U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

September 20, 2023

MR. JOHN R. GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1573025-000
Subject: FTX
(JANUARY 1, 2019 TO NOVEMBER 21, 2022)

Dear Mr. Greenewald:

The FBI has completed its review of records subject to the Freedom of Information/Privacy Acts (FOIPA) that are responsive to your request. The enclosed documents were reviewed under the FOIPA, Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
☐ (b)(1)	☑ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☑ (b)(3)	☑ (b)(7)(C)	☐ (k)(1)
50 U.S.C. § 3024(i)(1)	☐ (b)(7)(D)	☐ (k)(2)
Fed. R. Crim. P Rule 6(e)	☑ (b)(7)(E)	☐ (k)(3)
	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☑ (b)(6)		☐ (k)(7)

24 pages were reviewed and 23 pages are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

Based on the information you provided, we conducted a main and reference entity record search of the Central Records System (CRS) per our standard search policy. For more information about records searches and the standard search policy, see the enclosed FBI FOIPA Addendum General Information Section.

This is the final release of information responsive to your FOIPA request. This material is being provided to you at no charge.

Additional material responsive to your request was located in an investigative file. This material is exempt from disclosure in its entirety pursuant to Title 5, United States Code, Section 552, subsection (b)(7)(A), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to interfere with enforcement proceedings.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **"Part 1"** of the Addendum includes standard responses that apply to all requests. **"Part 2"** includes additional standard responses that apply to all requests for records about yourself or any third party individuals. **"Part 3"** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Additional information about the FOIPA can be found at www.fbi.gov/foia. Should you have questions regarding your request, please feel free to contact foipaquestions@fbi.gov. Please reference the FOIPA Request number listed above in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by emailing the FBI's FOIA Public Liaison at foipaquestions@fbi.gov. The subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Michael G. Seidel
Section Chief
Record/Information Dissemination Section
Information Management Division

Enclosures

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

(i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.

(ii) **Intelligence Records**. To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

(i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.

(ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

(iii) **Requests for Confidential Informant Records.** The FBI can neither confirm nor deny the existence of confidential informant records pursuant to FOIA exemptions (b)(7)(D), (b)(7)(E), and (b)(7)(F) [5 U.S.C.§ § 552 (b)(7)(D), (b)(7)(E), and (b)(7)(F)] and Privacy Act exemption (j)(2) [5 U.S.C.§ 552a (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records would reveal confidential informant identities and information, expose law enforcement techniques, and endanger the life or physical safety of individuals. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

(i) **Record Searches and Standard Search Policy.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems, such as the Central Records System (CRS), or locations where responsive records would reasonably be found. The CRS is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. The standard search policy is a search for main entity records in the CRS. Unless specifically requested, a standard search does not include a search for reference entity records, administrative records of previous FOIPA requests, or civil litigation files.

a. *Main Entity Records* – created for individuals or non-individuals who are the subjects or the focus of an investigation
b. *Reference Entity Records*- created for individuals or non-individuals who are associated with a case but are not known subjects or the focus of an investigation

(ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.

(iii) **Foreseeable Harm Standard.** As amended in 2016, the Freedom of Information Act provides that a federal agency may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions that FOIA enumerates, or (2) disclosure is prohibited by law (5 United States Code, Section 552(a)(8)(A)(i)). The FBI considers this foreseeable harm standard in the processing of its requests.

(iv) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative "FBI file." An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault

The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **http://www.theblackvault.com**

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1573025-000

Total Deleted Page(s) = 1
Page 1 ~ b3; b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

[redacted] b7A

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Preservation of Inca Digital Geotagging Crypto Derivatives Traders with NLP Report **Date:** 08/02/2021

CC: [redacted]

From: NEW YORK
NY-ID06
Contact: [redacted] b6 b7C b7E

Approved By: SIA [redacted]
SSA

Drafted By: [redacted]

Case ID #: [redacted] (U) [redacted] b6 b7A b7C b7E
(U) [redacted]
[redacted]
(U) [redacted]

Synopsis: (U) Preservation of Inca Digital Geotagging Crypto Derivatives Traders with NLP Report

Enclosure(s): Enclosed are the following items:
1. (U) Inca Digital Intelligence Report

Details:

On July 30, 2021, SOS [redacted] accessed and preserved the attached report relating to geotagging cryptocurrency derivatives platforms. b6 b7C

♦♦

UNCLASSIFIED

geolocation is not correlated to the actual traffic

path and therefore resistant to such location spoofing methods.

