RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: AFD-W02

Hydra: Where Crypto Money Laundering Trail Goes Cold

Vlad Cuiujuclu
Team Lead
Flashpoint
handle

Andras Toth-Czifra
Senior Analyst
Flashpoint
@NoYardStick

Kim Grauer
Director
Chainalysis
@Chainalysis_Kim

Ian Gray
Senior Director
Flashpoint
@iw_gray

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

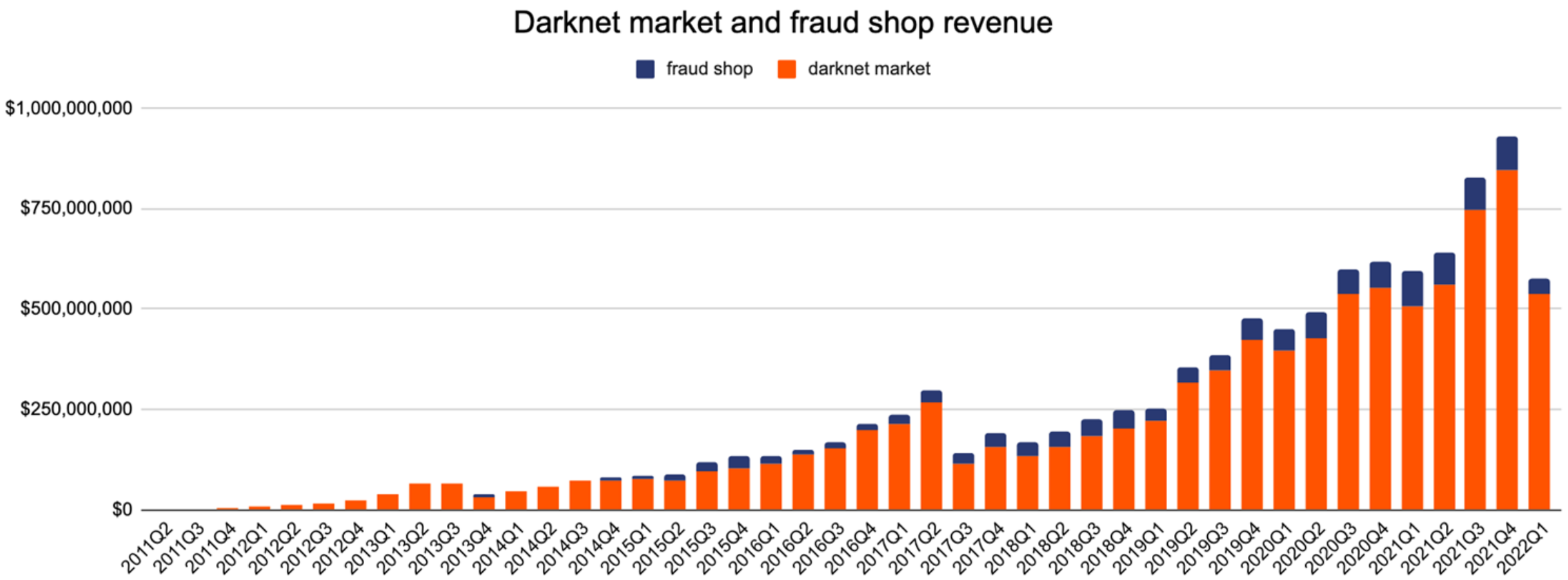
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

