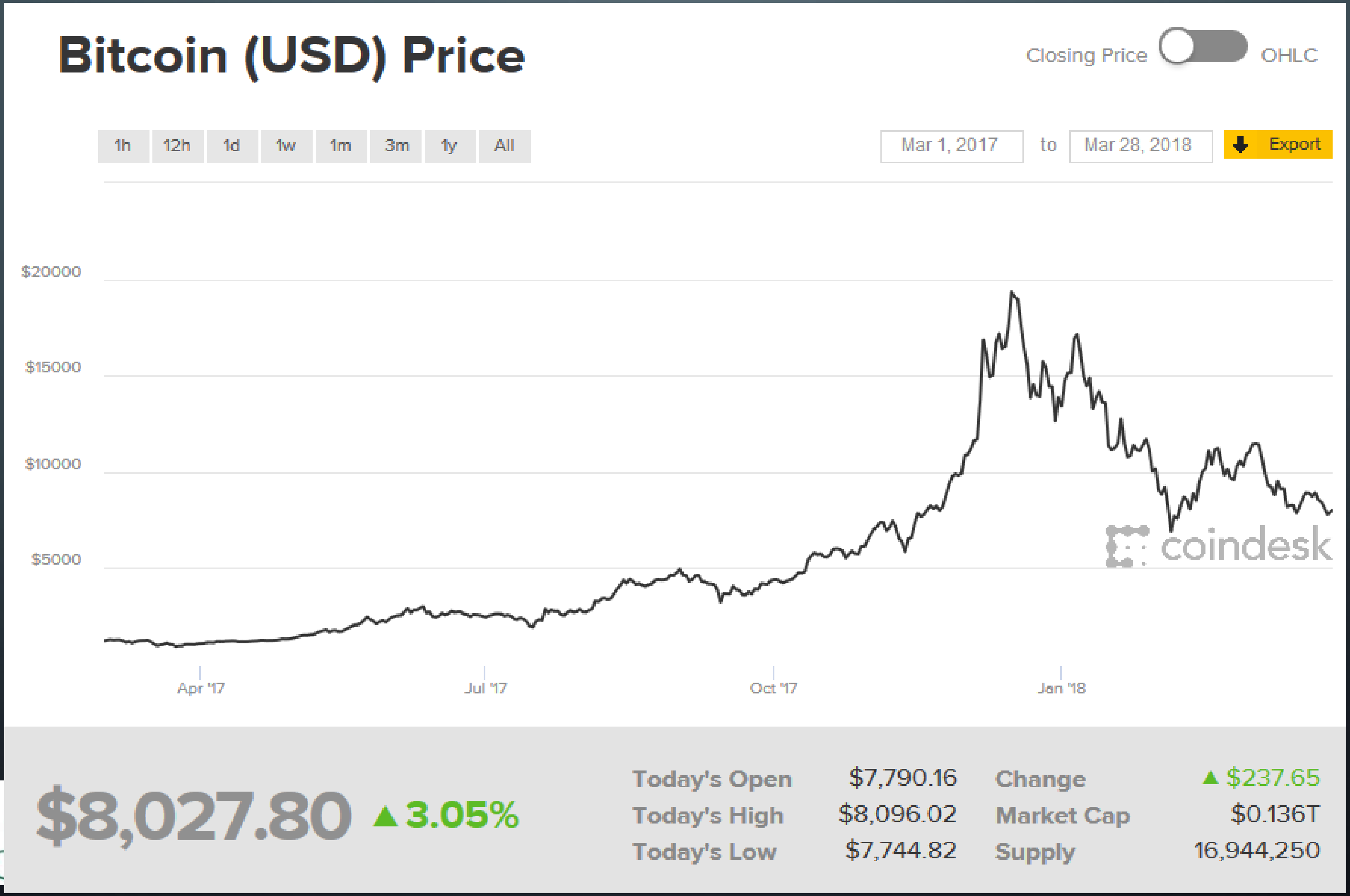
# CYBERSECURITY OF THE NEW DIGITAL CURRENCY ECOSYSTEM

DR. WEICHAO (CHAO) WANG

COLLEGE OF COMPUTING AND INFORMATICS

UNC CHARLOTTE

# BITCOIN PRICE CHANGE IN LAST 12 MONTHS



## Bitcoin (USD) Price

Closing Price OHLC

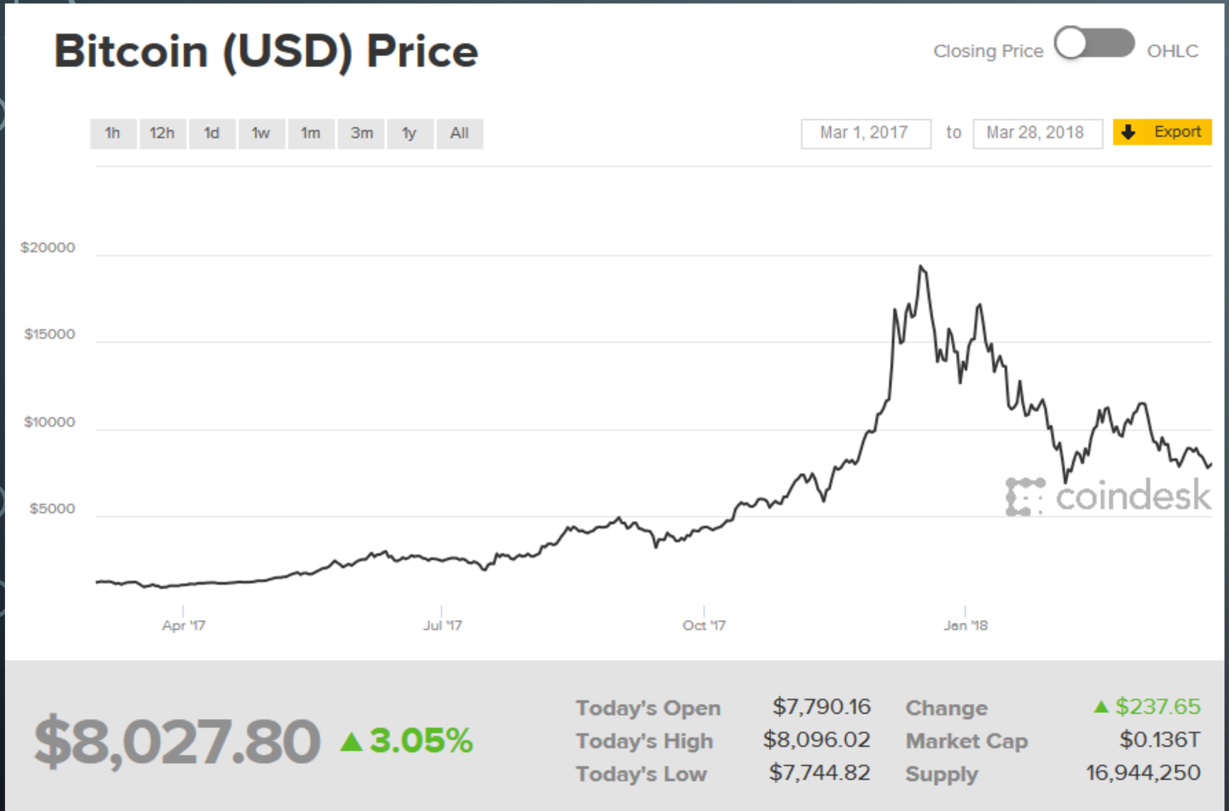
1h 12h 1d 1w 1m 3m 1y All

Mar 1, 2017 to Mar 28, 2018 Export

**$8,027.80** ▲3.05%

| | | | |
|---|---|---|---|
| Today's Open | $7,790.16 | Change | ▲ $237.65 |
| Today's High | $8,096.02 | Market Cap | $0.136T |
| Today's Low | $7,744.82 | Supply | 16,944,250 |

