INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 1, PP. 1–6
Manuscript received December 6, 2025; revised February, 2026. doi: 10.24425/ijet.2026.157874

Processing heterogeneous cryptocurrency exchange data for law enforcement: A proposal for an online tool

Przemysław Rodwald, and Natan Kołodziej

***Abstract*—The growing number of criminal investigations involving cryptocurrency-related offenses, mainly investment fraud or crypto scams, has led to an increased frequency of Law Enforcement Agencies requesting information from cryptocurrency exchanges. However, the data provided by these entities often varies significantly in terms of format, structure, and level of detail, which complicates efficient processing and analysis. This article proposes the development of an online tool designed to automatically process data received from various cryptocurrency exchanges. The tool aims to convert disparate datasets into a standardized and readable format, thereby enhancing the effectiveness of investigative procedures and improving the consistency and quality of data analysis in criminal cases. The paper outlines the core functional assumptions of the proposed solution, presents its system architecture, and discusses example use cases. A prototype implementation has been deployed and evaluated on sample datasets from five major cryptocurrency exchanges.**

***Keywords*—cryptocurrencies; investigations; crypto exchanges data**

I. Introduction

A RAPID expansion of the cryptocurrency ecosystem has fundamentally reshaped the global financial landscape, creating both novel economic opportunities and complex regulatory and investigative challenges. Cryptocurrencies enable fast, borderless, and pseudo-anonymous transactions, characteristics that—while beneficial for innovation and financial inclusion—simultaneously present significant obstacles for Law Enforcement Agencies seeking to detect and prevent criminal misuse. Digital assets have been increasingly implicated in a variety of illicit activities, including money laundering, ransomware operations, fraud, tax evasion, illicit trade, and financing of terrorism. The ability to monitor and analyze cryptocurrency transaction data has therefore become a crucial component of contemporary financial crime investigations. From an operational perspective, access to comprehensive, accurate and timely cryptocurrency data enables investigators to reconstruct transaction chains, identify clusters of related blockchain addresses, and uncover links between pseudonymous digital identities and real-world individuals or organizations. Such analytical capabilities are indispensable for tracing the flow of illicit funds and for supporting judicial proceedings with verifiable digital evidence. Moreover, the integration of exchange data with other sources—such as blockchain explorers, know-your-customer (KYC) databases, and financial intelligence reports—enhances contextual understanding of suspect activities and facilitates international cooperation between regulatory bodies and investigative institutions. However, the heterogeneous and fragmented nature of cryptocurrency exchange data remains a major impediment to effective enforcement. Exchanges differ widely in terms of their data structures, reporting standards, compliance practices, and jurisdictional regulations. This lack of uniformity complicates the aggregation, normalization, and comparative analysis of data, often resulting in incomplete or inconsistent information.

In recent years, Law Enforcement Authorities have increasingly conducted investigations into crimes involving the use of cryptocurrencies, requiring the acquisition of data from cryptocurrency exchanges. Practice shows that the feedback information provided by these entities is highly heterogeneous, differing in format, scope, and data structure, significantly hampering effective analysis and evidentiary use during proceedings. The lack of standardization in the data received not only prolongs the work of investigative bodies, but also increases the risk of interpretative errors and complicates international cooperation.

The purpose of this article is to present the concept of an innovative online tool that enables the automatic processing and standardization of data originating from various cryptocurrency exchanges. The proposed solution allows the conversion of information supplied in diverse formats into a unified and transparent form, facilitating its analysis, visualization, and further use by Law Enforcement Authorities and blockchain forensic experts. The tool accounts for the specific nature of blockchain data while ensuring compliance with security and privacy requirements. The article discusses the key challenges associated with processing cryptocurrency-related data, presents the architecture and functionalities of the proposed system, and highlights the potential benefits of its implementation for the practice of the justice system.

P. Rodwald is affiliated with the Educational Division of the Cyber Security Training Centre of Excellence, Warsaw, Poland (e-mail: prodwald@mon.gov.pl, ORCID 0000-0003-4261-8688).