The purpose of this analysis is not to single out any of the exchanges discussed in this report. In fact, we see similar problems with unregistered financial product offerings across most crypto trading venues with significant volumes.

Request full list of geotagged crypto derivatives traders

Share: Facebook Twitter LinkedIn Telegram

BACK TO ALL NEWS

1100 15 Street NW Floor 4 Washington, DC 20005 +1 (908) 219-7750 info@inca.digital

VARIETY OF NATURAL LANGUAGE PROCESSING (NLP) TECHNIQUES THAT CAN PRODUCE RELIABLE DATASETS BASED ON THE DIGITAL FOOTPRINT OF CRYPTO USERS.

Featured Investigation NLP

Cryptocurrency Analytics

Inca Digital's Investigation Team is often tasked with collecting hidden data on crypto market participants. Although the blockchain space supplies troves of open data to sift through, trading venue activity often remains a mystery due to unreliable trade data and a lack of transparency from trading venue owners. To fill these data gaps, we leverage a variety of Natural Language Processing (NLP) techniques that can produce reliable datasets based on the digital footprint of crypto users. In the example below, we show how particular exchange users can be identified and geotagged.

Identifying Traders

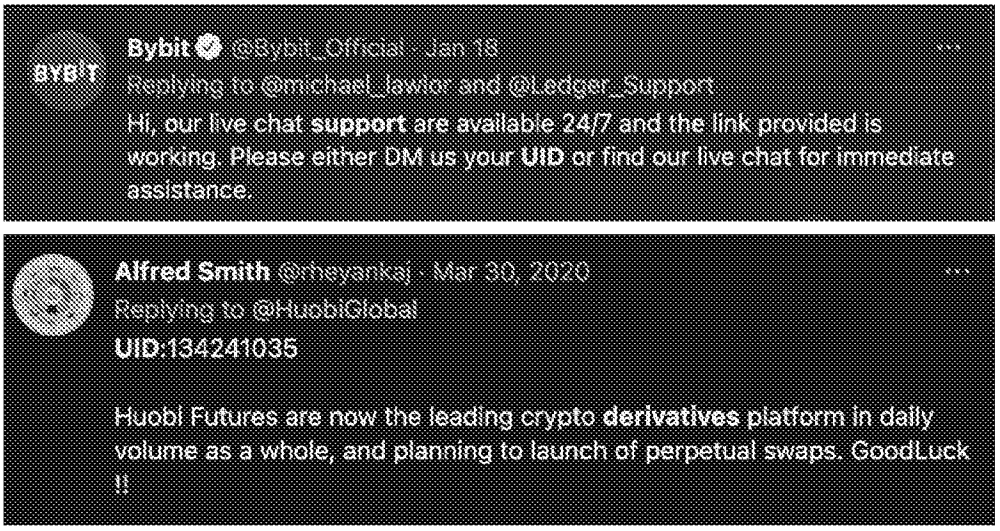
To underline the importance of such datasets, we take derivatives traders operating on the major derivatives venues and try to show that their geographic locations are far more diverse than what is claimed by the exchange operators and is allowed by local securities regulations.

For this report, we include in our sample some popular derivatives platforms such as Bybit, Bitfinex, FTX, Binance Futures, BitMEX, OKEx, and Huobi Futures. Most of them are providing derivatives trading as their major service along with spot markets.

To start, we needed to identify platform users who are actively engaged in derivatives trading, rather than trading spot or just being curious about the exchange website or its activities. For this, we trained BERT models on a small set of known traders' Tweets and analyzed unique embeddings that trigger a positive classification. This approach helped us discover particular tweet patterns that are inherent in those Twitter users who are involved in trading on derivatives platforms.

The tweet patterns include PNL (profit and loss) proofs, a specific screenshot that displays a derivatives trade execution, a referral link posting, and tweets mentioning a UID (trader's unique identifier) along with a support request.

