NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Challenges of Digital Currency from the Perspective of Financial Crimes

Professor LAM Kwok Yan

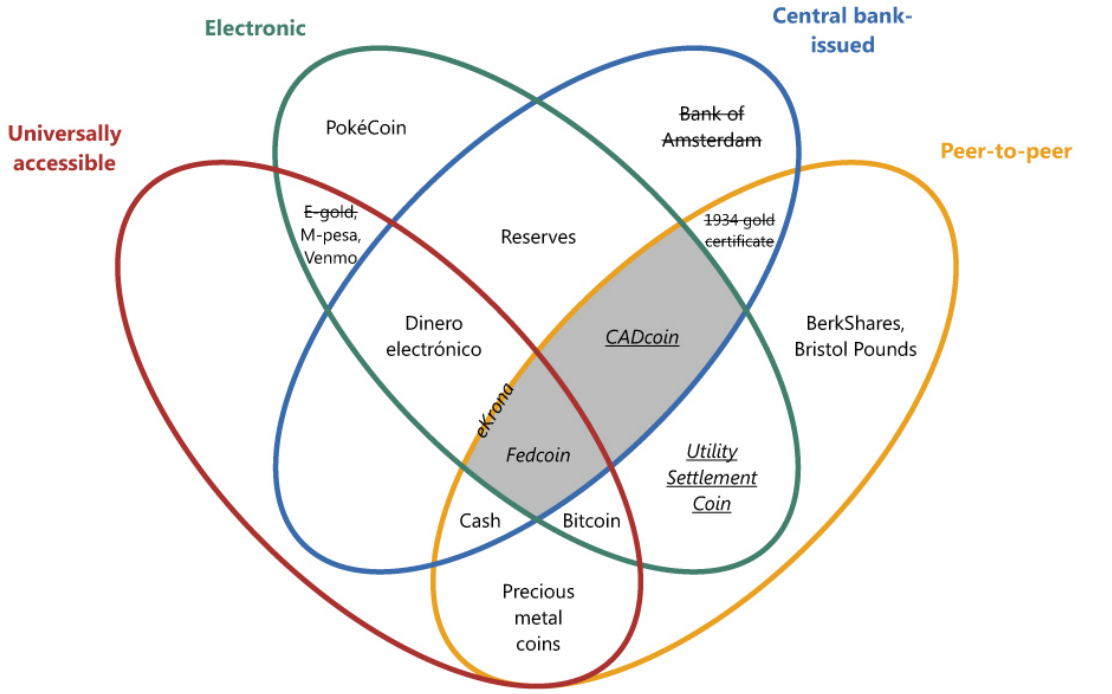
Professor of Computer Science
Director, Nanyang Technopreneurship Center
Director, Strategic Centre for Research in Privacy Preserving Technologies and Systems (SCRiPTS)
Director, SPIRIT Smart Nation Research Centre

With part of the materials contributed by:
Mr Boon-Hiong Chan
Dr Mark Van Staalduinen, NTU

Introduction: Before Digital Cash

To appreciate the significance of the technology underpinning digital currencies, it is instructive to consider traditional payment methods.

The money flower: example — Graph B



A standard font indicates that a system is in operation; an *italic* font indicates a proposal; an *italic and underlined* font indicates experimentation; a ~~strikethrough~~ font indicates a defunct company or an abandoned project.

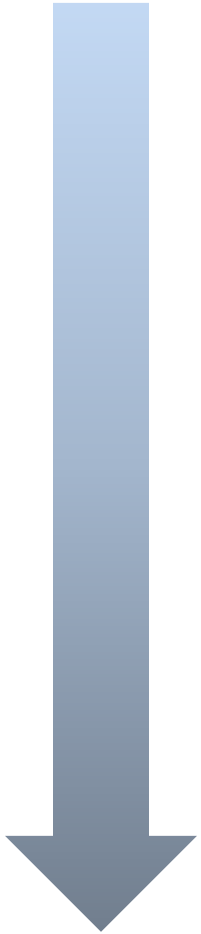
Cash payments

- Immediate and final.
- No trust required, no delay in executing payments.
- No third party can intervene, but transacting parties need to be physically present.

Intermediated payments

- Requires trusted third party to facilitate clearance (e.g. cheques, credit/debit cards, bank transfers).
- No need for transacting parties to be physically present.
- Higher cost and processing time.

Why Blockchain?



Transact through a Trust Provider

High Transaction Overhead

Cryptocurrency

Possibility of Double Spending

Distributed Ledger

Implemented as a Distributed System Service

Blockchain

Track and Trace of Digitized Assets

Blockchain Applications

Track moving value or money

What applications are Blockchain suitable for ?

Decentralized Finance (DeFi) Trends

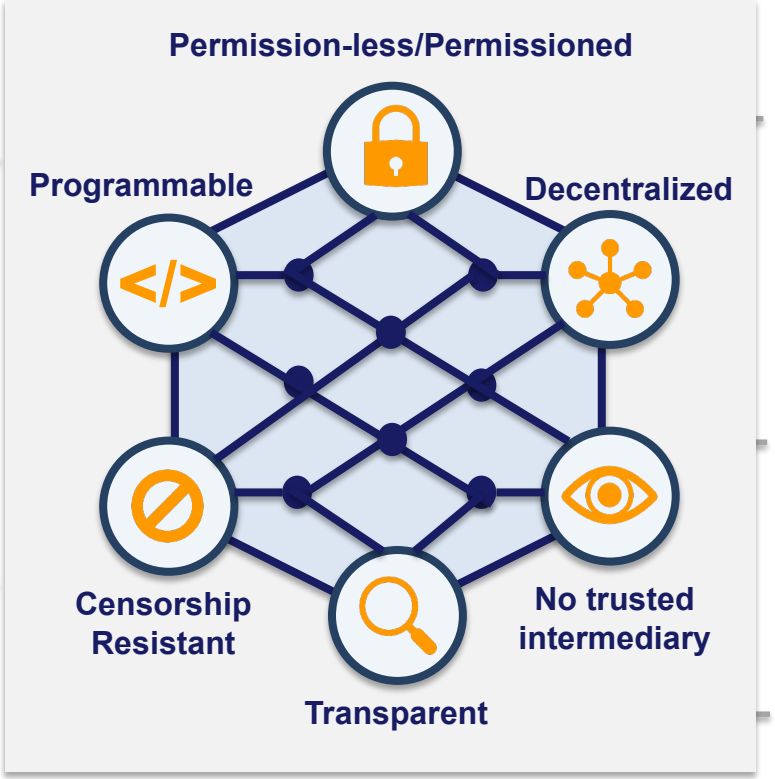
The DeFi movement has shifted traditional financial products towards **decentralized networks and open source software** through smart contracts and distributed systems.

