RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-F02

Nation-State Exploitation of Cryptocurrencies

Tom Robinson
Chief Scientist and Co-Founder
Elliptic
@tomrobin

Yaya J. Fanusie
Senior Fellow
Foundation for Defense of Democracies
@SignCurve

Overview

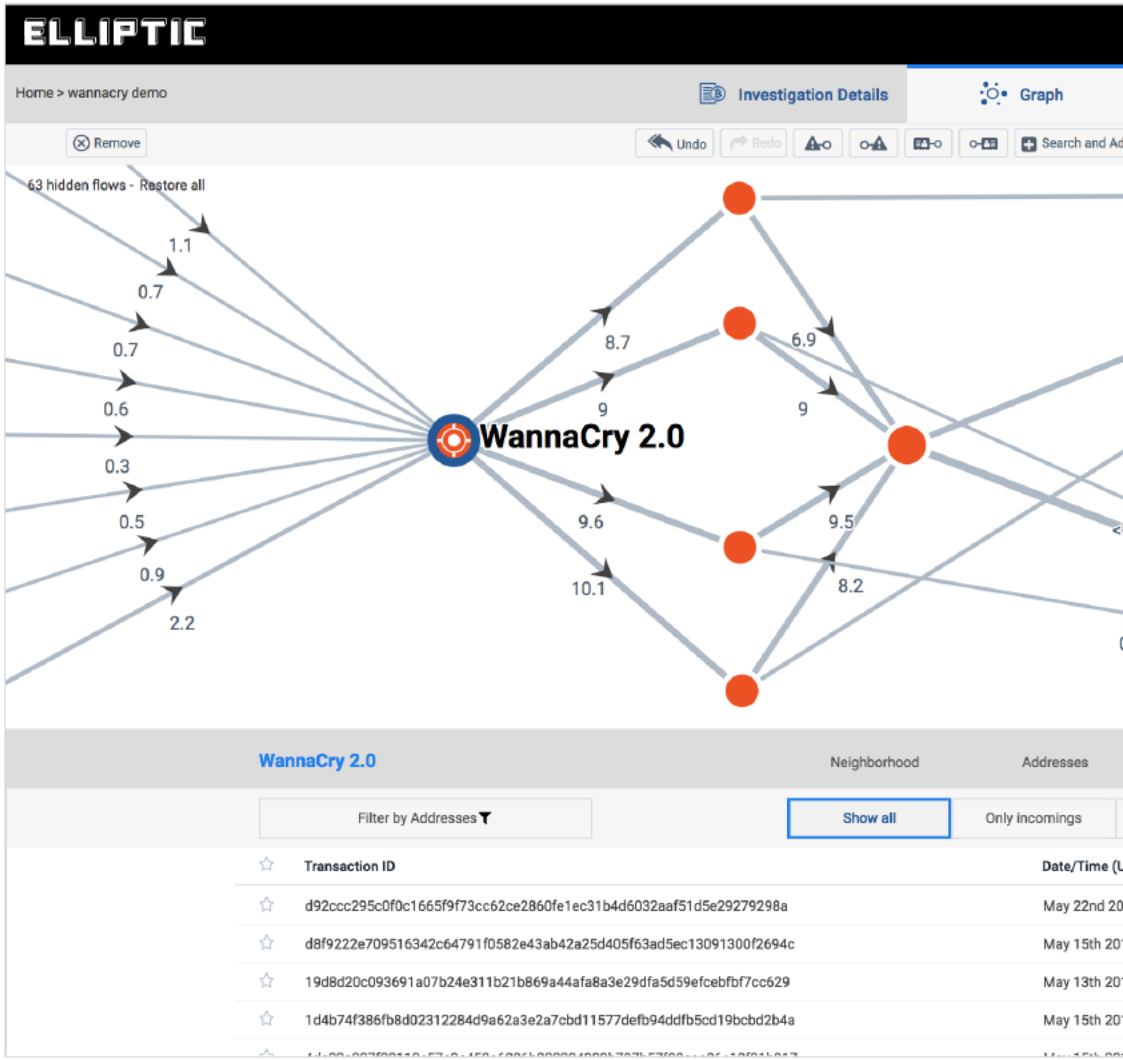
1. Why use cryptocurrencies?
2. Blockchain analysis
3. Crypto-espionage
4. Monetary gain
5. Sanctions evasion
6. Emerging issues
7. Conclusions

Why Would a Nation State Use Cryptocurrencies?

- Non-sovereign money
- Lack of consistent global regulation – ease of laundering
- Vulnerable infrastructure (exchanges etc.)
- Permissionless
- Censorship resistant
- Irreversible
- Digital
- Anonymous and untraceable (?)