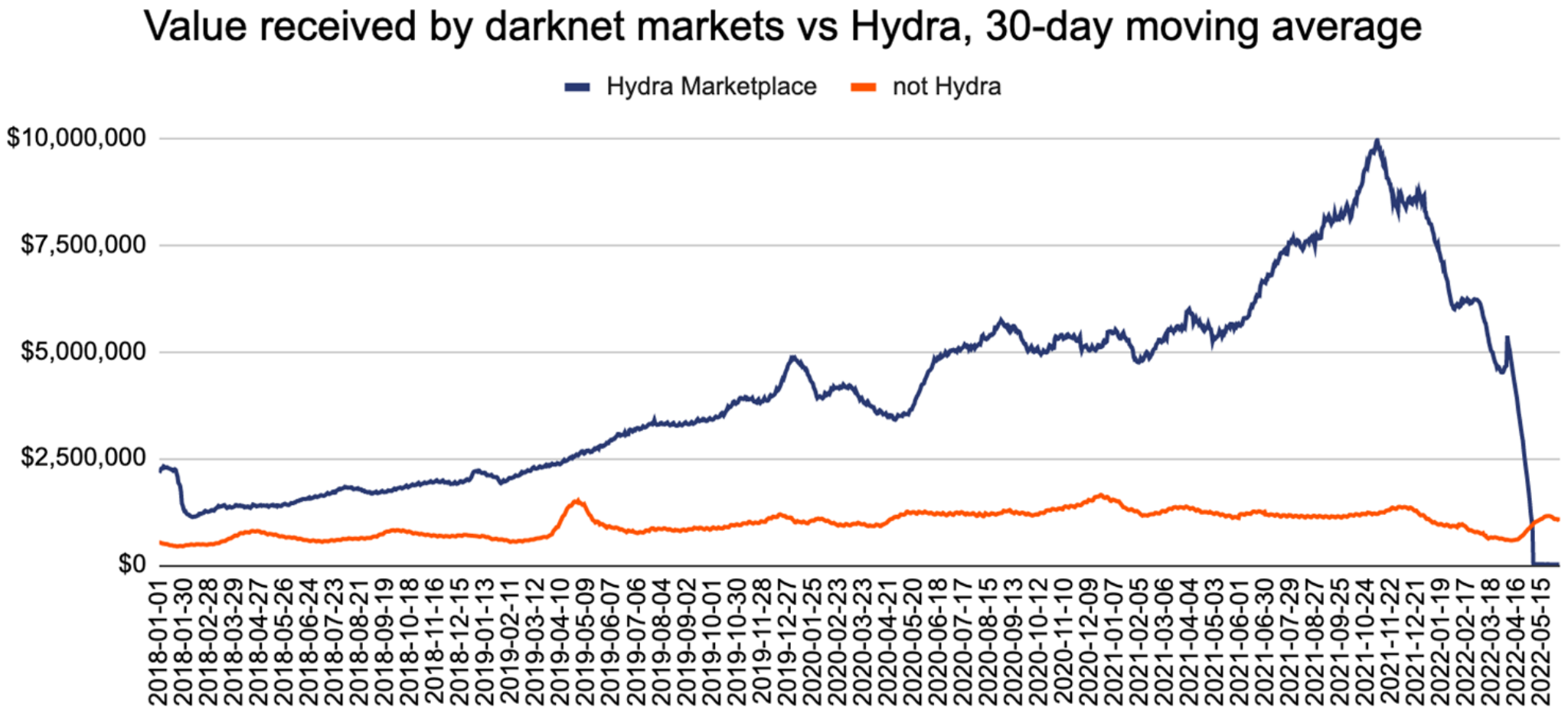
Hydra: Where Crypto Money Laundering Trail Goes Cold

Sequencing Cryptocurrency Flows on the Russian Cybercrime Market “Hydra”

