“Coins for Bombs”

Increased Transparency of the Global Financial System: Evidence from Terrorist Attacks Financing Detection in Blockchain-based Currencies

Dan Amiram

Tel Aviv University

Bjørn N. Jørgensen

Copenhagen Business School

Daniel Rabetti

Tel Aviv University

Motivation

- Rise of Bitcoin as an alternative cash transfer mechanism, **BUT**:
  - Wide usage in dark markets
    - Silk Road, FBI cease, Foley et al (2019);
  - Money laundering, inflated volumes (BitWise report), manipulate Tether (Griffin and Shams 2019)...
  - Increasing evidence of terrorist crypto-financing (DOJ intervention), chainalysis crypto crime report;
    - Small amounts: donation campaigns.
- This paper:
  - *Assumption: untracked wallets.*
  - *Goal: given blockchain transparency, is it possible for **outsiders** to identify evidence of financing on-the-ground terrorist attacks?*

U.S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups
The New York Times

Terrorists Turn to Bitcoin for Funding, and They're Learning Fast
The New York Times

Source: Middle East Media Research Institute

Increasing relevance of blockchain on accounting research

*"**Blockchain is an accounting technology. It is concerned with the transfer of ownership of assets, and maintaining a ledger of accurate financial information**. The accounting profession is broadly concerned with the measurement and communication of financial information, and the analysis of said information. Much of the profession is concerned with ascertaining or measuring rights and obligations over property, or planning how to best allocate financial resources. **For accountants, using blockchain provides clarity over ownership of assets.**"*

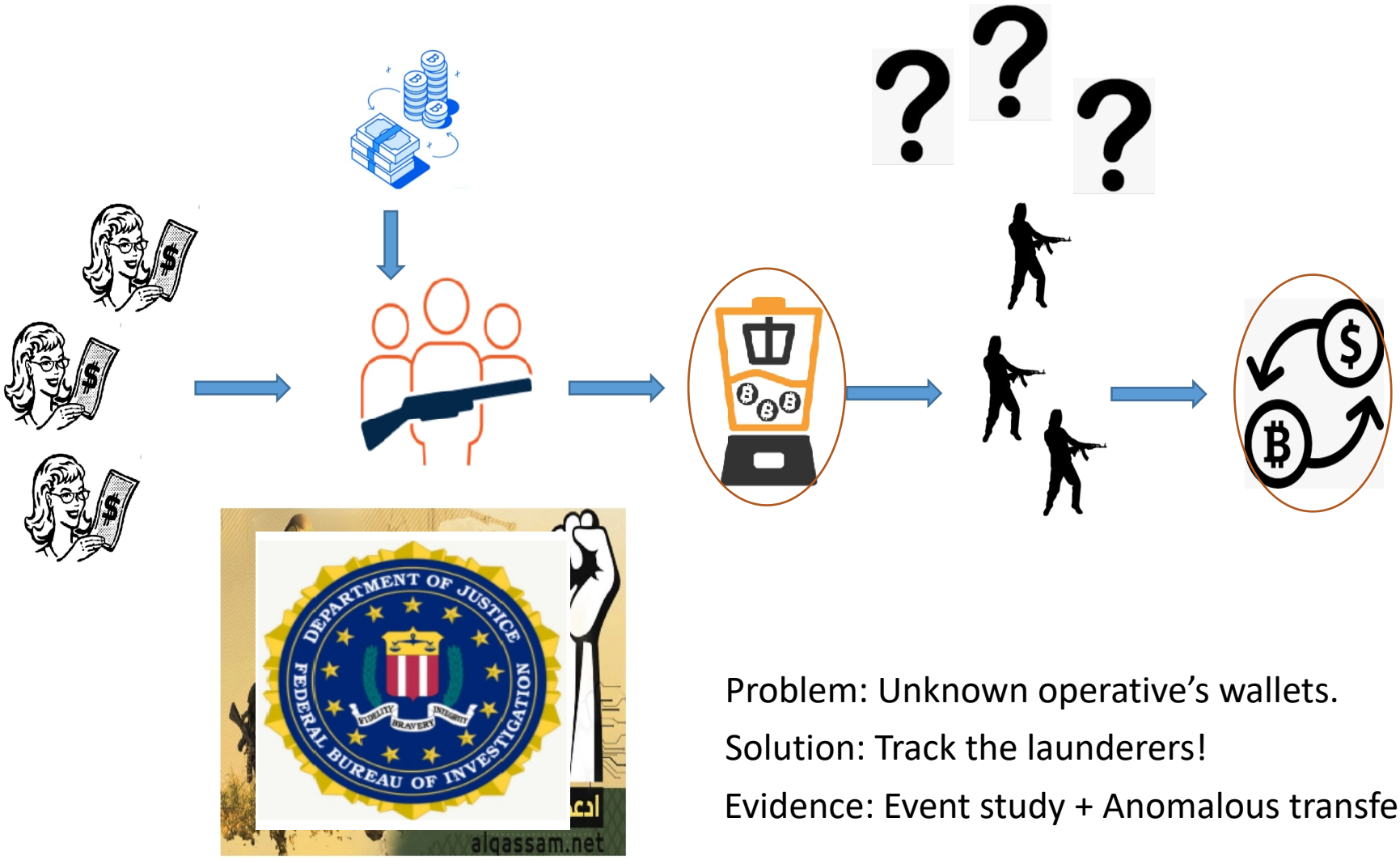
Institute of Chartered Accountants in England and Wales (2018)

Increasing relevance of cryptocurrency research

*"Resolution to **commend Bitcoin for its success in becoming the first decentralized trillion dollar asset** and to **encourage** the state and local governments to consider ways that could help them **benefit from the increased use of this new technology**."*

The Louisiana House of Representatives resolution (HR 33)
by Representative Mark Wright (2021)

Problem, Solution (exploiting transparency)



Problem: Unknown operative's wallets.

Solution: Track the launderers!