Blockchain Analysis

- Cryptocurrencies are pseudonymous
- The pseudonyms (addresses) can sometimes be linked to actors
- The blockchain can then be used to monitor payments between those actors
- Elliptic's software is used by law enforcement to trace criminal proceeds, and by financial institutions for anti-money laundering checks
- ..and can give insights into nation state use of cryptocurrencies.

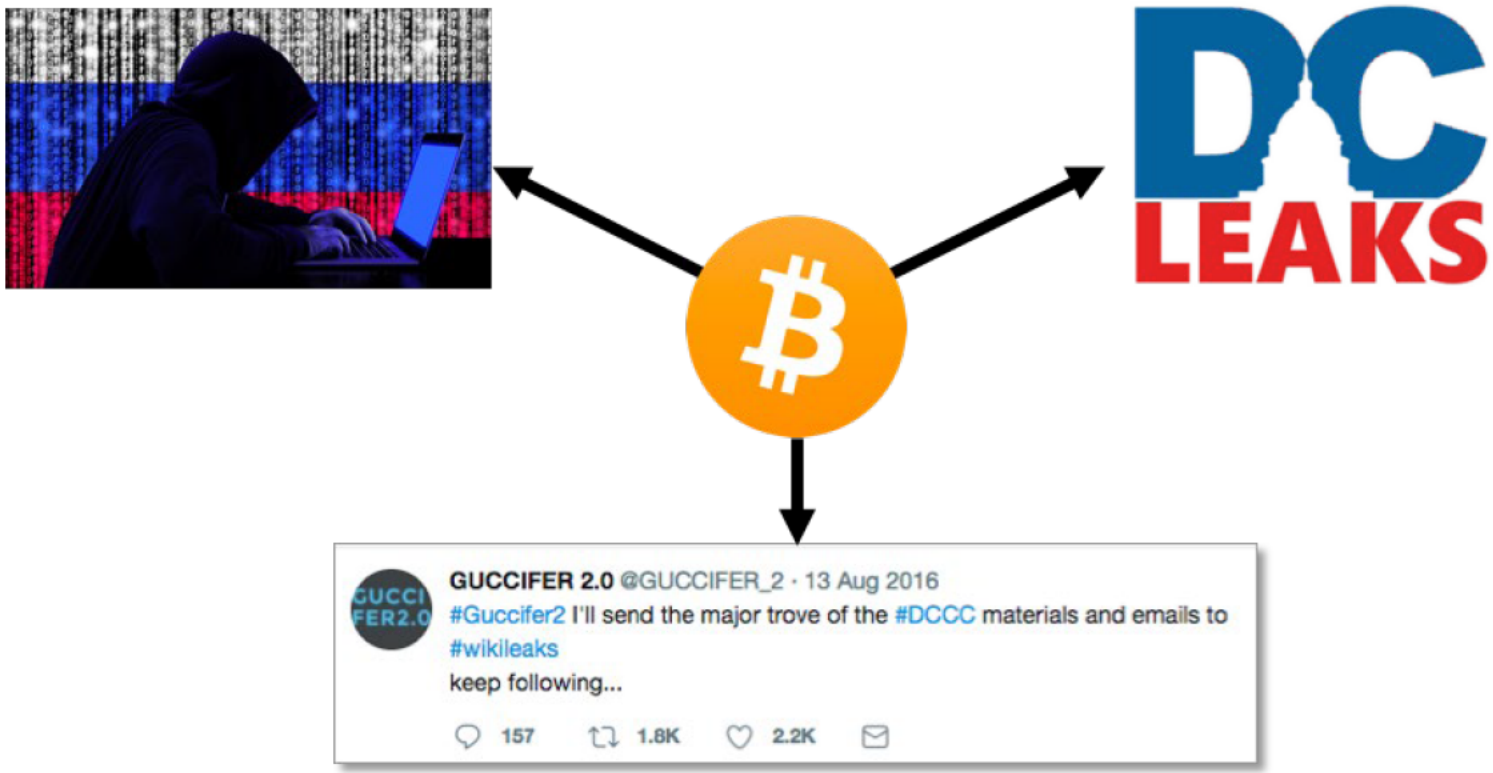


RSAConference2019

Nation State Exploitation of Cryptocurrencies: Espionage

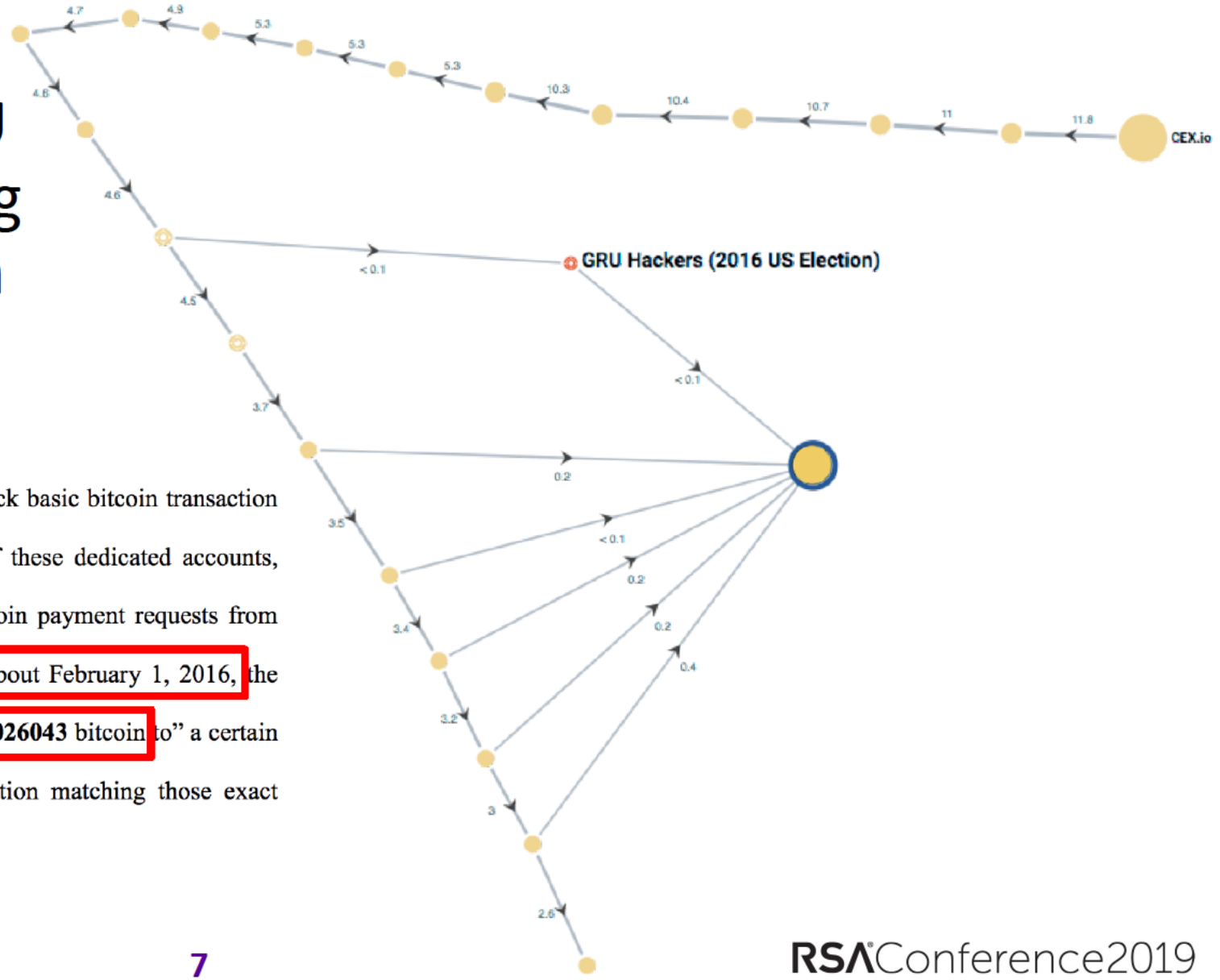
Crypto-espionage

Bitcoin has been used by nation-states to pay for infrastructure used in espionage and cyber attacks



Crypto-espionage

The US indictment of GRU officers provides a starting point for some blockchain detective work…



60. The Conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts, registered with the username "gfadel47," received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about February 1, 2016, the gfadel47 account received the instruction to "[p]lease send *exactly* **0.026043** bitcoin to" a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

Crypto-espionage

Cryptocurrency has been considered by intelligence agencies for the payment of overseas agents/informants

Homeland Security

China is considering blockchain's role in paying "intelligence professionals and informants"

"Blockchain and Suitability for Government Applications", 2018
Public-Private Analytic Exchange Program