N. Kołodziej is a student of Computer Science at the Polish Naval Academy, Gdynia, Poland (e-mail: kolodziej.nat@outlook.com).

© The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

II. Crypto Crime Reports Summary

This section summarizes selected findings from the latest analytical reports on cryptocurrency-related crimes.

According to The Chainalysis Crypto Crime Report 2025 [1], cryptocurrency-based fraud remains one of the most significant sources of illicit on-chain activity. In 2024, scam-related addresses received at least USD 9.9 billion, representing a lower bound estimate that is expected to increase as additional illicit addresses are identified. Chainalysis projects that the final total may exceed USD 12 billion, marking a continuation of the long-term upward trend observed since 2020, with an average annual growth rate of approximately 24%. Two categories dominated the scam ecosystem: high-yield investment scams (HYIS) and pig butchery scams, which together accounted for more 83% of total scam revenues. Although HYIS revenues decreased by 36. 6% year over year, pig butchering scams increased by almost 40%, with the number of incoming transfers increasing by 210%. The median transaction size within pig butchering schemes, however, dropped by 55%, indicating a shift toward broader victim targeting through smaller, more frequent deposits.

The TRM Labs 2025 Crypto Crime Report [2] provides a comprehensive analysis of fraudulent activity in the cryptocurrency ecosystem throughout 2024, revealing a notable reduction in overall scam-related transaction volumes despite persistent structural sophistication among perpetrators. Total funds transmitted to addresses associated with fraudulent schemes were estimated at USD 10.7 billion, representing a 40% year-over-year decline and amounting to approximately 24% of total illicit crypto activity. The study identifies Ponzi and pyramid schemes, investment grooming ("pig butchering"), and phishing operations as the dominant scam typologies, collectively accounting for the majority of illicit flows.

III. Overview of the importance of cryptocurrency data in law enforcement

Atlam et al. in their Blockchain Forensics Review [3] highlight the utility of blockchain's transparency for tracing cryptocurrency flows and link pseudonymous addresses to real-world entities. Commonly employed techniques include transaction graph analysis, clustering heuristics, and the correlation of on-chain data with external (off-chain) information, such as cryptocurrency exchange records. They also identify several limitations: the anonymity mechanisms inherent in cryptocurrencies, frequent address changes, and the global scope of blockchain networks hinder the full attribution of illicit activities. Moreover, most existing frameworks lack automation and scalability, making large-scale investigations challenging. The studies collectively emphasize that effective cryptocurrency forensics requires not only advanced technical tools for blockchain analytics but also cross-institutional data sharing, regulatory cooperation, and continuous methodological development to keep pace with the evolving landscape of crypto-enabled financial crimes.

IV. Challenges in Processing Cryptocurrency Data

Processing cryptocurrency-related data poses significant challenges for Law Enforcement and judicial authorities due to the lack of standardized formats, structures, and data quality across exchanges. Files obtained from cryptocurrency platforms are typically delivered in diverse formats ranging from spreadsheets (e.g., CSV, XLSX), through structured data files (JSON, XML) to proprietary exports generated directly from trading systems (e.g. PDF). Such heterogeneity severely limits automation and requires case-by-case adaptation of data extraction and transformation tools.

In addition, the functionality and level of detail available from each exchange vary substantially: some platforms provide full transaction histories enriched with metadata (e.g. wallet identifiers, transaction fees, UNIX timestamps), while others offer only minimal records sufficient to confirm the occurrence of a transaction. However, additional analytical steps are required to uniquely identify the transaction hash.

Another layer of complexity stems from inconsistent cryptocurrency and token nomenclature - different exchanges may use different abbreviations, tickers, or localized symbols for the same digital assets, which increases the risk of misinterpretation during analytical processing.[1]

Consequently, investigative bodies must employ advanced analytical and normalization techniques to ensure the consistency, comparability, and evidential reliability of the data obtained from multiple sources.

