Wallet Trust Report

Address: TFoTE4QcDZzZptkdS3PXWFaS1MTnZNoiSo

Blockchain: Tron - Asset: 2 assets analysed

157,103.03
USD Balance

64
Transactions

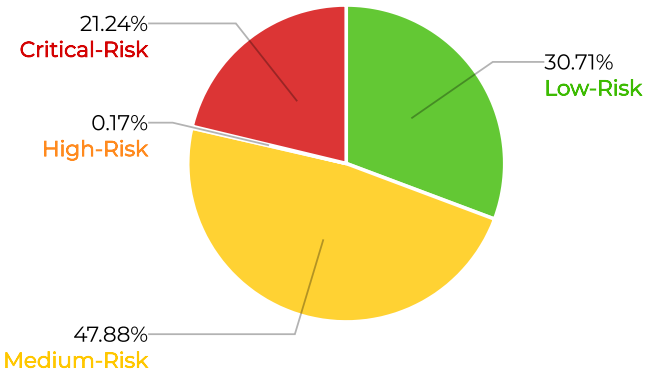
461,499.36
USD Received

304,382.75
USD Sent

Incoming

4

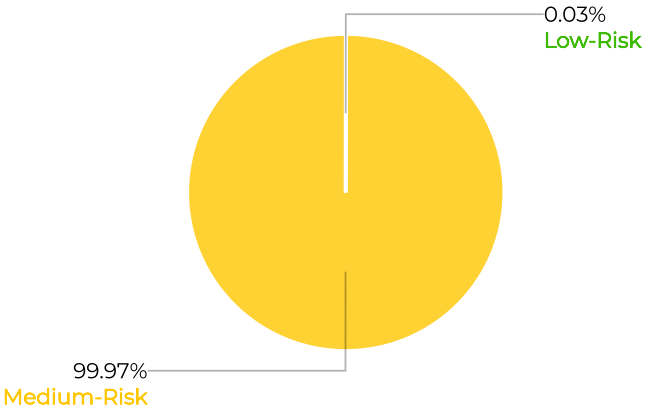
High risk
Incoming risk score



Outgoing

Medium risk
Outgoing risk score

61



AI Summary

Executive Summary

The wallet exhibits a Critical risk profile with a risk score of 4. The primary risk factor stems from significant incoming exposure to a sanctioned entity, GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC). This direct interaction with a sanctioned entity elevates the overall risk to critical, indicating potential sanctions evasion and severe compliance implications.

Wallet Profile

This wallet is currently classified as "Unknown" with an undefined classification and risk level, indicating that Scorechain has not attributed a specific identity or function to it. The risk score of 4/100 (where lower scores indicate higher risk) places the wallet in the Critical risk category. This scoring reflects the presence of highly severe risk indicators identified within its transaction history. The jurisdictional context for this wallet is global, meaning no specific national or regional regulatory framework beyond international standards is applied for its classification.

Incoming Funds Analysis

The wallet received a total of $461,499.36, with an overall incoming severity of High risk. A significant portion of incoming funds, 21.1%, originated from GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC), which is identified as a sanctioned entity. This direct exposure to a sanctioned list entity is a critical risk indicator. Other major senders include WhiteBIT.com (27.8% of flow, Low risk), Bybit.com (23.5% of flow, Medium risk), Okx.com (5.3% of flow, Medium risk), and Binance.com (4.5% of flow, Medium risk). These entities are identified as exchanges, which are typically regulated Virtual Asset Service Providers (VASPs). The exposure to GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC) is the primary driver of the High risk severity for incoming funds, as direct transactions with sanctioned entities are considered red flags for money laundering and terrorist financing activities FATF: Red Flag Indicators in the Source of Funds or Wealth: Red Flag Indicators in the Source of Funds or Wealth. The majority of senders operate in Estonia (77.7%), which is also the operational jurisdiction for the sanctioned entity. The incoming funds analysis indicates a incoming-high-risk profile due to the sanctioned entity exposure.

Outgoing Funds Analysis

The wallet sent a total of $304,383, with an overall outgoing severity of Medium risk. The outgoing funds are predominantly directed to exchanges. Binance.com received 63.4% of the sent funds, and Bybit.com received 36.5% of the sent funds. Both are classified as exchanges with a Medium risk severity. The operational jurisdictions for these recipients include the United States, Lithuania, Malta, United Arab Emirates, and Canada. While exchanges are generally regulated, the volume of funds sent to these platforms warrants standard monitoring. The outgoing funds analysis indicates a outgoing-moderate-risk profile.

Risk Assessment and Implications

Risk Level: The overall risk classification for this wallet is Critical risk. This assessment is driven by the direct and significant exposure to a sanctioned entity, GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC), which accounts for 21.1% of incoming funds.

