Fraudes, Crimes e Ataques Cibernéticos em Criptomoedas

Luciano Porto Barreto

lbarreto@cvm.gov.br / luciano.barreto@ime.uerj.br

Comissão de Valores Mobiliários (CVM)
Universidade do Estado do Rio de Janeiro (UERJ)

São Paulo - 07/12/2017

Fraudes, Crimes e Ataques Cibernéticos em Criptomoedas

As declarações e conteúdo desta apresentação são de inteira responsabilidade do autor, não representando necessariamente a opinião oficial ou visão de seus empregadores sobre os assuntos abordados.

O autor não recomenda, defende ou atesta o uso, compra, investimento ou serviço associado a qualquer projeto de criptomoeda, exchange, ICO, desenvolvedor, auditor ou provedor de tecnologia relacionados a tais tecnologias ou serviços.

Criptomoedas - Interesse

Bloomberg Technology | Markets | Tech | Pursuits | Politics | Opinion | Businessweek

One of the Biggest Bitcoin Exchanges Just Added 100,000 Users in a Single Day

By **Brandon Kochkodin**

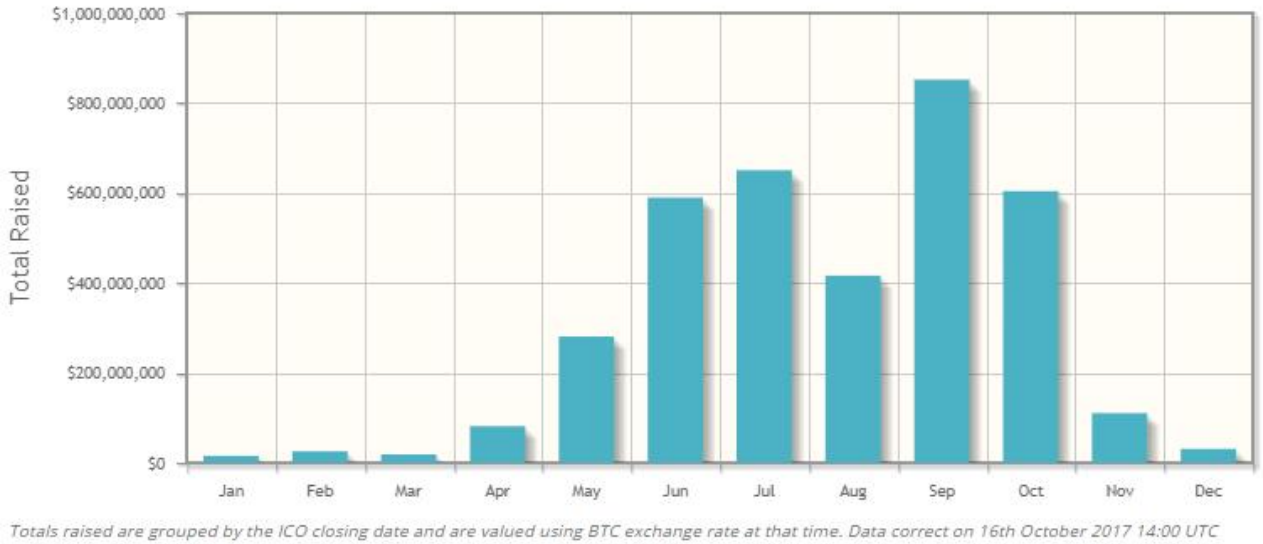
2 de novembro de 2017 13:59 BRST

Bitcoin: histórico de cotação

Última atualização: 6/12/17 (URL)

ICOs: Captação em 2017

Cryptocurrency ICO Stats 2017



Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data correct on 16th October 2017 14:00 UTC

Total Raised: $3,675,135,293

Total Number of ICOs: 234

Top Ten ICOs of 2017

Position	Project	Total Raised
1	Filecoin	$257,000,000
2	Tezos	$232,319,985
3	EOS Stage 1	$185,000,000
4	Paragon	$183,157,275
5	Bancor	$153,000,000
6	Kin Kik	$97,041,936
7	Status	$90,000,000
8	TenX	$64,000,000
9	MobileGO	$53,069,235
10	KyberNetwork	$48,000,000

Total em setembro/2017 era de US$ 2.1 bilhões

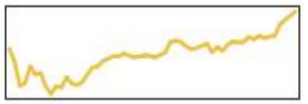
Fonte: https://www.coinschedule.com/stats.php

Cryptocurrencies: 1326 / Markets: 7120 Market Cap: $377.904.594.244 / 24h Vol: $21.950.304.635 / BTC Dominance: 57.9%

Cryptocurrency Market Capitalizations

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾ Search Currencies

All ▾ Coins ▾ Tokens ▾ USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$218.961.624.345	$13.092.60	$9.864.260.000	16.724.075 BTC	10.10%	
2	Ethereum	$43.094.254.061	$448.11	$1.633.270.000	96.169.133 ETH	-3.46%	
3	Bitcoin Cash	$24.726.167.784	$1.468.23	$1.048.930.000	16.840.800 BCH	-5.97%	
4	IOTA	$13.489.477.393	$4.85	$2.632.470.000	2.779.530.283 MIOTA *	57.75%	
5	Ripple	$9.272.253.097	$0.239351	$246.959.000	38.739.145.009 XRP *	-3.82%	

- **Hoje: US$ 377 bi. Em 2/nov era US$ 193 bi**

Fonte: http://coinmarketcap.com/

Criptomoedas - blocos básicos

- "Carteiras" (virtual ou física): endereços

- Comunicação P2P (descentralização):
  - Envio de dados, operações...
  - funcionamento da rede independe da autorização ou ação de nodo central, mas requer cooperação para aprovação das operações (consenso).