Evidence: Event study + Anomalous transfers

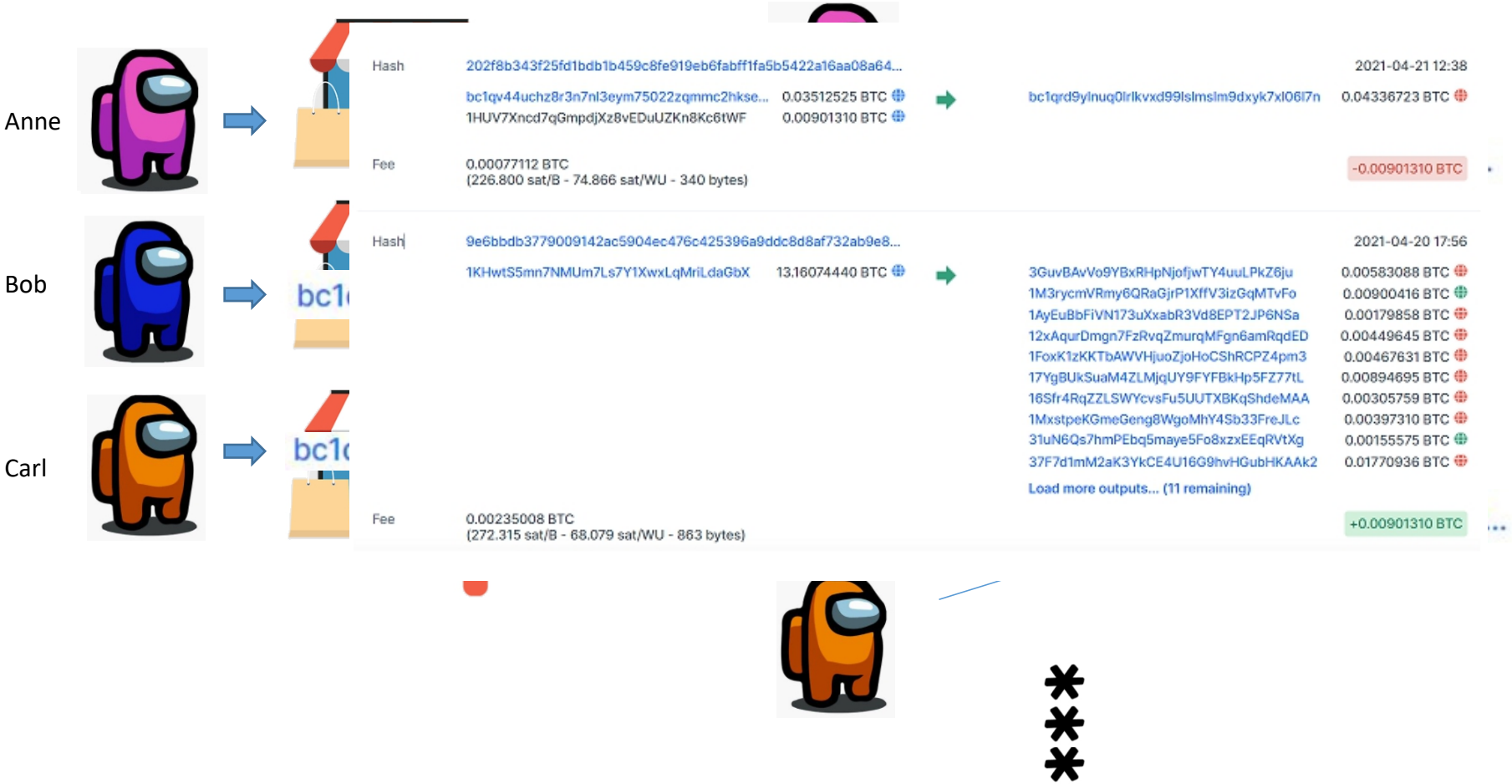
Economic implications

- Our results suggest that:
  - Transparency alone, without specific supporting regulation, is not enough to curb illegal activities - at least in the **short term**;
  - If so, policy considerations:
    - ***What*** *to regulate?* ***How*** *to regulate?*
- However:
  - Transparency of the public blockchain system opens the possibility for greater scrutiny of these activities *by* the public - scare off illicit players in the **long term**;
- Therefore:
  - Financing terrorist activities with blockchain-based currencies is essencialy a disclosure choice.

Strategy

- Terrorist financing:
  - short-term (**financing attacks**);
  - long-term (donations, payments, storage).
- Study Bitcoin transactions in the vicinity of terrorist attacks:
  - no need to know terrorist wallets in advance; 
  - need to know a vast array of **users**. 
    - Focus on **large users** such as exchanges, dark markets, mixers, miners, gambling platforms, and other services.
    - Reveal user's **identity**:
      - wallet explorers;
      - specialized social media communities;
      - dark web user's lists.
    - Addresses **mapping**:
      - union spending algorithm (Ron and Shamir (2013), Kappos et al (2018), Tasca, et al. (2018), and Foley et al. (2019));

Exploiting Transparency: Mapping Bitcoin transfers



Data

- Focus on **large users** such as exchanges, dark markets, mixers, miners, gambling platforms, and other services for 2014 to 2019.
- The users in *Exchange* and *Service* have the largest number of transactions (~78% of the total transactions in the period).

Panel A - Blockchain

	Users	Transactions	Address	Volume	Average	Median	Balance	Life
Obtained:	339	136.50	99.79	222.24	21.90	0.010	1,429.57	1287
			(in millions)					
Excluded:								
- mining	1	613.11	668.71	3.32	78.07	15.205	0.06	2220
- cold storages	-	134.86	169.58	1.12	658.03	1.742	83.86	979
- lower interaction	-	0.01	0.01	0.01	182.03	45.106	0.00	125
			(in thousands)					
Used:								
Dark Markets	96	11.26	7.27	31.21	23.69	0.010	10.30	1583
Exchange	97	62.12	51.99	155.31	7.85	0.016	4,884.85	1496
Gambling	49	18.53	6.64	7.78	0.78	0.002	2.83	1345
Mixer	35	0.34	0.28	0.37	6.13	0.010	1.55	81
Service	55	43.50	32.48	23.12	2.00	0.010	165.61	1287
Total	338	135.75	98.95	217.80	10.24	0.010	1,458.19	1290
			(in millions)					

Summary

- First part (Main Analysis):
  - Event study
    - Patterns associated with large-scale events (CAV responses);
    - Exchange and Exchange-like services;
    - Crowd out effects on other services;
    - ISIS and al-Qaeda terrorist attacks overseas;
- Second part (Complementary Analysis):
  - Forensic and Network Analysis
    - Siri Lankan Eastern Bombing;
    - Association with other reported crimes and convertion to Ripple;
    - Chain of money-laundering wallets;
- Third part (Additional Analysis):
  - Predicting
    - Machine learning algorithms.