# SAME PERIOD DOW CHANGES

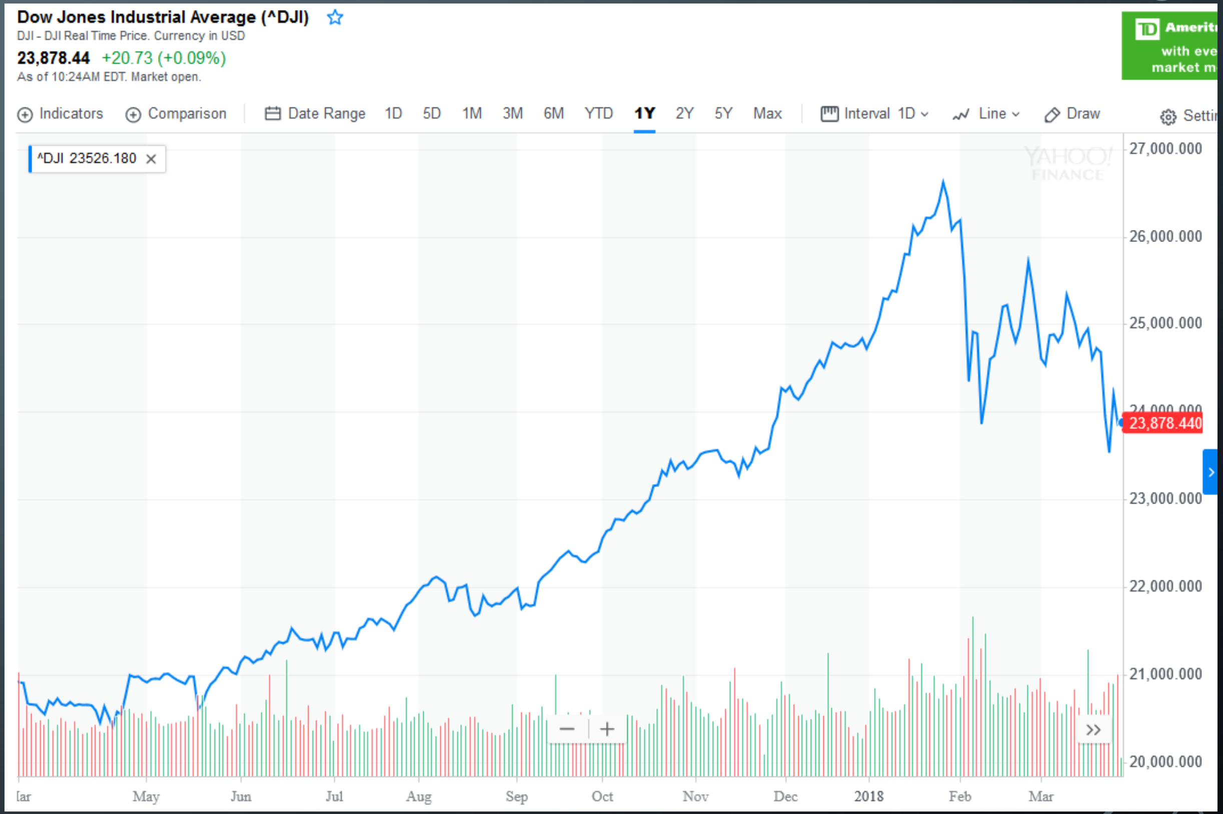


## Bitcoin (USD) Price

Mar 1, 2017 to Mar 28, 2018

**$8,027.80** ▲3.05%

| | | | |
|---|---|---|---|
| Today's Open | $7,790.16 | Change | ▲ $237.65 |
| Today's High | $8,096.02 | Market Cap | $0.136T |
| Today's Low | $7,744.82 | Supply | 16,944,250 |



**Dow Jones Industrial Average (^DJI)**

DJI - DJI Real Time Price. Currency in USD

**23,878.44** +20.73 (+0.09%)

As of 10:24AM EDT. Market open.

^DJI 23526.180

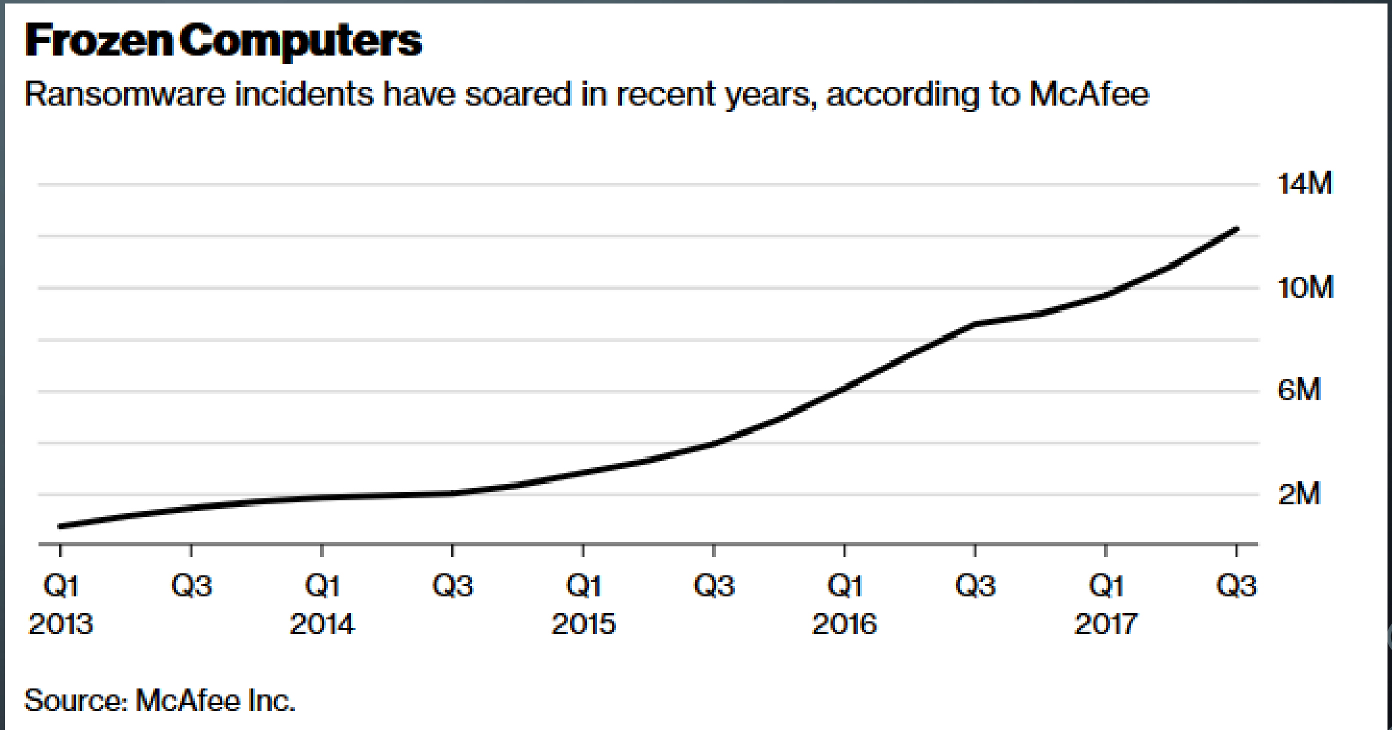
# When there is a lot of money and it is tax free, dark industry will join