- DLT/Blockchain (dados replicados):
  - Cadeia de blocos que armazena as operações de transferência
  - Resistente à violação (após validação)
  - Diversos modelos: Público/privado, controle de escrita...

- Criação de moeda (recompensa ou troca):
  - mineração, trabalho realizado produz moedas, ao mesmo tempo que viabiliza o consenso sobre as operações da Blockchain.
  - ICO viabiliza troca entre (cripto)moedas

Criptomoedas : Características

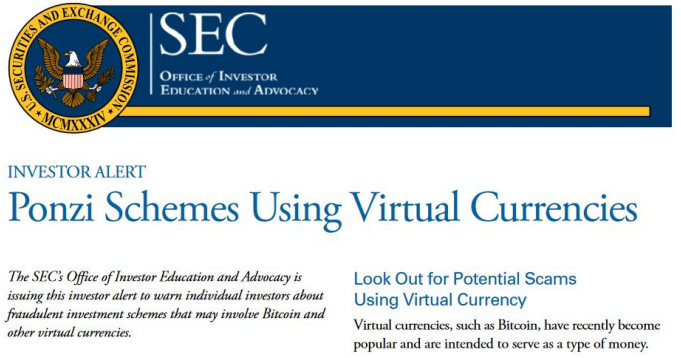
- **Principais características:**
  - "Software como moeda"
    - » Algoritmos controlam a emissão, validação de operações, registro de operações válidas, distribuição de informações na rede
  - Controle descentralizado: nós da rede validam e registram operações localmente
    - » Transações verificáveis e resistentes à adulteração (ex: *blockchain* – cadeia de blocos)
  - Diversos níveis de anonimato possíveis (carteiras, contas)
  - Abrangência mundial
  - Acessibilidade facilitada
  - Sem lastro ou reconhecimento governamental (tecnicamente não se trata de uma "moeda")

Criptomoedas: Riscos e Golpes

- **Variantes de golpes e usos conhecidos:**
  - Lavagem de dinheiro, financiamento de terrorismo, evasão fiscal (AML)
  - Fraudes diversas, estelionato, pirâmide, investimentos e serviços falsos, ganhos exagerados e garantidos etc.
  - Ataques cibernéticos, roubo de identidade digital

- **Diversos alertas emitidos: BACEN, CVM, SEC,...**

- **Específico para criptomoedas (passos do atacante):**
  1. Conseguir as chaves privadas
  2. Obter a propriedade das moedas/tokens
  3. Embaralhar (mixing) as transações
  4. Liquidar as moedas -> cash/outros ativos


SEC
Office of Investor Education and Advocacy

INVESTOR ALERT

Ponzi Schemes Using Virtual Currencies

The SEC's Office of Investor Education and Advocacy is issuing this investor alert to warn individual investors about fraudulent investment schemes that may involve Bitcoin and other virtual currencies.

Look Out for Potential Scams Using Virtual Currency

Virtual currencies, such as Bitcoin, have recently become popular and are intended to serve as a type of money.

Criptomoedas – Riscos de Fraudes

- Onecoin:
  - "Criptomoeda global transparente", curso de gestão financeira, venda de pacotes, diversos países, "revistas especializadas"
  - Alertas: Stop order BaFin (Alem), FSMA Bélgica, Bancos centrais da Hungria, Nigeria, Uganda, suspensão provisória na Itália e multa de 2.6 mi euros, prisões na Índia, investigações em andamento UK, Finlândia, Suíça.

ROOKIE PACKAGE
FREE

STARTER PACKAGE
110 €

TRADER PACKAGE
550 €

PRO TRADER PACKAGE
1 100 €

TYCOON TRADER PACKAGE
5 500 €

PREMIUM TRADER PACKAGE
13 750 €

INITIAL LAUNCH PACK
55 555 €

Criptomoedas – Riscos de Fraudes

- CryptoDouble (jan/15): 2.233 BTC ($500 mil)

- Confido (nov/17): $370 mil

CNBC

Cryptocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the founders

Arjun Kharpal | @ArjunKharpal

Published 7:40 AM ET Tue, 21 Nov 2017 Updated 2:34 PM ET Wed, 22 Nov 2017

CNBC.com

- Confido billed itself as a "smart contract" start-up.
- It raised $375,000 through an initial coin offering.
- The website and social media accounts related to the company and the founding team have been deleted.
- TokenLot, which hosted the ICO, dubbed it an "exit scam" and said it is going to contact the FBI.

Criptomoedas – Riscos de Fraudes

- Bitcoin Savings and Trust: (2011) 764.000 BTC $ 40 milhões
  - Promessa de 7% de retorno no investimento
  - Prisão dos operadores
  - SEC litigation case