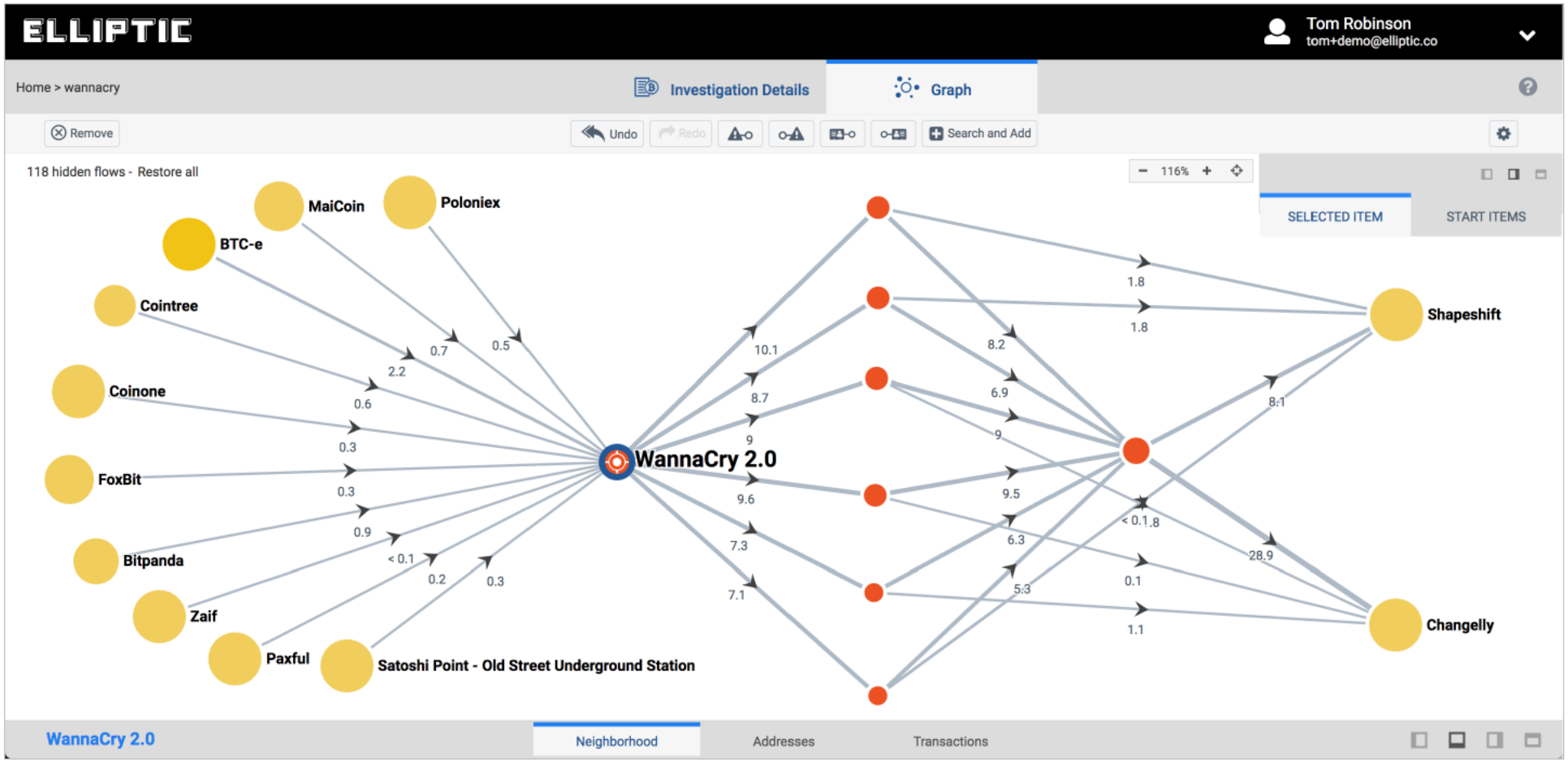
RSAConference2019

Nation State Exploitation of Cryptocurrencies: Monetary Gain


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy

Monetary Gain

Following the money from the WannaCry ransomware…



Monetary Gain

Following the money from the WannaCry ransomware…

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

Monetary Gain

The North Korea-linked Lazarus Group has been implicated in a number of thefts from South Korean cryptocurrency exchanges:

YAPIZON

$5m

April 2017

YouBit

Digital Currency Exchange

~$10m

December 2017

bithumb

글로벌 가상화폐 거래소 빗썸

$7m

June 2017

$31m

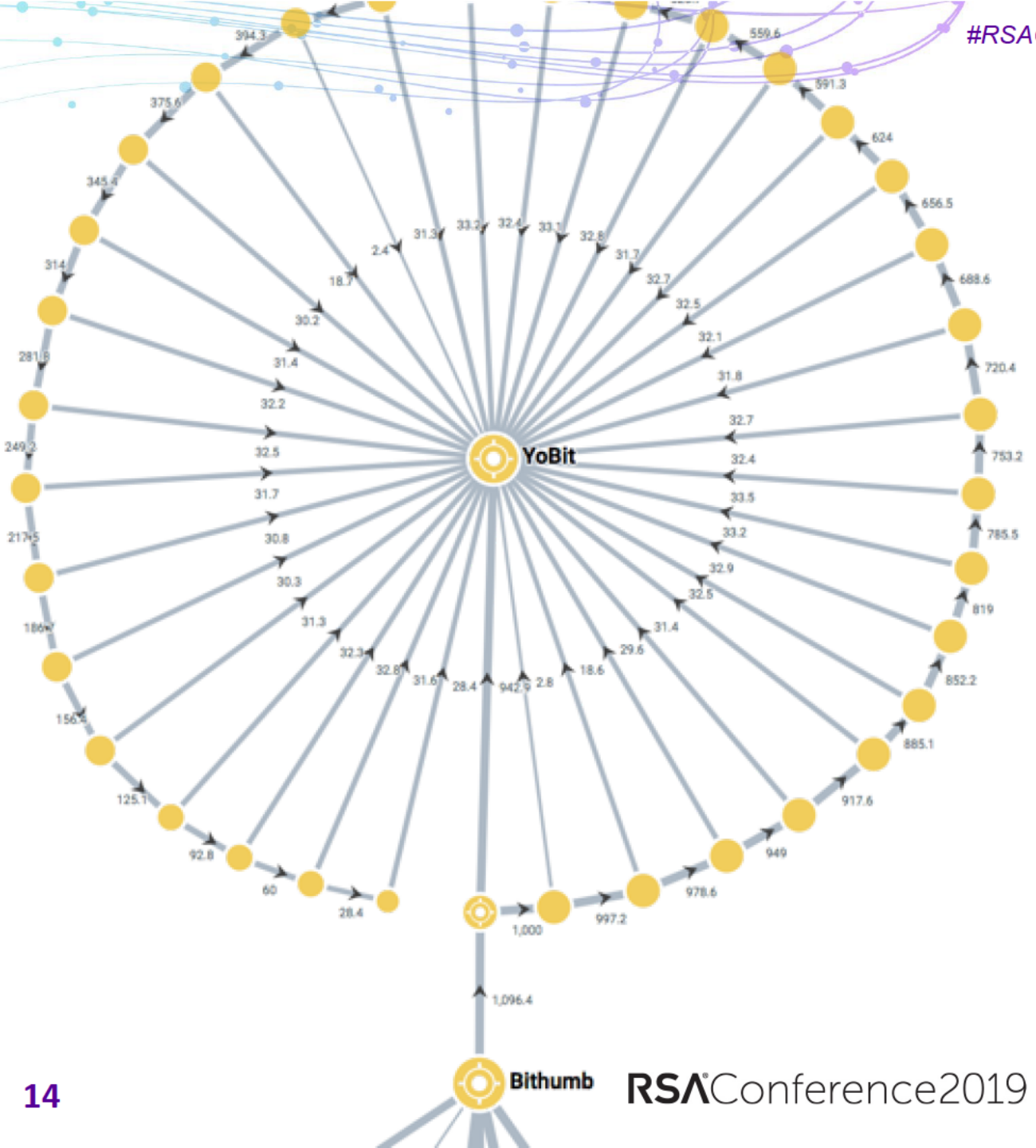
June 2018

Monetary Gain

Bitcoins from the 2018 Bithumb hack can be traced to a Russian cryptocurrency exchange

bithumb

YoBit.net

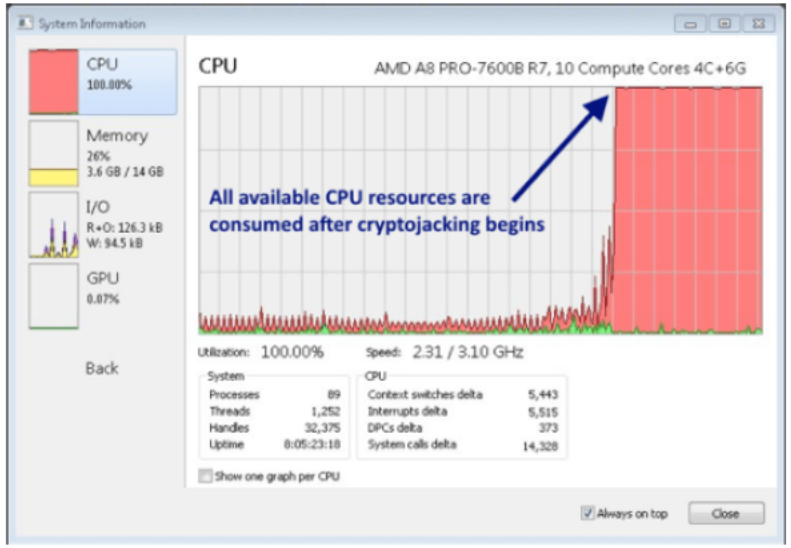


Monetary Gain

South Korean intelligence agencies have reported the use of cryptojacking by North Korea

An analysis of cryptojacking malware shows the use of monero mining servers at Kim Il Sung University in Pyongyang

But how does this fit into the overall sanctions picture..?