Innovative new products

Simple services like **low-cost, fast international transfer** (remittance), and more complex products including *insurance*, **prediction markets**, **decentralized leverage trading**, **lending protocols** and **synthetic assets.**

Decentralized Lending Protocols

Put up **crypto collateral via smart contracts** on the blockchain to free up cash for day-to-day expenses or trading.



Ethereum blockchain continues to dominate DeFi landscape

Every major DeFi protocol, barring Bitcoin's lightning network, is **built on the Ethereum blockchain**, and new projects join all the time.

Rise in Stablecoin interest

Large and growing appetite for stablecoins as traders seek on-(block)chain ways to hedge and store value.

Evolving exchanges

Exchanges are moving beyond the paradigm of separate, purely centralized or decentralized services, with **new platforms that include the best of both paradigms**.

Source: Makerdao, "Decentralized Finance (DeFi) Trends" (11 June 2020)

Obstacles to Widespread Adoption

There are several **factors withholding the widespread adoption of virtual currencies** as a means of payment by consumers and businesses.

VOLATILITY

- Value of virtual currencies relative to fiat currencies fluctuates wildly.
- As a result, many perceive it as an volatile store of value, resulting in additional risk/complexity to their use for payments.

Bitcoin 1y Price Index (Jun 19' – Jul 20'):

EASE OF USE

- Users need a certain degree of technical knowledge to use virtual currencies competently and securely; it is often seen as too complicated for most people to understand.
- Virtual Assets Service Providers can handle the technical aspects on behalf of customers, but may be prone to hacks/data breaches.

NETWORK EFFECTS

- Ability to use virtual currencies as a means of payment lies in it being sufficiently widely-accepted.
- Without reaching critical mass, it would not be suitable for general use to exchange for goods and services.

SECURITY

- There have been high-profile attacks on exchanges and wallet providers.
- One can hold virtual currencies securely in an offline "cold wallet", but there is no way to recover lost keys.
- No safeguards against transferring virtual currencies to the wrong wallet address.

ZDNet June 24, 2020
CryptoCore hacker group has stolen more than $200m from cryptocurrency exchanges

Forbes Aug 15, 2019,
Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018

The Guardian 12 Jul 2019
$32m stolen from Tokyo cryptocurrency exchange in latest hack

Security Concerns – Vulnerable Wallets

The **nature of storage for virtual currencies can lead to the loss of funds**. The wallets in which such funds are held can be physical, software-, or web/exchanged-based.

COLD WALLETS

Hardware

Widely considered to the safest option for storing virtual currencies. In USB format, the wallet can be connected to the internet for exchange or trading, but can be disconnected so funds are stored offline and inaccessible to hackers. This type of wallet provides full isolation between private keys and computer/smartphone.

Paper

A paper wallet is an offline mechanism for storage. The user literally prints out public and private keys on paper and stores them somewhere safe. This method is extremely safe and cheap, but if the paper is misplaced, the private keys cannot be recovered.

HOT WALLETS

Software

A software wallet is an application that be downloaded to the user's computer/smartphone. It is safer than a web/exchange wallet because the private keys are not controlled by a third party. However, such devices may be vulnerable to attacks.

Online/Exchange

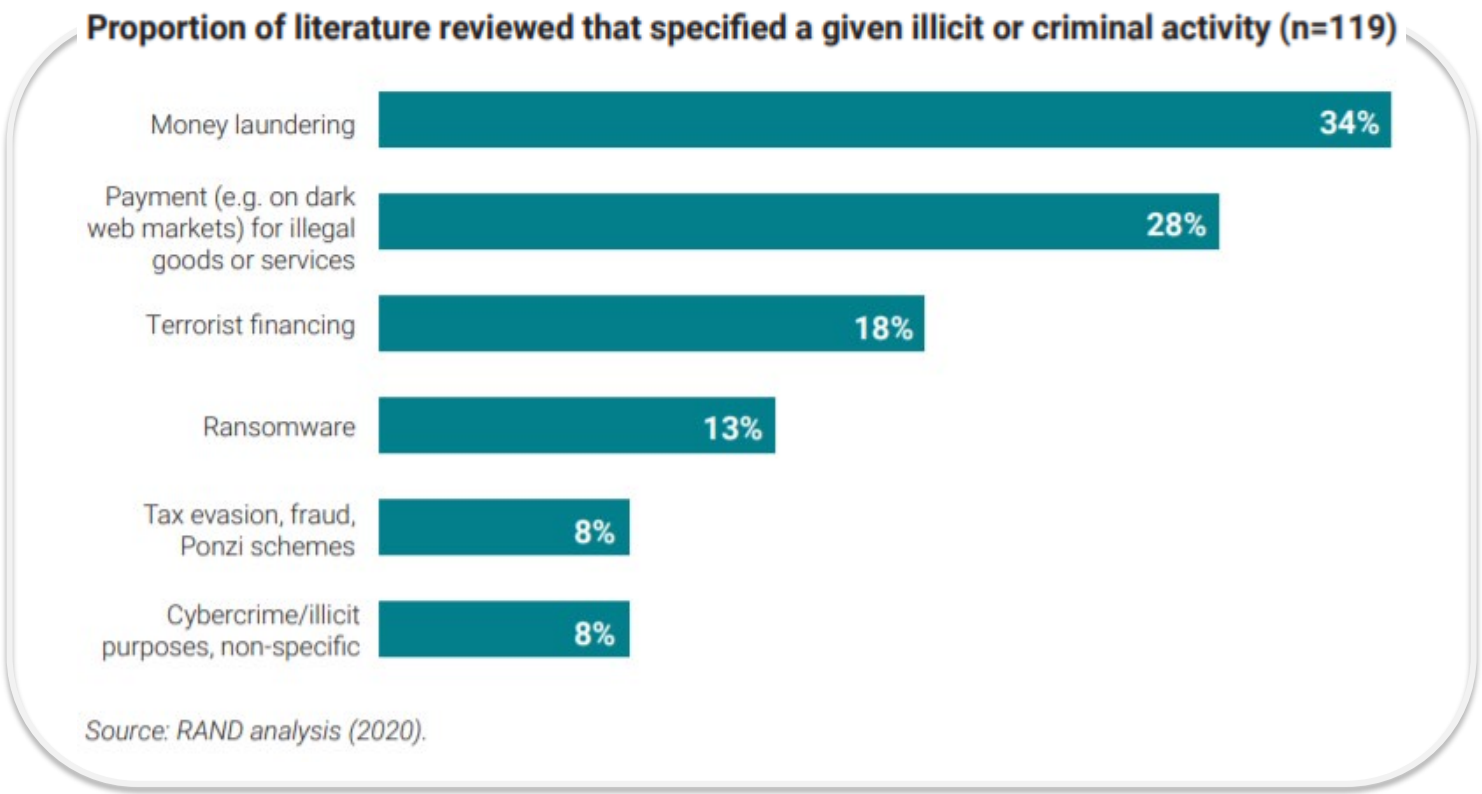
Leaving the virtual currency on an exchange is the most unsecure and susceptible to being hacked, having user's e-mail or login info stolen, or to a counterparty risk.