- GemCoin: (site) (fb)
  - Minas de âmbar
  - SEC: $74 milhões

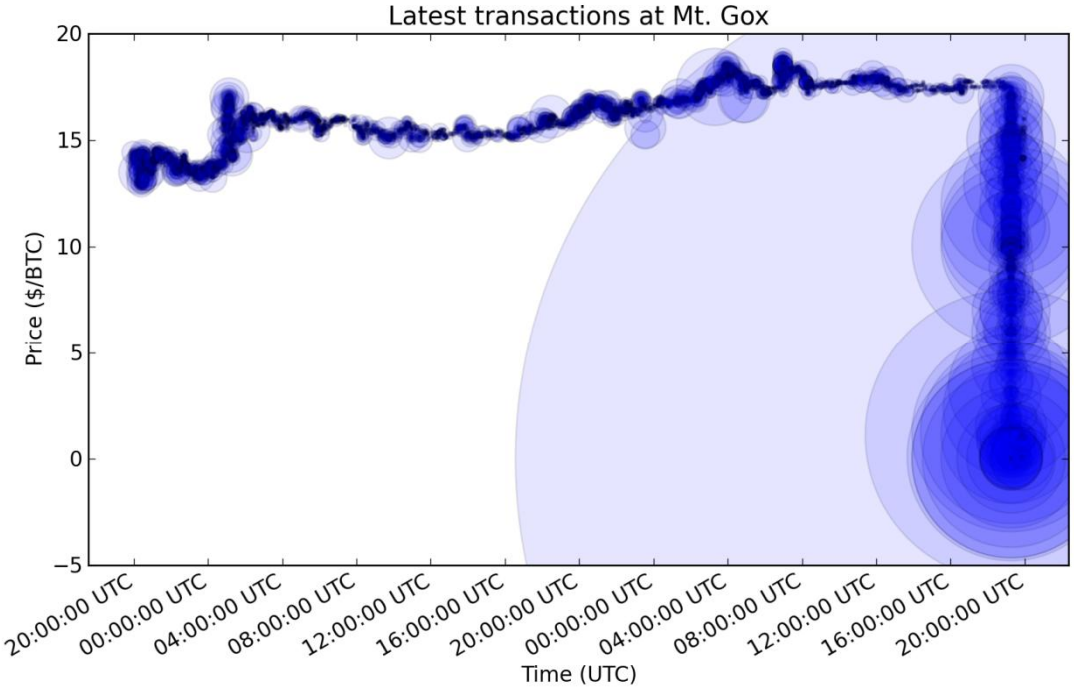
Sobre

USFIA is a US corporation with more than $50 Billion in cash and assetts, it's main product is the 'GemCoin' backed by gems from the ten mines worldwide

- GawMiners, ZenMiner (2015)
  - Venda de poder de mineração inexistente (HW)
  - Retorno pago a investidores advindo de vendas a outros investidores
  - Estimado: $10 milhões, 10.000 investidores
  - 4/out (SEC): US$ 9 mi + juros, risco de 20 anos de reclusão

Criptoexchanges - ataques

- **Allinvain** (jun/11): 25.000 BTC. Wallet no HD - Windows
- **Mt.Gox** :
  - (jun/11): 850.000 BTC e (fev/14): 750.000 BTC
  - aprox 6% dos bitcoins em circulação



- **Bitcoin7** (out/11): 5.000 BTC (hackers russos ou insider ?)

Criptoexchanges - ataques

- **Bitcoin7** (out/11): 5.000 BTC (hackers russos ou insider ?)
- **Bitcoinica**:(mar/mai/12): 46.703 BTC (ataque ao provedor de nuvem Linode)

Bitcoins worth $228,000 stolen from customers of hacked Webhost

ars TECHNICA BIZ & IT

Hackers exploited a vulnerability in cloud services provider Linode that ...

DAN GOODIN - 3/2/2012, 2:59 AM

POLICY —

Bitcoinica users sue for $460k in lost Bitcoins

A complaint filed in SF accuses the trading platform of breach of contract.

MEGAN GEUSS - 8/11/2012, 9:10 PM

Bitcoins, units of virtual currency which are cryptographically signed and transferred without the influence of banks or government oversight, experienced a boom about a year ago (in June 2011 one BTC was equivalent to $15), but crashed to less than $3 only 5 months later when slews of Bitcoin-stealing malware and hacks of Bitcoin "banks" unsettled the market. The nascent currency bounced back, however, and the price of Bitcoins surged this past July, rising above $9 for the first time in a year.

Criptoexchanges - ataques

- **Poliniex**:
  - (2011): 12.3% dos recursos: erro de programação (verificação de fundos). (mai/17): DDoS - liquidez

- **BitFloor**:
  - (set/12): 24.000 BTC

- **Inputs.io**:
  - (out/13): 4.100 BTC. Email comprometido.

- **Picostocks**:
  - (nov/13): 6.000 BTC

Criptoexchanges - ataques

- Coin.mx :
  - bolsa acusada de lavagem de dinheiro de milhares de dólares 2013-2015 (ransomware, compras na Dark Web) através de cia de fachada (US dois condenados em 1ª instância a 20 anos). Programador condenado a 19 meses
- MyCoin (2015): $ 8 milhões – Hong Kong
- Bitstamp (2015): $ 5 milhões
- BitPay (2015): $3.5 milhões –phishing p/ CEO
- Bitfinex (ago/16): $ 70 milhões
  - Queda de 20% no valor do Bitcoin
- Cryptsy (2016): $ 6 milhões
- Bithumb (jun/17): maior exchange da Coréia do Sul. Dados pessoais de 32 k usuários comprometidos.

