INTERPOL

GLOBAL COMPLEX FOR INNOVATION

BLOCKTEST

Toxic cocktail facilitating Cybercrime

+

Rethinking Blockchain Security

Challenges towards a responsible Blockchain eco-system

Dr Mark van Staalduinen
Innovation Manager
Deputy Director TNO Singapore
Seconded Cybercrime expert to INTERPOL

TNO innovation for life

About TNO

- TNO is The Netherlands Organisation for Applied Scientific Research
- Largest applied scientific research organisation in the Netherlands (~3000 employees)
- 85 years of experience in providing (technical) solutions
- Not-for-profit and pre-competitive by Dutch Law
- TNO is not a Company nor a University, in Europe known as: Research and Technology Organisation (RTO)
- Registered in Singapore since 2013 as a full branch office
- Goal: Research Office with and within the Singapore Research and Innovation eco-system
- Strategy develop long-lasting partnerships

About myself

- Since January 2016 based in Singapore
- Ten years history within TNO
- Driven by innovation and cyberspace
- Fascinated by criminals

Dr M. van Staalduinen, innovation manager for Dark Web, cybercrime and cyber security at the Netherlands Organisation for Applied Scientific Research, said the WannaCry ransomware shows the vulnerability of society. ST PHOTO: LIM YAOHUI

Partnerships

TNO – SUTD collaboration
under MoU, March 2016

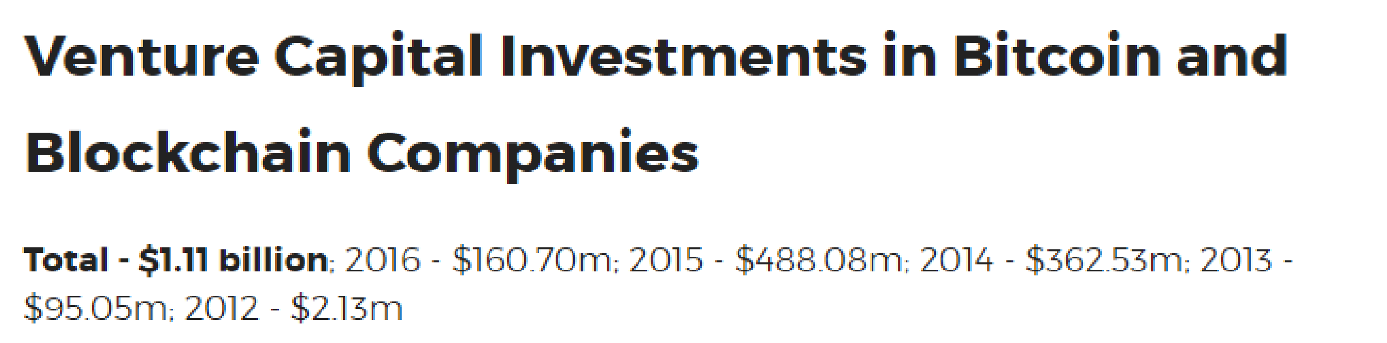
SUTD
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
TNO innovation for life
SUTD-TNO
MEMORANDUM OF UNDERSTANDING
SIGNING CEREMONY
31 MARCH 2016

TNO is INTERPOL
partner since 2017
Collaborate since 2014

TNO – CSA collaboration under
MoU Between CSA and NCSC, July 2016

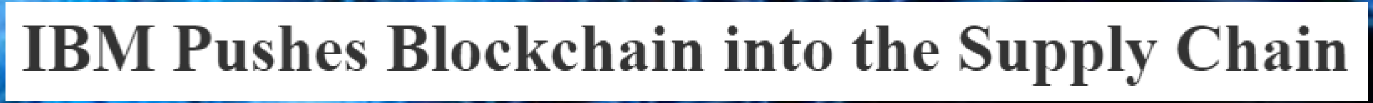
TNO – CyberDevOps,
Collaborate since 2017
Formalized August 2018

Blockchain Technology



Venture Capital Investments in Bitcoin and Blockchain Companies

Total - $1.11 billion; 2016 - $160.70m; 2015 - $488.08m; 2014 - $362.53m; 2013 - $95.05m; 2012 - $2.13m



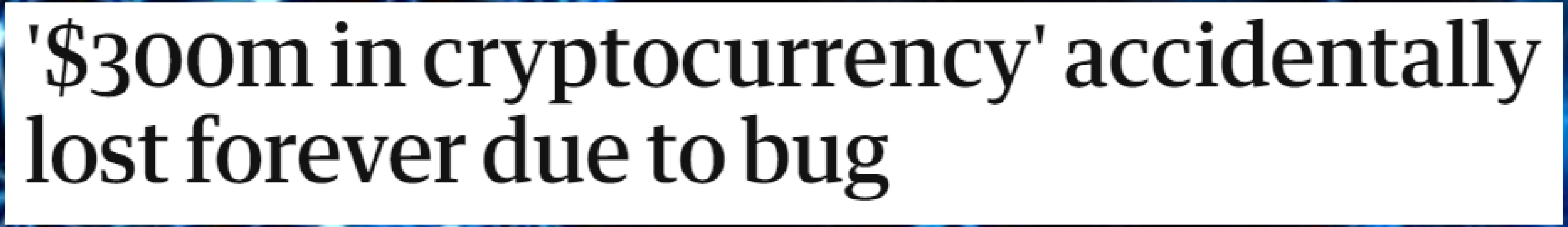
IBM Pushes Blockchain into the Supply Chain

Innovation Green Field

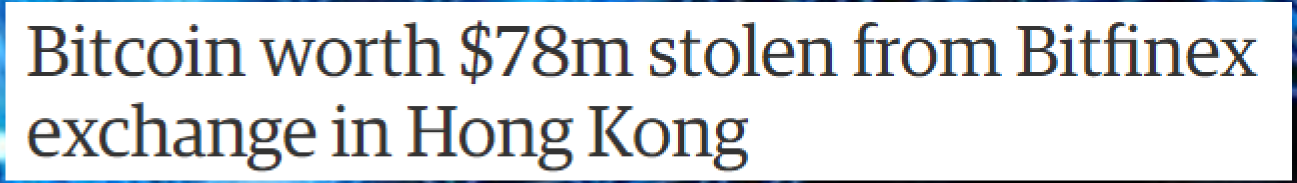
How Blockchain Startups Are Disrupting The $15 Billion Music Industry

We are professional investors and entrepreneurs driving innovation based on Blockchain technology.