Event study rationale

- The costs of carrying attacks depend on scale, logistics, weapons used, and location;

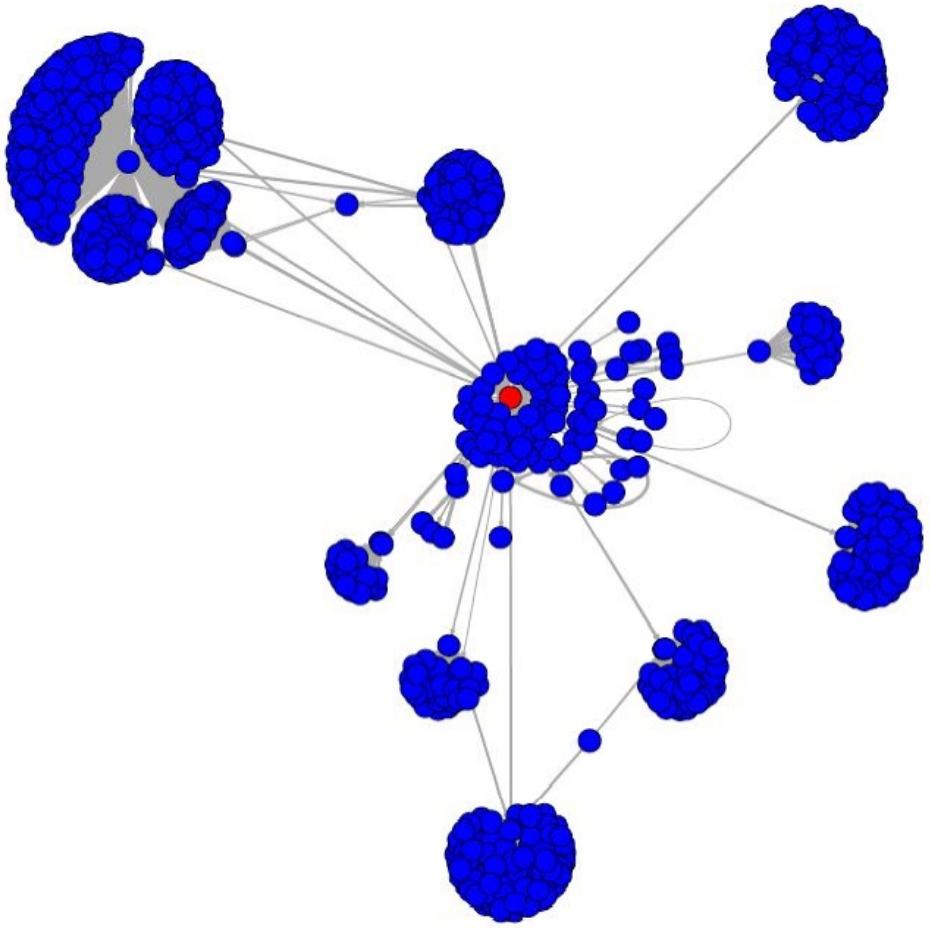
Location	Date	Killed	Method	Estimated Cost
New York (World Trade Center)	1993	6	bombing	$18,000
Yemen (USS Cole)	2000	17	bombing	$10,000
New York (World Trade Center)	2001	3,000	Airplane hijack	$500,000
Hormuz (US Ships)	2002		Foiled	$130,000
Bali	2002	180	Suicide and car bombing	$74,000
Paris	2015	130	Shooting	$10,000
Kenya and Tanzania (US Embassy)	2018	200	Car bombing	$10,000

- If **money laundering techniques** are in place to camouflage these transfers, we should observe an abnormally large Bitcoin volume in the event's vicinity.

Reshuffling funds on Bitcoin blockchain

- Blue dots near the center of gravity represents direct donations to al Qassam wallet;
- The blue dots further away from the center of gravity (cloud), represents addresses involved in reshuffling Bitcoin funds;
- Al Qassam address received 51 final transfers with a total of $4,247.26.
- Total of 920 Nodes (addresses) and 1,939 Edges (transfers) = 38x reshuffling factor.

al Qassam donation campaign network analysis



Event Study: Methodology

- Cumulative Abnormal Volume (CAV)
  - Bitcoin volume is the daily sum of total inbound and outbound transfers at the user level;

$$AV_{u,t} = \ln V_{u,t} - \ln \hat{V}_{u,t}$$

  - Where abnormal mean-adjusted volume *AV* is calculated at the user *u* and time *t*. The average abnormal mean-adjusted volume *AAV* on a given day *t* is calculated by summing the abnormal volume for each user in the group and dividing by the number of users in the group *N*. The cumulative abnormal mean-adjusted volume *CAV* is also constructed by the sum of *AAV* in the specified event windows *T*.

$$AAV_{u,t} = 1/N \sum_{t=1}^{N} AV_{u,t}$$

$$CAV_{u,t} = \sum_{t=1}^{T} AAV_{u,t}; \quad t = 1, \ldots, n.$$

  - References (Beaver (1968), Copeland (1979), Bamber (1987)).

Event Study: Methodology

- Cumulative Abnormal Volume (CAV) windows:
  - Event window is (t - 15,t + 15);
  - Estimated normal window is (t - 35, t - 16) or 20 days;
  - **Choice:** (a) short term, (b) clustering;
- Portfolio of users
  - Mitigates concerns with heterogeneous responses due to different business characteristics;
- Vector of terrorist attacks
  - Global Terrorist Database (e.g., Cuculiza et al. (2020));
  - For each event, we collect information on the number of dead and injured, location, and perpetrator;
  - Filters: large-scale attacks occurred overseas with some level of logistics in place (e.g., multiple bombs, mass shooting).

CAV Responses - Interpretation

- How to differentiate market reactions from terrorist financing?
  - Cumulative Abnormal Volume (CAV)
- Before the event:
  - CAV ↓ (crowd out)
  - **CAV ↑ (terrorist financing - consistent with unexpected money laundering)**
- Given before CAV ↑, after the event:
    - CAV ↑ (market reaction - compensation?);
    - **CAV ↓ (terrorist financing - normalization of volume levels);**
    - CAV ↓ (market reations - negative news);
    - CAV ↓ (unrelated illicit activities - under the radar);