These challenges collectively highlight the need for standardized and automated processing tools for Law Enforcement.

V. Crypto Exchanges data structures

A. Binance

Established in July 2017 by Changpeng Zhao, Binance has become the world's leading cryptocurrency exchange by trading volume. Initially based in China, the company later relocated its operations to Japan and Malta and now identifies itself as a globally decentralized organization without a specific headquarters [4], although the Polish LEA can contact the national representation directly by the Warsaw office[2]. The official channel of communication in criminal cases is through accounts created by LEA representatives on the Kodex platform[3] as a part of Government Law Enforcement Request System (LERS)[4]. According to a 2024 study conducted by John Griffin [5], a finance professor at the University of Texas at Austin, Binance is the exchange most frequently used in so-called "pig butchering" scams.

[1] For example, some exchanges use XBT as the symbol for Bitcoin, while others use BTC. The abbreviation XBT originates from the International Standards Organization (ISO), which maintains the list of globally recognized currency codes. According to ISO rules, if a currency is not associated with any specific country, its code should begin with the letter X — hence Bitcoin's designation as XBT.

[2] Binance Poland sp. z o. o., Aleje Ujazdowskie 41, 00-540 Warsaw

[3] https://app.kodexglobal.com/binance/signup

[4] https://www.binance.com/pl/support/law-enforcement

The dataset from Binance is a well organized as a multi-sheet Excel file, with each sheet corresponding to a distinct category of user or transaction information. The sheet *Customer Information* contains general user metadata, with a header indicating basic details such as the user ID, email address, name, nationality, etc. The *Account Balance* sheet contains aggregated data on the balance of assets. The *Current Assets Wallets* sheet presents data on the user's current holdings, with columns titled: Asset Ticker, Asset Name, Total Position, Estimated BTC Value, Deposit Wallet Address, and Label/Tag/Memo. The *Order History* sheet records transactional details, containing the columns User ID, Market ID, Price, Qty, Average Price, Remain Qty, Trade Qty, Time, Update Time, Side, Status, Type, Stop Price, Price Unit, and Amount Unit. The *Deposit History* tab includes both fiat and crypto deposit information, organized under User ID, Currency, Amount, Account Type, BUSD, Deposit Address, Source Address, TXID, Create Time, Status, Network, and CounterParty ID. The *Fiat Deposit History* sheet provides more granular information about fiat currency deposits, including Status, Create Time, UserID, Email, Amount, Currency, USD equivalent (date extracted), Internal Serial Number, External Serial Number, Second External Serial Number, Source Account Id, Source Account Name, Golden Channel, Remark, Is Replacement Order, Abnormal Reason, Error Code, Error Reason, Channel Fee, Platform Fee, Completed Time, Update Time, Network Provider, Expect Recharge Amount, Narrative, Source Account, Arrived Time, and Order Type. Similarly, the *Withdrawal History* sheet mirrors the structure of the deposit history but pertains to outgoing transactions, listing User ID, Currency, Amount, Account Type, BUSD, Destination Address, Label/Tag/Memo, txId, Apply Time, Status, Network, and CounterParty ID. The *Fiat Withdrawal History* sheet captures detailed information about fiat withdrawals, with columns such as Status, Create Time, UserID, Email, Amount, Currency, USD equivalent (date extracted), Internal Serial Number, External Serial Number, Target Account Id, Target Name, Withdraw Channel, Remark, Is Replacement Order?, Abnormal Reason, Error Reason, Channel Fee, Platform Fee, Completed Time, Update Time, Network Provider, Withdrawer, Narrative, Target Account, Arrived Time, Bic, Bank, Country, Sortcode, Bank Address, Bank City, Iban, and Flutterwave Proof. The *P2P* tab contains records of peer-to-peer transactions, structured with columns for Buy or Sell, Crypto, Amount, Fiat Currency, Total Amount, Unit Price, Create Time, Status, Payment method, Client, Payment Time, Release Time, and Update Time. The *Access Logs* sheet includes activity logs with fields User ID, Operation, Client, Client Version, Real IP, Geolocation, Browser, and Timestamp (UTC). The *Approved Devices* sheet lists devices authorized for account access, with columns Device Name, Client, IP Address, Geolocation, Recent Usage Timestamp (UTC), Status, Key, and Value. The *KYC Documents* sheet includes only an unnamed column, suggesting minimal or empty data content. Finally, the *OTC Trade Order* sheet documents over-the-counter trade details with columns OrderId, UserId, ChannelCode, QuoteId, PayType, UserStatus, UserCurrentPhase, ChannelStatus, ChannelCurrentPhase, symbol, BaseCoin, QuoteCoin, BaseCoinAmount, QuoteCoinAmount, SpreadAmount, SpreadCoin, UserQuotePrice, UserSpreadPrice, ChannelQuotePrice, RequestAmount, RequestAmountCoin, TransId, OtcUserId, SpreadUserId, ChannelUserId, CreateTime, UpdateTime, UserCompletedTime, ChannelCompletedTime, UserRemark, and ChannelRemark.