- Impacts on individual's life
  - Ransomware;
  - Mining without your knowledge;
    - Your P2P account
    - Your web browser
  - ICO: to be or not to be;

- Impacts on Players of Cryptocurrency
  - Directly hack into digital wallets;
  - Manipulate price change in coins
    - Fork based attack;
    - Recent Binance attack;

# Ransomware using coins

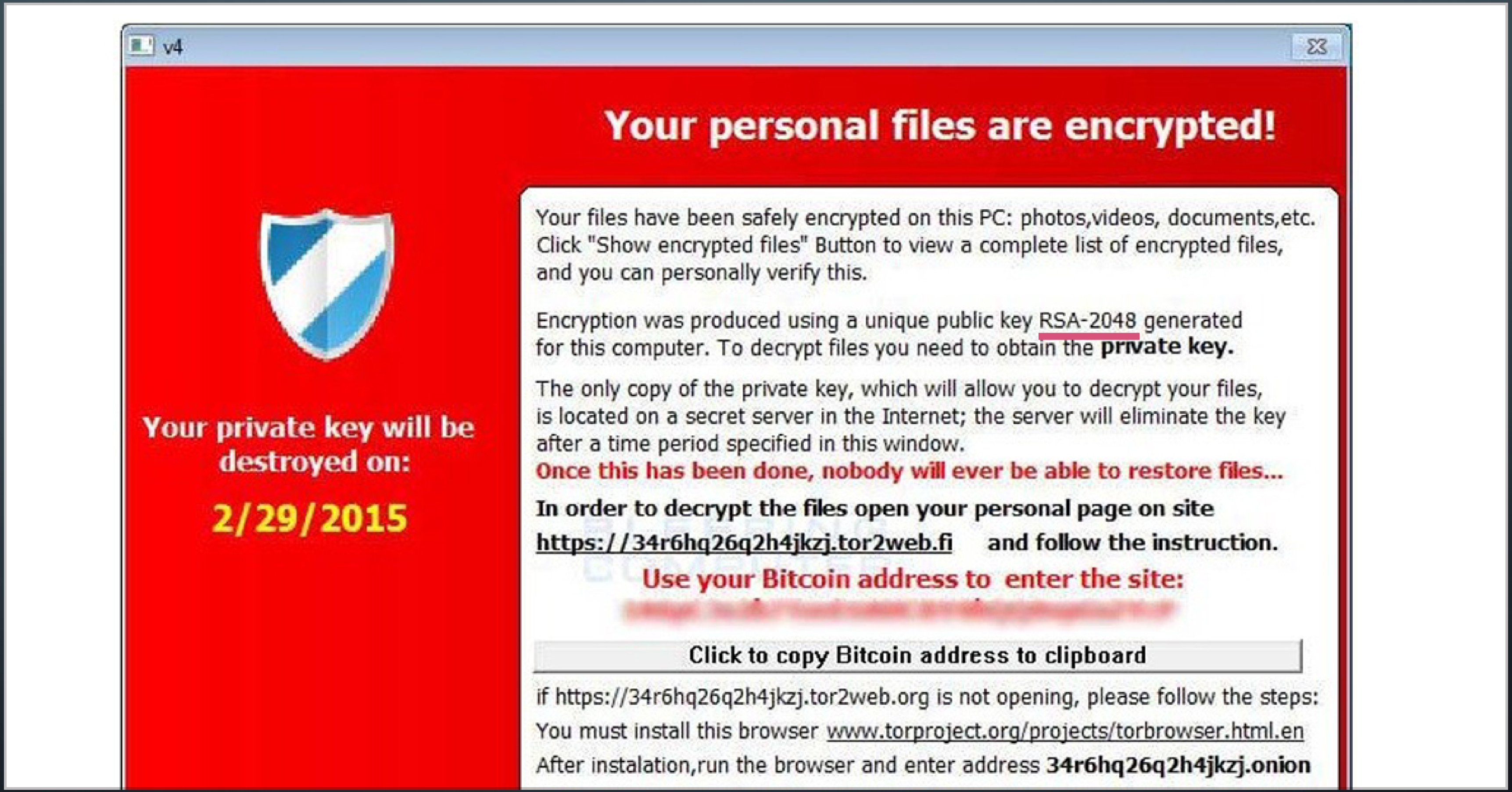
- Let us re-examine properties of crypto-currency
  - Anonymity: untraceable;
  - Can cash-out: valuable;
  - Online: remote;
- Perfect for criminals!
  - Avg payout increases 70% in 2017;
  - $Million case weekly;