Implications: The direct receipt of funds from a sanctioned entity, GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC), constitutes a critical compliance concern. Such transactions are red flags for potential sanctions evasion and money laundering, requiring immediate and enhanced due diligence FATF: Red Flag Indicators in the Source of Funds or Wealth: Red Flag Indicators in the Source of Funds or Wealth. Jurisdiction-specific regulations are not available in the knowledge base. Analysis is based on FATF standards and global AML best practices.

Potential Concerns: Exchanges and other VASPs are obligated to screen transactions against sanctions lists. The wallet's direct interaction with a sanctioned entity means that any VASP interacting with this wallet could flag it for sanctions exposure. This exposure presents a significant risk of being identified in illicit activity investigations.

Recommendations: The wallet owner must be aware of the severe implications of transacting with sanctioned entities. Further transactions involving GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC) are highly discouraged due to the direct sanctions exposure. Enhanced due diligence is required to understand the nature and purpose of the transactions involving this sanctioned entity.

Risk Indicators

Risk indicators identify and flag incoming or outgoing risks based on entity, behavioral, and geographical factors—refer to the appendix for details.

Incoming

Entity Type	Country
Terrorism	Lebanon
Community reported scam	Iran, Islamic Republic of
Suspicious	British Virgin Islands
Blacklisted	Bulgaria
Cross-chain Bridge Protocol	
Dex	
Gambling	
Sanction list	

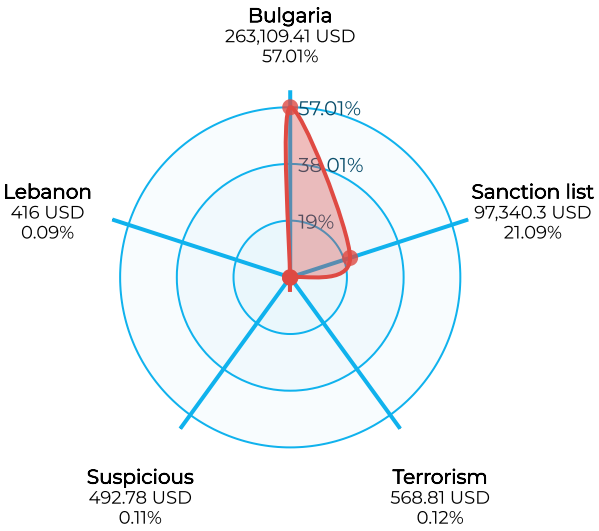
Outgoing

Country
Bulgaria

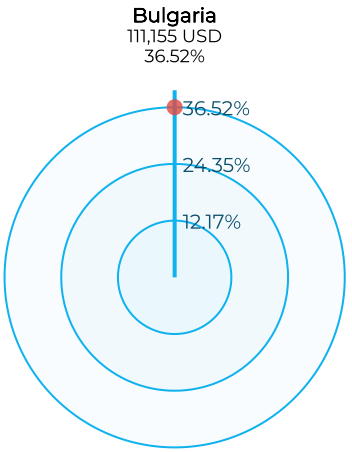
Top 5 Risk Indicators

This is the 5 bigger risk indicators exposure, shown in the percentage of the total amount of the funds the address has received/sent.

Incoming



Outgoing



Tokens balance 2 tokens

This section considers only tokens with a positive current balance.

Tether	157,024.02902 USDT 157,024.03 USD
Tron	278.778723 TRX 79 USD

Risk score details

This is the list of entities involved with this address, as senders or recipients.

Incoming

70	WhiteBIT.com Exchange	299,571.03 USD 64.91%
1	GARANTEX EUROPE OU - GARANTEX EUROPE OÜ (OFAC) Sanction list	97,430.07 USD 21.11%
50	Ignored small amounts Ignored small amounts	44,442.97 USD 9.63%
50	No entities found No entities found	18,332.84 USD 3.97%
1	Hezbollah (NBCTF ISR) Terrorism	568.81 USD 0.12%
15	Address TPqSXCF reported by Tether Blacklisted	282.68 USD 0.06%
25	OTCs in Dubai Suspicious	492.78 USD 0.11%
50	96ach.com Gambling	131.38 USD 0.03%
50	Wallet.tg Wallet	101.44 USD 0.02%
77	AlphaPo.net Payment Service Provider	80.58 USD 0.02%
60	Bridgers.xyz Cross-chain Bridge Protocol	23.85 USD < 0.01%
1	ITP Corporation - Itpro.top - Itp.club - Itpmax.com - itplb.com Scam	22.74 USD < 0.01%
75	Well Wallet Service	9.95 USD < 0.01%

Outgoing

65	Binance.com Exchange	304,255 USD 99.96%
83	Triple-A.io Payment Service Provider	91.47 USD 0.03%
50	Ignored small amounts Ignored small amounts	15.79 USD < 0.01%

Incoming

51	CryptoBot Bot	4.18 USD < 0.01%
45	Fluid.io Dex	3.38 USD < 0.01%
2	MaxTradeMarket.com Community reported scam	0.66 USD < 0.01%
95	Revolut.com Bank	0.01 USD < 0.01%

Frequently Asked Questions

How the score is calculated?