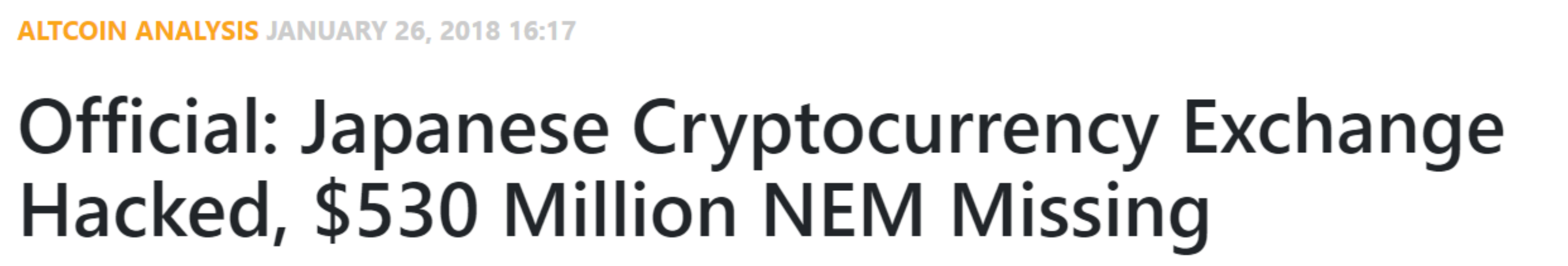
Emerging Cyber Threats



'$300m in cryptocurrency' accidentally lost forever due to bug

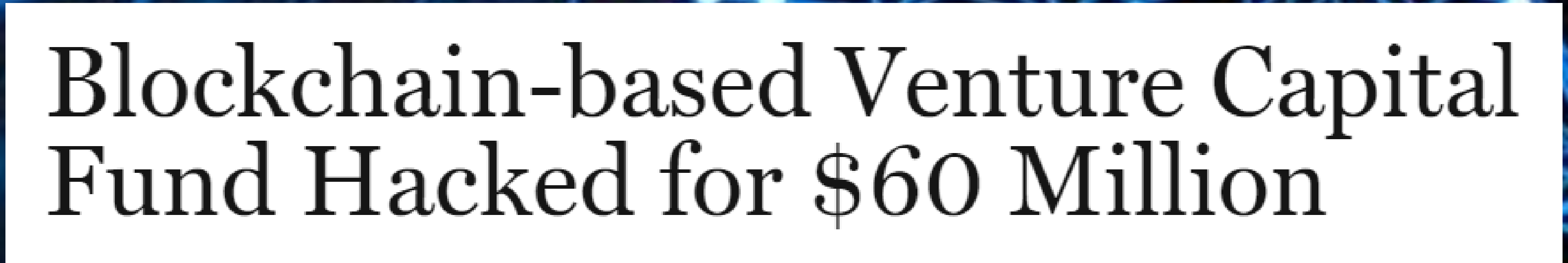


Bitcoin worth $78m stolen from Bitfinex exchange in Hong Kong



ALTCOIN ANALYSIS JANUARY 26, 2018 16:17

Official: Japanese Cryptocurrency Exchange Hacked, $530 Million NEM Missing

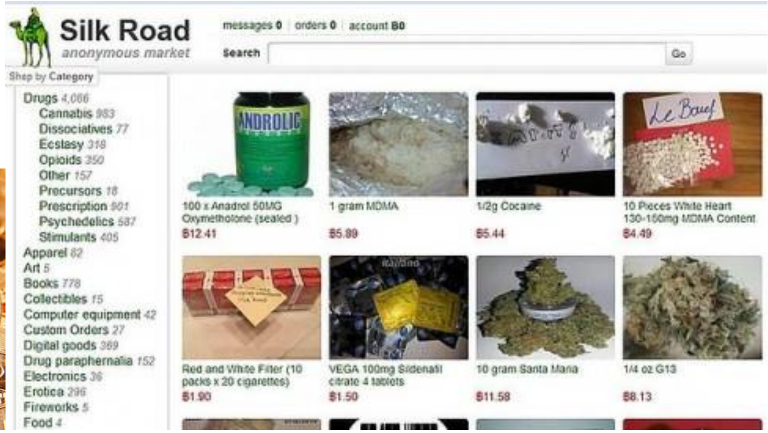


Blockchain-based Venture Capital Fund Hacked for $60 Million

Dark Web History since 2011

Toxic cocktail facilitating Cybercrime

- Exploits the anonymity of Tor (Hidden Services + Browser)
- Bitcoin was last step required to run large scale illegal markets with global coverage
- Uptake since early 2011
  - Silk Road 1.0 - 2013
  - Silk Road 2.0 - 2014
  - AlphaBay & HANSA, till July 2017
- 80% drugs, but what is it all about?
- Cybercrime or drugs trade?
- Cyber and physical are blurring together
- New concept: **Cyber-Physical Crimes**



Silk Road
anonymous market

messages 0 | orders 0 | account B0

Search [ ] Go

Shop by Category

Drugs 4,086
- Cannabis 983
- Dissociatives 77
- Ecstasy 318
- Opioids 350
- Other 157
- Precursors 18
- Prescription 901
- Psychedelics 587
- Stimulants 405

Apparel 82
Art 5
Books 778
Collectibles 15
Computer equipment 42
Custom Orders 27
Digital goods 369
Drug paraphernalia 152
Electronics 36
Erotica 296
Fireworks 5
Food 4

100 x Anadrol 50MG Oxymetholone (sealed) B12.41

1 gram MDMA B5.89

1/2g Cocaine B5.44

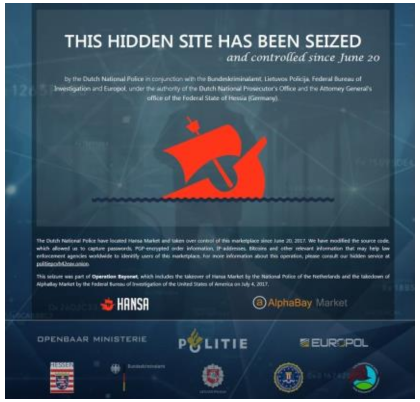
10 Pieces White Heart 130-150mg MDMA Content B4.49

Red and White Filter (10 packs x 20 cigarettes) B1.90

VEGA 100mg Sildenafil citrate 4 tablets B1.50

10 gram Santa Maria B11.58

1/4 oz G13 B8.13

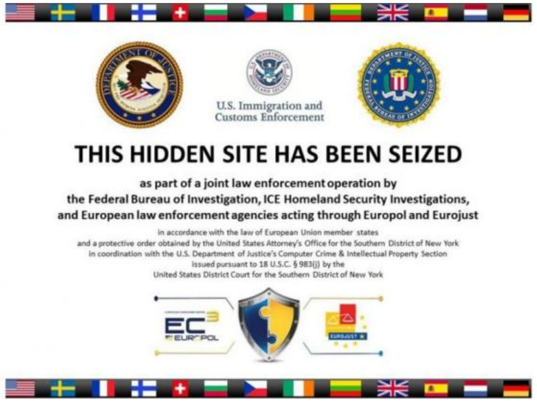


THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

by the **Dutch National Police** in conjunction with the **Bundeskriminalamt**, **Lietuvos Policija**, **Federal Bureau of Investigation** and **Europol**, under the authority of the **Dutch National Prosecutor's Office** and the **Attorney General's office of the Federal State of Hessia (Germany)**.

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.



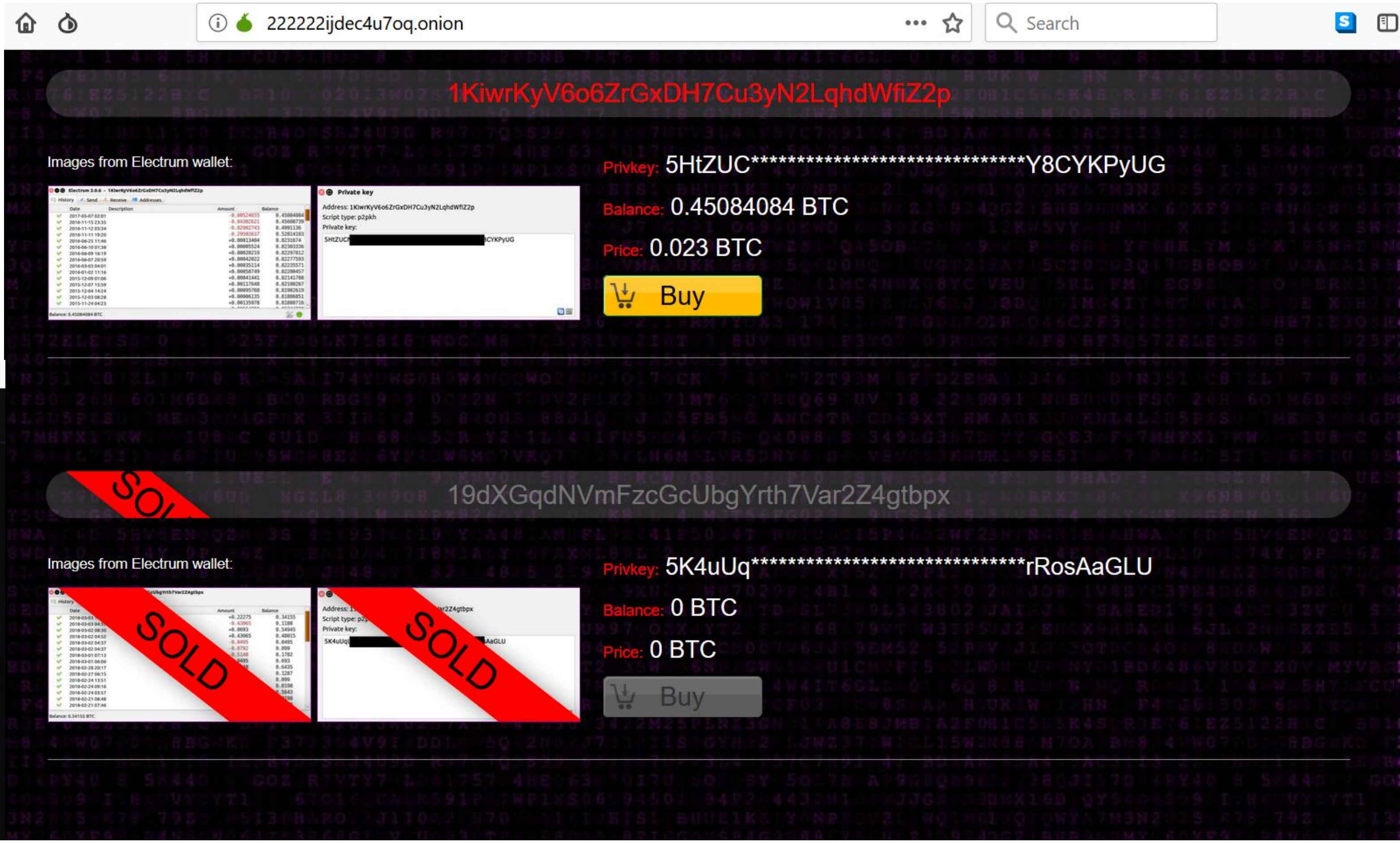
THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by the Federal Bureau of Investigation, ICE Homeland Security Investigations, and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Cryptocurrencies as facilitors