Screenshot of a PnL proof



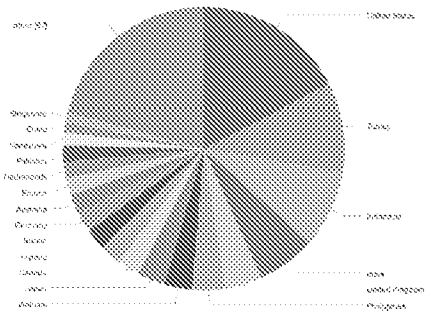
Trader's unique identifier mentions

PNL proofs and the associated screenshots are meant to brag, showing a derivatives trader's successful trades. The BERT model output for derivatives traders allowed us to collect a sample of 2,939 unique Twitter users engaged in derivatives trading on Bybit, FTX, Binance Futures, BitMEX, OKEx, Bitfinex and Huobi Futures.

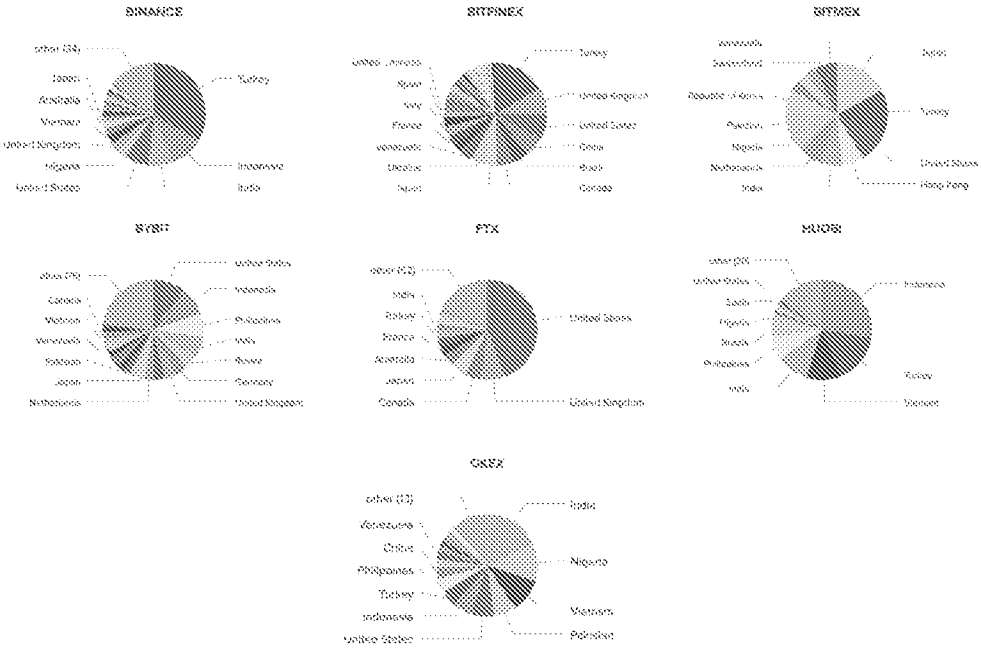
Geotagging

When dealing with geolocating social network users, we typically employ 3 complementary components of the NTerminal NLP module: metadata, language identification, and named entity recognition (NER).

From our sample of 2,939 unique Twitter users engaged in derivatives trading on FTX, Huobi Futures, Binance Futures, OKEx, Bybit, Bitfinex, and Bitmex, we identified the locations of 2,164 traders globally, and 372 from the United States specifically.



Location distribution of Twitter users involved in derivative trading on FTX, Huobi Futures, Binance Futures, OKEx, Bybit, Bitfinex, and Bitmex