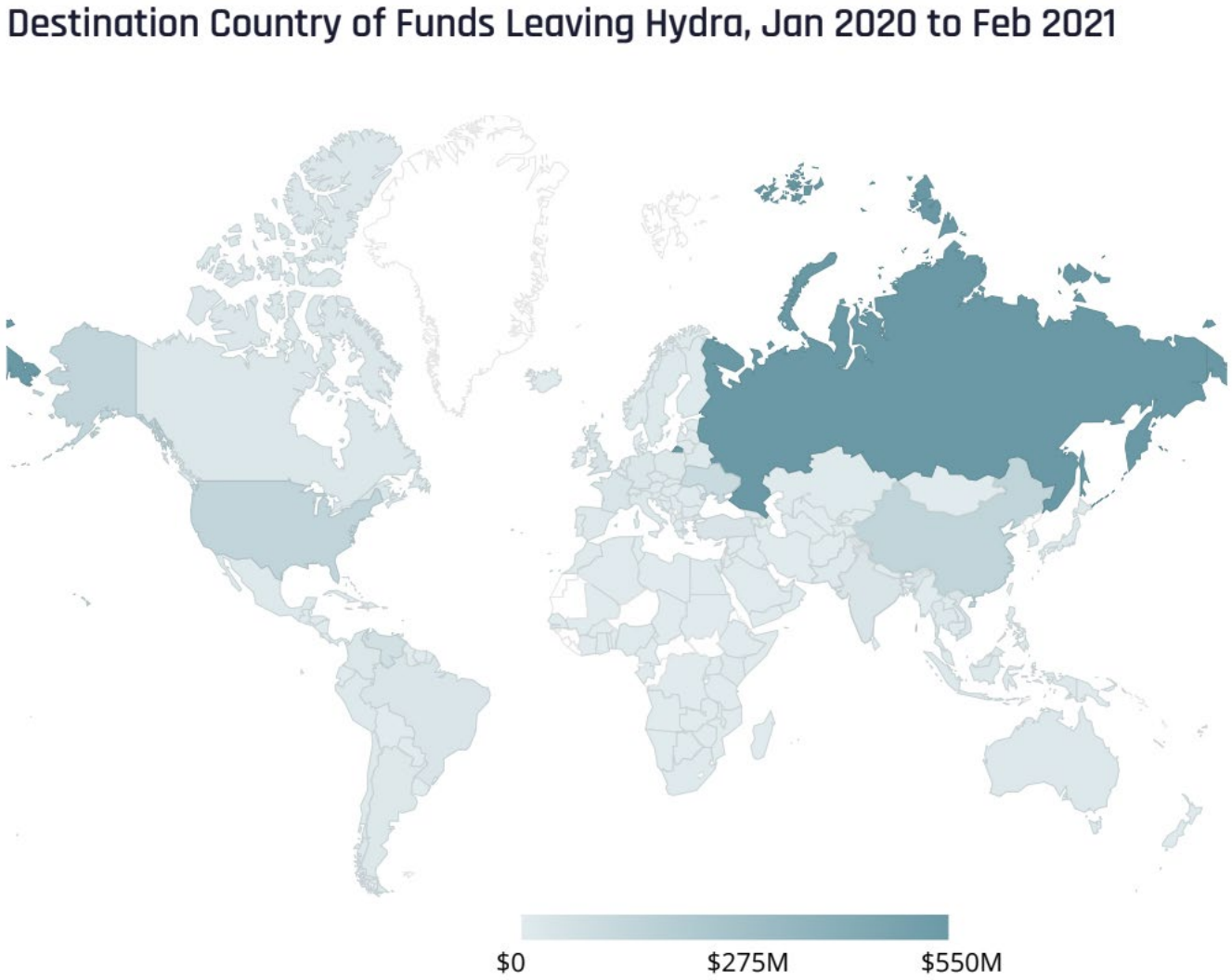
Darknet market activity has had some of the most consistent growth in all of cryptocurrency, absent market closures and disruptions



Much of the major growth happening in the darknet market world in crypto was occurring on the rails of Hydra