- Private key markets
- Mixers/tumblers
- Bitcoin investments



1KiwrKyV6o6ZrGxDH7Cu3yN2LqhdWfiZ2p

Images from Electrum wallet:

Private key

Address: 1KiwrKyV6o6ZrGxDH7Cu3yN2LqhdWfiZ2p

Script type: p2pkh

Private key:

5HtZUC[redacted]CYKPyUG

Privkey: 5HtZUC***********************************Y8CYKPyUG

Balance: 0.45084084 BTC

Price: 0.023 BTC

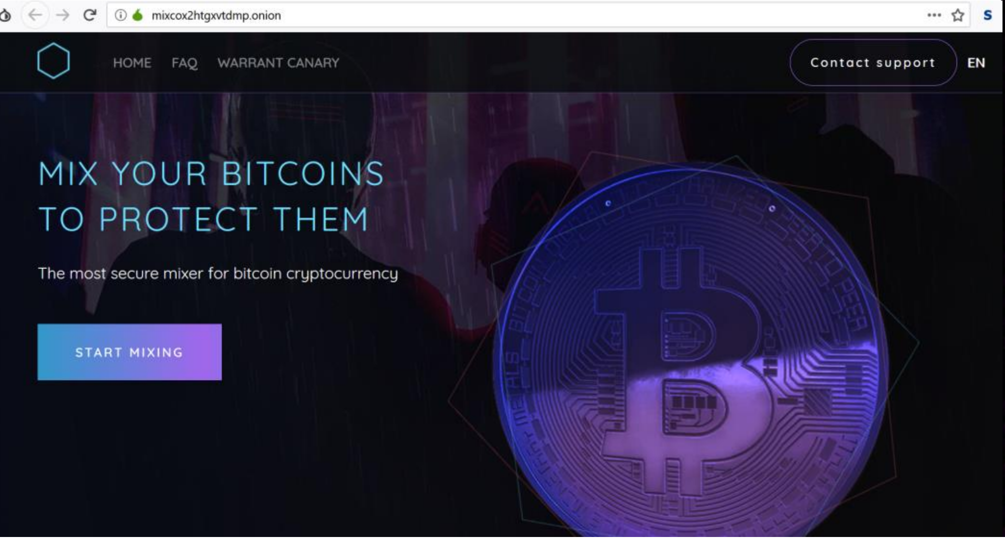
19dXGqdNVmFzcGcUbgYrth7Var2Z4gtbpx

Images from Electrum wallet:

Privkey: 5K4uUq***********************************rRosAaGLU

Balance: 0 BTC

Price: 0 BTC

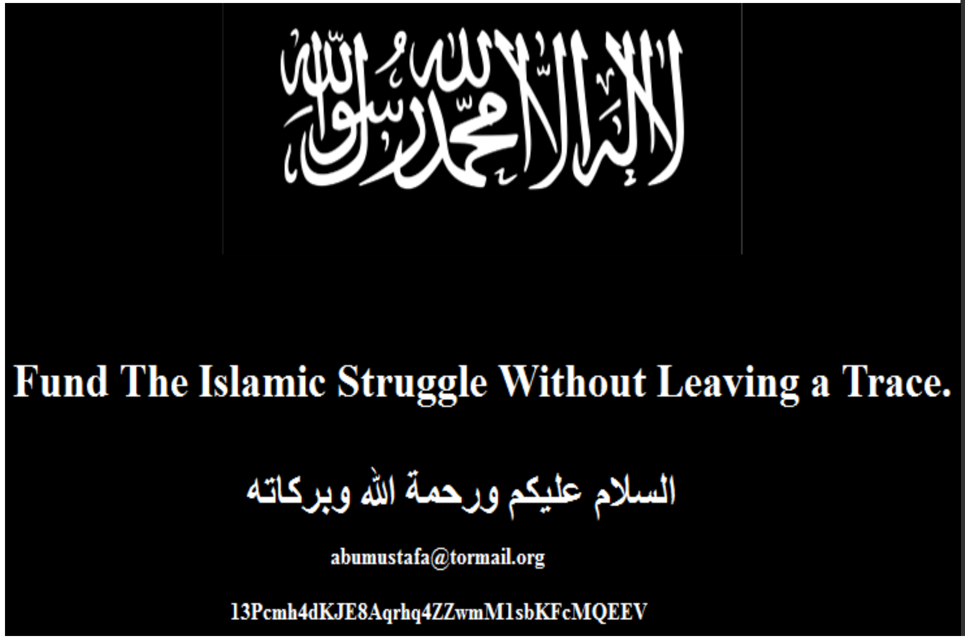


MIX YOUR BITCOINS
TO PROTECT THEM

The most secure mixer for bitcoin cryptocurrency

Cryptocurrencies for Terrorism

- Crowdfunding platform with own coin: SadaqaCoins

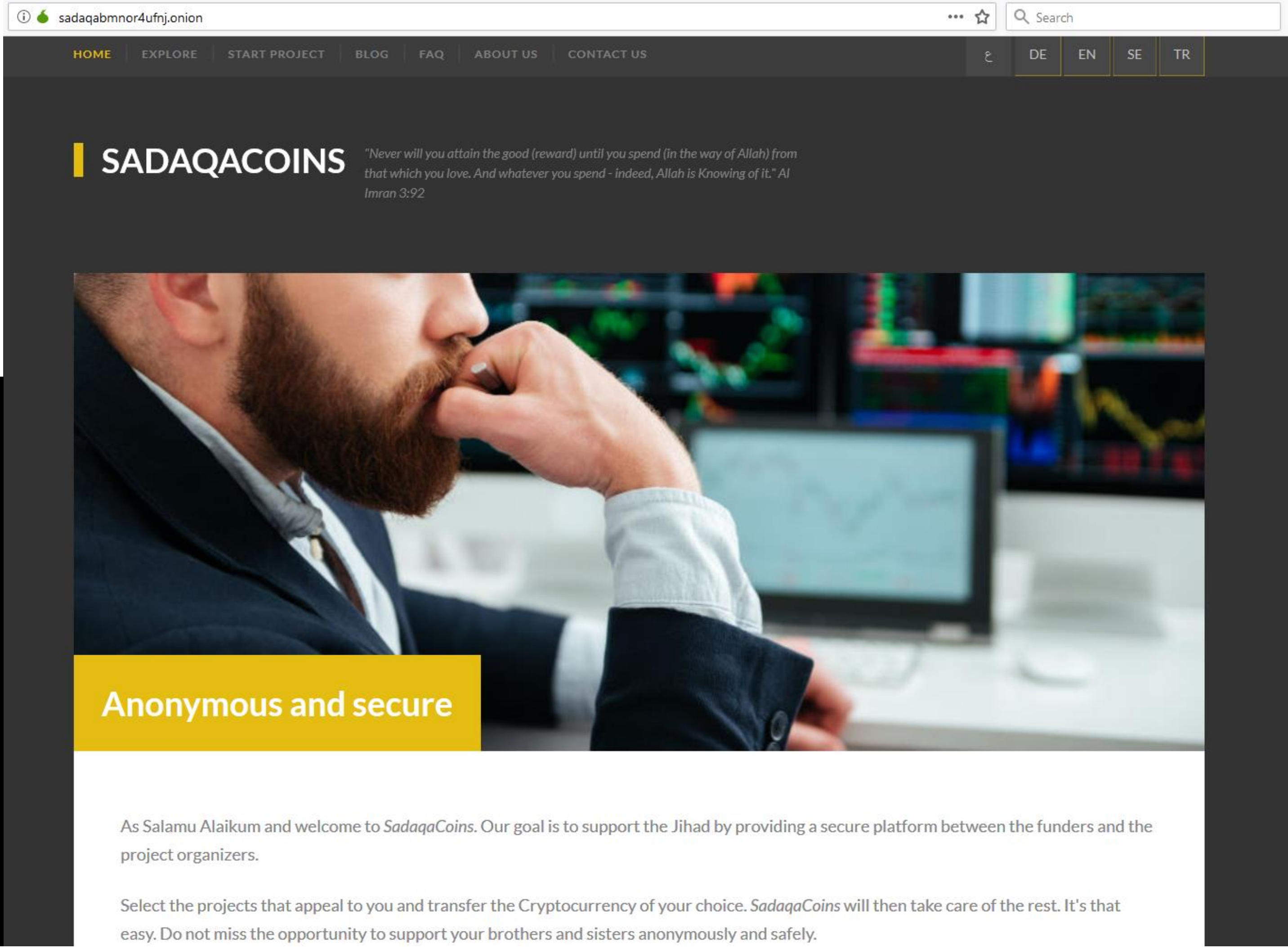

لا إله إلا الله محمد رسول الله

Fund The Islamic Struggle Without Leaving a Trace.

السلام عليكم ورحمة الله وبركاته

abumustafa@tormail.org

13Pcmh4dKJE8Aqrhq4ZZwmM1sbKFcMQEEV



SADAQACOINS

"Never will you attain the good (reward) until you spend (in the way of Allah) from that which you love. And whatever you spend - indeed, Allah is Knowing of it." Al Imran 3:92

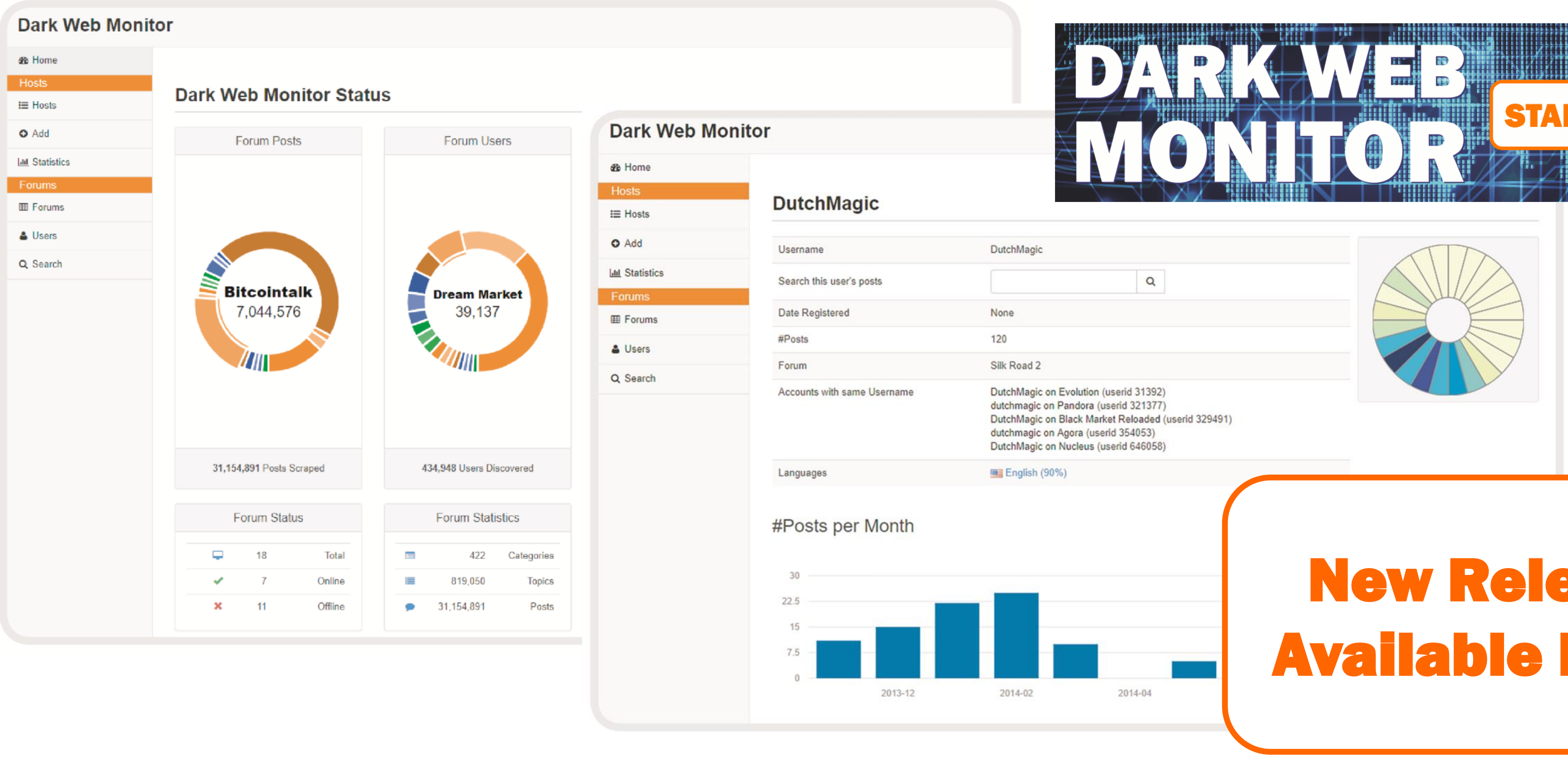
Anonymous and secure

As Salamu Alaikum and welcome to *SadaqaCoins*. Our goal is to support the Jihad by providing a secure platform between the funders and the project organizers.

Select the projects that appeal to you and transfer the Cryptocurrency of your choice. *SadaqaCoins* will then take care of the rest. It's that easy. Do not miss the opportunity to support your brothers and sisters anonymously and safely.