Event Study I - All Users

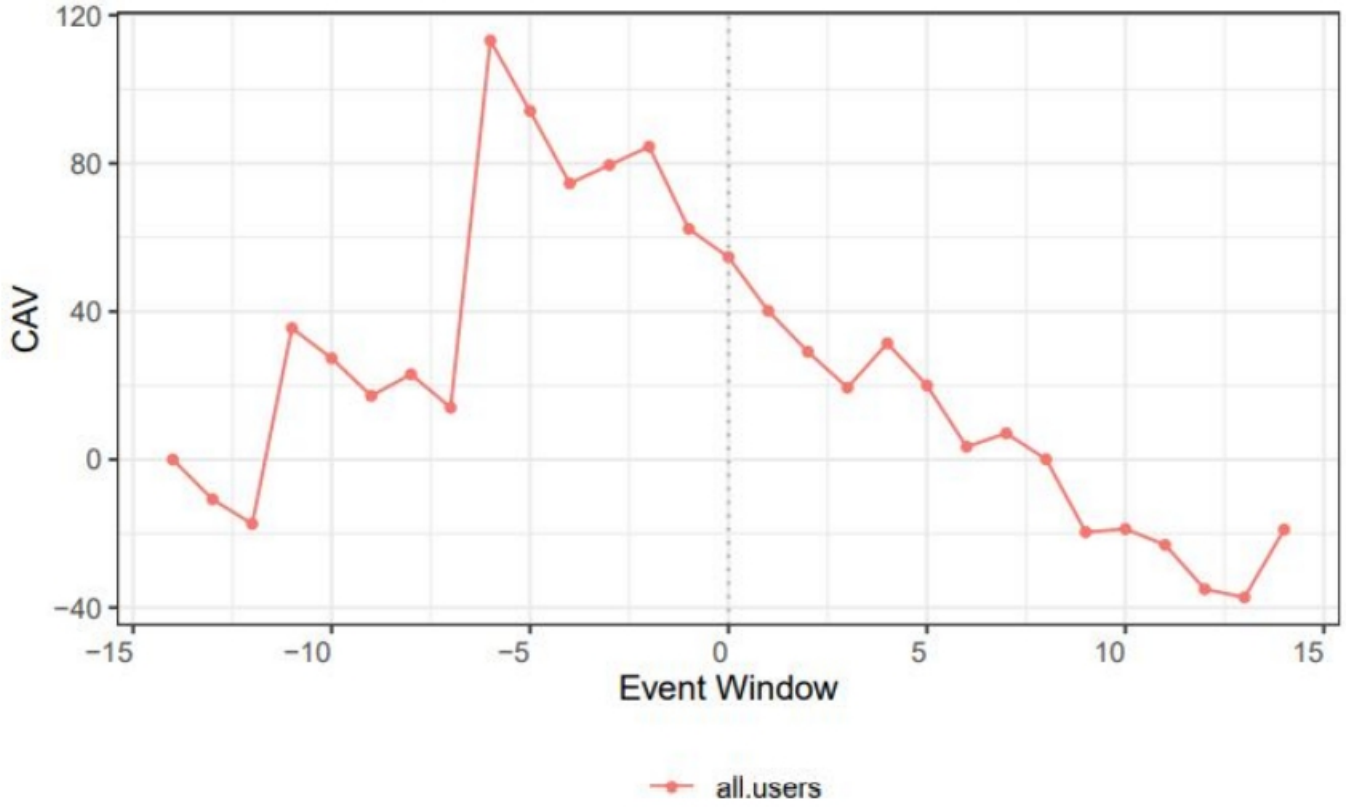
Panel A - CAV Responses (Before and After) Means

Period	All users
Days before:	46.56
	(4.52)
Days after:	-42.03
	(-6.96)
Vicinity (Whole period):	22.42
	(3.27)

*Estimated upper-bound cost = (2900 BTC / 100) x $3,600 = $105,000

- (H1): evidence of abnormal volume before the event takes place:
  - consistent with money laundering mechanism;

Event Study I - All Users



Event Study I - Robustness

Panel A (Robustness test for the event window)

	I	II	III
Event window:	15 days	30 days	45 days
Days before:	46.56	46.68	82.25
	(4.52)	(4.29)	(2.86)
Days after:	-42.03	-36.77	-3.78
	(-6.96)	(-5.80)	(-0.40)

Panel B (Robustness test for the estimated normal window)

	I	II	III
Estimated normal window:	20 days	90 days	180 days
Days before:	46.56	42.80	63.34
	(4.52)	(3.80)	(4.50)
Days after:	-42.03	-26.35	-12.75
	(-6.96)	(-5.24)	(-2.99)

Issue: induced volatility in larger windows

Event Study II - Size effects

CAV Responses by Size

Period	Boot-Mid	Boot-Low	Mid-Low	High-Mid
Days before:	2.36	0.27	2.09	44.20
	(2.22)	(3.10)	(2.00)	(4.42)
Days after:	-2.47	-0.05	-2.42	-39.56
	(-1.69)	(-1.65)	(-1.64)	(-6.68)
Vicinity (whole period):	6.29	0.52	5.77	16.12
	(5.44)	(3.34)	(4.87)	(3.21)

quantiles by destruction

10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0.0	1.0	2.0	2.0	3.0	5.0	7.0	11.4	24.2	822.0

- (H2): Bitcoin financing is increasing in destruction:
  - level destruction measured as the sum of dead and injured;

