Cryptocurrencies & Counterterrorism: Cooperative Solutions for Law Enforcement Agencies

Daniel G. Arce M.

Ashbel Smith Professor of Economics

AUSTRIAN INSTITUT OF TECHNOLOGY

universität innsbruck

SYMPOSIUM ON POST-BITCOIN CRYPTOCURRENCIES

Overview

Terrorism is the use (or threat of use) of violence against civilians and inactive military personnel for the purpose of influencing an audience beyond the immediate victims in order to achieve political, ideological, or religious goals.

Terrorism and the **criminal use of cryptocurrencies** are **borderless phenomena**. As such, both require **coordination** among law enforcement agencies.

How can successes in counterterror coordination can be adapted to address the use of cryptocurrencies for money laundering and terrorism financing?

Both Terrorists and Cryptocurrencies Cross International Borders

- Terrorists often travel on fraudulent passports.
- According to the **9/11** Commission, **two** of the **hijackers** entered the U.S. using fraudulent passports, and **six** other **cell members** used fraudulent passports.
- Prior to **Q4 2007** most countries had to have bilateral agreements to share data about stolen and lost travel documents (SLTDs).

Solution: Interpol's Database on Stolen and Lost Travel Documents (SLTDs)

- Known as **MIND/FIND**.
- Each country inputs their own data.
- Each country decides who can see this data.
- Linked to a nominal database identifying suspected criminals and terrorists.
- Global database alternative to the Schengen Information System (SIS) for EU countries.

INTERPOL's FIND-MIND Database

Number of fraudulent passport intercepts at entry points, **Visa Waver Countries**

Country of Issuance	US's Own Database Hits, January-June 2005[a]	INTERPOL SLTD Hits January-June 2008[b]
Austria	5	
Belgium	5	
France	67	
Italy	52	
Germany	6	
Ireland	3	
Japan	29	
Netherlands	9	
Norway	4	
Portugal	19	
Singapore	24	
Slovenia	14	
Spain	19	
Sweden	2	
Switzerland	2	
United Kingdom	38	
Total	**298**	**1,249**

All of this is some form of illegal activity.

[a] Source: General Accounting Office (2006)
[b] Source: INTERPOL data

Counterterror Benefits of MIND/FIND

[Even though it was not designed with terrorism specifically in mind]

- Benefit/cost ratio of about $200.

[U.S. DHS benefit/cost ratio no greater than 0.25 (Arce 2018).]

- Only 0.29% of the U.S. hits would need to be terrorism-related to justify the ENTIRE MIND/FIND budget.

- 30% reduction in transnational terror for participating countries.

Requirements

- Nations must cede some autonomy over security matters.
- Large countries (by population) with GDP per capita above US$ 3 945 threshold and democratic liberties are more likely to join MIND/FIND.
- Non-adopting outliers were mainly SIS countries in EU.
- Adopting outliers received external funding to do so. E.g. West Indies and Cricket World Cup.
- 174 countries currently contribute to the database.

ONYMOUS Operational Action Day
Nov. 2014

- Coordinated via Europol
- 17 countries involved in the collaborative effort.
- 27 darknet websites on Tor taken down. 17 arrests.
- Sites sold illegal drugs, fake/stolen credit cards, counterfeit currency, fake IDs, including passports.
- US$ 1 million in Bitcoin seized.

Financial Activities Task Force (FATF)
Special Recommendations on Counter Terrorism Financing (CTF)

Each country should …

i. Ratify 1999 UN Convention for the Suppression of the Financing of Terrorism.

ii. Criminalize the financing of terrorist acts & organizations.

iii. Implement measures to freeze assets and confiscate property that is the proceeds of or used in terrorism financing.

iv. Require that all financial entities subject to AML obligations be required to report promptly suspicions transactions.

v. Afford other countries the greatest possible measure of assistance in terrorist financing investigations and not provide safe haves.

vi. Require all legal entities engaged in the transmission of money or value be subject to all FATF regulations.

vii. Require accurate and meaningful originator information on funds transfers and messages.

viii. Ensure that non-profit agencies are not abused for terrorism financing.

ix. Have measures in place to detect physical cross-border transportation of currency and bearer negotiable instruments.