Delivered by TNO innovation for life CyberDevOps.IT We do IT

Dark Web Monitor – DWM.pm



Dark Web Monitor

- Home
- Hosts
- Hosts
- Add
- Statistics
- Forums
- Forums
- Users
- Search

Dark Web Monitor Status

Forum Posts	Forum Users
Bitcointalk 7,044,576	Dream Market 39,137
31,154,891 Posts Scraped	434,948 Users Discovered

Forum Status

🖥	18	Total
✓	7	Online
✗	11	Offline

Forum Statistics

▤	422	Categories
≡	819,050	Topics
💬	31,154,891	Posts

Dark Web Monitor

- Home
- Hosts
- Hosts
- Add
- Statistics
- Forums
- Forums
- Users
- Search

DutchMagic

Username	DutchMagic
Search this user's posts	🔍
Date Registered	None
#Posts	120
Forum	Silk Road 2
Accounts with same Username	DutchMagic on Evolution (userid 31392) dutchmagic on Pandora (userid 321377) DutchMagic on Black Market Reloaded (userid 329491) dutchmagic on Agora (userid 354053) DutchMagic on Nucleus (userid 646058)
Languages	English (90%)

#Posts per Month

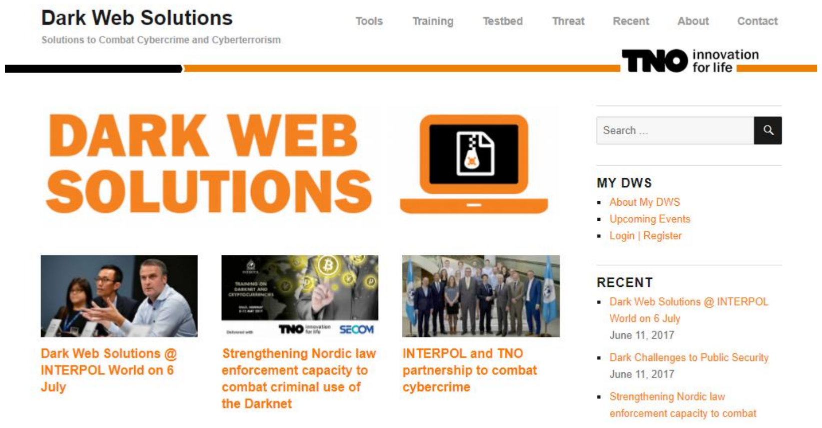
DARK WEB MONITOR START

New Release Available Now!!

Dark Web Solutions – DWS.pm

Toxic cocktail facilitating Cybercrime

- Tax agencies receive many claims from investors who bought bitcoin in early stage
- AmsterdamUnited – From online drugs lord to (almost) Bitcoin Exchange


Dark Web Solutions

Solutions to Combat Cybercrime and Cyberterrorism

Dark Web Solutions @ INTERPOL World on 6 July

Strengthening Nordic law enforcement capacity to combat criminal use of the Darknet

INTERPOL and TNO partnership to combat cybercrime

MY DWS

- About My DWS
- Upcoming Events
- Login | Register

RECENT

- Dark Web Solutions @ INTERPOL World on 6 July
  June 11, 2017
- Dark Challenges to Public Security
  June 11, 2017
- Strengthening Nordic law enforcement capacity to combat

Key Challenge

- Cross-ledger analytics and attributions for cryptocurrencies and tokens

Blockchain Security by Design

- Ambition to secure blockchain technologies and applications as simple as possible, secured by nature

- Use Cases
  - FinTech (*cross-border* payments, settlements, online identity, assets/rewards)
  - Logistics (provenance, trade finance, improved collaborations)

- To develop practical security challenges, and test solutions on operational cases.

Large variety of use cases

And many,
Many more!

BLOCKTEST

In partnership with SUTD / iTrust
Sponsored by NRF/EDB as part of the Second NCR Call since October 2017 for 2 years

Top 8 Blockchain Incidents (USD)

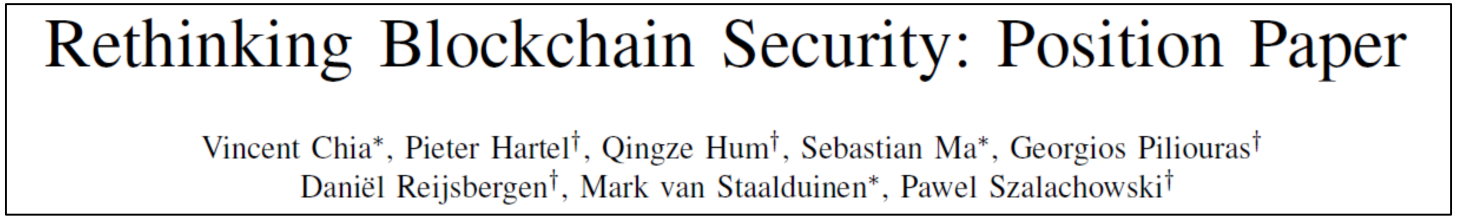
1. Coincheck hack, Japanese Crypto Exc missing NEM (530M, 2018)
2. Mt. Gox (450M, 2014)
3. Parity Multi-sig Wallet Hack (300M, 2017)
4. Italian Crypto Exc BitGrail Loss (170M, 2018)
5. Bitfinex Exchange Hack (78M, 2016)
6. DAO Smart Contract Hack (60M of initial 150M, 2016)
7. NiceHash Mining Market Breach (60M, 2017)
8. Tether Token Hack (30M, 2017)

OPSEC   Smart Contract   Consensus

Blockchain Incident Database

- Analysed 110 incidents
- Total loss more than 3 bUSD
- Most incidents due to OPSEC issues
- Blockchain specific categories
  - Smart Contract Security (16%)
  - Consensus Protocol Incentives (14%)

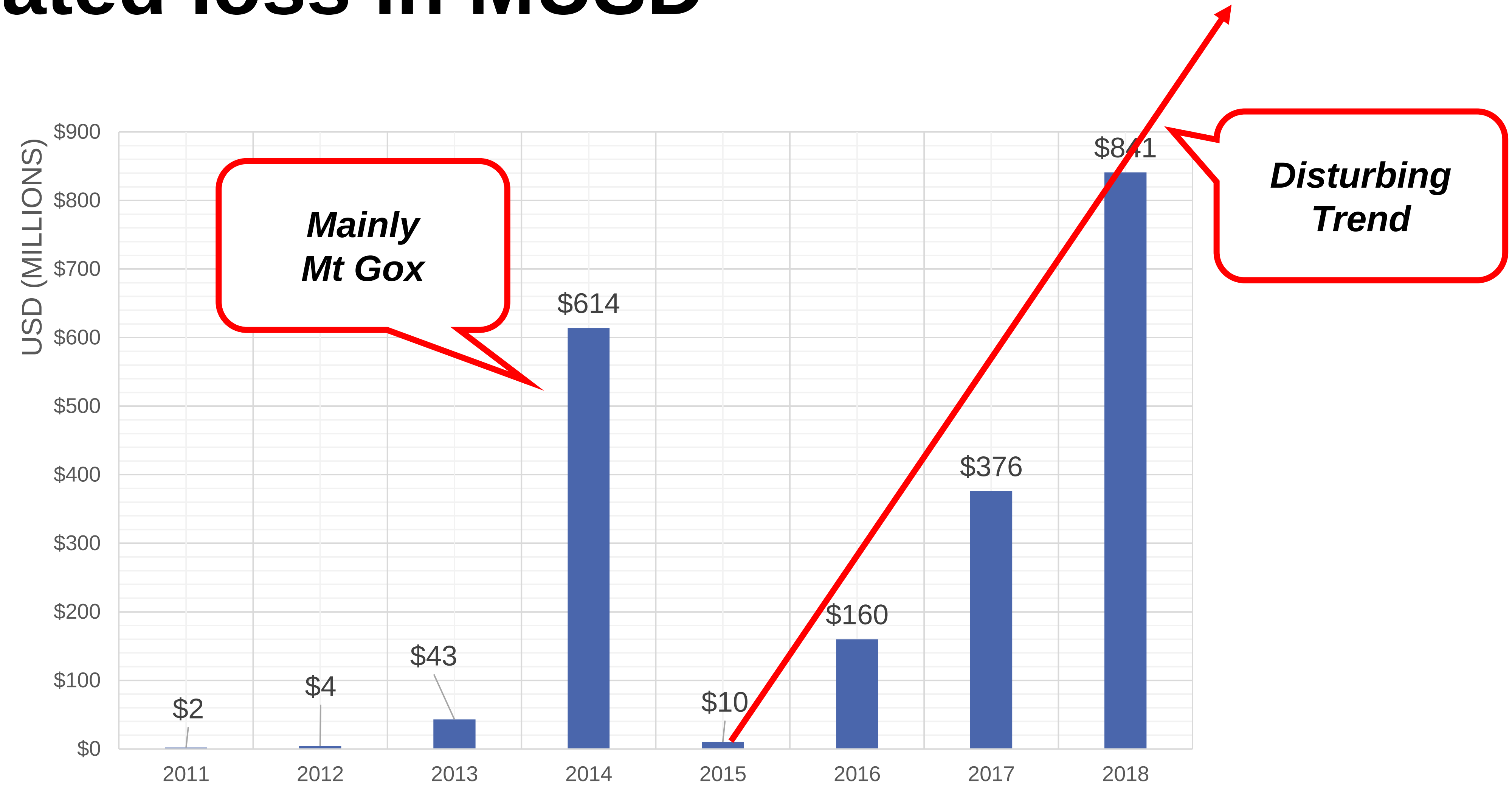
Blockchain Incidents described using Cybersecurity incident standards