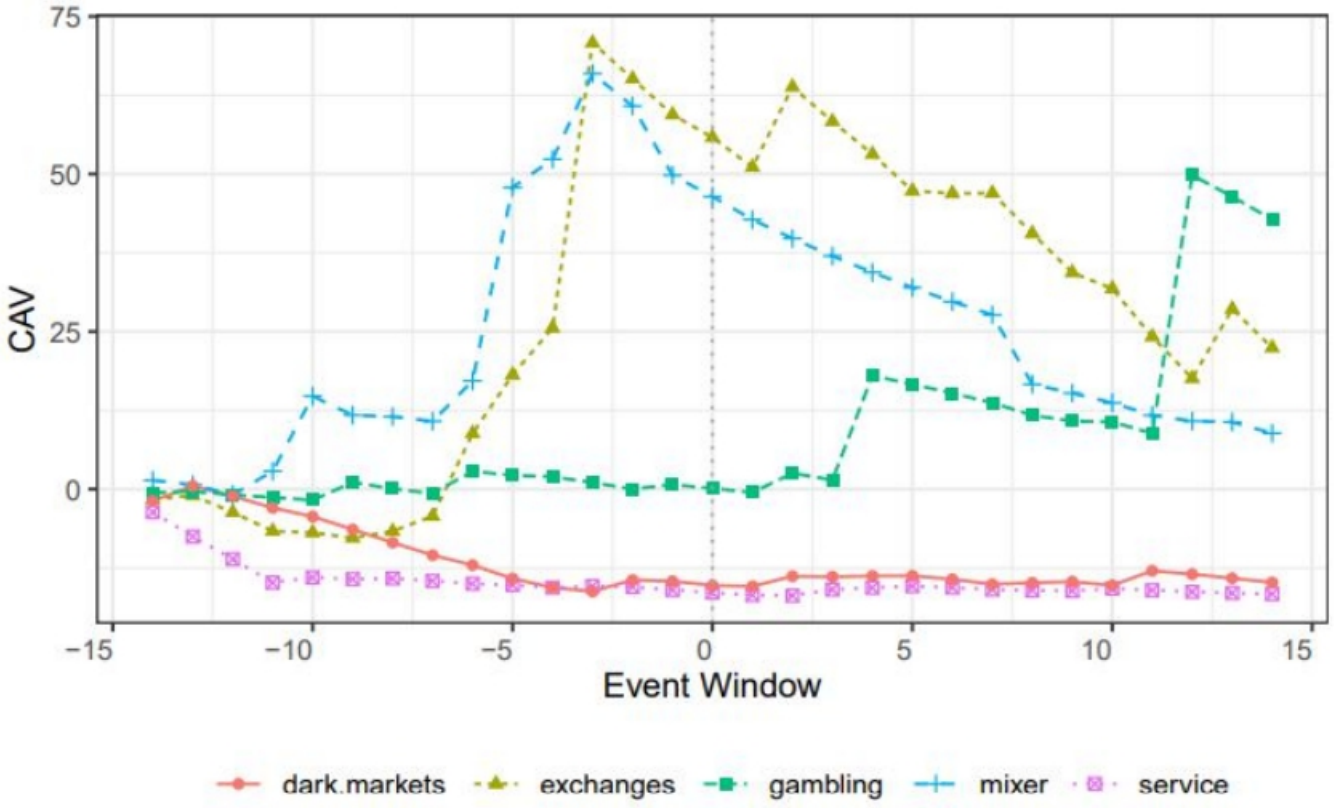
Event Study III - Business Type

Panel A - CAV Responses (Before and After) Means

Period	Exchange	Mixer	Gambling	Service	Dark markets
15 days before:	14.96	24.77	0.32	-13.34	-8.72
	(3.52)	(6.69)	(1.58)	(-18.17)	(-9.37)
15 days after:	-15.30	-22.78	17.60	0.33	0.97
	(-7.11)	(-11.45)	(7.06)	(4.84)	(8.61)
the whole period:	28.70	24.97	8.71	-14.78	-11.64
	(7.33)	(8.63)	(4.03)	(-34.57)	(-15.44)

- (H3): evidence in exchange or exchange-like services:
  - most transfers pass through (~75% of transactions);
  - services for payments and withdrawn;
- (H4): crowd out effects on other services wallets:
  - large demand from terrorist funds leads to slower services to other laundering services, likely *Dark Markets* wallets;

Event Study III and IV - Business Type



Event Study V - Terrorist Groups

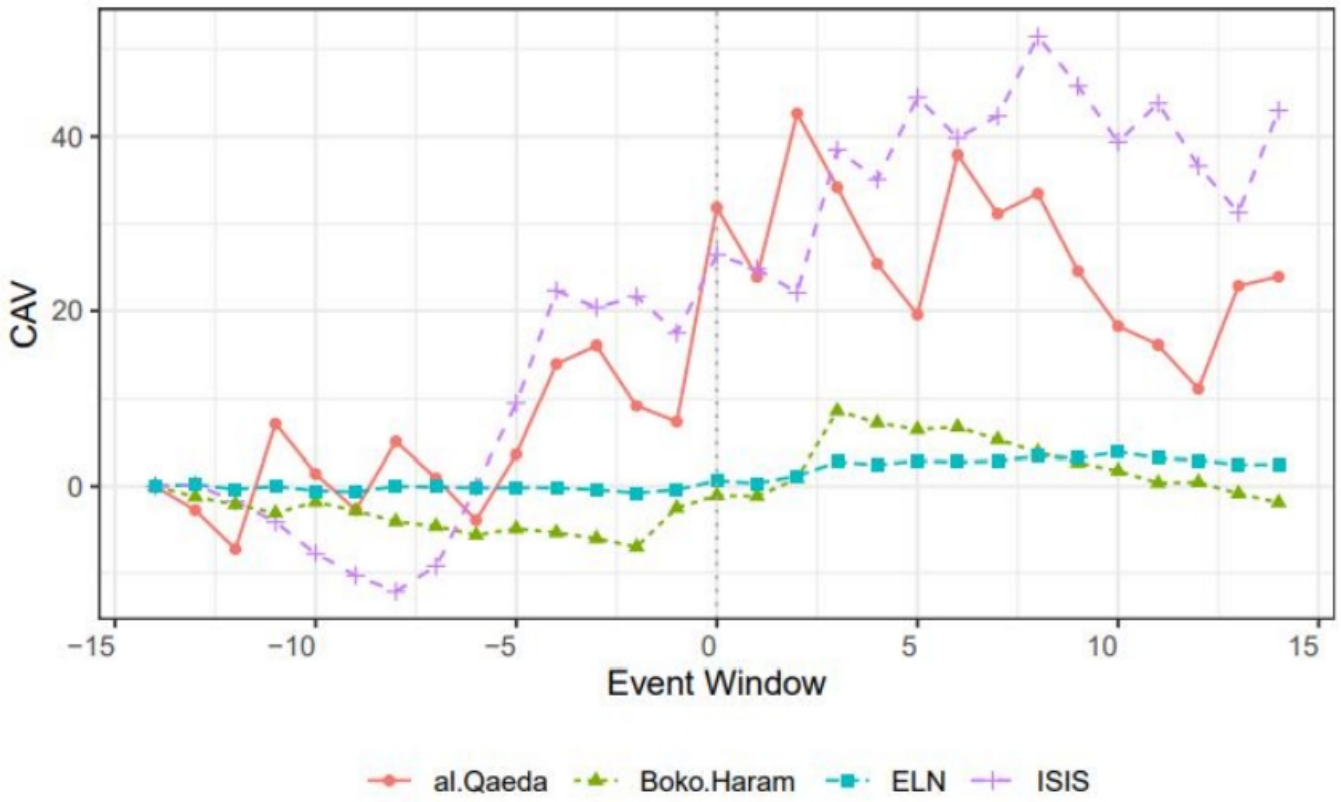
Panel A - CAV Responses (Before and After) Means

Period	al Qaeda	Boko Haram [1]	ELN [1]	Islamic State
15 days before:	5.72	~~-3.68~~	~~-0.20~~	5.19
	(3.86)	(-11.91)	(-3.85)	(2.55)
15 days after:	0.48	4.08	2.26	11.86
	(0.30)	(7.96)	(13.67)	(6.24)
the whole period:	15.35	-0.38	1.17	21.07
	(7.28)	(-0.60)	(4.93)	(6.88)

[1] placebo

- (H5): evidence in terrorist groups with experience in terrorist attacks overseas:
  - history of carrying out terrorist attacks overseas;
  - presence in the crypto space (donation campaigns);

Event Study V - Terrorist Groups



Conclusions and Limitations

- Evidence of Bitcoin **cumulative abnormal volume** **concentrated** in time in the vicinity of large terrorist attacks.
- **Patterns** consistent with Bitcoin flows **likely** financing terrorist attacks:
  - CAV tends to **increase** in the week **before** the event
  - CAV tends to **decrease** in the week **after** the event.
- As predicted, **exchange** and **exchange-like** wallets drive most of the effect, and;
- **Crowd out** effects on other business often related to mixer activities;
- **al Qaeda** and **Islamic State** terrorist attacks **overseas**;
- Although results are potentially informative, event studies, in general, should be exploited to **raise awareness** rather than taken at face value.