Criptoexchanges - ataques

- **Etherdelta** (sep/17)
  - Exchange descentralizada para Ether
  - Funcionamento controlado por um smart contract
    - » Usuários colocam ordens de compra e venda
  - Atacante usou chats e fóruns para induzir usuários a acessarem links específicos
  - Injeção de código no site via smart contract malicioso para capturar chaves privadas usadas em negociações na exchange

Criptomoedas – Ataques (Ethereum)

- DAO – Decentralized Autonomous Organization (mai/16):
  - Objetivo: crowdfunding/kickstarter/VC descentralizado/P2P
    - » Incentivar ideias de negócio/votação:
      - Infraestrutura: Ethereum
      - Pode-se votar nas ideias com base nos tokens DAO
    - » Captação :
      - esperado: $ 5 mi, efetivado: $ 150 mi (11K contas)

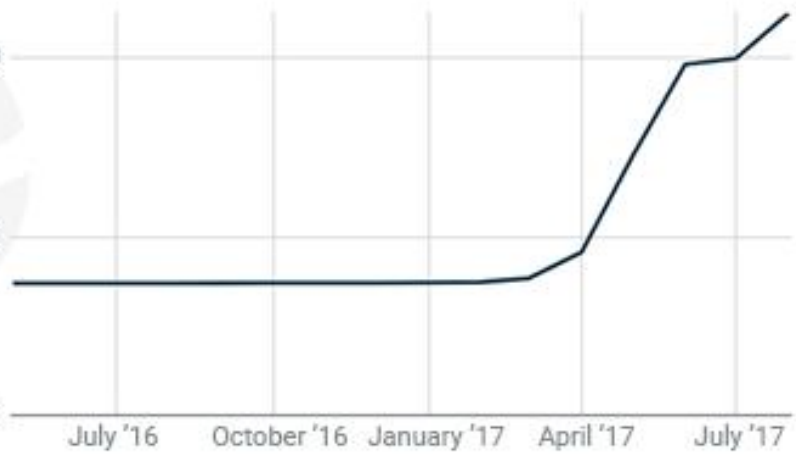
  - DAO hub: pote de dinheiro
  - Smart contracts escritos em Solidity (à la JavaScript com tipos específicos) e executados pela EVM
    - » Código associado à blockchain (e imutável !) – "code is law"
      - Ex: transferir tokens entre contas após uma transação
    - » Código + Chamadas de função
  - Resolução controversa/diversas críticas:
    - hard fork: interferência de pessoas do Ethereum: retornar os tokens (volta ao passado)
      - Consenso de 89% ? Defaults
      - "codewaslaw"
      - "too big to fail ?"
    - Nascimento do Ethereum Classic (dissidentes)

Criptomoedas – Fraudes (Ethereum)

- Relatório: Chainanalysis :
  - Crescimento conjunto market cap vs cybercrime
  - Ethereum: +800 tokens após lançamento em 2015
    - » Investimentos via ICOs: > US$ 1.6 bi
  - Crime cibernético: +- 10% do volume de capital envolvido
  - Phishing: maior abrangência e volume (valor)

Fig. 1 - Total ICO funds raised on Ether ($Bn)

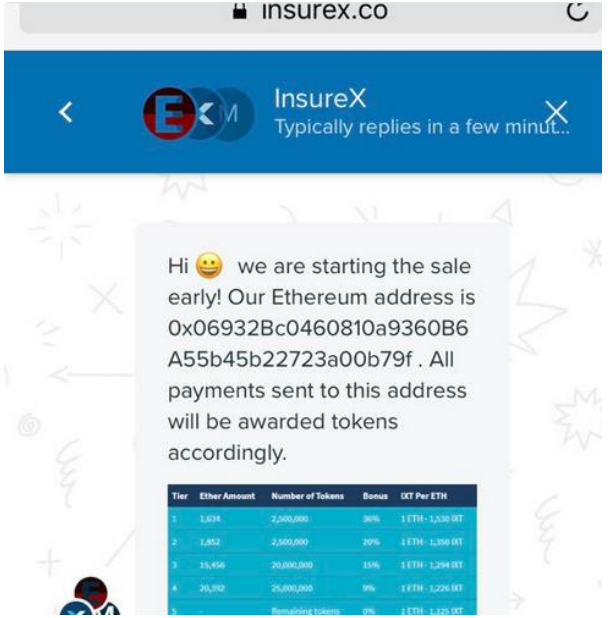
Fig. 2 - Total Cybercrime Revenue ($M)



Criptomoedas – ataques (ICOs)

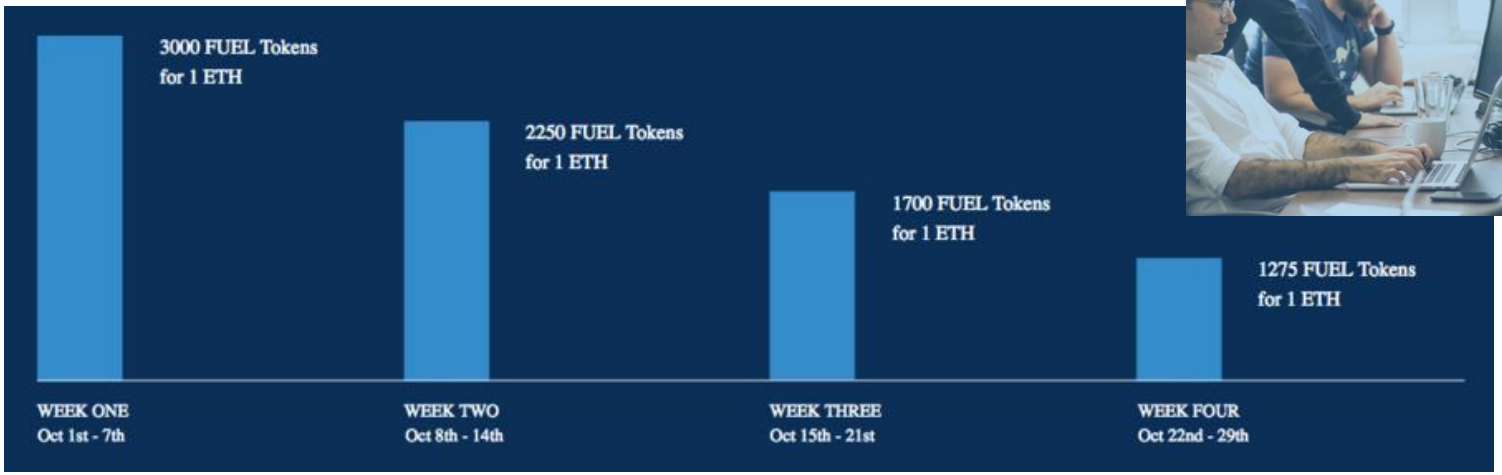
- CoinDash (jul/17): whitepaper
  - Negociação de criptomoedas
  - Roubo de US$ 7 mi (ETH)
  - Atacante alterou o endereço de depósito no site da ICO