Financial Activities Task Force (FATF)
[37 full members (EC included), nine regional groupings]

Main tool: peer reviews of the implementation of FATF standards in the financial sector.

- In order to recognize progress, each category in the FATF review receives a grade of:

⊗ Non-Compliant (NC)

↔ Partly Compliant (PC)

↔ Largely Compliant (LC)

✓ Largely Compliant (FC)

- Work in progress: in 2011, the IMF found that among 46 advanced economics, the implementation rate was 50%, whereas it was 24% for 115 emerging and developing countries.

- Banks appear to prefer accept the cost of CTF measures in order to avoid the loss of reputation (aka ‘risk management’).

- Still, it is a **weakest link environment** for terrorists.

Advantages of Cryptocurrencies for Criminal Behavior

- Can be received as payment for illegal goods and services.
- Can be used as payment for goods and services, both legal and illegal, without having to be exchanged for fiat currencies. One less step in the money laundering process.
- Easy to create multiple accounts to hide true value of total holdings and avoid triggering reporting requirements.
- (Pseudo) anonymous.
- Private key implies that there is no financial intermediary (e.g. bank) that can grant access to authorities.
- Hard to freeze an account or confiscate crypto assets.
- No borders to consider when transferring funds. Completely portable.

Advantages …

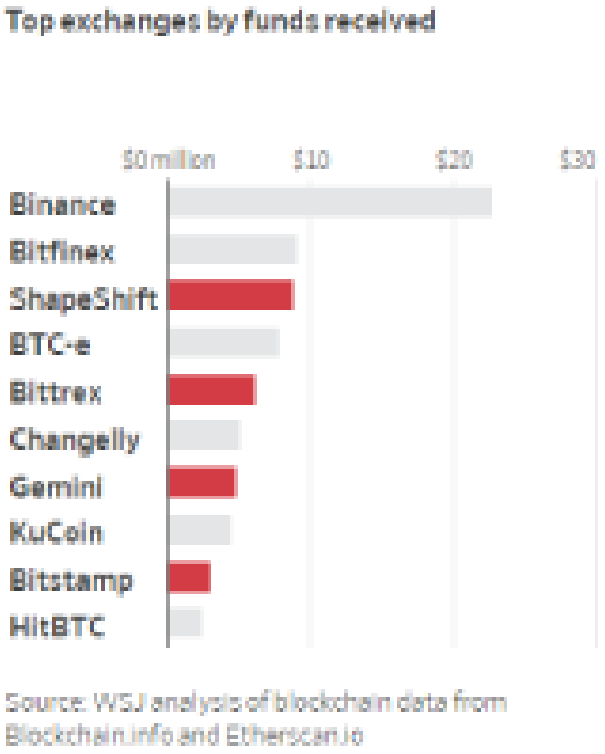
- Transactions are nearly instantaneous.
- Transactions are difficult to interdict or disrupt because the blockchain ledger is decentralized.
- Impossible for law enforcement or regulators to reverse a transaction once it is on the blockchain.
- Miners process cryptocurrency transactions but have very little input on the specific transactions that they process.
- Mining itself as a method of money laundering?
- Enables money launderers to move illicit funds faster, cheaper, and more discretely than ever before.