II - Complementary Analysis
Anomalous Transfers

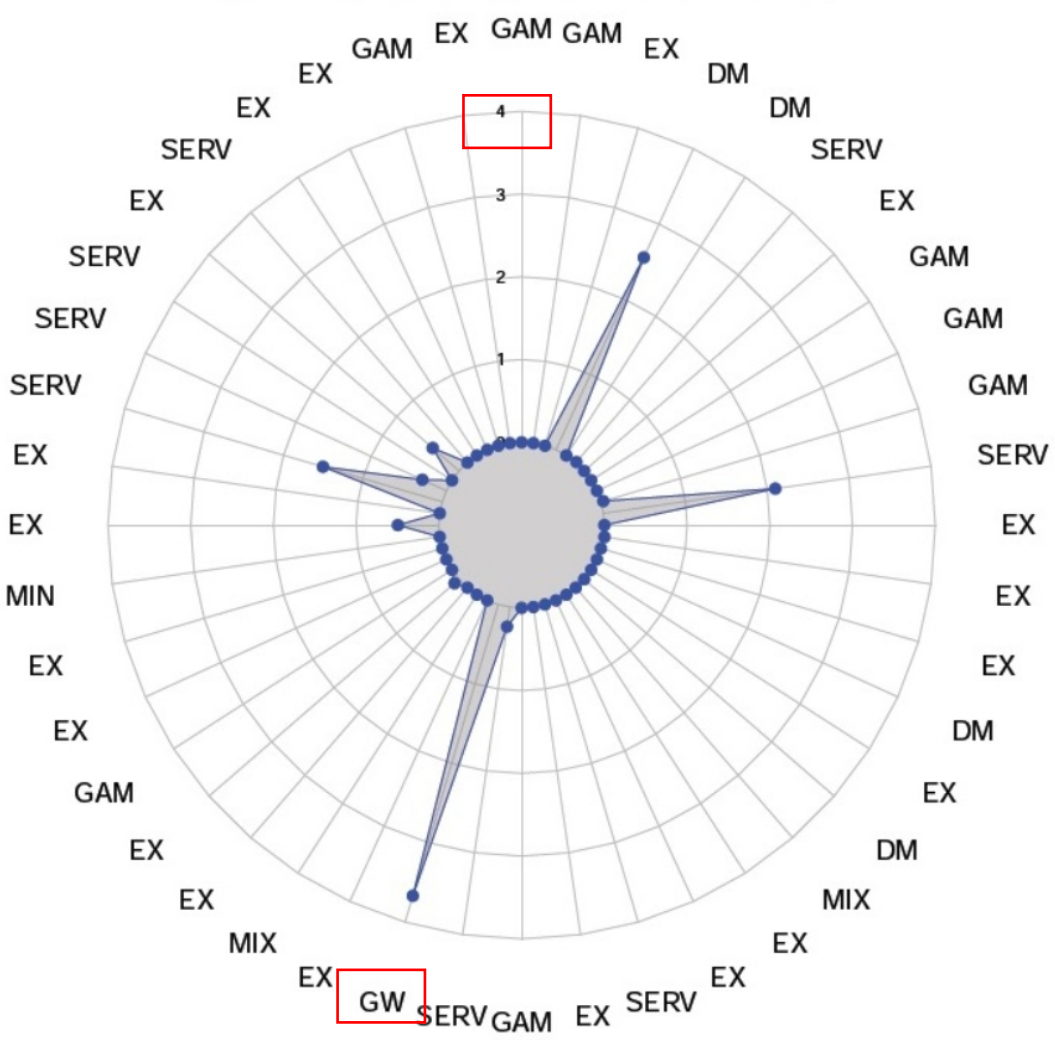
- Additional evidence;
- Focus on Sri Lanka Easter bombing;
- Anomalous detecting technique based on a **rolling three-sigma rule**;

Anomalous transfers (3-sigma rule)

Groups	users	$>3\sigma$	#	$\frac{\#}{user}$	mean	max
Dark markets	3.00	0.02	11.00	3.67	57.86	255.48
Exchange	24.00	0.02	65.00	2.70	2,163.24	54,320.28
Gambling	8.00	0.02	22.00	2.75	18.15	194.00
Mixer	3.00	0.01	7.00	2.33	7,581.20	26,122.56
Service	9.00	0.02	28.00	3.11	188.84	1,382.84
Total	48.00	0.02	135.00	2.81	1,481.50	54,320.28

Anomalous transfers (3-sigma rule)

DM = Dark Market
EX = Exchange
GW = Gateway
GAM = Gambling
MIN = Miner
MIX = Mixer
SERV = Service