Rethinking Blockchain Security: Position Paper

Vincent Chia[*], Pieter Hartel[†], Qingze Hum[†], Sebastian Ma[*], Georgios Piliouras[†]
Daniël Reijsbergen[†], Mark van Staalduinen[*], Pawel Szalachowski[†]

Estimated loss in MUSD



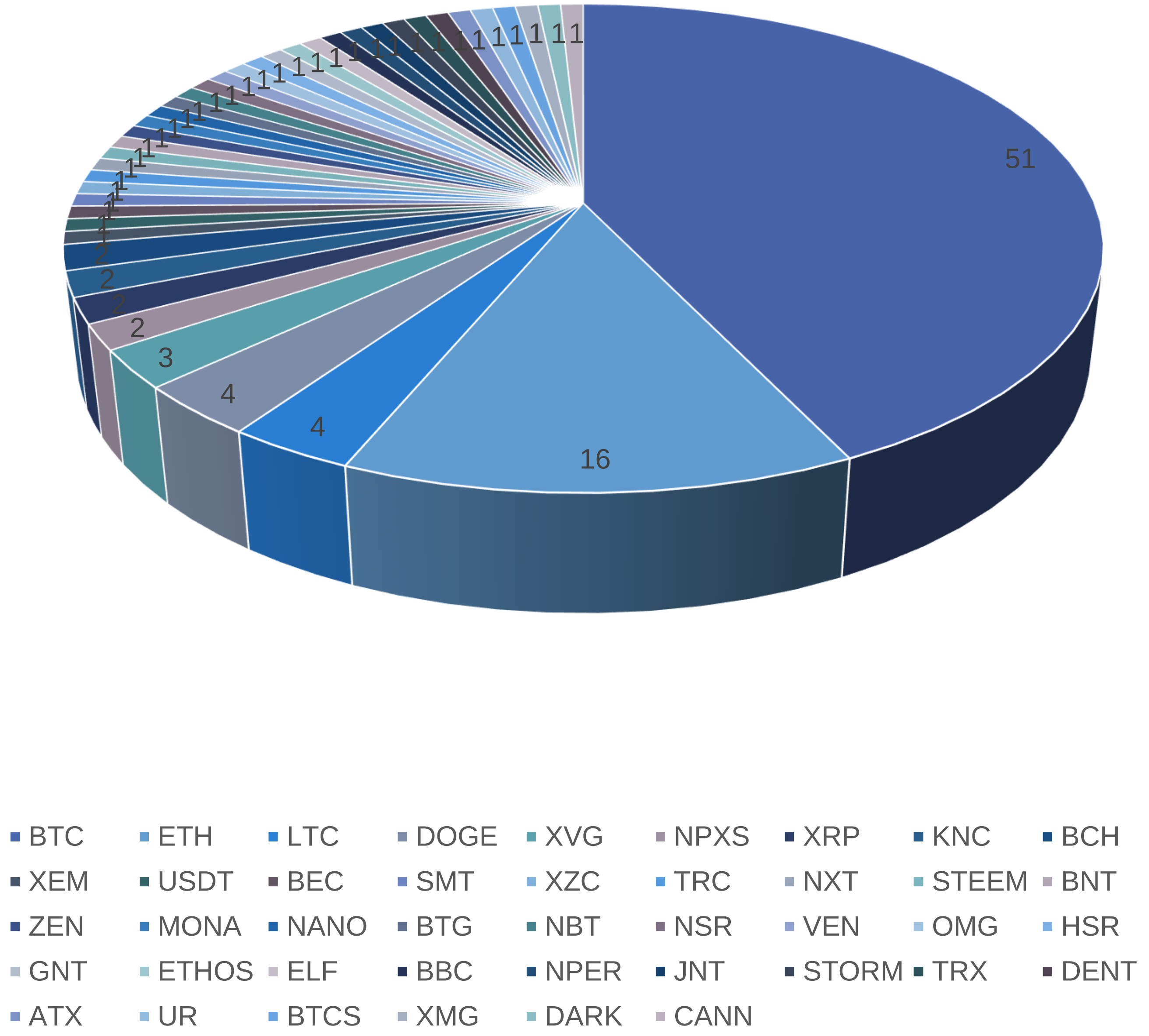
Mainly Mt Gox

Disturbing Trend

Bitcoin launched on Jan 3rd, 2009

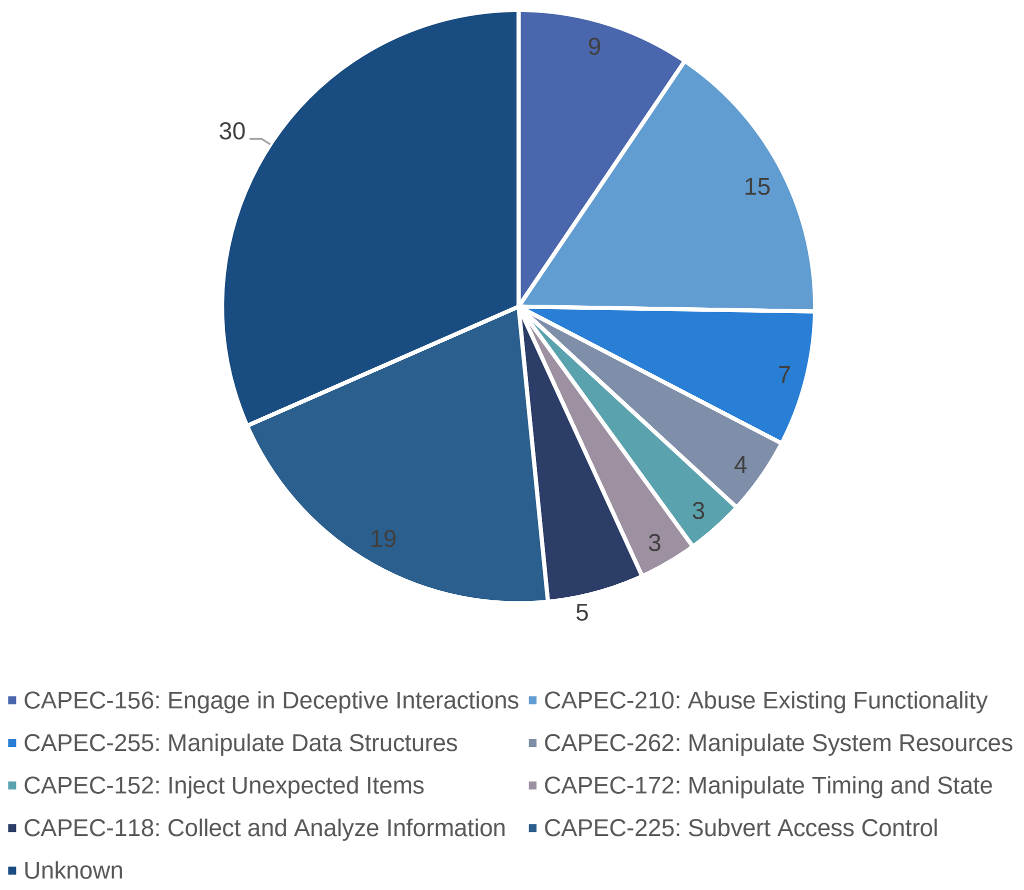
Ethereum launched on Jul 30th, 2015

Not only Bitcoin Related Incidents



OPSEC Attack Patterns

- Each OPSEC incident is classified based on the CAPEC coding as developed by MITRE
- Common Attack Pattern Enumeration and Classification (CAPEC) is a list of software weaknesses
- 19 out of 77 incidents are tagged as Subvert Access Control