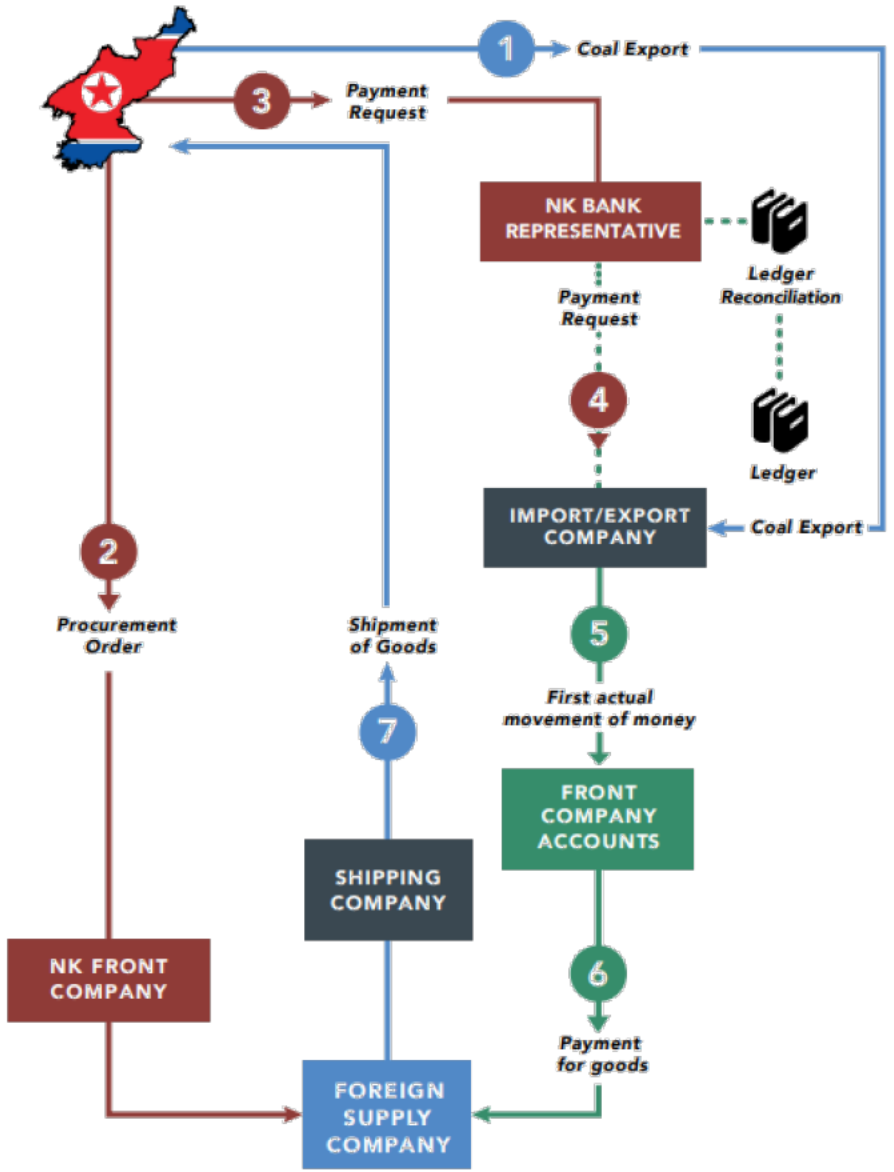


RSAConference2019

Nation State Exploitation of Cryptocurrencies: Sanctions Evasion

Sanctions Evasion

- Sanctions evasion schemes in the conventional financial sector are well-established and robust
- E.g. one form of North Korean sanctions evasion, through international trade, accounted for almost $200 million during a 9 month period in 2017.
- Monero's total market cap is around $700-800 million.



The Petro

- ICO scam meets regime propaganda
- A failed, but ongoing experiment
- Ethereum/NEM/Dash-based?
- Other nations are likely gaining lessons-learned

Petro

Iran's national currency in the works

- Iranian banks have experienced being "de-SWIFTed"
- Huge incentive to develop an alternative payments system
- Collaborating with Russia
- Building new platforms through Hyperledger & Stellar
- Iran Blockchain Labs is a key center of Iranian crypto/blockchain education

Russia investing in blockchain technology

- Many Russian banks are under U.S. and EU sanctions
- Russia piloting Ethereum and Hyperledger projects
- Crypto-Ruble? Some politicians want it, but financial authorities not on board
- Russia interested in a multilateral digital currency, e.g., with Eurasian Economic Union, BRICS

Cryptocurrencies on the US Treasury's Radar

- President Trump issued an Executive Order against the Petro
- OFAC adding digital currency addresses to its sanctions blacklist
- Treasury probably will designate wallet addresses when it wants to send a strong message
- A more compliant crypto sector is growing, but a smaller noncompliant underground is evolving as well

Sanctions Resistance?