The **computed risk score** (incoming/outgoing) evaluates the **risk exposure** of an address, wallet, or transaction based on the **origin and destination of funds**. It ranges from **1 (high risk/untrusted)** to **100 (low risk/trusted)** and helps assess financial threats.

- Incoming risk score: Evaluates the risk of received funds.
- Outgoing risk score: Assesses the risk of sent funds.
- Assigned risk score: The assigned risk score is first determined by a default risk score based on the entity type. Then, a risk matrix may be applied to adjust the score according to additional risk factors.

The risk score uses a **harmonic mean formula**, where **high-risk entities** (e.g., dark web, scams) have greater impact. **Named entities** are explicitly listed, while **unnamed ones undergo recursive analysis**.

The **Scorechain algorithm** explores the **blockchain transaction history** to identify wallet addresses and assess risk based on **direct (1 hop) and indirect (≥2 hops) connections**.

- UTXO blockchains (Bitcoin, Litecoin, etc.): Up to 100 hops.
- Account-based blockchains (Ethereum, Ton, Solana, etc.): Up to 6 hops.

What are the risk indicators?

The risk indicators displayed in the report come from a default configuration designed to help users detect suspicious activities without manual setup. This setup includes predefined entity risks and geographical risks, ensuring compliance with international standards.

Full List of Entity Risks:

- Scam - Entities associated with known scams or fraudulent schemes.
- Hack - Addresses linked to hacking incidents or unauthorized data breaches.
- Phishing - Entities involved in phishing schemes aiming to steal personal data.
- Darkweb - Transactions tied to dark web marketplaces or forums.
- Sanction List - Entities flagged in international sanction databases.
- Terrorism - Transactions potentially linked to terrorist financing.
- Child Abuse - Entities suspected of involvement in child exploitation activities.
- Ransomware - Addresses linked to ransomware payments or networks.
- Seized Assets - Addresses associated with assets seized by law enforcement.

Geographical Risk: FATF Grey & Black Lists

The system also monitors transactions involving high-risk countries from the FATF Grey and Black Lists, which flag jurisdictions with deficiencies in anti-money laundering (AML) and counter-terrorism financing (CFT) regulations.

These default risk indicators ensure that transactions linked to high-risk entities or regions are automatically flagged for compliance monitoring.

For more details on the FATF Grey & Black Lists, refer to this link: Grey & Black List.

Appendix - Glossary 1/3

List of the terms used in this document and their meaning

100 **Auctioned assets**
Crypto assets that were confiscated by authorities and later auctioned, making them legally reintroduced into circulation.

100 **Unspent output**
Represents funds sent to an unnamed address/entity that remain unspent. The status changes when funds are moved or the entity is identified.

100 **Block reward**
Newly minted crypto awarded to miners for validating transactions and adding blocks to the blockchain. These assets originate directly from the network.

100 **Token minting**
The process of creating new tokens on a blockchain, increasing the total supply. Often used in DeFi, NFTs, and governance models.

100 **Token burning**
The destruction of tokens to reduce the total supply, often used for deflationary purposes or project governance.

95 **Bank**
Financial institutions engaged in crypto-related activities such as trading, custody, or conversion between crypto and fiat.

90 **Investment management firm**
Firms that manage crypto assets, offering investment strategies, portfolio management, and trading services for institutional or retail clients.

90 **Real World Asset**
Tokenized representations of financial instruments, commodities, or currencies issued by institutions and tradable via blockchain technology.

80 **Mining pool**
Groups of miners combining computational power to mine crypto more efficiently and share rewards proportionally.

80 **Token**
Blockchain-based digital assets that can represent value, ownership, or access rights, often issued via ICOs or DeFi protocols.

75 **Service**
Centralized cryptocurrency services that are not exchanges, such as lending platforms, payment processors, and custodial wallets.

70 **Staking pool**
A collective staking mechanism where users pool their crypto to increase the chances of earning rewards in Proof of Stake (PoS) networks.

65 **Decentralized service**
Non-exchange DeFi platforms, including lending protocols, yield farming services, and smart contract-based applications.

60 **Cloud mining**
A remote mining service where users lease computing power to mine cryptocurrencies without owning mining hardware.

60 **Cross-chain Bridge Protocol**
Platforms facilitating cross-chain swaps, allowing assets to be transferred between different blockchains using smart contracts.