https://capec.mitre.org

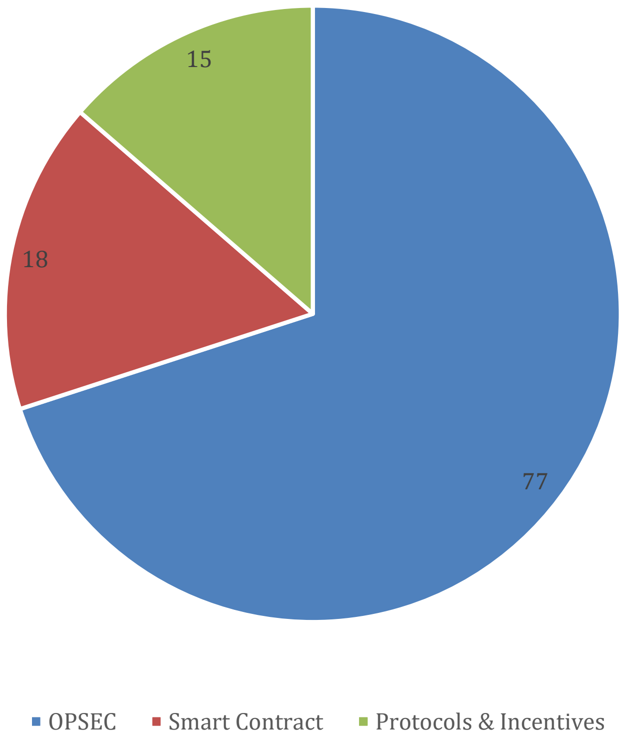
Trends in Blockchain Incidents

- Cryptocurrency Exchanges good alternative to attack, instead of Banks
- Crypto-jacking, crypto-malware aims to compromise devices for crypto mining
- Ransomware is still a major cyber threat exploiting cryptocurrencies
- Limited incidents reported on non-cryptocurrency cases
    - Not clear whether due to maturity or financial component

Blockchain Security Checklist

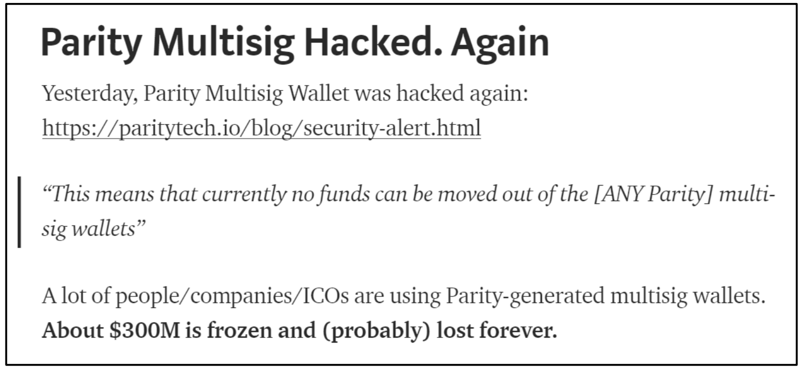
1. Key Management
2. Smart Contract Security
3. Consensus Protocol Incentives
4. Transactions Privacy
5. Digital Identities
6. Blockchain Security Policy

Blockchain Specific Challenges



Smart Contract Security

- Substantial number of security incidents are due to (un)intentional bugs in smart contracts.
- Several types of analysis tools
  - Fuzzing of the input of the contract,
  - Mutating of the code of the contract,
  - Static analysis of properties of the contract,
  - Model checking of behaviors of the contract,
  - Theorem proving of properties of the program.
  - Runtime verification techniques, such as proof carrying code*.
- Even more complex than blockchain and smart contracts



Parity Multisig Hacked. Again

Yesterday, Parity Multisig Wallet was hacked again: https://paritytech.io/blog/security-alert.html

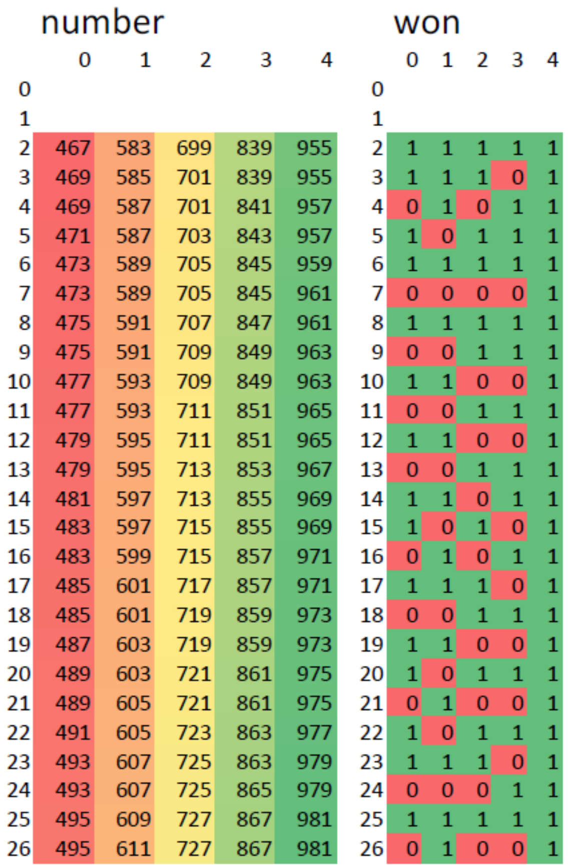
> *“This means that currently no funds can be moved out of the [ANY Parity] multi-sig wallets”*

A lot of people/companies/ICOs are using Parity-generated multisig wallets. **About $300M is frozen and (probably) lost forever.**

* Eg. Verification of Smart Contract (https://securify.ch/) by ChainSecurity / ETH Zurich.

Smart Contract Testing and Visualization

- ContractFuz
- ContractVis



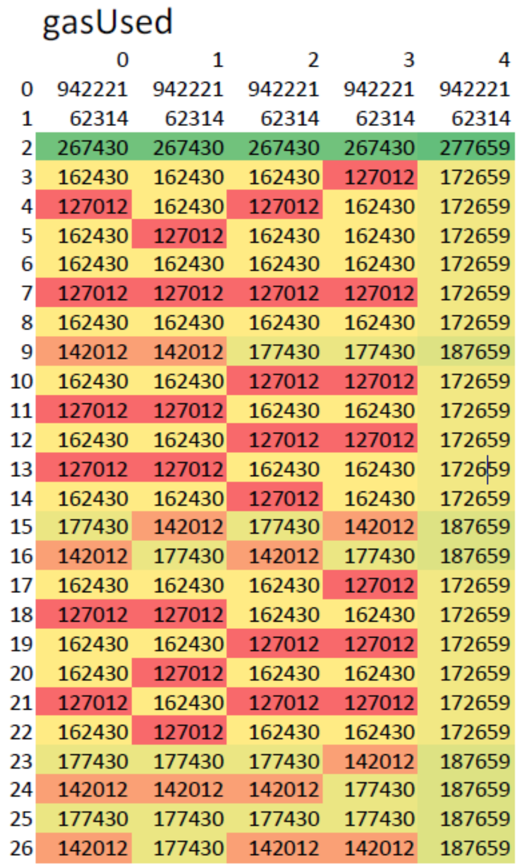
number

	0	1	2	3	4
0					
1					
2	467	583	699	839	955
3	469	585	701	839	955
4	469	587	701	841	957
5	471	587	703	843	957
6	473	589	705	845	959
7	473	589	705	845	961
8	475	591	707	847	961
9	475	591	709	849	963
10	477	593	709	849	963
11	477	593	711	851	965
12	479	595	711	851	965
13	479	595	713	853	967
14	481	597	713	855	969
15	483	597	715	855	969
16	483	599	715	857	971
17	485	601	717	857	971
18	485	601	719	859	973
19	487	603	719	859	973
20	489	603	721	861	975
21	489	605	721	861	975
22	491	605	723	863	977
23	493	607	725	863	979
24	493	607	725	865	979
25	495	609	727	867	981
26	495	611	727	867	981

won

	0	1	2	3	4
0					
1					
2	1	1	1	1	1
3	1	1	1	0	1
4	0	1	0	1	1
5	1	0	1	1	1
6	1	1	1	1	1
7	0	0	0	0	1
8	1	1	1	1	1
9	0	0	1	1	1
10	1	1	0	0	1
11	0	0	1	1	1
12	1	1	0	0	1
13	0	0	1	1	1
14	1	1	0	1	1
15	1	0	1	0	1
16	0	1	0	1	1
17	1	1	1	0	1
18	0	0	1	1	1
19	1	1	0	0	1
20	1	0	1	1	1
21	0	1	0	0	1
22	1	0	1	1	1
23	1	1	1	0	1
24	0	0	0	1	1
25	1	1	1	1	1
26	0	1	0	0	1