B. Bybit

Bybit was founded in 2018 by Ben Zhou and is registered in the British Virgin Islands, with global headquarters based in Dubai, United Arab Emirates In February 2025, the exchange was hacked resulting in the loss of $1.5 billion in assets, marking the largest cryptocurrency theft on record [6]. The prefered contact fo LEA is by web form [5] with selected "Law Enforcement Request".

The file received by LEA from Bybit is in the .xlsx format, contains transactional data organized into two distinct worksheets: "Deposit history" and "Withdrawal history." Each worksheet documents user-level financial activities associated with cryptocurrency deposits and withdrawals, respectively.

The "Deposit history" sheet contains following fields: *user_id* field represents the unique identifier of the user who initiated the deposit; *coin* specifies the ticker symbol of the deposited cryptocurrency; *tx_id* denotes the unique transaction identifier recorded on the blockchain; *maker_user_id* refers to the user acting as the maker in the related transaction, while *taker_user_id* identifies the taker; *taker_side_name* indicates the role or transaction orientation of the taker; *token_name* provides the full name of the cryptocurrency token involved; *currency_id* is an internal identifier corresponding to the deposited asset; *price* shows the market price of the cryptocurrency at the moment of deposit; *quantity* indicates the volume of cryptocurrency deposited; *from_address* specifies the blockchain address from which the deposit originated, and *to_address* is the destination address—typically the exchange's wallet; *deposit_coin_time* records the timestamp when the deposit was confirmed on the blockchain; *change_amount* expresses the change in the user's account balance as a result of the deposit, while *change_amount_usd* reflects the equivalent value of this change in USD; finally, *wr_type_desc* provides a textual description of the deposit type or its classification.

The "Withdrawal history" worksheet contains fields like: *user_id* field identifies the user performing the withdrawal; *coin* represents the symbol of the withdrawn cryptocurrency; *amount* indicates the total withdrawn amount, and *amount_usd* provides its corresponding value in USD; *fee* denotes the withdrawal fee charged in the native cryptocurrency, while *fee_usd* gives the equivalent fee value in USD; *tx_id* refers to the blockchain transaction hash that uniquely identifies the withdrawal; *maker_user_id* specifies the identifier of the maker, and *taker_user_id* denotes the taker associated with the transaction; *taker_side_name* indicates the taker's role or orientation in the transaction; *token_name* contains the full name of the withdrawn cryptocurrency; *currency_id* serves as the internal identifier of the asset; *price* provides the market value of the cryptocurrency at the time of withdrawal; *quantity*

[5]https://www.bybit.com/en/help-center/s/webform

specifies the number of tokens involved in the transaction; *from_address* identifies the blockchain address from which the withdrawal was initiated, while *to_address* specifies the destination address receiving the funds; *submitted_time* records the moment when the withdrawal was submitted or processed; lastly, *data_src_desc* provides a descriptive label indicating the source or origin of the transaction data.