**Frozen Computers**

Ransomware incidents have soared in recent years, according to McAfee

Source: McAfee Inc.



## Your personal files are encrypted!

Your private key will be destroyed on:

**2/29/2015**

Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
**Once this has been done, nobody will ever be able to restore files...**

**In order to decrypt the files open your personal page on site https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.**

**Use your Bitcoin address to enter the site:**

[redacted]

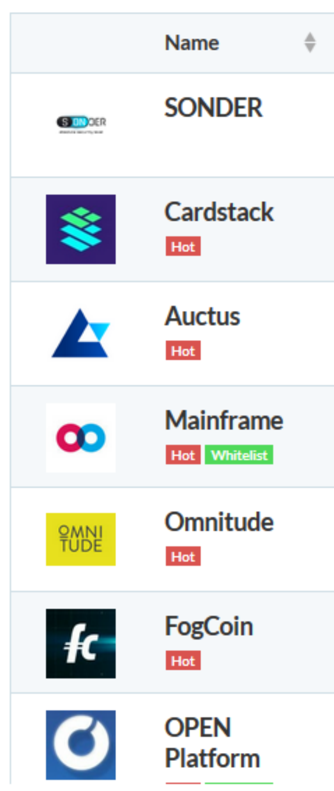
Click to copy Bitcoin address to clipboard

if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**

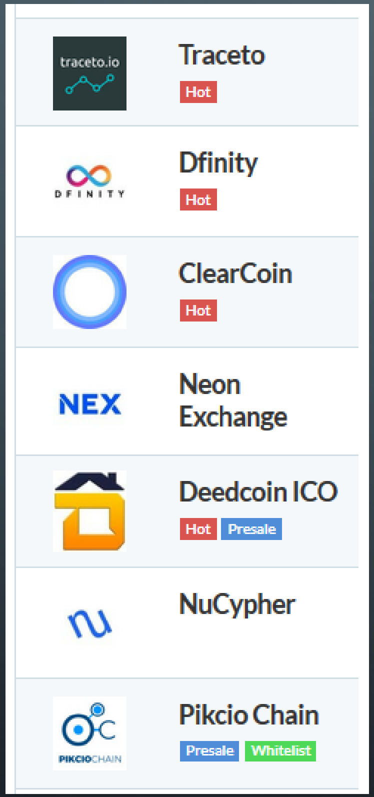
# Mining machines: who are the victims

- Using your computers for mining
  - Many high performance computing clusters/servers have been hacked for coin mining:
    - Top cyberthreat of 2018 based on Forbes: illicit cryptomining
    - Hackers exploit Jenkins servers, make $3million (Feb/18): Russian nuclear scientists,
  - Now your personal computers are targets as well:
    - CBS's Showtime webpage exposed to have browser based mining software (Sep/17);
      - The justification is to avoid ads;
    - BitTorrent client side software compromised, 400,000 PC infected;