- Insurex / iXledger(jun/17): whitepaper
  - Market place para seguros via Blockchain
  - Atacantes controlaram uma conta do twitter e postaram mensagens falsas sobre pré-venda de tokens direcionando os depósitos para contas administradas pelos atacantes.
  - Roubo de US$ 113 k (1.100 ETH)



Criptomoedas – ataques (ICOs)

- Etherparty (out/17): whitepaper
  - Ferramenta para facilitar a escrita de smart contracts
  - ICO: Fuel tokens (stats) Icodrops total: US$ 33 mi
  - Sequência de eventos (comunicado oficial):
  - 9h: início da ICO
  - 9h45: detecção - atacante alterou o endereço de depósito no site da ICO
  - 10h: Web site em manutenção
  - 11h35: rebuild e retorno do website
  - Não revelado o montante de tokens desviados, porém estes foram/serão convertidos em Fuel (após 29/out).

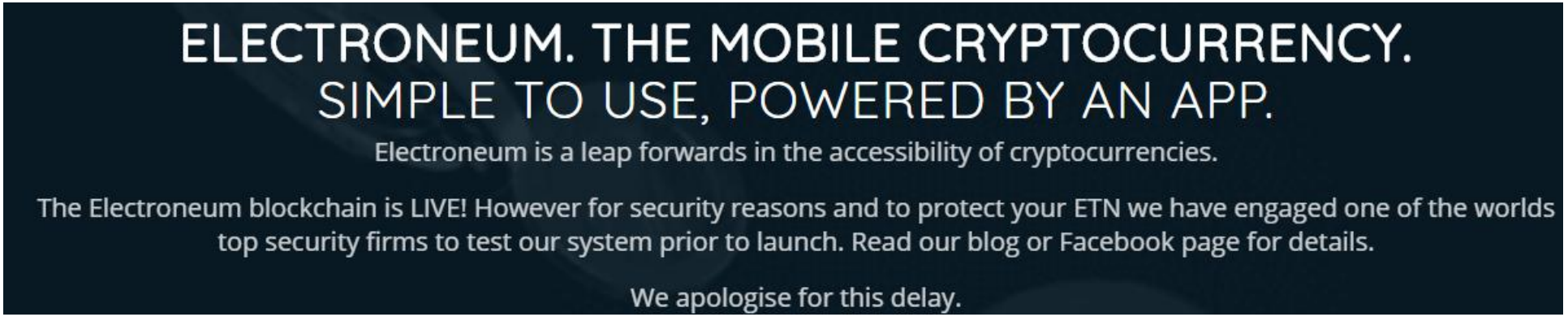


Criptomoedas – ataques (ICOs)

- Electroneum (nov/17): whitepaper
  - Mineração de criptomoedas (celular, pool de mineração...)
  - 140.000 usuários, 30 milhões de libras
  - Ataque: DDoS

Technology

British cryptocurrency Electroneum hit by cyber attack after raising £30m



Criptomoedas – ataques (Wallets)

- Parity (jul e nov/17): whitepaper
  - Gavin Woods: fundador e ex-desenvolvedor core do Ethereum
  - 1º ataque: roubo de 32 mi em Ether . White Hats recuperaram parte do dinheiro. Correção em 20/jul. Porém...

Bad hackers steal $32 million worth of Ethereum, good hackers save the remaining $75 million

  - 2º ataque conseguiu congelar 500.000 Ether devido a um erro no smart contract: carteira com multi signature (alerta oficial)
  - Dúvida: erro ou hacker (DevOps199 ?) tornou-se dono do contrato
  - Resolução mais provável: hard fork com novo contrato
  - Já foi feito antes para resolver o DAO, mas alguns (ex: Vitalik) não se manifestaram favoráveis.

Was Parity hacked? Nearly $300m Ethereum wallet freeze may not have been caused by bug

A startup called Cappasity, a Parity user whose wallet was also frozen, claims "deliberate hacking" caused the incident.

Criptomoedas – ataques (Wallets)

- Tether (nov/17): whitepaper
  - Inicialmente era a Realcoin
  - Facilita a troca de criptomoedas entre exchanges, ATMs (omni protocol): token USDT vinculada ao dólar (1 para 1): supostamente reduz a volatilidade. Cada Tether é lastreado por 1 dólar
  - Anúncio de roubo de US$ 30 mi de uma carteira corporativa para endereço Bitcoin
  - Mesmo endereço usado no ataque da Bitstamp (2015)
  - Polêmica interligação com a exchange Bitfinex (um dono em comum, suspeita de manipulação de mercado)
  - Dados públicos (transparência)

Tether says nearly $31 million worth of its digital tokens have been stolen after hack