C. Coinbase

Founded in 2012 by Brian Armstrong and Fred Ehrsam, Coinbase is a U.S.-based cryptocurrency exchange headquartered in San Francisco, California. It is one of the most regulated major crypto platforms, serving retail and institutional users. On April 2021, Coinbase became a public company on the Nasdaq exchange [7]. Criminal subpoenas and official requests for criminal matters should be submitted by Kodex[6].

The dataset is stored as a single CSV file containing sequential, text-based sections that encode user-level information in a hierarchical format. The file uses semicolons as delimiters but contains only one populated column, with remaining columns being empty. Each section begins with a capitalized header line, followed by rows containing attribute–value pairs separated by commas. The empty rows function as delimiters between the logical segments of the data.

The file begins with the section *USER ATTRIBUTES* ***, which includes key fields such as USER ID, NAME, EMAIL, and CREATED, indicating the user's unique identifier, registered name, email address, and account creation timestamp.

The next section, *IDENTITY* ***, contains personal identification data including FIRST NAME, LAST NAME, SSN, ADDRESS1, ADDRESS2, CITY, STATE, ZIP, COUNTRY, and BIRTHDATE M/D/Y. These variables correspond to self-reported or verified identity information such as residential address and date of birth.

Following this, the *JUMIO PROFILES* *** section summarizes identity verification records performed via the Jumio system. It contains the header DATE, TYPE, ID NUMBER, STATUS, NAME, DOB, ADDRESS, and additional metadata fields. Example entries record document type (e.g., ID Card), document number, verification status, name, and date of birth.

The *PERSONAL DETAILS* *** section reiterates key personal data in a standardized presentation, including DOB, Street Address, City, State, ZIP, and Country.

The next segment, *PREVIOUS EMAILS* ***, appears to document email address changes associated with the account, using columns CHANGED FROM, CHANGED TO, CHANGED AT, and CONFIRMED AT.

The *MERCHANT PROFILES* *** and *COMPANY EDD REQUESTS* *** sections are included as placeholders for business-related or enhanced due diligence information. The latter contains column headers NAME, DBA, WEBSITE, BUSINESS TYPE, BUSINESS CATEGORY, and related company-level identifiers, although in the present dataset these rows appear unpopulated.

Subsequently, the *PHONE NUMBERS* *** section provides registered contact information, listing NUMBER, COUNTRY, and VERIFIED, indicating the user's verified phone number and associated country code.

The dataset also includes a *BILLING ADDRESSES* *** section, which introduces the columns ADDRESS 1, ADDRESS 2, ADDRESS 3, CITY, STATE, POSTAL CODE, COUNTRY, and VERIFIED. This section records billing addresses used for payment or verification purposes.

D. Kraken

Kraken, founded in 2011, officially launched trading operations in 2013. It was one of the first bitcoin exchanges to be listed on Bloomberg Terminal. The official LEA request should be send via a general-purpose web form[7] or by e-mail[8].

The data package received from the Kraken exchange consists of 6 or 7 files: *[USER_ID] - Account Balance - [CASE_ID].pdf*, *[USER_ID] - Exhibit 2 - [CASE_ID].pdf*, *[USER_ID]_accounts.csv*, *[USER_ID]_ip.csv*, *[USER_ID]_ledger_full.csv*, *[USER_ID]_logins.csv* and sometimes a file *Understanding Data Reports.pdf* with column descriptions and information about CSV files.