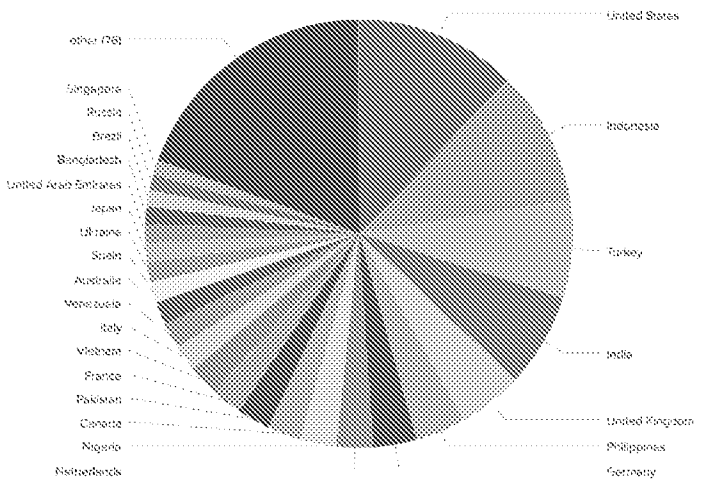


Country distribution of the identified derivatives traders per exchange

TWITTER API GEODATA

The simplest of the 3 geolocation methods analyzes post metadata from the Twitter API. The geolocation metadata, residing in the tweet itself or a user's bio, allowed us to identify the location of 911 of the 2,939 derivatives traders sampled.

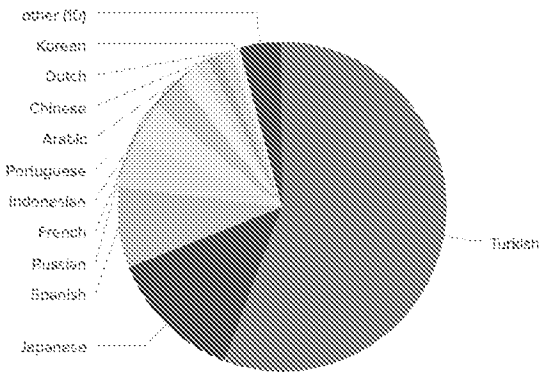
Location of derivatives traders (Twitter API)



Most popular locations of derivatives exchange users according to Twitter API data (100 total)

LANGUAGE IDENTIFICATION

The language identification technique relies on utilizing geographically isolated languages to identify, with high confidence, where a user lives. It does not correlate with the Twitter API metadata and provides a unique signal that can be overlaid on the other datasets to provide more accurate localization. In some cases, a regional variety of a language is characteristic of a particular region, which makes geotagging even more precise. The trader sample utilized in this analysis includes various dialects, such as Simplified and Traditional Chinese, as well as Latinized versions of Japanese, Hindi, and Korean. In the derivatives trader sample dataset, this approach allowed us to identify 21 unique spoken languages and identify the location of 189 out of 2,939 traders over 14 territories.



Top languages spoken by derivatives traders, excluding English (language identification)

Location of derivatives traders (language identification)

NER for Place Recognition

The final method is the most sophisticated, requiring a much more extensive speech sample collection and state-of-the-art multi-language Geographical Named Entity Recognition models. By running hundreds of tweets of each of the identified users through our models, NER geotagged 2,079 out of 2,939 derivative traders.

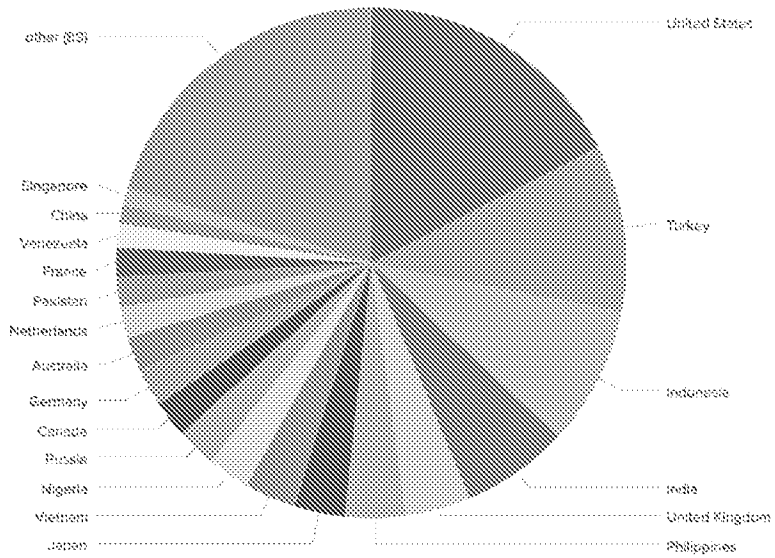
By referencing favorite coffee shops, upcoming

By referencing favorite coffee shops, upcoming concerts, ongoing elections, landmarks, and even traffic jams, Twitter users produce invaluable geotags that can be aggregated to predict the true residency of a derivatives trader, regardless of the statements made during their KYC onboarding process and the paperwork they provide to the trading venue.