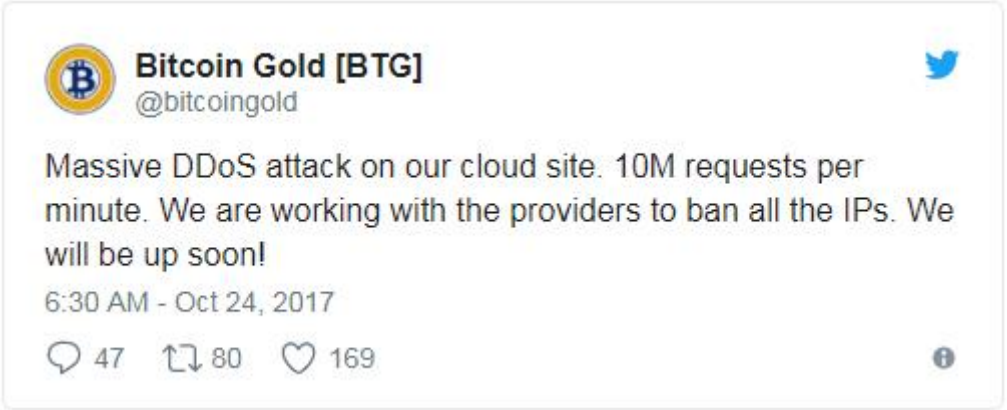
Tether allows users to send and receive digital tokens pegged to currencies like the dollar and yen

By Thuy Ong | @ThuyOng | Nov 21, 2017, 8:28am EST

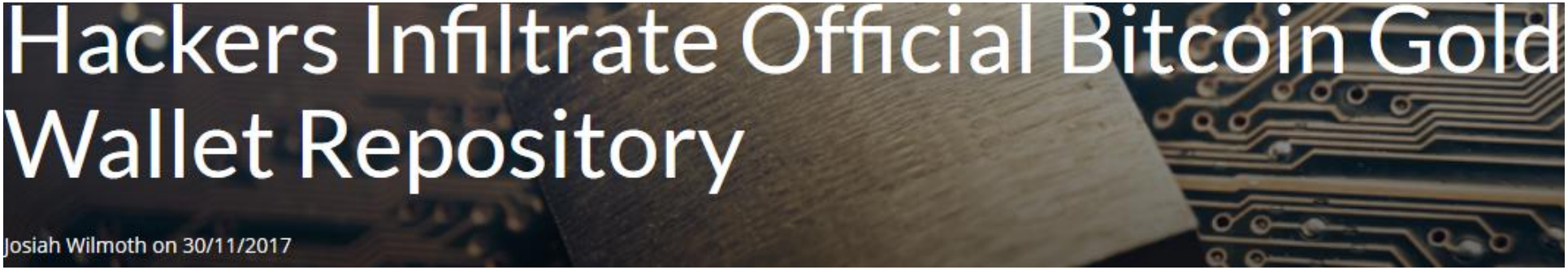
Criptomoedas – ataques

- Bitcoin Gold (out e nov/17): roadmap

  - Concorrente direto do Bitcoin: Fork
  - Out/17: Ataque: DDoS



  - Nov/17: comprometimento do repositório contendo software das carteiras digitais para download (aviso oficial)



Criptomoedas - Malware

- **Mineração:**
  - Forte tendência: substituição de adware por miner
  - Coinhive : JS miner - Monero
    - » Website: captchas PoW, link short. PoW, ad-free browsing
    - » Clone: Crypto-loot
  - **Instalação de software de mineração** (cryptominers):
    - » PirateBay, Vidzi.tv, WatchFree.to, uptostream.com
    - » SafeBrowse (chrome ext.)
  - **ethOS**:
    - » Linux distro customizada para mineração (pago)
      - Versão antiga tem credenciais comprometidas