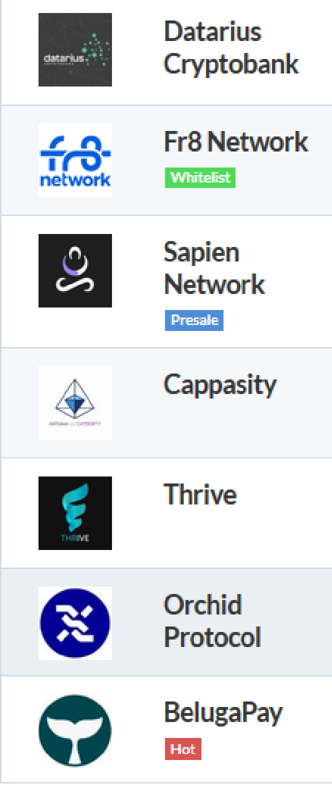
- ICO (Initial Coin Offering): to be or not to be
  - Many successful cases: ETH (100 times return), Augur Token (1 to 5 times profit)
  - Many more cases of losses: too many pitfalls;



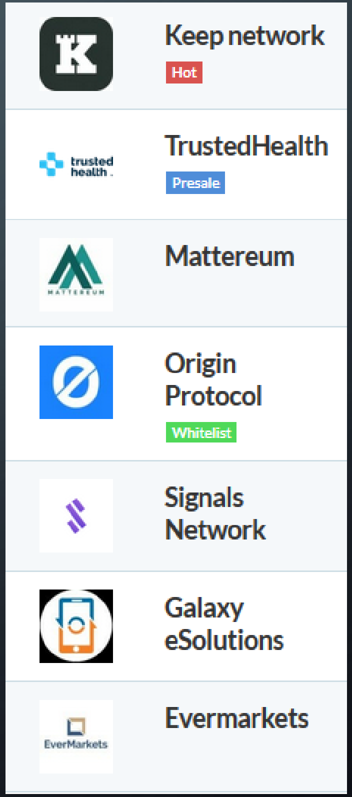
| Name |
|---|
| SONDER |
| Cardstack<br>Hot |
| Auctus<br>Hot |
| Mainframe<br>Hot Whitelist |
| Omnitude<br>Hot |
| FogCoin<br>Hot |
| OPEN Platform |



| |
|---|
| Traceto<br>Hot |
| Dfinity<br>Hot |
| ClearCoin<br>Hot |
| Neon Exchange |
| Deedcoin ICO<br>Hot Presale |
| NuCypher |
| Pikcio Chain<br>Presale Whitelist |



| |
|---|
| Datarius Cryptobank |
| Fr8 Network<br>Whitelist |
| Sapien Network<br>Presale |
| Cappasity |
| Thrive |
| Orchid Protocol |
| BelugaPay<br>Hot |



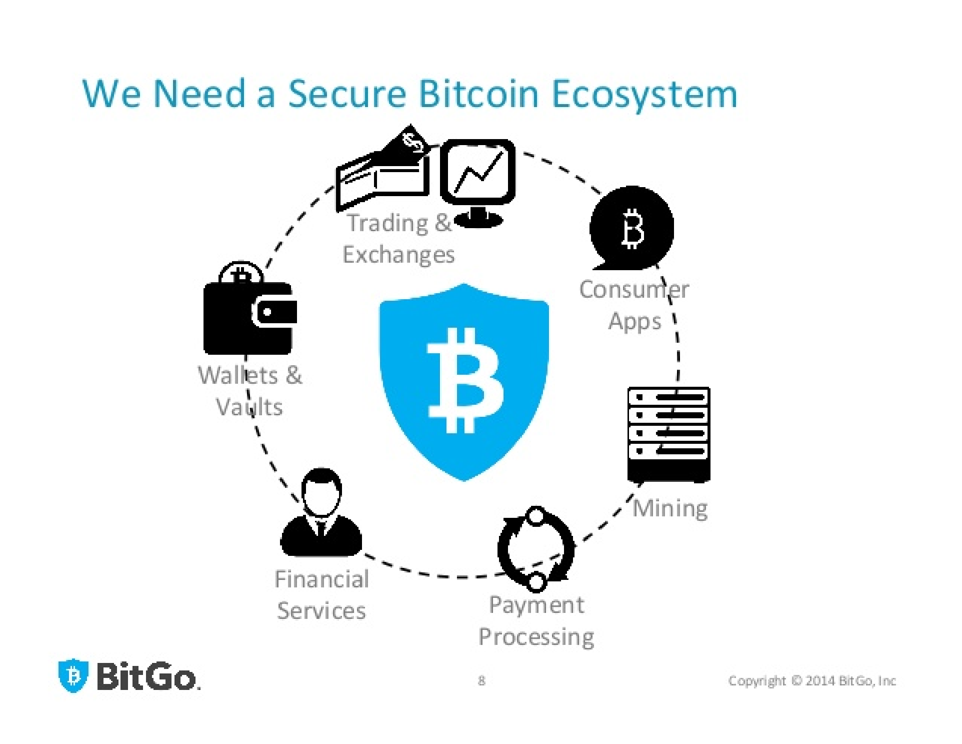
| |
|---|
| Keep network<br>Hot |
| TrustedHealth<br>Presale |
| Matteruem |
| Origin Protocol<br>Whitelist |
| Signals Network |
| Galaxy eSolutions |
| Evermarkets |