MOST SECURE — **LEAST SECURE**

Source: F. Atkinson, "How to properly safeguard massive amounts of cryptocurrency assets", 1 May 2019

“Privacy” Concerns: Illicit/Criminal Purposes

..but such virtual currencies also **provide cybercriminals with the opportunity to perform illicit activities** behind the veil of anonymity.



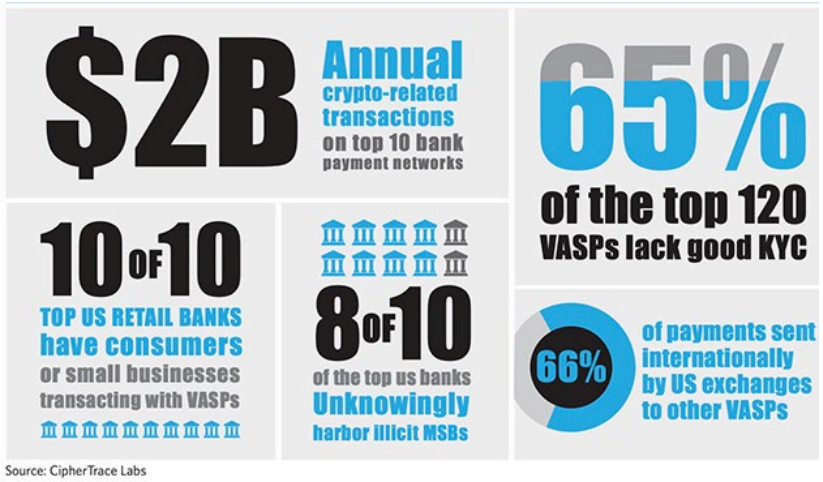
While most transactions made with virtual coins are legitimate, **cryptocurrencies are also used for a wide range of illicit or criminal purposes by a diverse group of malicious actors**. The three most prominent illicit use-cases of cryptocurrencies are:

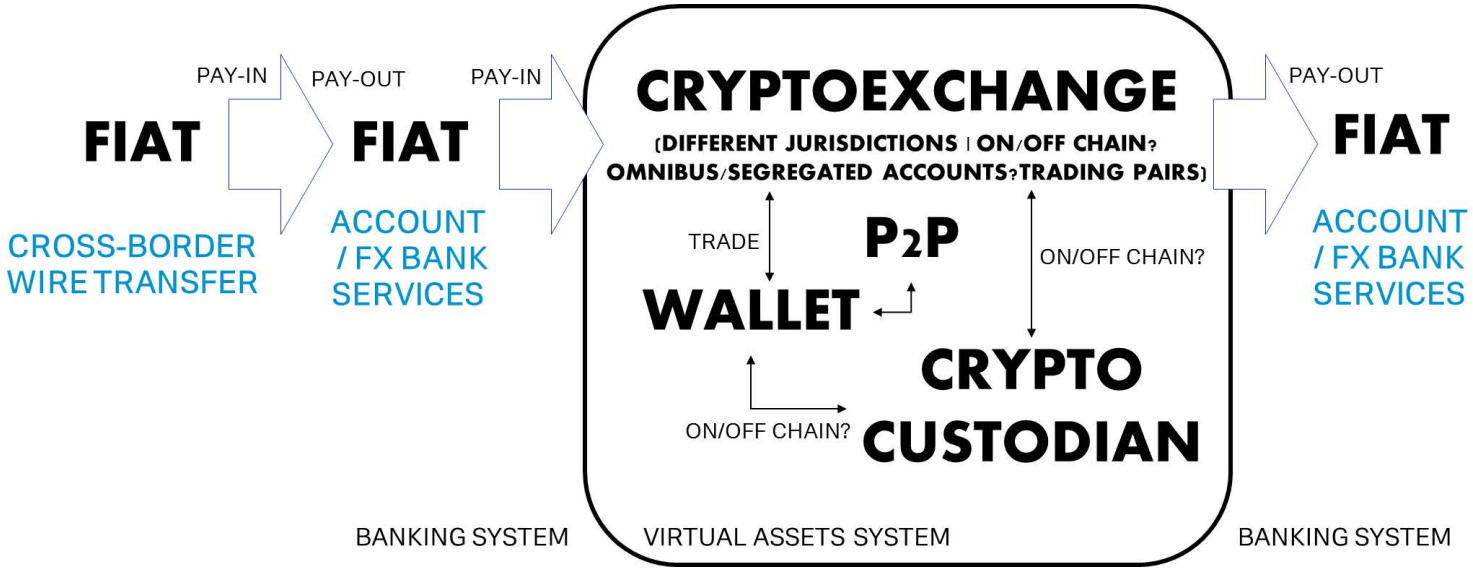
- Money laundering
- Trade in illicit goods and services
- Terrorism financing

Source: E. Silfversten et al, “Exploring the use of Zcash cryptocurrency for illicit or criminal purposes”, (2020)

Banking Industry Crypto-Asset Blind Spots

Banks and cryptocurrencies are becoming increasingly intertwined.





- Banks cannot “see” what is happening in the virtual assets system, may unknowingly send fiat to VASPs.
- **High risks of being unwitting participants of money laundering and/or terrorism financing**.
- As ecosystem becomes more complex (e.g. DeFi, Paypal/bitcoin, Expedia/Travala to accept crypto payments, etc.), ↑ **AML and CFT compliance risks**.