MOBO/CPU/RAM/ethOS
Bundle for 4 GPUs

$ 159 shipped

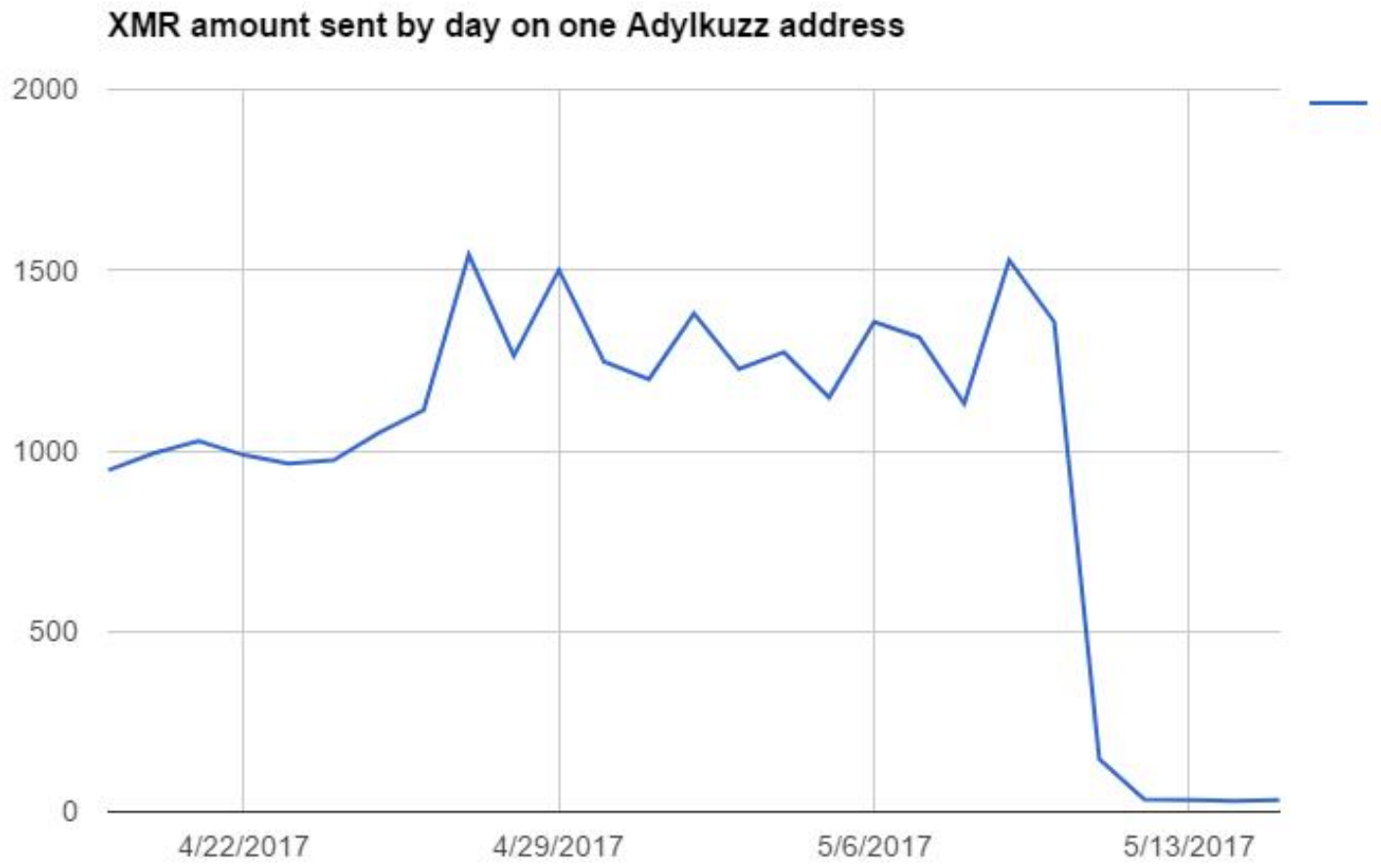
Criptomoedas - Malware

- **Wannacry (variantes) – Windows SMB**
  - **Adylkuzz (abr/17):**
    - » Ativo antes da disseminação do Wannacry (mai/17)
    - » Simples: infecta, fecha SMB (bom!), minera Monero
  - **SambaCry (mai/17):**
    - » Sistemas Linux

- **CryptoShuffler** (out/17):
  - » 150 $ K em Bitcoins (endereço)
  - » Monitoramento/comprometimento do Clipboard
    - Troca do endereço de envio (wallet addr)

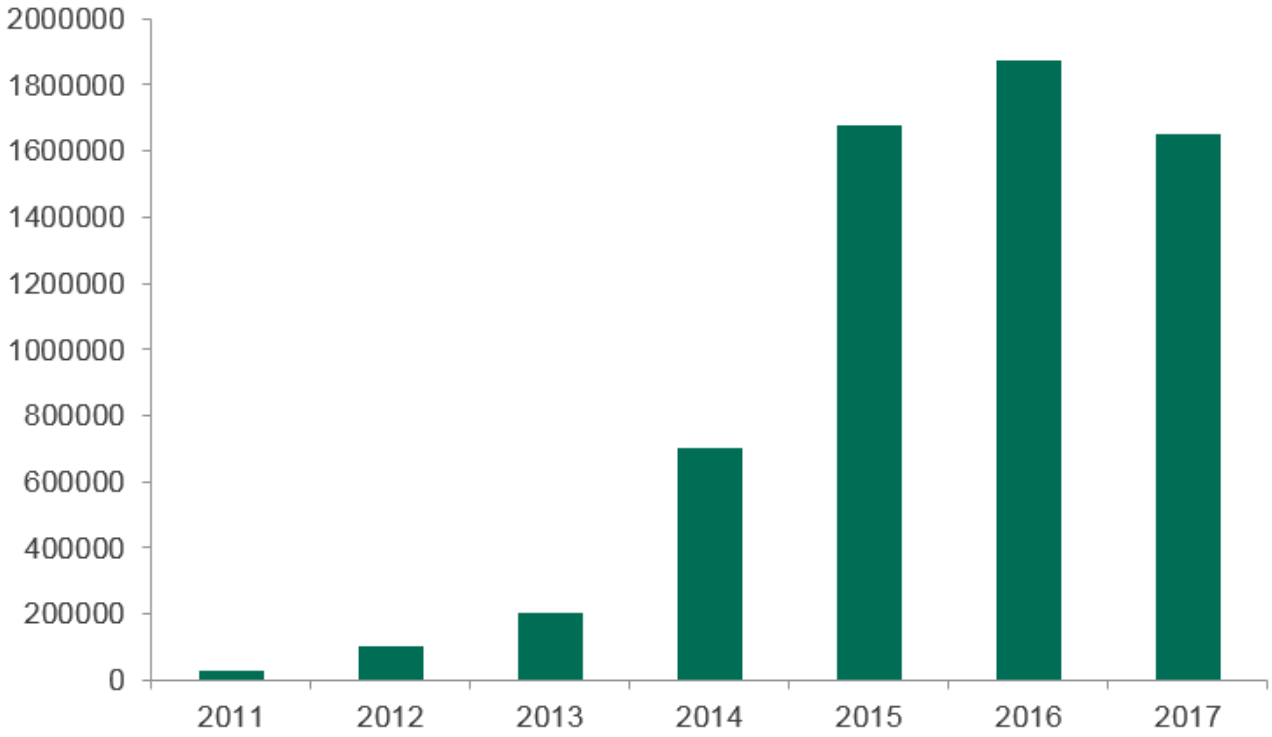
Criptomoedas - Malware

- ProofPoint: (mai/17):
  - Mining Botnet
  - Exploit: EternalBlue/DoublePulsar (WannaCry)