# When there is a lot of money and it is tax free, dark industry will join

- Impacts on individual's life
  - Ransomware;
  - Mining without your knowledge;
    - Your P2P account
    - Your web browser
  - ICO: to be or not to be;

- Impacts on Players of Cryptocurrency
  - Directly hack into digital wallets;
  - Manipulate price change in coins
    - Fork based attack;
    - Recent Binance attack;

# Crypto-currency ecosystem

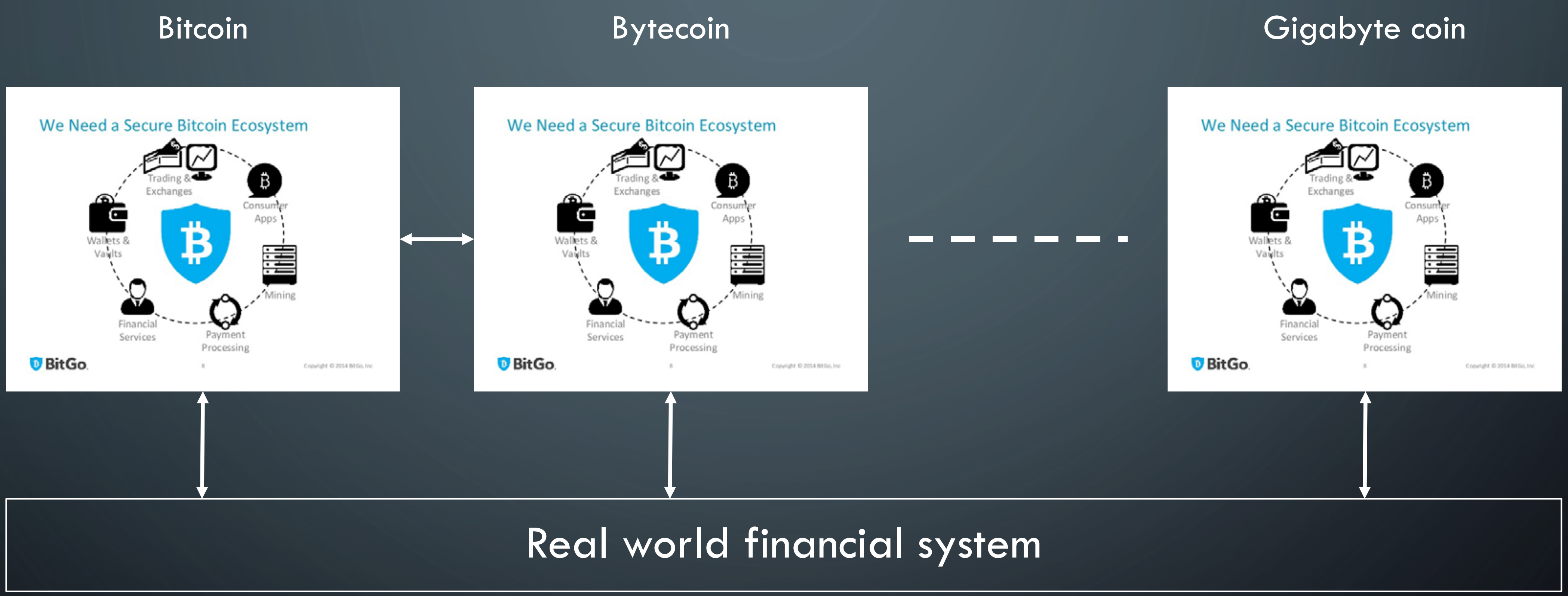


We Need a Secure Bitcoin Ecosystem

BitGo 8 Copyright © 2014 BitGo, Inc

- We need to secure
  - Computation: mining, exchange;
  - Transaction;
  - Storage;
  - Processing;

