offers and sales.**

According to the SEC's order, before any tokens were delivered to investors, Munchee Inc. refunded investor proceeds after it intervened. Munchee was seeking \$15 million in capital to improve an existing iPhone app centered on restaurant meal reviews and create an "ecosystem" in which Munchee and others would buy and sell goods and services using the tokens.

The SEC's new Cyber Unit is focused on misconduct involving distributed ledger technology and ICOs, the spread of false information thru electronic and social media, brokerage account takeovers, hacking to obtain nonpublic information, and threats to trading platforms.



# US SEC Action on Arise Bank

Jan 30, 2018 at 14:50 UTC

- The U.S. SEC is suing cryptocurrency banking company AriseBank, according to public documents.
- AriseBank, together with its co-founders Jared Rice Sr. and Stanley Ford, is being charged by SEC for alleged fraud and **issuing unregistered securities** during its recent ICO, according to the latest court filing.
- Texas State's Department of Banking also announced a cease-and-desist order on AriseBank's operation went into effect.
- AriseBank is a cryptocurrency banking firm that claims to offer several banking products related to cryptocurrency. Its ICO was notably endorsed by former boxer Evander Holyfield.
- It started an ICO to launch its own token dubbed AriseCoin around November last year and claimed to have raised over \$1 billion through both private and public token sales.

# Phil. SEC CDO against KROP

## HOWEY TEST

### 1. INVESTMENT IN MONEY

- The term “Money”, in the Howey Test pertains to “any valuable consideration” as highlighted in the US DAO Report
- The Ethereum used to buy KROPSCOINS is considered as money

### 2. IN A COMMON ENTERPRISE

- KROPS is a technology-based start-up company as described in its WHITEPAPER



Are tokenized shares of its start-up company “Krops” as described in its Whitepaper

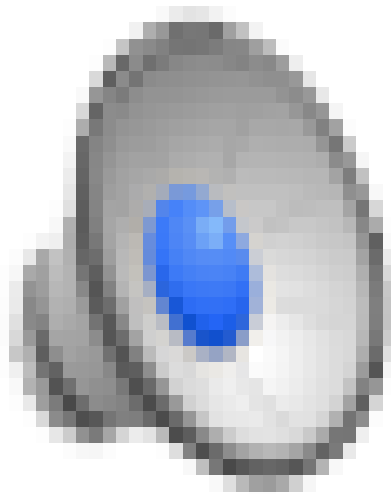
### 3. EXPECTATION OF PROFIT

- Investors are led to believe that KROPSCOINS will appreciate in value

### 4. PRIMARILY FROM EFFORTS OF OTHERS

- Investors need not participate in the envisioned agricultural market
- It is the efforts of the company that creates profit and coin price appreciation

# SEC Regulatory Focus on ICOs



# SEC Advisory

dated June 2, 2017



The public is warned about **MONSPACE PHILIPPINES**. It claims that it has a system wherein investors can invest and become stockholders of its subsidiaries by simply investing an initial capital amounting to P7,600.00 with a possible daily income of P5,000.00 and/or monthly income of P150,000.00.

In its Facebook Account **MONSPACE PHILIPPINES** introduced its newest scheme called the MSCOINS, wherein part of their marketing plan as shown in said FB Account is to persuade the public to join them by investing an initial capital of P7,600.00, P800.00 representing Registration Fee and P6,800.00 for 500 Product Points, respectively. Accordingly, after 30 days, the 500 Product Points will be converted into MSCOINS based on the following, to wit:

500 product points = \$100

\$100/\$.10 per mscoin = 1,000 mscoins

After a week: \$.50 x 1000 mscoins = \$500 (P25,000)

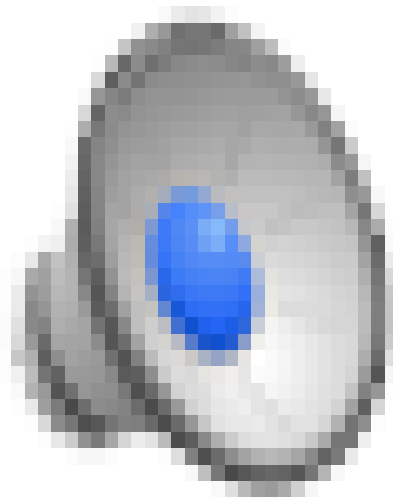
After a month: \$1 x 1,000 mscoins = \$1,000 (P50,000)