Criptomoedas - Malware

- **Kaspersky Labs** (set/17):
  - 1.65 milhões de computadores infectados
  - Mineração: Monero e Zcash

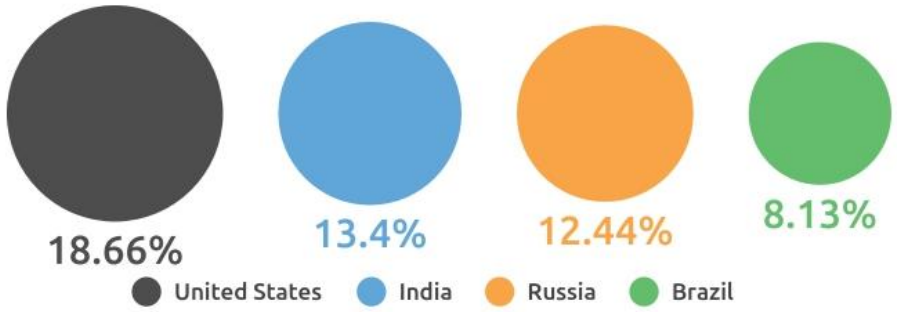


Criptomoedas – Malware/adware

- **Adguard** (out/17):
  - 220 de 100k web sites usando scripts de mineração
  - 500 milhões de usuários potenciais afetados
  - $ 43.000 de ganho estimado em 3 semanas

Top Countries

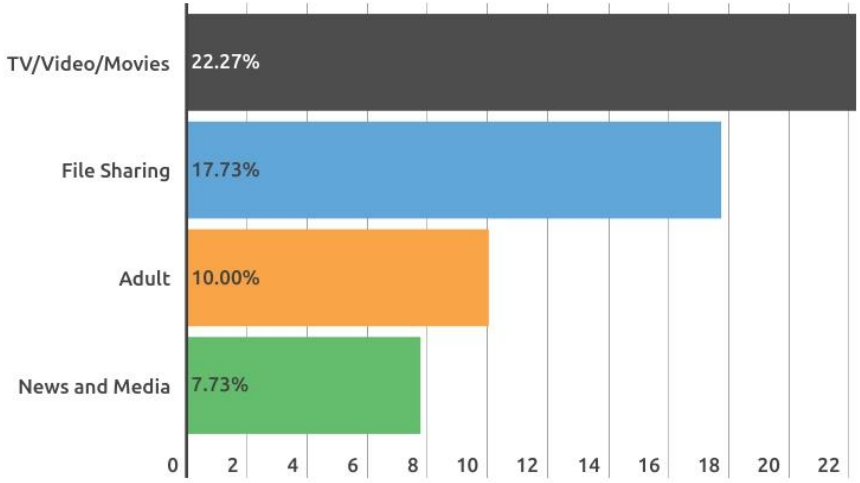
More than a half of the websites engaged in using in-browser cryptocurrency mining scripts focus on 4 countries: US, India, Russia and Brazil.



Research by AdGuard (adguard.com)
October 12, 2017

Top Categories

Over 57% of the websites that utilize in-browser cryptocurrency mining belong to four categories: TV/Video/Movies, File Sharing (mostly Torrents), Adult, and News/Media.



Research by AdGuard (adguard.com)
October 12, 2017

Criptomoedas – Cuidados

- **Fraudes - Sinais de alerta:**
  - Rentabilidade exagerada ou garantida
  - Taxas de transferência inexistentes
  - Adesão inicial (pacotes, combos, em níveis:gold, silver, diamond...)
  - Verifique a origem, confirme no site oficial e fóruns qualificados
- **Outras precauções:**
  - Peça confirmações adicionais por telefone/email
  - Identidade pública dos criadores dos projetos e membros da equipe
  - Analisar entregáveis do projeto (real vs ilusão) e fase (pré-operacional, protótipo, produto viável, rodadas com startups)
- **Consulte sites sobre fraudes e golpes:**
  - Ex: https://etherscamdb.info/scams/
- **Gerencie o risco:**
  - Considere o uso de múltiplas carteiras (tipos: física, HW)
  - Minimize/evite uso sites/exchanges para guarda de criptomoedas.

Considerações finais

- **Retorno atraente: cybercrime + criptomoedas**
  - Retorno imediato (liquidez > do que ransowmare)
  - Desnecessário efetuar ataque em escala mundial
    - » Um bom ataque a uma exchange é suficiente
    - » Contramedidas: congelamento de ativos ilícitos (ex: wannacry)
- **Novos desafios em Cybersecurity:**
  - Já era difícil proteger sites... (Ddos, malware, ataques)
  - Agora, há bastante dinheiro envolvido e cada vez mais empresas/sites (startups, fintechs...)
  - Pressão (desenvolvedores e investidores):
    - » Tradeoff antigo: time to market vs segurança

- **Perspectivas**
  - Discussão sobre Governança de blockchains/DLTs/Projetos
  - Frameworks e linguagens mais seguras para implementação de smart contracts
  - Interoperabilidade entre "moedas" (blockchain), oráculos

Fraudes, Crimes e Ataques Cibernéticos em Criptomoedas

Luciano Porto Barreto

lbarreto@cvm.gov.br / luciano.barreto@ime.uerj.br

Comissão de Valores Mobiliários (CVM)
Universidade do Estado do Rio de Janeiro (UERJ)

São Paulo - 07/12/2017