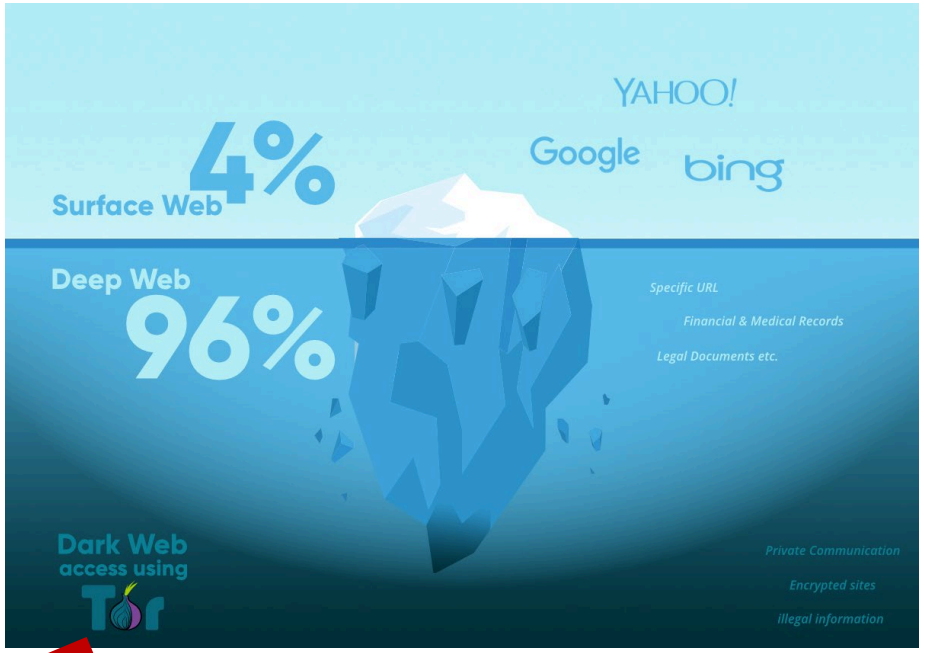
Dark Web Means

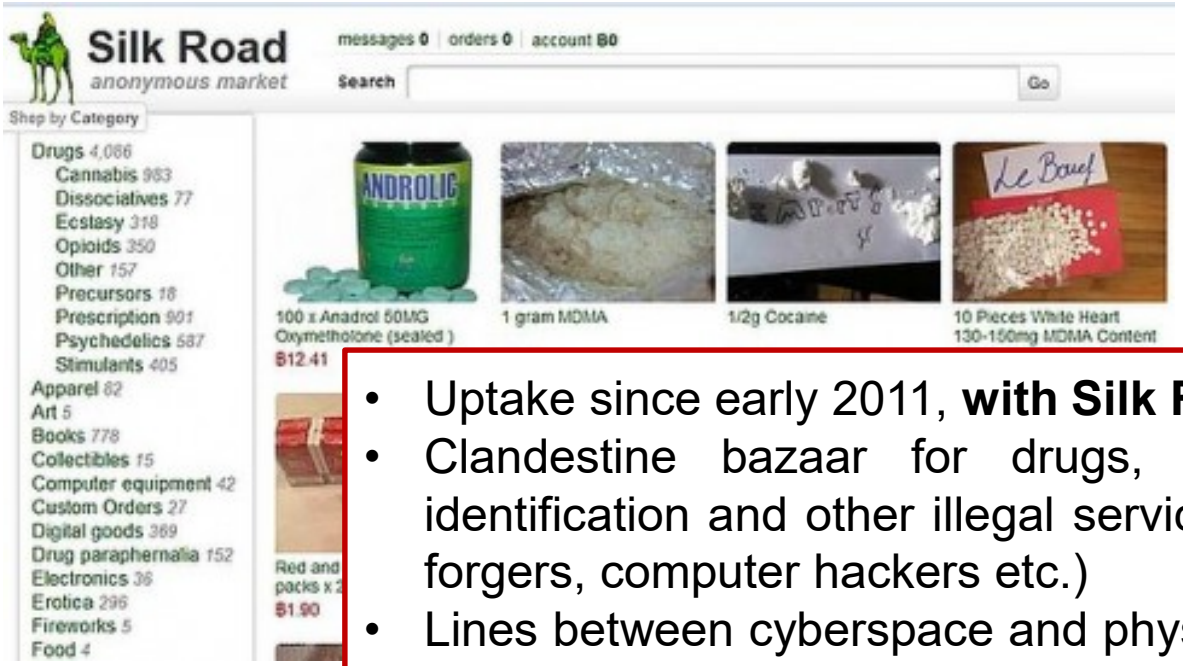
Bitcoin support more-or-less anonymous payments

Tor Browser

Extremely simple to install, allows user to remain completely anonymous online through its peer-to-peer setup

History of Dark Web





- Uptake since early 2011, **with Silk Road 1.0**.
- Clandestine bazaar for drugs, guns, fake identification and other illegal services (hitmen, forgers, computer hackers etc.)
- Lines between cyberspace and physical blurred - new concept of **Cyber-Physical Crimes**.

Exploit the anonymity of Tor and its Tor Browser. **Bitcoin commonly used to facilitate illicit transactions on the darknet markets.**

'Bitcoin transactions are anything but anonymous'

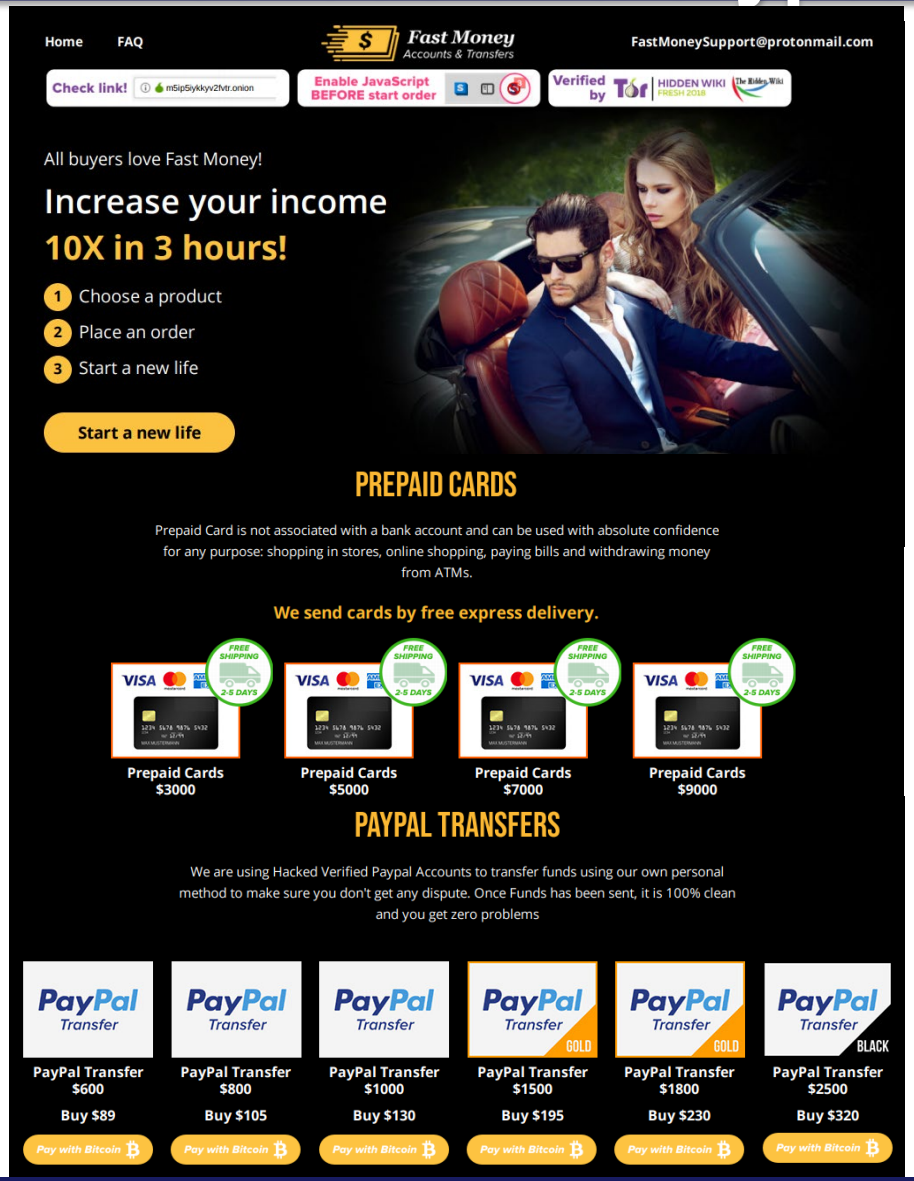
CASE EXAMPLE:

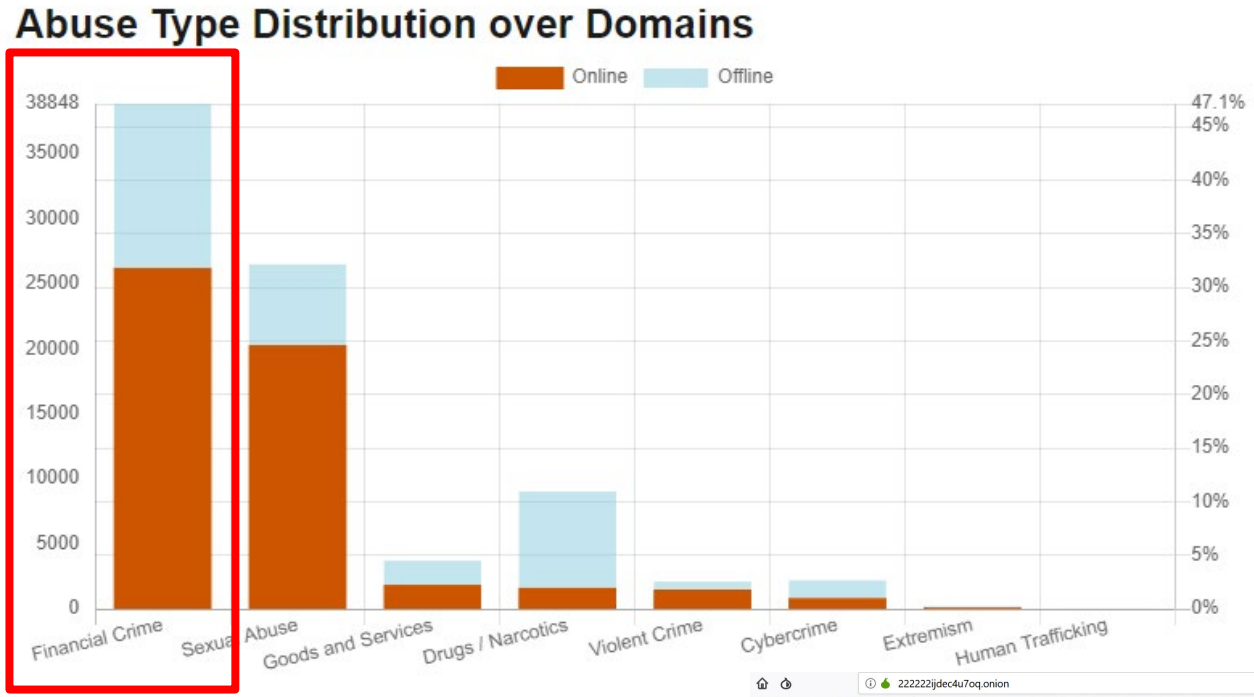
Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop

ANDY GREENBERG 01.29.15 01:55 PM

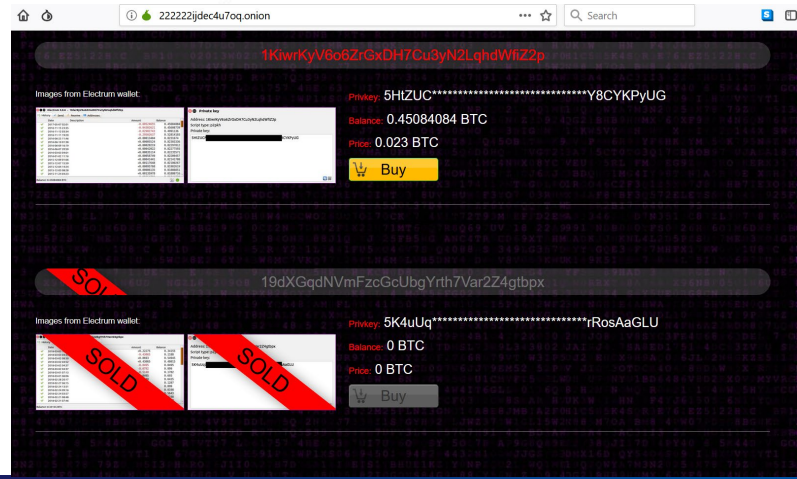
Source: The Wired

Trend 1. Trade in credentials of cards, new payment methods and cryptocurrencies



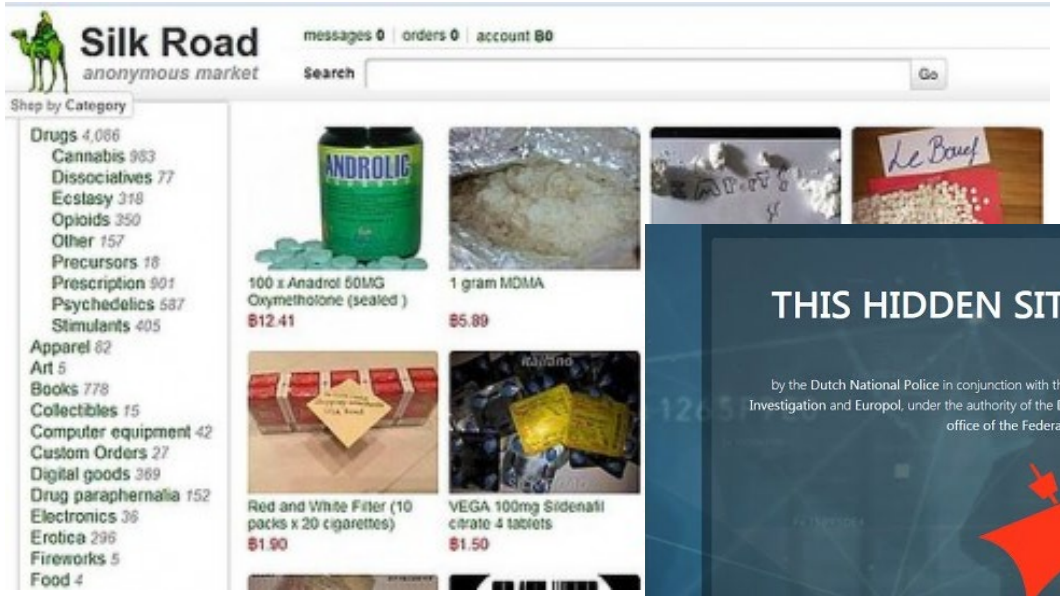


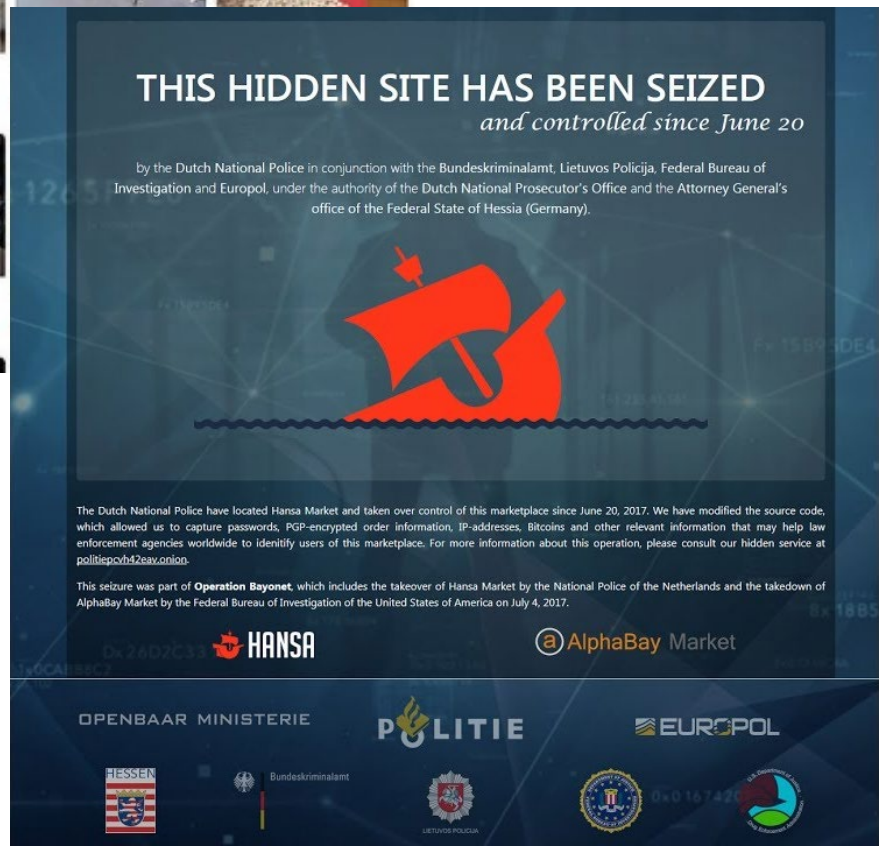
And many, many other stolen accounts of payment service providers for sale with BTC



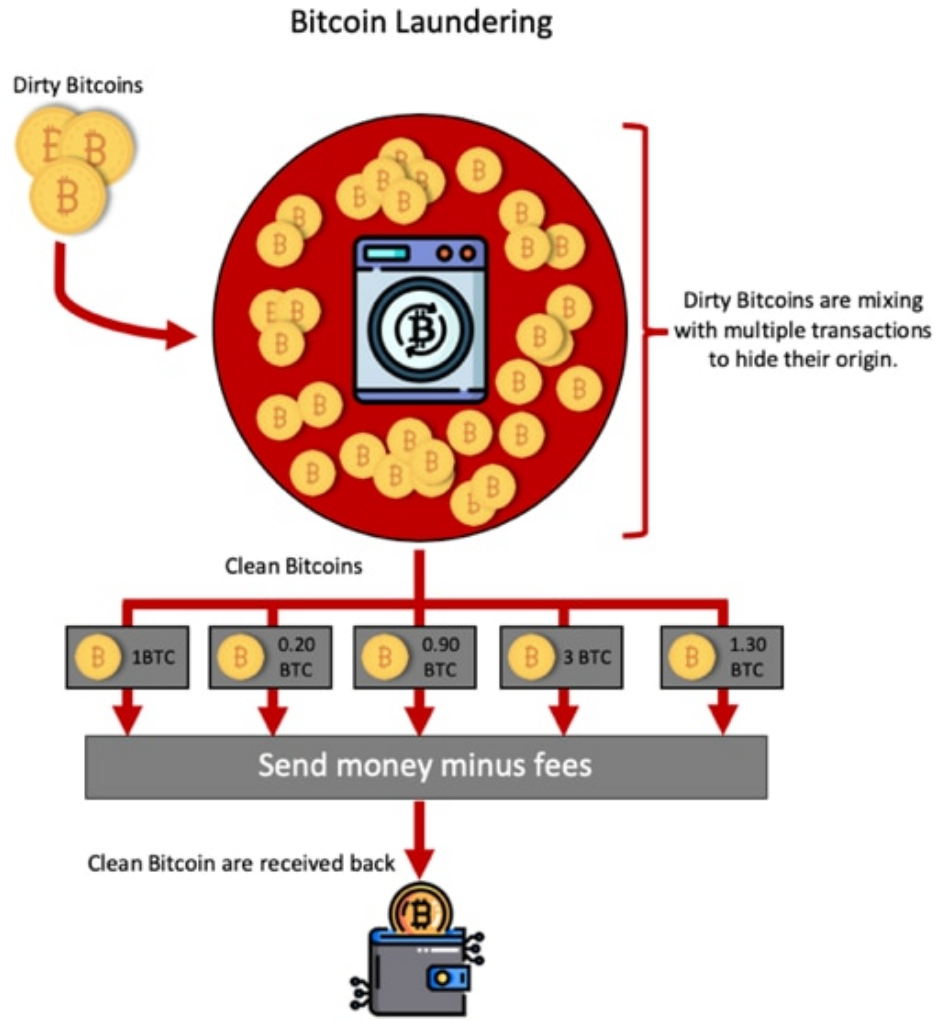
Private key shops

Trend 2. Cryptocurrency payments to facilitate illegal transactions





Currently ~100 Dark Markets operational (June 2020)



Trend 3. Suspicious transactions on specific cryptocurrency addresses (hubs)

Blockchain.com

Address	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX
Format	BASE58 (P2PKH)
Transactions	358,669
Total Received	$937,830,407,134.05
Total Sent	$937,804,728,461.97
Final Balance	$25,678,672.08