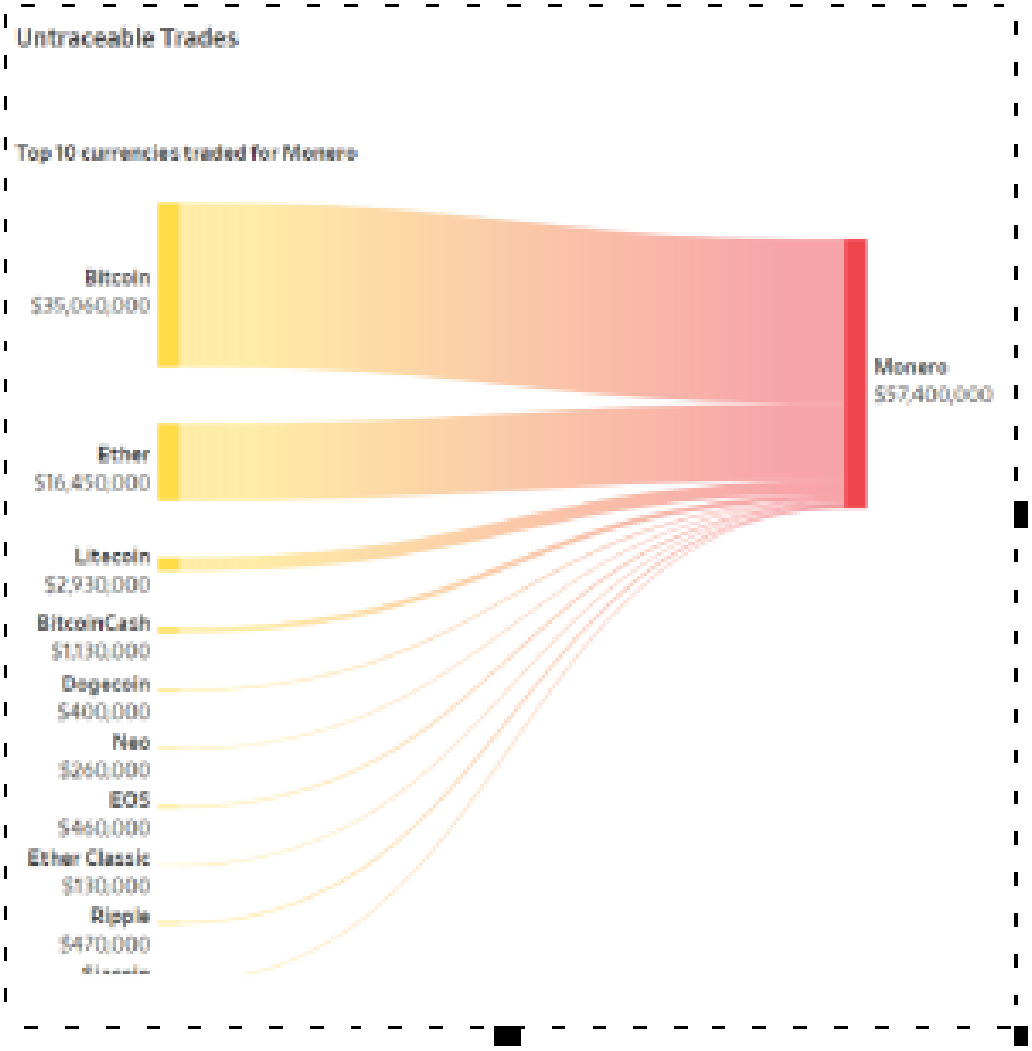
Disadvantages of Cryptocurrencies for Criminal Behavior

- Limited acceptance as compared to fiat currencies.
- Fewer points of contact for turning cryptocurrencies into fiat money (dependency on exchanges).
- Blockchain records every transaction that has ever occurred. Blockchains could be used to create AML-compliant registries.
- Price volatility.
- Exchanges may be susceptible to ‘bank’ runs and other forms of failure.
- Risk of holding cryptocurrency versus cash?

- Monitoring Trends in Virtual Currency and Darknet Market Ecosystems.
- Analyzing Transactions Across Different Virtual Currency Ledgers.
- Generating Court-Proof Evidence Reports Based on Reproducible and Legally Compliant Analytical Procedures.

WSJ Sept 2018 Traffic Analysis of US$ 90m in Criminal Proceeds [Suspected Frauds, Hacks, Blackmailing, and Other Alleged Crimes]





In summary these are:

- TECHNICAL solutions.
- Involving NETWORKS.
- “Need to share” instead of “need to know.”
- Have yet to leverage decentralization, incentives, code and consensus in the way that blockchain-based cryptocurrencies have.

¿Questions/Comments/Suggestions?

darce@utdallas.edu