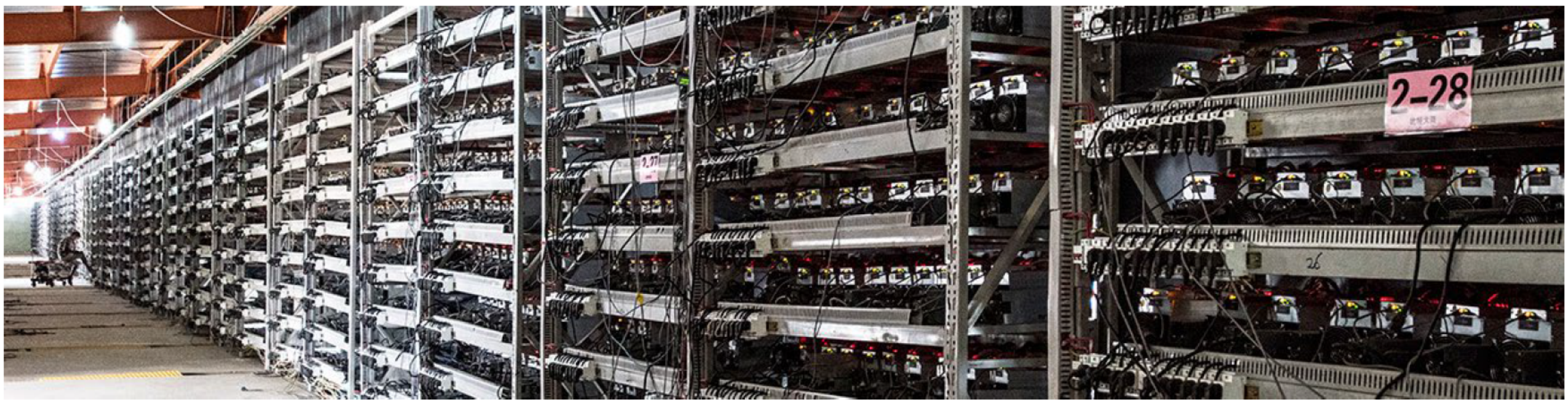
- Nation-state cryptocurrency / blockchain efforts are unlikely to counter sanctions power, in short term
- SWIFT unlikely to be displaced even if an alternative is technically "better"
- But there is one nation that could alter these dynamics…

China

- Beijing wants an alternative to the dollar as the world's dominant reserve currency
- The People's Bank of China has a Digital Currency Research Initiative
- Developing blockchain projects in financial centers in various provinces
- A Chinese digital currency may not be a matter of "if," but "when"