The most important file *[USER_ID]_ledger_full.csv* contains transactional records exported from the Kraken cryptocurrency platform. Each row corresponds to an individual operation, and the file follows a consistent tabular format with seven columns: TxID, RefID, Time, Type, AClass, Asset, Amount, Fee, and Balance. The column TxID stores the unique transaction identifier assigned by the platform, while RefID provides a secondary reference linking related internal transactions. The Time column records the exact timestamp of each operation in the format "YYYY-MM-DD HH:MM:SS," allowing a precise temporal reconstruction of trading activity. The Type field categorizes the nature of the transaction, including the following options: Trade - non-margin exchange of one currency for another; PTL-Sale – orders placed through the Kraken app, Margin Trade - profits/loss for a margin trade; Rollover - borrowing charge for a margin trade; Deposit - deposit of funds into the Kraken account; Withdrawal - withdrawal of funds from the Kraken account; Transfer - credit of supported airdrops and forks and funds transferred to/from Kraken's OTC desk; Spend - transactions via the Buy Crypto button or Kraken app, indicating asset amount debited from the account; Receive: transactions via the Buy Crypto button or Kraken app, indicating asset amount credited to the accoun; Reward - credit of staking rewards; Settled - settlement of a margin position on spot account; Staking - updates to staked balances, including initial staked balances and changes due to crediting staking rewards; Adjustment - conversion of one currency to another outside of trading. The AClass column indicates the asset class, in this case consistently labeled as "Currency," whereas the Asset field specifies the traded or transferred cryptocurrency symbol (for example, XXBT for Bitcoin or ZEUR for Euro-denominated balances). The Amount variable captures the quantitative value of each transaction, represented as positive or negative depending

[6]https://app.kodexglobal.com/coinbase/signup

[7]https://support.kraken.com/hc/forms

[8]lawenforcement@kraken.com

on directionality—credits versus debits to the account. The Fee field lists transaction fees deducted in the corresponding currency, while Balance represents the user's account balance immediately following the completion of the transaction.

The file *[USER_ID]_accounts.csv.csv* contains all wallet addresses, external bank accounts, or payment processors linked to the client's account. Detailed description of columns: Type - the type of account for fiat currencies or the cryptocurrency associated with the related wallet address; Account - all bank account numbers or wallet addresses linked to the client's account; Deposits - a "1" indicates that the wallet or account was used, not the number of times it was used; Withdrawals - the number of withdrawals from the client's account to the listed account or address; DFirstSeen: the date that the listed deposit account or address was first linked to or used by the client; DLastSeen - the date the listed deposit account or address was last used by the client; WFirstSeen - the date the listed withdrawal account or address was first linked to or used by the client; and WLastSeen - the date the listed withdrawal account or address was last used by the client.

The file *[USER_ID]_ip.csv* contains records of network connections associated with the analyzed account. It includes information about: IP - the IP address used, Interface - the system interface through which the connection occurred, Cnt - the number of interactions recorded for each IP, as well as the timestamps of the first (column Firstseen) and last (column Lastseen) observed activities.

The file *[USER_ID]_logins.csv* contains logs of authentication and account-related actions. It records the type of action performed, the exact time of its occurrence, and the IP address from which it originated. The dataset provides a temporal and spatial view of account access and confirmation events, which can be used to analyze login behavior and potential security-related anomalies.

Apart from four CSV files, there are also two PDF files. The Exibit file contains account opening and verification documents: Government Identification, Identification Verification Photos, Proof of Residence Documentation. The Account Balance file is a screenshot showing the user's balance with a breakdown of individual cryptocurrencies.

E. OKX

OKX was founded by Star Xu who established OKGroup in 2013; the exchange launched in 2017 under the OKEx brand and was later rebranded to OKX [8]. It is registered in the Seychelles. Law Enforcement Officials can make requests by emailing OKX[9] and provides LEA officials with a Law Enforcement Request Guide[10].