# Crypto-currency ecosystem



Bitcoin

Bytecoin

Gigabyte coin

We Need a Secure Bitcoin Ecosystem

We Need a Secure Bitcoin Ecosystem

We Need a Secure Bitcoin Ecosystem

Real world financial system

# Directly hack into your digital wallets

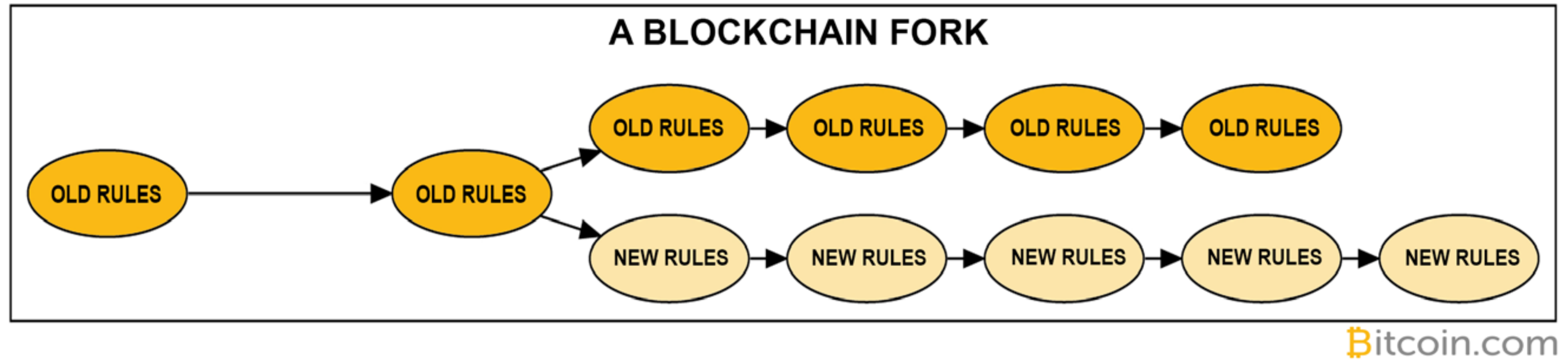
- NiceHash, a crypto mining service company, was hacked in December 2017
  - Hackers emptied the entire contents of digital wallets, about $63 million;
- One server of CoinPouch was hacked in November 2017
  - About $675,000 worth of Verge coin impacted;
- Inputs.io, a bitcoin web wallet, was hacked in January 2018
  - 4100 BTC stolen;

# Manipulating price of crypto-currency: more fun

- Attacks caused by different views (fork)
  - Blockchain is about unanimous view of the world: what has happened and what has not;
  - If two groups of machines have different views, a fork happened;
  - On March 11, 2013, starting from block 225430, the blockchain literally split into two for 6 hours;
- Short term forks: duplicate or conflicting transactions;
- Long term forks: fluctuation in price;

# Manipulating price of crypto-currency: more fun

- Short term forks: duplicate or conflicting transactions:
  - Attackers can double spend her/his bitcoin in different forks, both of which could commit;
  - Fake block attacks: lead to drastic changes in bitcoin price and allow profit through shorting;



# Manipulating price of crypto-currency: more fun

- Last example: March 7th 2018, Binance attack
  - Hack into Binance system, the 2nd largest digital currency exchange system (through API of certain group of users);
  - Control user accounts;
  - Exchange almost all other coins for BTC;
  - Other users notice the transactions, panic, exchange for bitcoins as well: many coin price crashes;
  - Hacker chooses one type of digital currency, VIA, and spend 10,000 BT to buy VIA, so the price of VIA increases 100 times in a short period of time ($0.000225 to $0.025);
  - Then what?

# Manipulating price of crypto-currency: more fun

- Last example: March 7th 2018, Binance attack
  - If you think the hackers will sell VIA under their control and cash-out, you are only 50% correct ☺
  - Binance notices the abnormal conditions, stops any cash-out (31 accounts try to cash out but were blocked);
  - Hackers are prepared for this:
    - they short many types of coins on other markets (probably including BTC);
    - Some 2nd or 3rd level markets allow 20 times or even 100 times leverage;
    - BTC price drops 10% in 1 hour;

# Manipulating price of crypto-currency: more fun

- Is that true? Should we blame hackers?
  - What is the role of exchange software system?
  - Do you remember the Mt.Gox case in 2014?

# Last thoughts

- Crypto-currency is built upon math and software system:
  - We can prove the safety of math (Maybe);
  - We cannot really guarantee the safety of software systems;
- No authority: your freedom and risk;
- We cannot use centralized approach to manage decentralized crypto-currency;
- Who is controlling the computation power?