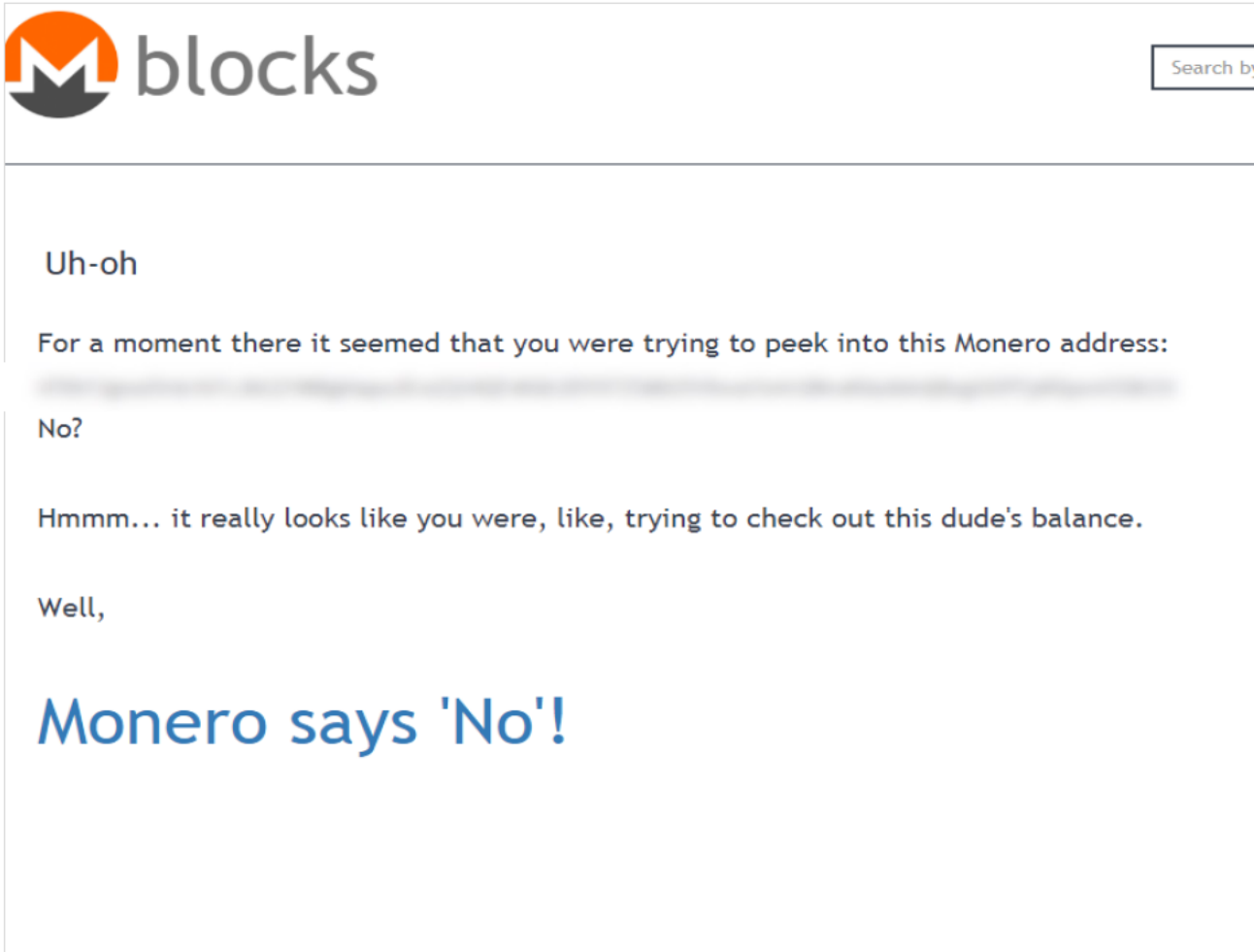
Cryptocurrency Mining

- 74 % of Bitcoin mining power is in China
- If public blockchains become more relevant for global business, centralized mining power brings vulnerabilities



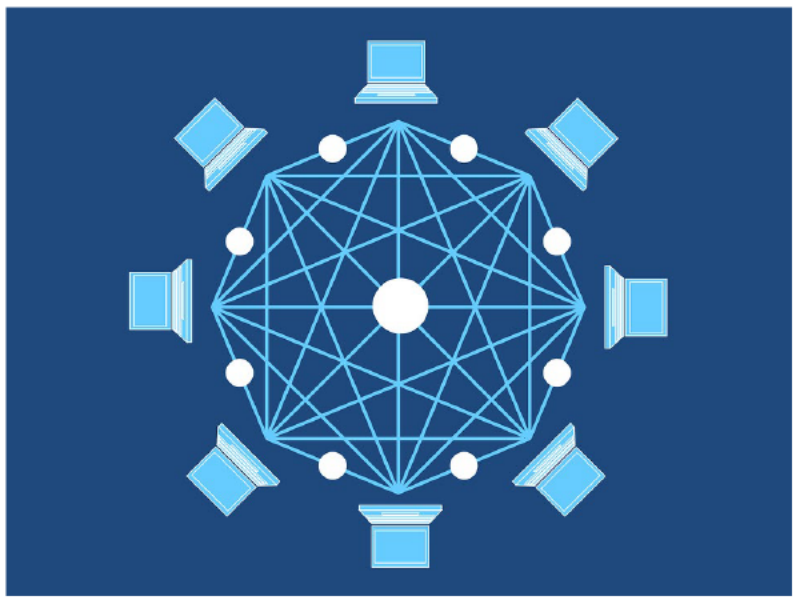
New Innovations, Emerging Threats

- "Privacy coins" growing in response to the traceability of the blockchain and de-anonymization tools
- Privacy coins are more likely to be relevant for lower-value transactions, or for small, non-state illicit actors



Decentralized exchanges bring new challenges

- Generally decentralized exchanges do not take custody of coins
- Crypto-to-crypto transactions, no fiat currency
- May not identify customers
- Illicit actors (state and non-state) will likely move away from regular, centralized exchanges



Closing thoughts

- Cryptocurrencies will continue to be used in espionage – although there is likely to be a shift to privacy coins
- Cryptocurrency exchanges remain low-hanging fruit for nation states willing to conduct theft
- States will continue experimenting with how they might issue their own cryptocurrencies, perhaps a hybrid between public and private blockchains
- The financial sector is going to have to evolve and adapt to this technology, although how the evolution will occur is unclear