Bitcoin hub with large amount of bitcoin received, and context where this bitcoin address is found

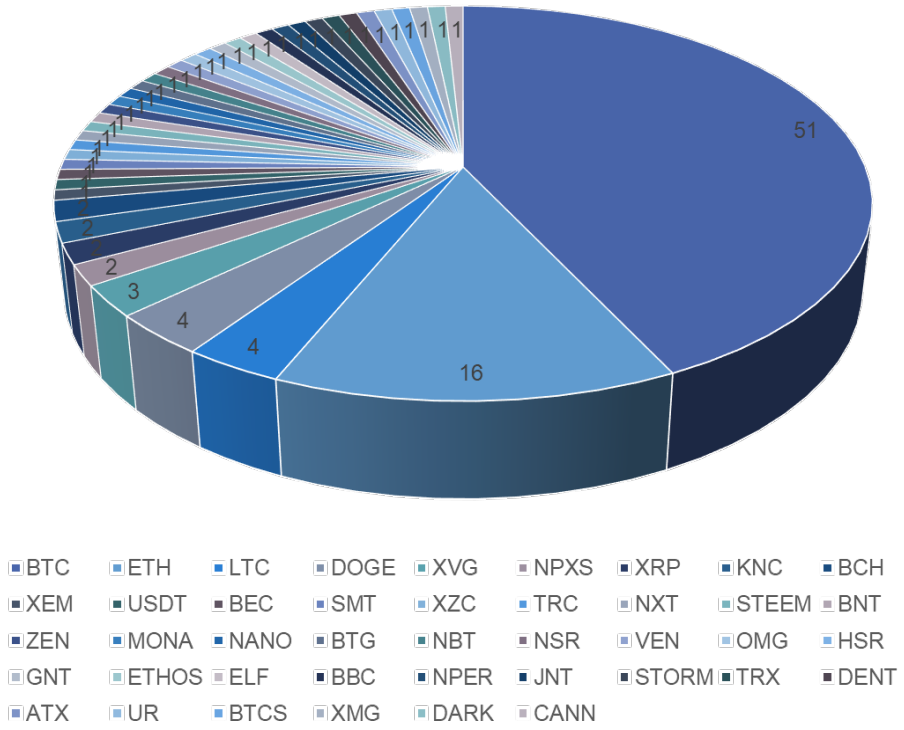
Cryptocurrency Address

Cryptocurrency	Bitcoin [BTC]
Address	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX [Inspect]
Discovered	31 Jan 2019, 00:07 UTC
Last Discovered	07 Apr 2020, 17:44 UTC
Domains	235
Appearances	438

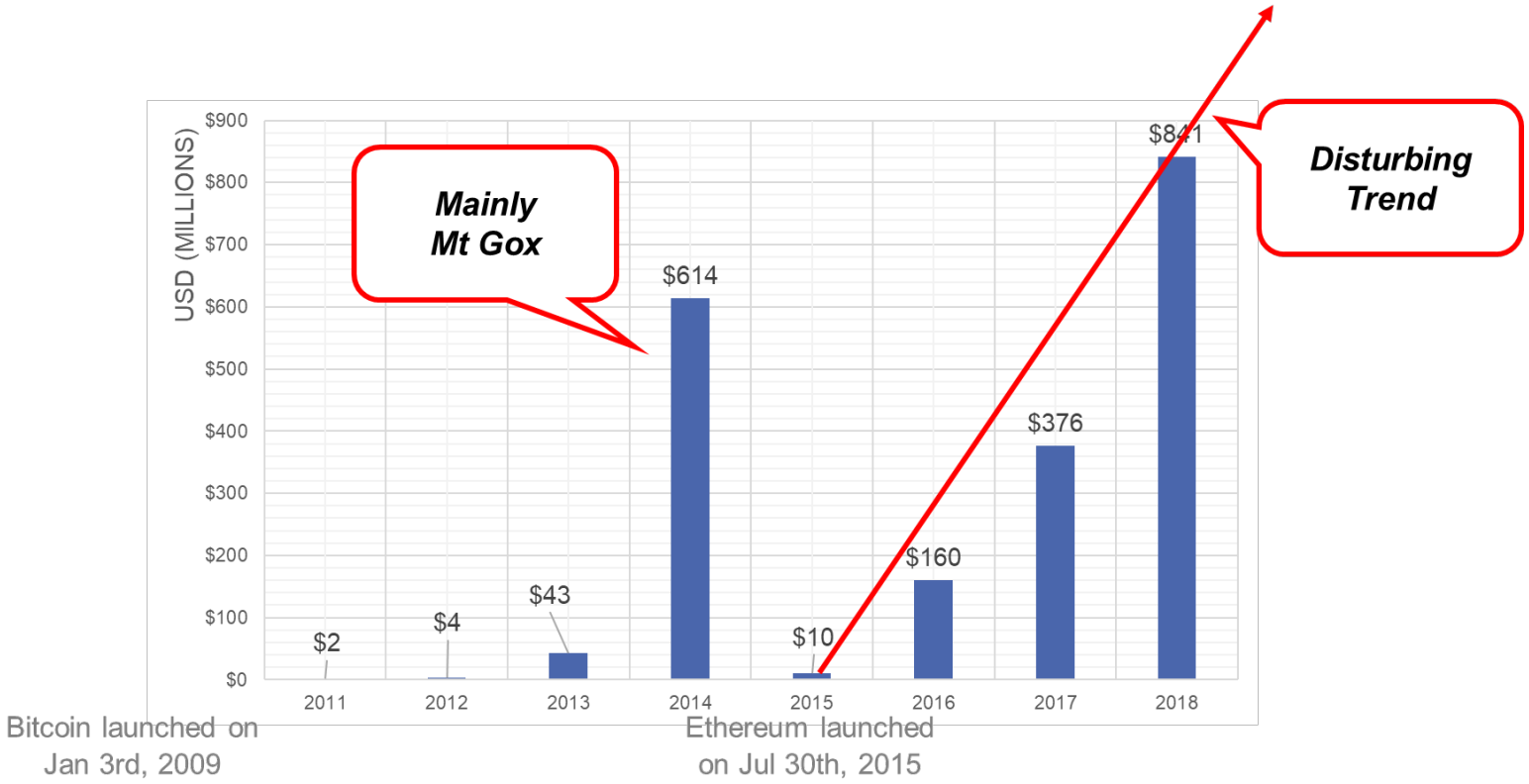
Domains (235) Pages (438)

Domain	Title
	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous
http://ep6ws7uqhavtpfdx.onion	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous
http://2222222ep67fw3hd.onion	100x Your Coins in 24 Hours - Officially Hidden Service Anonymous

Trend 4. Cyber-attacks on cryptocurrency exchanges and other VASPs



Range of cryptocurrencies affected during different cyber incidents.