The file received by LEA from OKX is in the .xlsx format and consists of several sheets, each documenting a different aspect of user activity and account status: Sheet *User_Info* provides basic user information. The columns include: account creation time, user name, country/region, id number, mobile number, email, uuid and nationality en. Sheet *Funding_Account_History* allows tracking of all deposits, withdrawals, OTC trades, transfers, and other account operations. It is the main transaction history for the funding account, with columns: currency_id, symbol, type_en_name, size, before_balance, after_balance, refer_id and create_time. Sheet *Withdrawal_History* lists all withdrawals from the account. The columns are: uuid (user ID), currency, address (destination wallet address), amount, txid (blockchain transaction ID), creation time (when the withdrawal was initiated), update time (when the withdrawal was processed) and chain name (blockchain network, if applicable). Sheet *Login_info* logs user login events, allows tracking when and from where the user accessed their account. The columns are: uuid (user ID), login time, login ip (IP address), device id, ua (user agent string, identifying device and app) and update time. Sheet *Fiat_History* documents fiat currency transactions (buying/selling). The columns include: creation time (order creation time), order id, base currency, quote currency, price (exchange rate), token_amount, fiat_amount, payment time, seller bank account number, seller_bank_branch, seller_bank, payment_type and type (transaction type). Sheet *Deposit_History* contains details of each deposit, including addresses and transaction hashes. The columns are: uuid (user ID), currency, address (deposit address), amount, txid (blockchain transaction ID), creation time, update time. Sheet *Account_Balance* allows tracking of balance changes over time for each currency, shows daily account balances. The columns are: currency_symbol, total_equity_account (total balance for the currency) and date.

VI. Proposed Online Tool for Data Processing

The presented project, called Interpreter, is developed entirely in pure PHP, without the use of external frameworks. The project is presented in a minimal raw visualization focused on simplicity, as shown in Figure 1. Its architecture is modular and designed for clarity and extensibility. The main controller file, index.php, manages user input and validation. It receives the uploaded transaction history file (Excel or CSV) together with the selected name of the cryptocurrency exchange. After verifying that both the file and the exchange selection are valid, the script securely stores the uploaded file and invokes the corresponding exchange-specific module (e.g., binance.php, bybit.php). This design facilitates the easy addition of new exchanges and ensures separation between input validation and data processing logic.

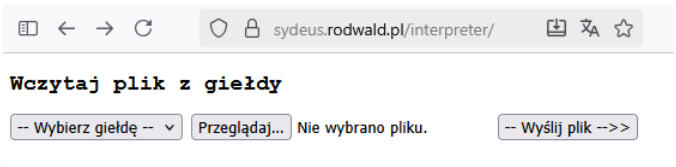

Fig. 1. The screenshot from the start page of the Interpreter.

The module [exchange_name].php performs data parsing and visualization specific to the selected exchange. Using, when necessary, the PhpSpreadsheet library[11], it extracts relevant information from multiple worksheets or single file.

[9] e-mail address enforcement@okx.com

[10] https://www.okx.com/help/okx-law-enforcement-request-guide

[11] https://github.com/PHPOffice/PhpSpreadsheet

The processed data are rendered in a structured, text-oriented format, styled in HTML to emulate the appearance of a terminal interface. This presentation format was also motivated by the fact that Interpreter's output is often incorporated into reports produced by cryptocurrency analysts. The final presentation, as shown in Figure 2, emphasizes clarity through color coding: increases and decreases in cryptocurrency balances are highlighted in green and red, respectively, while each cryptocurrency symbol is automatically assigned a unique randomly generated color to improve readability and quick identification. This combination of minimalistic design and color differentiation significantly improves the interpretability of transaction data and the overall user experience.

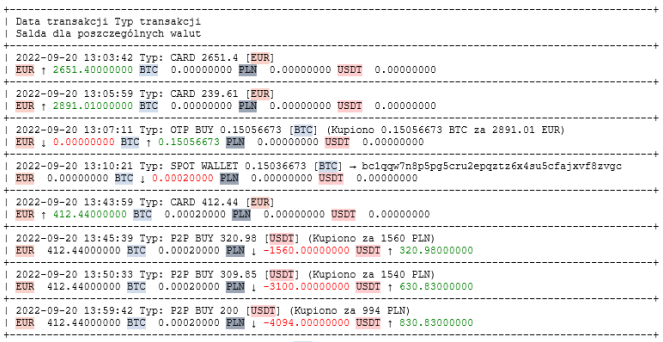

Fig. 2. The screenshot from the sample result page of the Interpreter.