Examples of geographical named entities mentioned by derivative traders

These tags are often much more reliable and precise than any other methods we use, enabling city-level granularity.

Location of derivatives traders (NER)



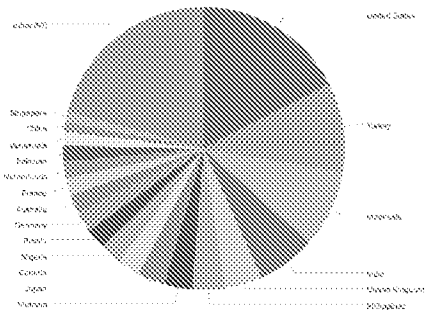
Country location of derivatives traders (total: 108 countries)

ALL METHODS COMBINED

The true power of natural language processing for geotagging entities - crypto traders or otherwise - comes from combining all methods and overlaying geotags from multiple sources. This often gives enough corroborating evidence that an exchange user is actively trading certain financial products, rather than just visiting a website out of curiosity or using it for other purposes.

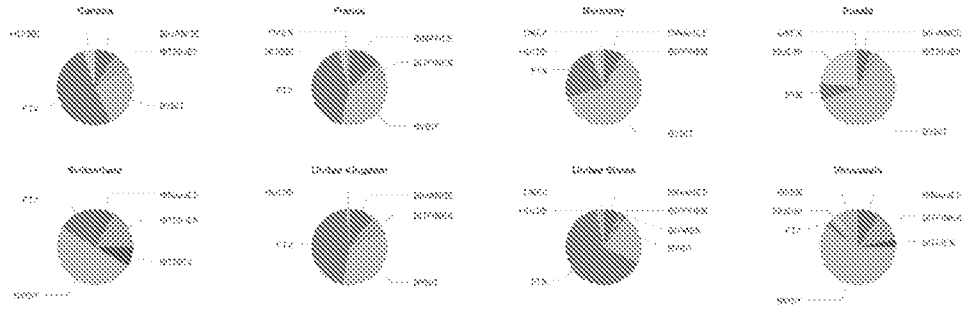
We geotagged 2,164 out of 2,939 unique derivative traders from 116 countries.

Derivatives trader map: countries, 2,164 unique users (NER, Language Identification, and Twitter API combined)



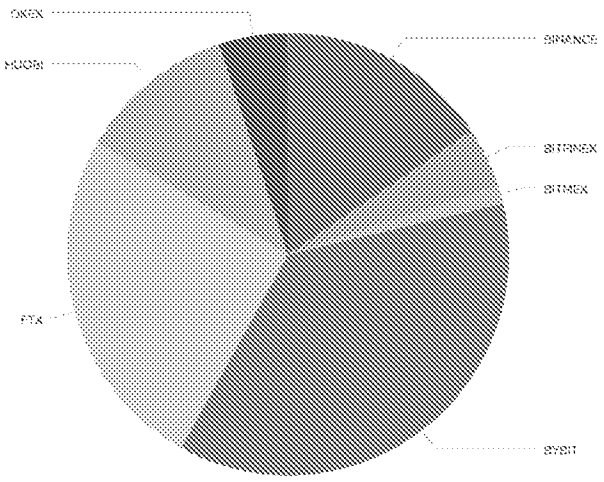
Most popular locations of derivative exchange users (116 total)

TRADER LOCATION (VENUE BREAKDOWN)



Exchange distribution of the identified derivatives traders by country

traders by country



Identified derivatives trader distribution per exchange

3-COMPONENT MODEL AND API DISCREPANCY

Actual location	Identified	Location API
United States	United Kingdom	Canada
Russia	Kazakhstan	Canada
Nigeria	Netherlands	United States
United States	Switzerland	Qatar

A number of geotagged users have different location information acquired from the Twitter API relative to the model estimation. According to the model's estimate, most of the users that are supposed to reside in the United States, United Kingdom and Turkey, are showing other locations in their bio.