Fig. 1. Tracking the outputs of the Vitaluck contract showing how low entropy randomness leads to unfair behaviour.



gasUsed

	0	1	2	3	4
0	942221	942221	942221	942221	942221
1	62314	62314	62314	62314	62314
2	267430	267430	267430	267430	277659
3	162430	162430	162430	127012	172659
4	127012	162430	127012	162430	172659
5	162430	127012	162430	162430	172659
6	162430	162430	162430	162430	172659
7	127012	127012	127012	127012	172659
8	162430	162430	162430	162430	172659
9	142012	142012	177430	177430	187659
10	162430	162430	127012	127012	172659
11	127012	127012	162430	162430	172659
12	162430	162430	127012	127012	172659
13	127012	127012	162430	162430	172659
14	162430	162430	127012	162430	172659
15	177430	142012	177430	142012	187659
16	142012	177430	142012	177430	187659
17	162430	162430	162430	127012	172659
18	127012	127012	162430	162430	172659
19	162430	162430	127012	127012	172659
20	162430	127012	162430	162430	172659
21	127012	162430	127012	127012	172659
22	162430	127012	162430	162430	172659
23	177430	177430	177430	142012	187659
24	142012	142012	142012	177430	187659
25	177430	177430	177430	177430	187659
26	142012	177430	142012	142012	187659

Fig. 2. Tracking the gas used by the Vitaluck contract showing how information clearly visible on the blockchain correlates perfectly with the functionality.

Consensus Protocol Incentives

- NiceHASH, Crypto-Mining Malware or Stealing power/electricy for Cryptocurrency mining
- These attacks are attractive due to the Proof of Work consensus protocol
- Possible solution: alternative for Proof of Work, but would it really become better?

Service Unavailable

By **Helen Partz** JAN 28, 2018

Crypto-Mining Malware Epidemic: 55% of Businesses Affected Worldwide, Including YouTube

101382 Total views **974** Total shares

Four accused of stealing power from Chinese oil company to generate bitcoins

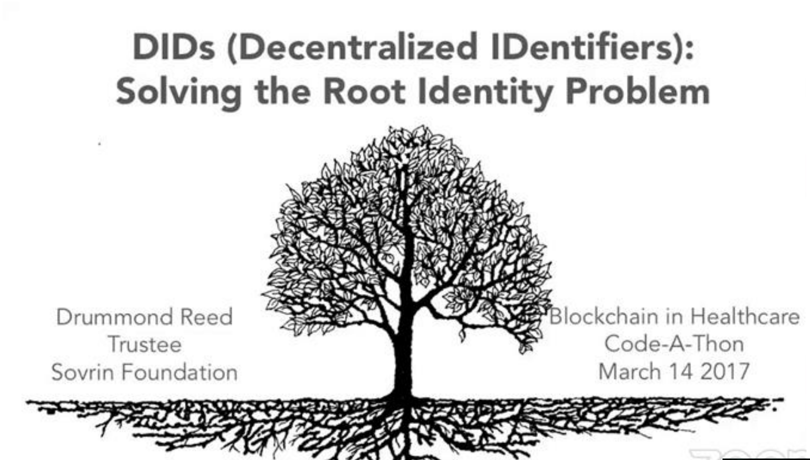
Police say 'mine' used to create digital crypto-currency had been hooked up to company's electricity network

PUBLISHED : Sunday, 27 August, 2017, 4:46pm
UPDATED : Sunday, 27 August, 2017, 4:45pm

COMMENT: 1

Blockchain driven Cybersecurity Solutions

Next Generatoin Cybersecurity solutions requires immutable "biometrics" of persons and systems in untrusted digital ecosystems like the internet.



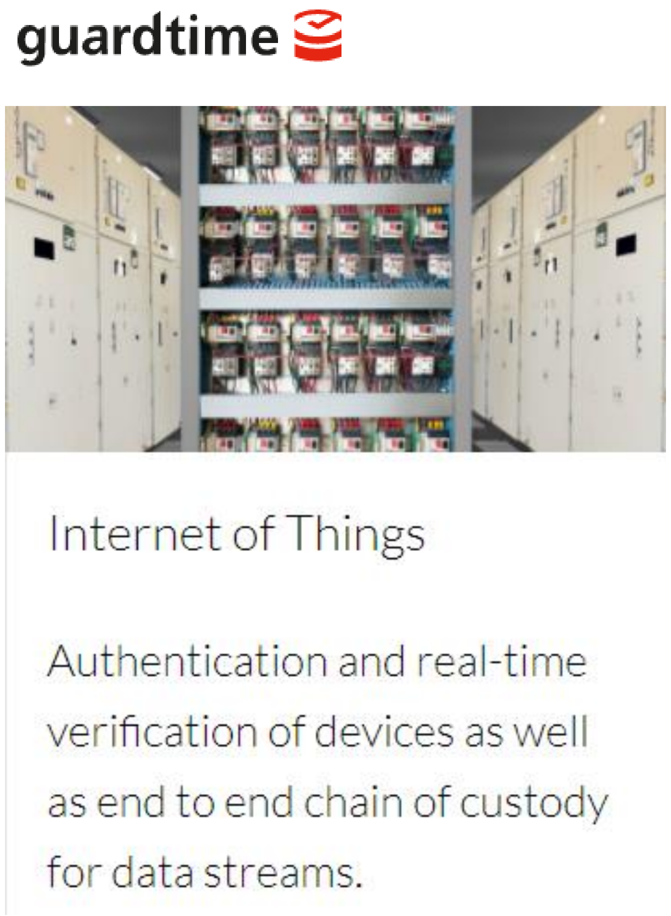
DIDs (Decentralized IDentifiers):
Solving the Root Identity Problem

Drummond Reed
Trustee
Sovrin Foundation

Blockchain in Healthcare
Code-A-Thon
March 14 2017

Proposed PoC with

- Sovrin
- IOTA
- Guardtime



guardtime

Internet of Things

Authentication and real-time verification of devices as well as end to end chain of custody for data streams.

Test on layers

- BC Application
- BC Network
- BC Technology

IOTA

THE ECONOMY OF THINGS

As the Internet-of-Things keep expanding, the need for interoperability and sharing of resources become a necessity. IOTA enables companies to explore new business-2-business models by making every technological resource a potential service to be traded on an open market in real time, with no fees.

Summary – Rethinking Blockchain Security

- **Dark Web Solutions –** [Blockchain as a Threat] Develop understanding, capacities and capabilities to combat criminal and terrorist use of blockchain. Dark Web Solutions program: https://dws.pm

- **Blockchain Security by Design –** [Blockchain for Innovation] Define security and privacy by design for blockchain and develop solutions to accelerate Blockchain innovations secured by nature: https://bcss.pm

- **Blockchain-enabled Cyber Security –** [Blockchain for Cybersecurity] Exploit the immutability, distributed and resilient characteristics of blockchain to improve or realize cybersecurity for the IoT era.

Key Challenges for Blockchain Security

- Attribution of Crimes with Cryptocurrencies
- Secure Smart Contract through Testing and Verification
- Security by Concensus Protocol Incentives
- Blockchain Security Auditing

Questions

Feel free to contact

Dr Mark van Staalduinen

Mark.vanStaalduinen@tno.nl

https://www.linkedin.com/in/markvanstaalduinen/

Relevant links

- https://dws.pm
- https://bcss.pm
- https://cyberdevops.it

DARK WEB MONITOR

START

DARK WEB SOLUTIONS

BLOCKCHAIN SECURITY SOLUTIONS