The general architecture of the Interpreter tool follows a modular pipeline structure, as shown in Figure 3, designed for extensibility, transparency, and security.

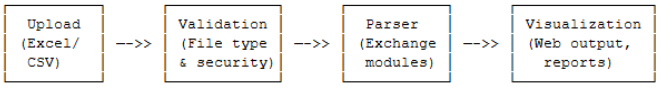

Fig. 3. System architecture of the Interpreter tool showing sequential data processing stages.

VII. Summary

Processing Heterogeneous Cryptocurrency Exchange Data for Law Enforcement is a specialized field that focuses on analyzing and investigating cryptocurrency transactions for criminal investigations. This area has gained significant importance as cryptocurrencies have become increasingly prevalent in financial crimes, presenting unique challenges for Law Enforcement Agencies due to their pseudonymous nature and rapid transfer capabilities [9]. LEA employs various computational approaches, forensic tools, and analytical methods to process cryptocurrency exchange data [10]. These include specialized blockchain analysis tools, clustering heuristics, and attribution tags to track suspicious transactions and identify criminal activities. The process involves the collaboration with legitimate cryptocurrency exchanges, which provide valuable transaction data and help identify account holders involved in suspicious activities [11] . The field faces several significant challenges, including technical complexities and the need for specialized training and expertise.

The tool, designed and made available[12] to Law Enforcement Authorities, is intended to assist blockchain investigators in the effective interpretation of data obtained from several leading cryptocurrency exchanges cooperating with Polish LEAs.

VIII. Limitations

At the current stage of development, the proposed system supports and processes data accurately originating from five cryptocurrency exchanges. Binance, Bybit, Coinbase, Kraken, and OKX. This limitation is a result of the fact that, during the author's work as a court-appointed expert in ongoing criminal proceedings, only data from these specific virtual asset service providers (VASP) were made available by the procedural authorities. Consequently, the system's data parsers and standardization logic have been tailored to the formats and structures used by these five platforms.

However, the tool has been designed with an open and modular architecture, which allows for the straightforward integration of additional data formats from other VASPs as they become available. This flexibility ensures that the system can be easily expanded and adapted to accommodate a broader range of data sources in the future.

References

[1] Chainalysis, "The 2025 crypto crime report." [Online]. Available: https://blog.chainalysis.com/reports/
[2] T. Labs, "2025 crypto crime report." [Online]. Available: https://trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
[3] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions," *Electronics*, vol. 13, no. 17, p. 3568, 2024.
[4] Wikipedia, "Binance." [Online]. Available: https://en.wikipedia.org/wiki/Binance
[5] J. M. Griffin and K. Mei, "How do crypto flows finance slavery? the economics of pig butchering," *The Economics of Pig Butchering (February 29, 2024)*, 2024.
[6] Wikipedia, "Bybit." [Online]. Available: https://en.wikipedia.org/wiki/Bybit
[7] ——, "Coinbase." [Online]. Available: https://en.wikipedia.org/wiki/Coinbase
[8] ——, "Okx." [Online]. Available: https://en.wikipedia.org/wiki/OKX
[9] MerkleScience, "How blockchain data can be leveraged by law enforcement agencies." [Online]. Available: https://www.merklescience.com/how-blockchain-data-can-be-leveraged-by-law-enforcement-agencies
[10] M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, and P. Pesch, "Safeguarding the evidential value of forensic cryptocurrency investigations," *Forensic Science International: Digital Investigation*, vol. 33, p. 200902, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619302567
[11] MerkleScience, "Strategies for law enforcement to identify and investigate crypto crimes." [Online]. Available: https://www.merklescience.com/strategies-for-law-enforcement-to-identify-and-investigate-crypto-crimes

[12] https://sydeus.rodwald.pl/interpreter