After 3 months: \$10 x 1,000 mscoins = \$10,000 (P500,000)

Month after month or after a year: \$100 x 1,000 mscoins = \$100,000 or

P5,000,000

# Monospace (MSCoin) Video



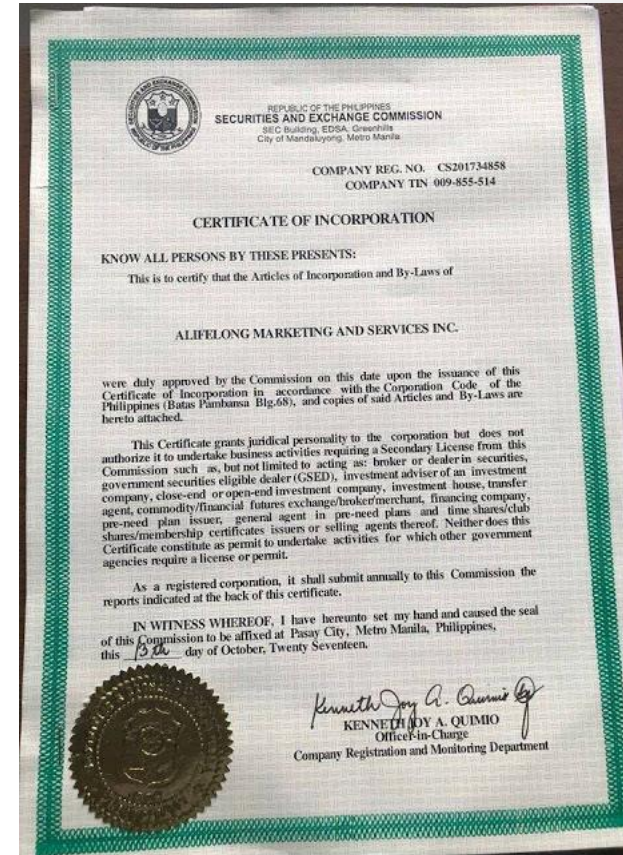
# SEC Advisory: Alifelong Marketing

The public is warned of ALIFELONG. It claims that it is an advertising/marketing company having clientele based abroad. It guarantees to its members significant gains from their P1,500 initial investment by buying “clicking accounts” or by referrals.

ALIFELONG requires its members to sign up through its website by clicking a sponsored link and purchasing an activation code worth P1,500 using either **bitcoin** or by depositing money in certain bank accounts.

ALIFELONG claims a member may earn in 6 ways:

1. Sign up Reward
2. Sponsoring an Affiliate Reward
3. Youclick Programme
4. Match Sales Reward
5. Sponsorship Level Reward
6. Leveling Bonus



SEC Advisory: Jan. 5, 2018

PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018 : The Mansion, Iloilo City

# ALIFELONG VICTIM



Nov 18, 2017 at 6:34pm • 🌐

Eto matindi nag invest sakin sa alifelong from Hongkong nag 120 accounts. 1 500 per account So total nito 180,000.00. Me pending pa sya sakin order na 15 codes. So total investment nya ay wapping 202,500.00. Which he just bought today. And meron pa syang existing na 15 account before this.

Mag duda ka lang. Ito hindi nag duda nag full blast.

Check dates check time if its legit.

**I-Remit Global Remittance**  
Owned and Managed by Lucky Star Management Limited  
Shop 223, 2/F World Wide Plaza, 18 Des Voeux Road,  
Central Hong Kong, SAR  
Tel. No.: +852 2490 - 3028 / +852 2521 - 2167  
+852 2521 - 2166  
Fax: +852 2521 - 5381  
Website: www.i-remit.com

**IREMIT**  
GLOBAL REMITTANCE

RAF No.:  
Remitter ID No.:  
Transaction Date:

**REMITTANCE APPLICATION FORM**  
**OFFICIAL RECEIPT**

RAF No.: L0HPA0002377499  
Remitter ID No.: 0006182740  
Transaction Date: Nov 18 2017 6:01PM

Remitter Name: **ON, ADRIAN**  
Address: **Room A, Lockhart Road, Wan Chai, Hong Kong.**  
Permanent Address:  
Tel. No.:  
Mobile No.:

Delivery Mode: Bank-to-Bank Provincial  
Payment Mode: Cash  
Beneficiary: **TOLENTINO, ED ELIZER RAMOS**  
Birth Date:  
Address:  
Service Center: **63-9175147843**  
Account No.: **Banco De Oro 003700214078**  
CONTROL NO.:

REMARKS: **Job: DJ/Musician Source: Salary Purpose: Savings**  
Double the Fun eTickets earned: 1

Pay Amount	HKG	27521.67
Service Charge	HKG	20.00
Total Payment Due	HKG	27541.67
Amount Tendered	HKG	275500.00
Change	HKG	8.33

Message to Beneficiary: **Exchange Rate = PHP 8,5403 / HKG 1.00**  
Net Remittance Proceeds = **PHP 180000.00**

This REMITTANCE APPLICATION FORM (RAF) when machine validated and signed by the Authorized Signatory of IRemit will serve as the OFFICIAL RECEIPT (OR). By signing this RAF, the remitter certifies having reviewed all the information validated herein and that all information are correct and complete. IREMIT shall not be liable for delays, mispayment or failure to deliver remittance due to errors arising from details provided by the remitter/client. IREMIT shall exercise best effort in executing delivery of transaction. In the event of Acts of God, fortuitous event and other unforeseen circumstances such as but not limited to, motorcycle breakdown, courier accident, typhoons, flood, earthquake, IREMIT shall, however not be liable for delays resulting from such incidents.

PLEASE COUNT YOUR CHANGE BEFORE LEAVING THE COUNTER

REMITTER'S SIGNATURE

Def Rio, Maurice

PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018, The Mansion, Iloilo City

# SEC Advisory:

dated Oct. 11, 2017

# Pluggle

EARN BITCOIN FROM DAILY LOGIN  
www.pluggle.com.ph

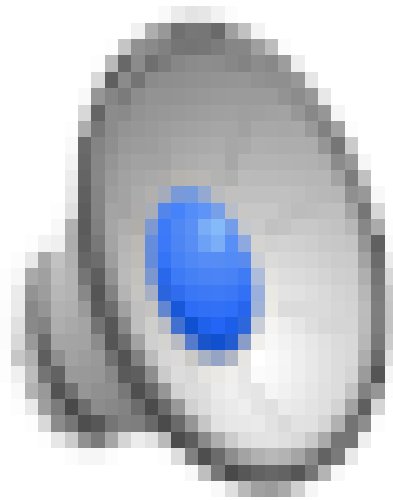


- The public is warned about PLUGGLE. It claims that it has an advertising website wherein its members can receive significant gains from their P1,000 initial investment by simply logging in everyday or by obtaining referrals.
- PLUGGLE requires its members to sign up to its website through a sponsored link and to purchase an activation code worth P1,000 through their accounts using bitcoin or through other legitimate members or leaders.
- PLUGGLE claims its members may earn in 6 ways:
  - Sign up bonus – The member will earn P100 upon registration;
  - Personal login bonus – The member will earn P100 every time he logs in his acct.;
  - Group login bonus – The member will earn P60 per login of his 1st level downlines and P40 per login of his 2nd level downlines;
  - Follow bonus – The member will earn P100 for every person he sponsors into the system. There are no limitations as to the number of persons the member intends to sponsor;
  - Leveling bonus – The member will earn P400 for 1 pair in each level down to the 10th level of the binary structure;
  - Pairing bonus – The member will earn P100 for every pair in the binary structure. There are no limitations as to the number pairs.
- In its Facebook Account PLUGGLE promises a return of 30% *100% in 12 days.*

*PAGBA 1st Quarterly Seminar and Meeting  
February 8, 2018 : The Mansion, Iloilo City*



# PLUGGLE VIDEO



# Some Take-Aways

- On Cryptocurrencies:

For Regulators: Balance between investor protection and innovative and cheaper ways to raise capital

For Investors: Avoid the Fear of Missing Out (FOMO)

- On Cybercrimes (Traditional but done online)

Take the Byte out of the Cybercrime Bite thru Education

Pause before you Post

- On Cybercrimes (Advanced or High Tech)

Think before you click

- On Cybersecurity

Plan Plan Plan

Have Regular Vulnerability Assessments

THANK YOU