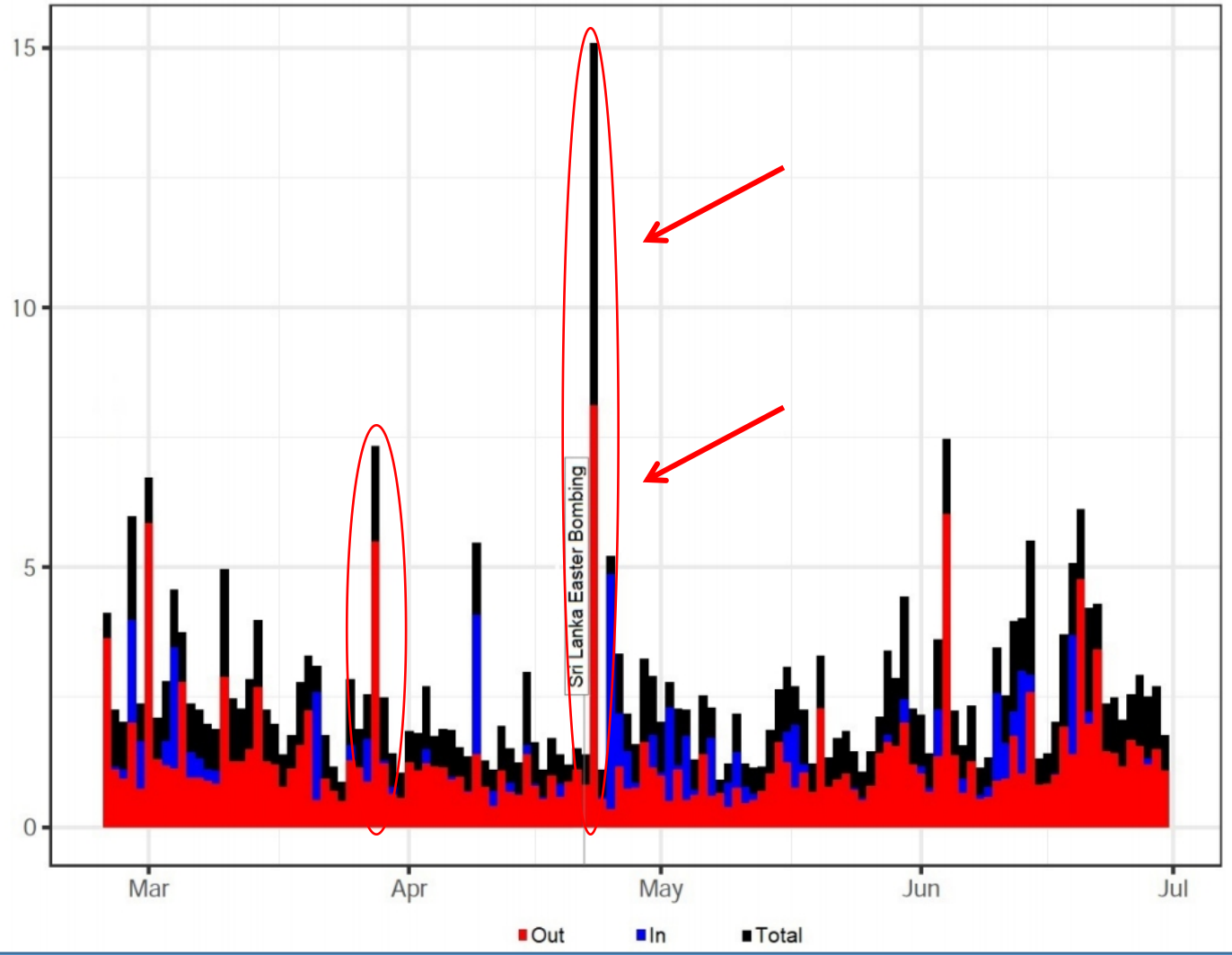


II - Complementary Analysis
Anomalous Transfers

- Additional evidence;
- Focus on Sri Lanka Easter bombing;
- Anomalous detecting technique based on a **rolling three-sigma rule**;

- One (1!) suspicious user with abnormally large (above one or two standard deviations) transfers in the vicinity of the event;
  - **backward**: association with other crimes such as ransomware and funding anti-government cells in Syria;
  - **forward**: large transfer to Exchange
    - check user wallet in other blockchains for abnormal inbound transfers;

Tracking the funds on Ripple Blockchain



Ripple wallet activity

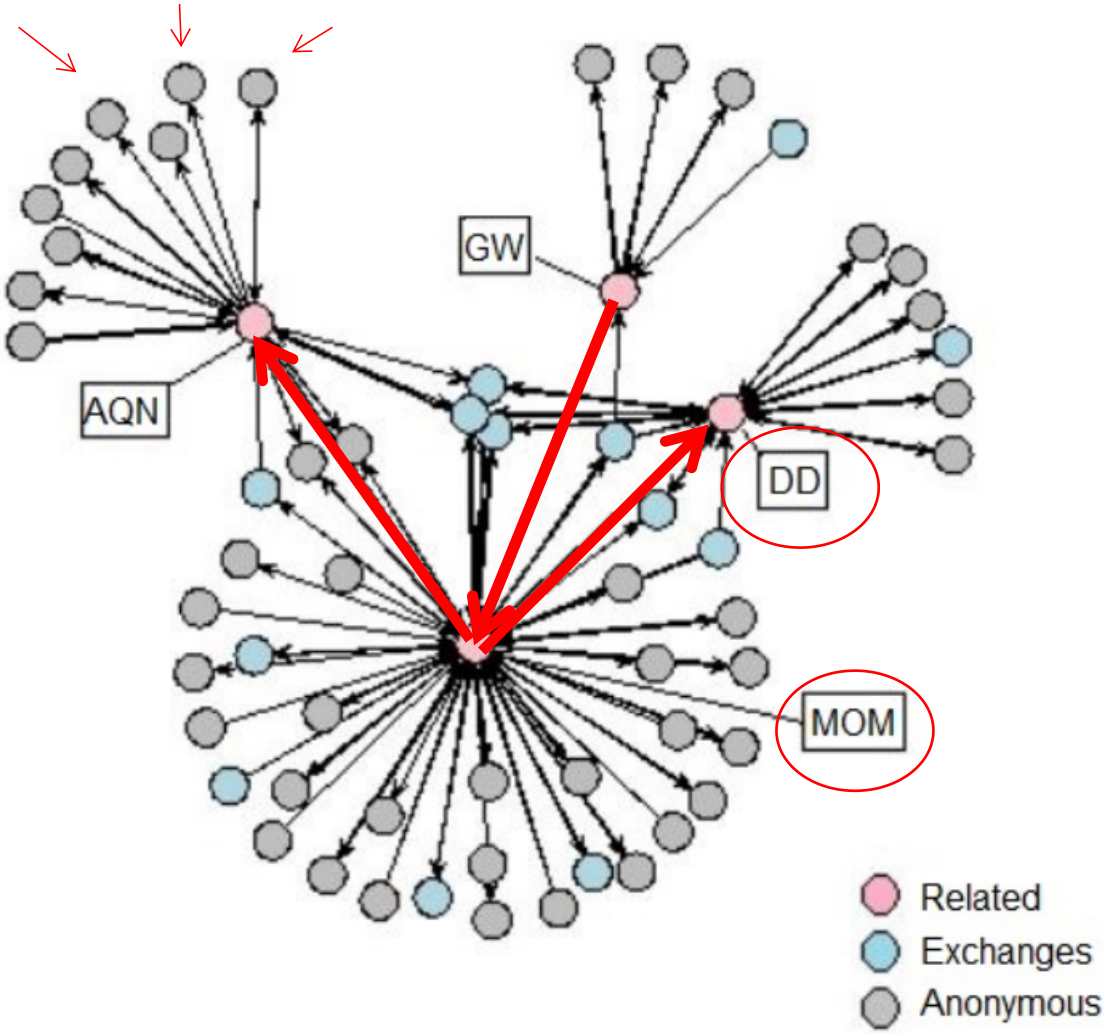
Panel A: Ripple transfers

	Inflows	Outflows
Min	34.44	31.93
Q1	64.20	58.60
Median	79.63	83.03
Mean	133.34	153.31
Q3	112.41	168.98
Max	811.50	696.35

Panel B: Volume frequency

Bins	Obs	Frequency
Below 1,000	43,805	90.589%
1,001 to 10,000	4,051	8.377%
10,001 to 100,000	481	0.995%
100,001 to 500,000	16	0.033%
Above 500,000	3	0.006%

Tracking the funds on Ripple Blockchain



III - Additional Analysis
Predicting Terror Attacks

- Does blockchain data have predictive value?
- Have we **learned anything useful** that can be used to predict terrorist attacks?
- Approach:
  - training the data on the flagged user (**Sri Lanka Eastern bombing**);
  - use different **machine learning** models (SVM, Neural Networks, and Random Forest);

Model of Choice

- A simple blockchain-based model:

$$Terror_{(t)} = Volume_{(t-1)} + In_{(t-1)} + Out_{(t-1)} + Life_{(t-1)} + Anonymous_{(t-1)} + Exchange_{(t-1)} + Mixer_{(t-1)} + DarkMarkets_{(t-1)} + Balance_{(t-1)} + Sigma_{(t-1)}$$

- This set has 8,043,285 transfers in the period of 2015 to end-2019;
- We split the sample into training and validation sets ~70% (30%);
  - which machine learning model?
  - data is **skewed to zero** values;
  - different performance parameters to consider;
  - lack of more informative (intel) inputs.