Trading venues often rely on IP address attribution-based filters, which are easy to circumvent by using a VPN with an exit node in another jurisdiction. NLP

Intelligence

#Finance #Investigation #Security #Technology #Politics

GEOTAGGING CRYPTO DERIVATIVES TRADERS WITH NLP

JULY 30, 2021

CHRISTINA TKACH

SOFIA SEDLOVA

EVGENY DMITRIEV

ADAM ZARAZINSKI

ALTHOUGH THE BLOCKCHAIN SPACE SUPPLIES TROVES OF OPEN DATA TO SIFT THROUGH, TRADING VENUE ACTIVITY OFTEN REMAINS A MYSTERY DUE TO UNRELIABLE TRADE DATA AND A LACK OF TRANSPARENCY FROM TRADING VENUE OWNERS. TO FILL THESE DATA GAPS, WE LEVERAGE A

Official Record

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Report on Cryptocurrency Insider Trading **Date:** 05/26/2022

From: NEW YORK
NY-C43
Contact: [redacted] b6 b7C b7E

Approved By: SSA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) [redacted] b7A

Synopsis: (U) To document open source reporting

Enclosure(s): Enclosed are the following items:
1. (U) Wall Street Journal Article

Details:

According to reporting, over six days in August 2021, one crypto wallet amassed a stake of $360,000 worth of Gnosis coins. On the seventh day, Binance—the world's largest cryptocurrency exchange by volume—said in a blog post that it would list Gnosis, allowing it to be traded among its users. The price of Gnosis rose sharply, from around $300 to $410 within an hour. Four minutes after Binance's announcement, the wallet began selling down its stake, liquidating it entirely in just over four hours for slightly more than $500,000—netting a profit of about $140,000.

The wallet buying Gnosis was among 46 that purchased a combined $17.3 million worth of tokens that were listed shortly after on Coinbase, Binance and FTX.

The Wall Street Journal article is attached in a 1A package.

Title: (U) Report on Cryptocurrency Insider Trading
Re: [redacted] 05/26/2022 b7A

♦♦

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/crypto-might-have-an-insider-trading-problem-11653084398

◆ WSJ NEWS EXCLUSIVE

Crypto Might Have an Insider Trading Problem

Anonymous wallets buy up tokens right before they are listed and sell shortly afterward

By Ben Foldy Follow and *Caitlin Ostroff* Follow
May 21, 2022 5:30 am ET

Public data suggests that several anonymous crypto investors profited from inside knowledge of when tokens would be listed on exchanges.

Over six days last August, one crypto wallet amassed a stake of $360,000 worth of Gnosis coins, a token tied to an effort to build blockchain-based prediction markets. On the seventh day, Binance—the world's largest cryptocurrency exchange by volume—said in a blog post that it would list Gnosis, allowing it to be traded among its users.

Token listings add both liquidity and a stamp of legitimacy to the token, and often provide a boost to a token's trading price. The price of Gnosis rose sharply, from around $300 to $410 within an hour. The value of Gnosis traded that day surged to more than seven times its seven-day average.

Four minutes after Binance's announcement, the wallet began selling down its stake, liquidating it entirely in just over four hours for slightly more than $500,000 —netting a profit of about $140,000 and a return of roughly 40%, according to an analysis performed by Argus Inc., a firm that offers companies software to manage employee trading. The same wallet demonstrated similar patterns of buying tokens before their listings and selling quickly after with at least three other tokens.

The crypto ecosystem is increasingly grappling with headaches that the world of

Copyright © 2022 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

they are found to have aided such trades.

Paul Grewal, Coinbase's chief legal officer, followed up with a blog post Thursday. The company has seen information about listings leak before announcements through traders detecting digital evidence of exchanges testing a token before a public announcement, he said. Coinbase has taken steps to mitigate that in addition to its efforts to prevent employee insider trading, he said.

Wallets like these have caused debate in the crypto community over whether targeted buying of specific tokens ahead of listings on exchanges points to insider trading. The crypto markets are largely unregulated. In recent years, regulators have looked more closely at the market's fairness for individual investors. The largest cryptocurrency bitcoin has fallen 24% in May, causing steep losses for individual investors across the market.

Insider trading laws bar investors from trading stocks or commodities on material nonpublic information, such as knowledge of a coming listing or merger offer.