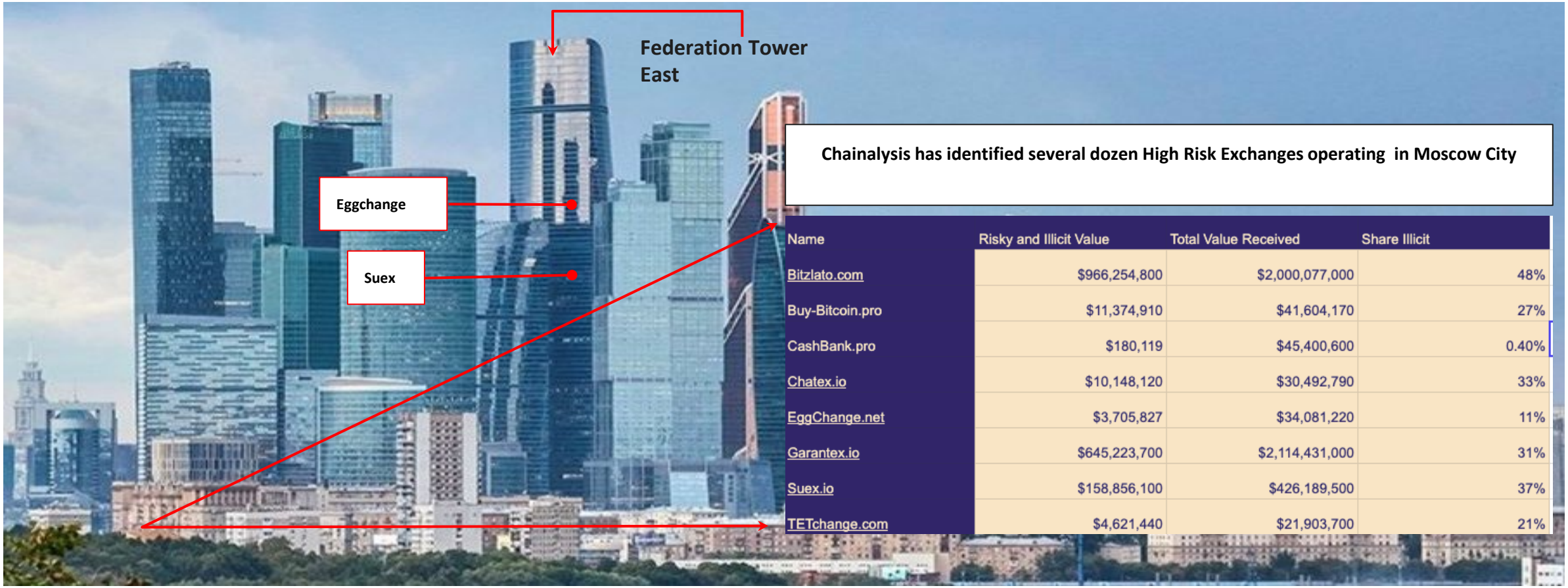


Destination Country of Funds Leaving Hydra



Federation Tower and the immediate area (Moscow-City), are home to dozens of high risk exchanges which launder ransomware, darknet market payments and other illicit transactions.

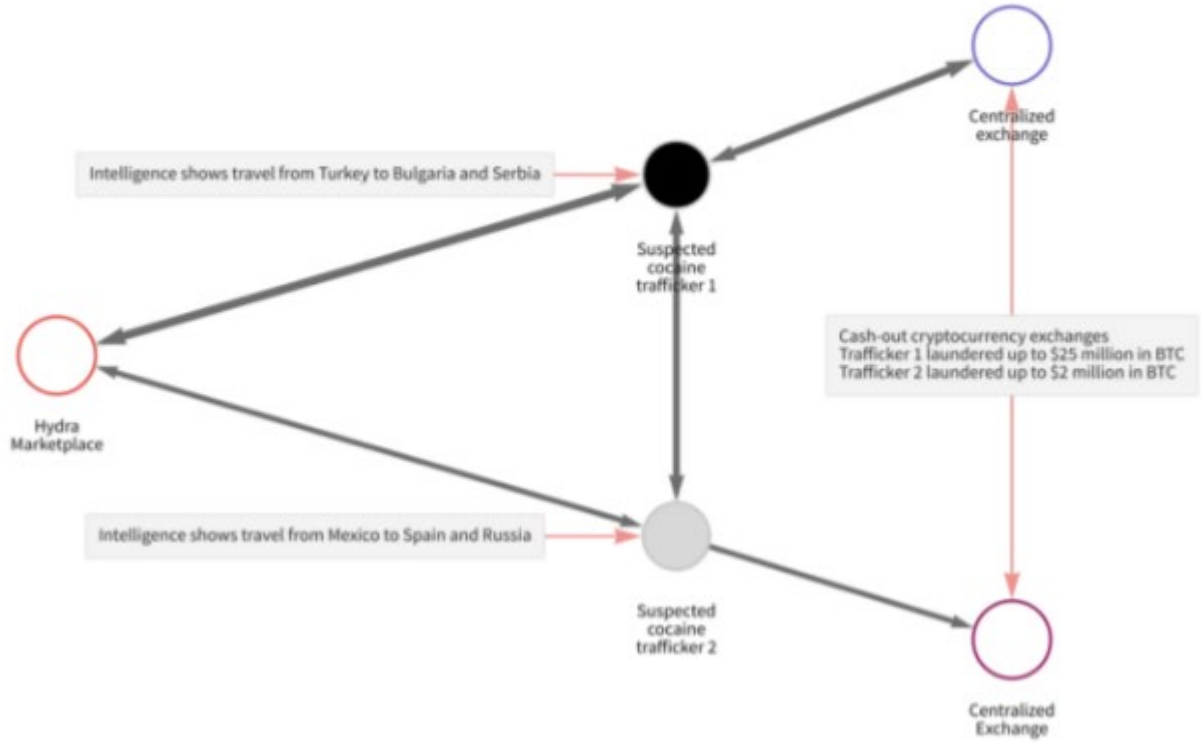
- Suex OTC, located on floor Q of Federation Tower was sanctioned by OFAC in September 2021 for processing ransomware payments.
- Eggchange, another exchange linked to ransomware payments, is located several floors above Suex.
- Chainalysis has identified wallets for numerous other exchanges located within the tower.