Training

- 10-fold cross-validation for parameter choices and model best fit.

	Supported Vector Machine	Neural Networks	Random Forest
Accuracy	0.9939	0.9939	1
Kappa	0.1076	0.0895	1
No Information Rate	0.9937	0.9937	0.9937
P-Value (ACC > NIR)	0.0525	0.0949	<0.0001
McNemar's p-value	<0.0001	<0.0001	<0.0001
Prediction (NO/NO)	285210	285216	285247
Prediction (NO/YES)	37	31	0
Prediction (YES/YES)	106	87	1812
Prediction (YES/NO)	1706	1725	0
Balances Accuracy	0.5292	0.5240	1
Precision	0.9941	0.9940	1
Recall	0.9999	0.9989	1
F-measure	0.9969	0.9969	1

Training

- 10-fold cross-validation for parameter choices and model best fit.

	Supported Vector Machine	Neural Networks	Random Forest
Accuracy	0.9939	0.9939	1
Kappa	0.1076	0.0895	1
No Information Rate	0.9937	0.9937	0.9937
P-Value (ACC > NIR)	0.0525	0.0949	<0.0001
McNemar's p-value	<0.0001	<0.0001	<0.0001
Prediction (NO/NO)	285210	285216	285247
Prediction (NO/YES)	37	31	0
Prediction (YES/YES)	106	87	1812
Prediction (YES/NO)	1706	1725	0
Balances Accuracy	0.5292	0.5240	1
Precision	0.9941	0.9940	1
Recall	0.9999	0.9989	1
F-measure	0.9969	0.9969	1

Training

- 10-fold cross-validation for parameter choices and model best fit.

	Supported Vector Machine	Neural Networks	Random Forest
Accuracy	0.9939	0.9939	1
Kappa	0.1076	0.0895	1
No Information Rate	0.9937	0.9937	0.9937
P-Value (ACC > NIR)	0.0525	0.0949	<0.0001
McNemar's p-value	<0.0001	<0.0001	<0.0001
Prediction (NO/NO)	285210	285216	285247
Prediction (NO/YES)	37	31	0
Prediction (YES/YES)	106	87	1812
Prediction (YES/NO)	1706	1725	0
Balances Accuracy	0.5292	0.5240	1
Precision	0.9941	0.9940	1
Recall	0.9999	0.9989	1
F-measure	0.9969	0.9969	1

Validation

	User	Exchange	Gambling	Service
Accuracy	0.627	0.752	0.815	0.701
95% Confidence Interval	(0.626, 0.629)	(0.742, 0.756)	(0.812, 0.818)	(0.695, 0.705)
Sensitivity	0.628	0.755	0.819	0.704
Specificity	0.424	0.246	0.25	0.277
Prevalence	0.996	0.996	0.995	0.995
Detection Rate	0.626	0.751	0.815	0.700
Detection Prevalence	0.628	0.755	0.818	0.704
Balanced Accuracy	0.526	0.500	0.534	0.490
Users	1	93	49	55

Bitcoin blockchain data has predictive power!

Conclusion

- We provide novel evidence that blockchain-based cryptocurrencies are used to finance terrorist attacks;
- Our results suggest that transparency alone is not enough to curb the financing of terrorist activities - at least not in the short term;
- However, the blockchain ledger underlying transparency also enables outsiders to identify the fund trails and predict terrorist attacks - lower regulatory demand in the long term(?);
- Thefore, financing terrorist activities with blockchain-based currencies is essencialy a disclosure choice.
- Red flag: more opaque cryptocurrencies (e.g., Monero, Zcash) are likely to accommodate the demand for terrorist financing.

Literature

- **Disclosure choice:**
  - Terror financiers essentially tradeoff disclosing more personal and less transaction information privately against less personal and more transactional information publicly (bank vs public debt (Dhaliwal et al. 2011), literature review (Beyer et al. 2010)).

- **The interplay of transparency and regulation:**
  - Transparency mitigates systematic risk on the international financial system (Bouvard et al. 2015);
  - The role of transparency in unregulated markets (Sivakumar and Waymire 2010);
  - Call for research on transparency and regulation (Leuz and Wysocki 2016), and policy-based research (Leuz 2018);
  - Debate on cryptocurrency regulation (Foley et al. 2019, Fusaro and Hougan 2019, Amiram et al. 2020, Cong et al. 2020, Griffin and Shams 2020, Makarov and Schoar 2020, and Sokolov 2020).

Literature

- **Transparency on alternative financing platforms:**
  - Means to mitigate asymmetric information on peer-to-peer lending markets (Michels 2012);
  - Crypto analyst's role in assessing the quality of initial coin offering's (ICO) projects (Bourveau et al. 2019);
  - The interplay between consumer regulation and disclosure on reward crowdfunding (Cascino et al. 2019);
  - Disclosure affects ICO operational and financial performance (Lyandres et al. 2020).

- **Terrorist financing:**
  - Qualitative research: Rudner (2010) surveys the different methods that Hezbollah employs to divert funds, Pieth (2002) discusses the role of financial institutions to curb terrorist financing;
  - Policy considerations: Schott (2006) guidance for AML practices and Navias (2004) review international efforts on post 9/11.

Implications

- Regulation should address resources to regulate exchange and exchange-like services, **NOT** Bitcoin;
- Policy consideration: Compliance measures (AML and KYC) should approximate traditional banking standards;
- Sheds light on the debate over regulation of cryptocurrencies (e.g., Amiram et al. (2020), Cong, et al (2020), Griffin and Shams (2020), Foley et al. (2019), Fusaro and Hougan (2019), Sokolov (2020), Makarov and Schoar (2020)).
- Provide tools for agencies to pinpoint, monitor, and shut down Bitcoin users associated with terrorist financing.

Thank you!

rabetti@mail.tau.ac.il