Some lawyers say that existing criminal statutes and other regulations could be used to go after those trading cryptocurrencies with private information. But others in the cryptocurrency industry say a lack of case precedent specific to crypto insider trading has created uncertainty over whether and how regulators might seek to tackle it in the future.

Argus CEO Owen Rapaport said that internal compliance policies in crypto can be undercut by a lack of clear regulatory guidelines, the libertarian ethos of many who work in the space and the lack of institutionalized norms against insider trading in crypto compared with those in traditional finance.

"Firms have real challenges with making sure the code of ethics against insider trading—which almost every firm has—is actually followed rather than being an inert piece of paper," Mr. Rapaport said.

Securities and Exchange Commission Chairman Gary Gensler said Monday that he saw similarities between the influx of individual investors into crypto markets and the stock boom of the 1920s that presaged the Great Depression, which led to the creation of the SEC and its mandate to protect investors."The retail public had

gotten deeply into the markets in the 1920s and we saw how that came out," Mr. Gensler said. "Don't let somebody say 'Well, we don't need to protect against fraud and manipulation.' That's where you lose trust in markets."

Spokespeople for the exchanges said that they have policies to ensure that their employees can't trade off of sensitive information.

A Binance spokeswoman said that employees have a 90-day hold on any investments they make and that leaders in the company are mandated to report any trading activity on a quarterly basis.

"There is a longstanding process in place, including internal systems, that our security team follows to investigate and hold those accountable that have engaged in this type of behavior, immediate termination being minimal repercussion," she said.

FTX CEO Sam Bankman-Fried said in an email that the company explicitly bans employees from trading on or sharing information related to coming token listings and has a policy in place to prevent that. The trading highlighted in Argus's analysis didn't result from any substantive violations of company policy, Mr. Bankman-Fried said.

Write to Ben Foldy at ben.foldy@wsj.com and Caitlin Ostroff at caitlin.ostroff@wsj.com

We want to hear from you

What's your investing strategy for 2022? Has the recent market turmoil changed your approach? Tell us about your experience here.

Name*

Age *

Occupation *

City, State *

Email*

SUBMIT

By submitting your response to this questionnaire, you consent to Dow Jones processing your special categories of personal information and are indicating that your answers may be investigated and published by The Wall Street Journal and you are willing to be contacted by a Journal reporter to discuss your answers further. In an article on this subject, the Journal will not attribute your answers to you by name unless a reporter contacts you and you provide that consent.

Appeared in the May 23, 2022, print edition as 'Crypto Data Suggest Insider Trading.'

traditional finance tackled decades ago. The collapse of a so-called stablecoin from its dollar peg earlier this month stemmed from crypto's version of a bank run. How cryptocurrency exchanges prevent market-sensitive information from leaking has also become a growing topic of concern. The focus comes as regulators are raising questions about the market's fairness for retail users, many of whom just booked major losses on steep declines in crypto assets.

The wallet buying Gnosis was among 46 that Argus found that purchased a combined $17.3 million worth of tokens that were listed shortly after on Coinbase, COIN -5.23% Binance and FTX. The wallets' owners can't be determined through the public blockchain.

Profits from sales of the tokens that were visible on the blockchain totaled more than $1.7 million. The true profits from the trades is likely significantly higher, however, as several chunks of the stakes were moved from the wallets into exchanges rather than traded directly for stablecoins or other currencies, Argus said.

Argus focused only on wallets that exhibited repeated patterns of buying tokens in the run-up to a listing announcement and selling soon after. The analysis flagged trading activity from February 2021 through April of this year. The data was reviewed by The Wall Street Journal.

Coinbase, Binance and FTX each said they had compliance policies prohibiting employees from trading on privileged information. The latter two said they reviewed the analysis and determined that the trading activity in Argus's report didn't violate their policies. Binance's spokesperson also said none of the wallet addresses were linked to its employees.

Coinbase said it conducts similar analyses as part of its attempts to ensure fairness. Coinbase executives have posted a series of blogs touching on the issue of front running.

"There is always the possibility that someone inside Coinbase could, wittingly or unwittingly, leak information to outsiders engaging in illegal activity," Coinbase Chief Executive Brian Armstrong wrote last month. The exchange, he said, investigates employees that appear linked to front running and terminates them if