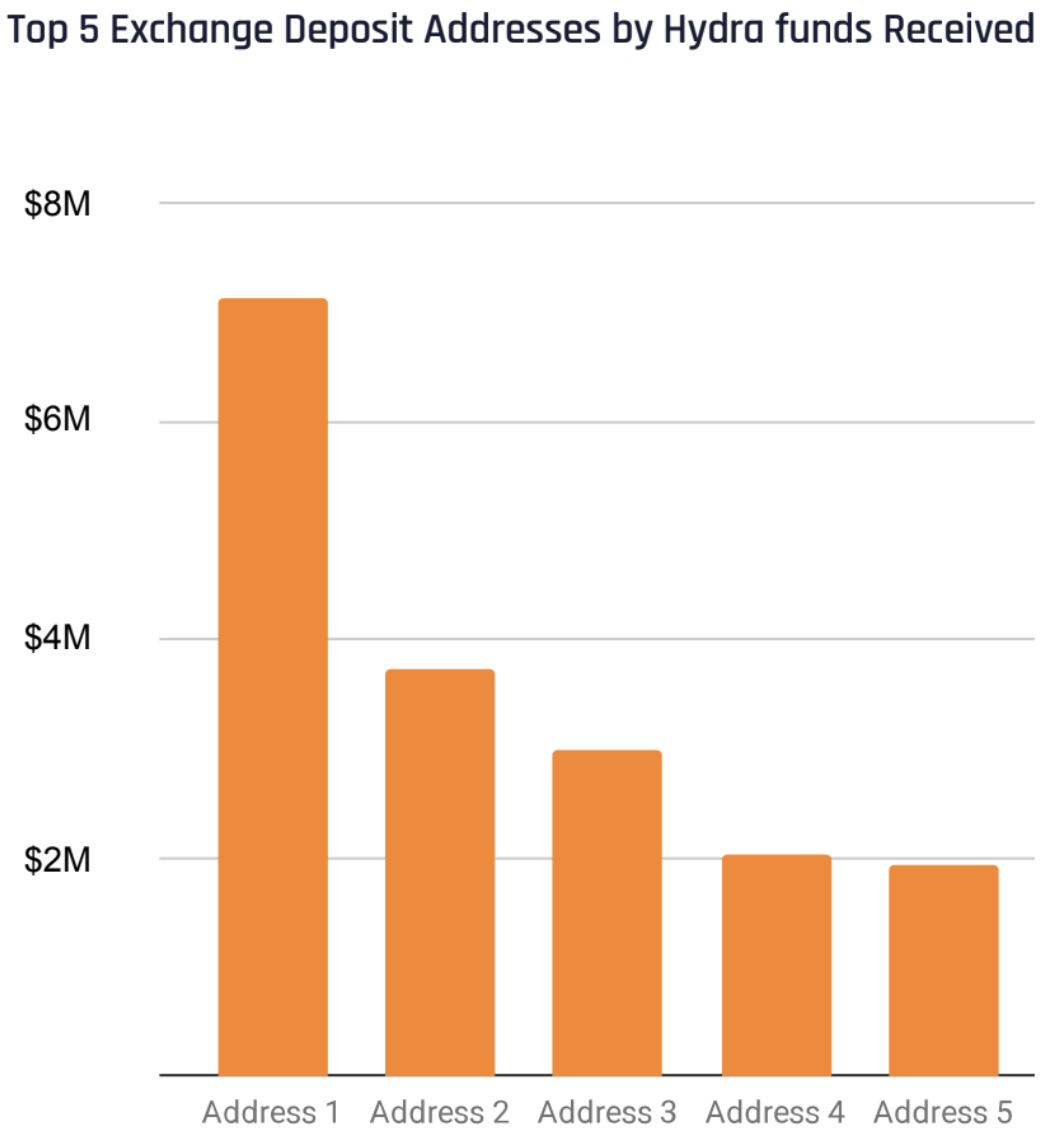
Chainalysis has identified several dozen High Risk Exchanges operating in Moscow City

Name	Risky and Illicit Value	Total Value Received	Share Illicit
Bitzlato.com	$966,254,800	$2,000,077,000	48%
Buy-Bitcoin.pro	$11,374,910	$41,604,170	27%
CashBank.pro	$180,119	$45,400,600	0.40%
Chatex.io	$10,148,120	$30,492,790	33%
EggChange.net	$3,705,827	$34,081,220	11%
Garantex.io	$645,223,700	$2,114,431,000	31%
Suex.io	$158,856,100	$426,189,500	37%
TETchange.com	$4,621,440	$21,903,700	21%

Cocaine trafficking from South America and Asia Minor to Eastern Europe via Hydra



Hydra Marketplace: By the Numbers



Address	Time Active	Number of transfers	% received from illicit sources
Address 1	05/31/2020 - present	1,026	30.1%
Address 2	08/18/2020 - 03/09/2021	24	16.5%
Address 3	11/25/2019 - 03/28/2021	2,467	11.6%
Address 4	01/22/2021 - present	97	91.3%
Address 5	01/21/2020 - 03/01/2021	4,215	26.2%

Mentions of “Buried Treasure” on “LegalRC” and “WayAway”