Outcomes based on analysis of 110 Blockchain Incidents

Trend 5. Large-scale manipulation within blockchain ecosystems

A Deep Dive into Bitcoin Mining Pools
An Empirical Analysis of Mining Shares

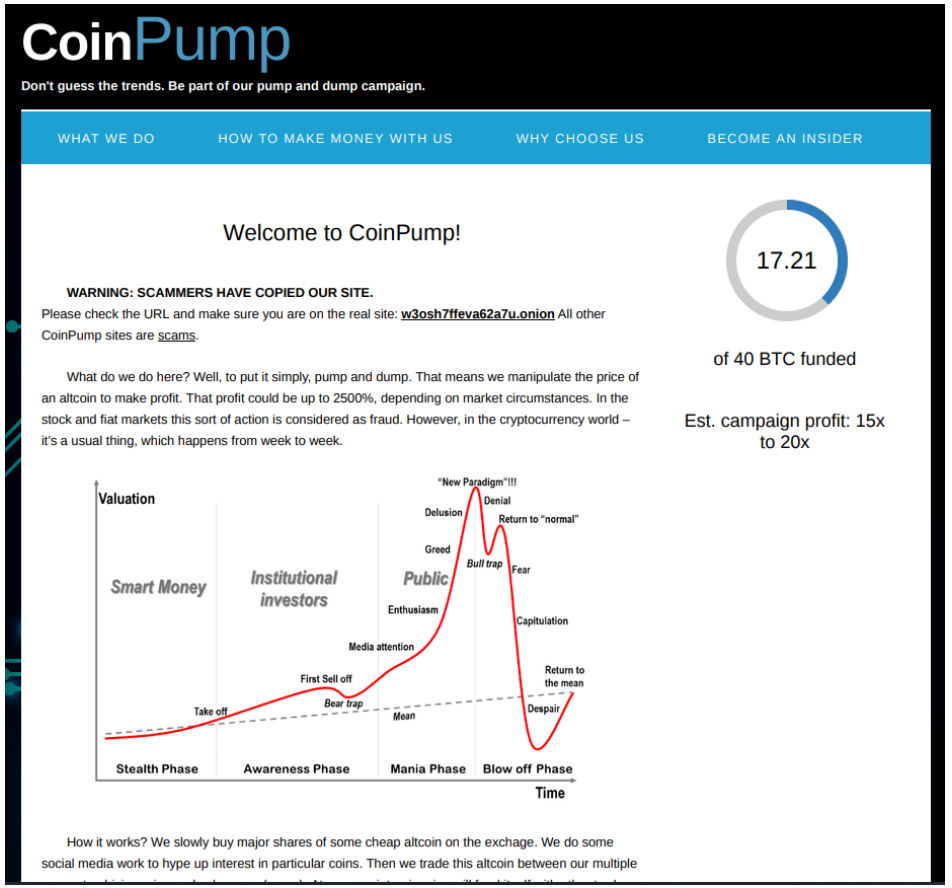
Matteo Romiti[1], Aljosha Judmayer[2], Alexei Zamyatin[2,3], and Bernhard Haslhofer[1]

[1] Austrian Institute of Technology {name.surname}@ait.ac.at
[2] SBA Research ajudmayer@sba-research.org
[3] Imperial College London a.zamyatin@imperial.ac.uk

Abstract. Miners play a key role in cryptocurrencies such as Bitcoin: they invest substantial computational resources in processing transactions and minting new currency units. It is well known that an attacker controlling more than half of the network's mining power could manipulate the state of the system at will. While the influence of large mining pools appears evenly split, the actual distribution of mining power within these pools and their economic relationships with other actors remain undisclosed. To this end, we conduct the first in-depth analysis of mining reward distribution *within* three of the four largest Bitcoin mining pools and examine their cross-pool economic relationships. Our results suggest that individual miners are simultaneously operating across all three pools and that in each analyzed pool a small number of actors (≤ 20) receives over 50% of all BTC payouts. While the extent of an operator's control over the resources of a mining pool remains an open debate, our findings are in line with previous research, pointing out centralization tendencies in large mining pools and cryptocurrencies in general.

https://arxiv.org/pdf/1905.05999.pdf

https://nairametrics.com/2020/07/01/there-are-now-1800-btc-whales/



Whales-as-a-Service

International Efforts …

- **The Financial Action Task Force (FATF) revised its Standards to require Virtual Asset Service Providers (VASPs) to be regulated for AML/CFT purposes.**

  - **October 2018:** Revised Recommendation 15 (New Technologies) and added new definitions of "virtual asset" and "virtual asset service provider" in order to clarify how AML/CFT requirements apply in the context of virtual assets.

  - **June 2019**: New Interpretive Note to Recommendation 15 (New Technologies) to set out the application of FATF Standards to virtual asset activities and service providers (including so-called "stablecoins").

- As of June 2020, **35 out of 54 reporting jurisdictions have implemented the revised FATF Standards**, with 32 of these regulating VASPs and 3 prohibiting the operation of VASPs. **The new review will be held in June 2021**.

International Efforts …

The FATF also updated its "*Guidance for a Risk-Based Approach to Virtual Assets and VASPs*" in June 2019 to help reporting jurisdictions understand and implement their AML/CFT obligations.

1. **Defined Virtual Asset Service Providers (VASPs)** - Includes virtual-to-virtual, and virtual-to-fiat transactions. - Recognises Decentralised Applications (DApp).
2. **Required national licensing or registration of VASPs** - Clear responsibilities on countries on VASPs AML/CFT compliance – Suspicious Transaction Reports (STRs) to be implemented in the context of VASPs and VA activities.
3. **Emphasized "Risk-Based Approach"** - VASP sector risk is determined at a national level - Not specifying for "wholesale termination or restriction…" with VASPs but to "…manage risks in line with FATF risk-based approach…"
4. **New "Travel Rule" –** requires VASPs to share and store sender (originator) and receiver (beneficiary) information of the participants prior to processing virtual asset transactions.
5. **Guidance to be further reviewed and updated -** to set out in more detail how AML/CFT controls apply to stablecoins, and address risks posed by anonymous P2P transactions via unhosted wallets.

Conclusion

- Blockchain, the technology underpinning cryptocurrencies, has **significantly revolutionized and transformed the digital economy**.
- The number of **key application areas will continue to increase** as blockchain evolves and becomes mainstream.
- **More work needed to tackle challenges** of cryptocurrency-related cyber crimes:
  - Cyber crimes targeted at cryptocurrency owners; and
  - Cyber crimes facilitated by the anonymity of cryptocurrency.

Thank You !


kwokyan.lam@ntu.edu.sg


https://twitter.com/lamkwok