50 **ICO**
Initial Coin Offerings used to raise funds for new crypto projects by selling tokens to investors in exchange for capital.

50 **Gambling**
Addresses associated with crypto-based gambling platforms, including casinos, betting sites, and lotteries, which pose money laundering risks.

50 **Wallet**
Self-custodial crypto wallets that allow users to store, send, receive, and interact with decentralized applications while retaining private key control.

Appendix - Glossary 2/3

List of the terms used in this document and their meaning

50 **Ongoing legal action**
Addresses linked to ongoing investigations by authorities, where legal proceedings are active but assets have not yet been seized.

50 **Peeling chain of unknown origin**
A transaction pattern used to obfuscate the source of funds by repeatedly sending small amounts through new addresses.

50 **Payment channel**
Off-chain payment channels, primarily within the Lightning Network, allowing fast and low-cost transactions before settling on-chain.

50 **Large unnamed entity**
Represents a significant entity with at least 100 addresses, impacting transaction analysis despite lacking direct identification.

50 **Ignored small amounts**
Refers to negligible transaction amounts that do not significantly impact blockchain analysis.

50 **No entities found**
Indicates that the blockchain exploration algorithm reached its limit without identifying any named entities.

50 **Large transaction**
A transaction with over 200 inputs or outputs, often indicating bulk transfers or high-volume activity.

25 **Suspicious**
Addresses flagged for potential involvement in illicit activities but lacking confirmed legal action or authoritative reports.

15 **Mixing service**
Platforms designed to mix cryptocurrencies, obscuring transaction histories and increasing privacy but often used for money laundering.

15 **Blacklisted**
Addresses restricted by stablecoin issuers due to non-compliance, regulatory violations, or suspected illicit activity.

15 **Mixing pattern**
Transactions displaying characteristics typical of coin mixing, suggesting an attempt to obscure the origin of funds.

2 **Community reported scam**
Addresses reported by the crypto community as scams, though no official enforcement action has been taken.

2 **Poisoning**
Addresses that seed look-alike addresses into victims history via dust or spoof-token transfers to induce copy-paste mistakes; detected by Scorechain similarity/timing heuristics

1 **Scam**
Addresses used in fraudulent schemes such as Ponzi schemes, phishing scams, fake giveaways, or investment frauds.

1 **Hack**
Addresses involved in cyberattacks, exploiting vulnerabilities to steal crypto assets from exchanges, protocols, or users.

1 **Phishing**
Addresses used to deceive users into revealing private keys or credentials by impersonating legitimate entities.

1 **Darkweb**
Addresses associated with dark web marketplaces, illicit services, and money laundering operations.

1 **Sanction list**
Addresses flagged by government agencies as being linked to illicit activities such as money laundering, terrorism financing, and fraud.

Appendix - Glossary 3/3

List of the terms used in this document and their meaning

1 **Terrorism**
Addresses associated with known terrorist organizations or individuals financing extremist activities.

1 **Child abuse**
Addresses linked to illegal content distribution or payments related to crimes against children.

1 **Ransomware**
Addresses used in ransomware attacks where victims must pay cryptocurrency to unlock encrypted files.

1 **Seized assets**
Crypto assets confiscated by authorities due to criminal or civil investigations.

1 **Decentralized Service**
Decentralized Service

* **Exchange**
Centralized cryptocurrency exchanges (CEXs) that facilitate trading, swapping, and staking of digital assets.

* **ATM**
Crypto ATMs allowing users to buy or sell crypto using cash or debit cards, often requiring KYC verification.

* **Payment Service Provider**
Companies facilitating crypto payments by offering transaction processing, fraud prevention, and merchant services.

* **Bot**
Automated software executing trades, managing smart contracts, or performing other blockchain tasks, with varying risk levels.

* **Donations**
Addresses used to collect crypto donations for projects, charities, or non-profits.

* **Dex**
Decentralized exchanges (DEXs) enabling peer-to-peer crypto trading without intermediaries.

* **NFT Marketplace**
Platforms facilitating the trading of Non-Fungible Tokens (NFTs), which represent unique digital assets on the blockchain.

* The risk score is calculated using a custom matrix, with no default score for this entity type. Developed by Scorechain, the matrix can be shared for more details.

Disclaimer

This Report is provided solely for informational purposes and is valid as of the date it is issued. Scorechain does not offer any explicit or implied guarantee regarding the validity of this Report beyond its date of issuance.

Scorechain commits to delivering independent, current, and accurate analysis within the Report. However, Scorechain is not accountable for any modifications in assumptions or updates to the report due to new facts or circumstances arising post-issuance, or facts that were unknown at the time the Report was generated.

Decisions made based on this Report are the sole responsibility of its recipient. Scorechain's liability is excluded to the greatest extent allowable under applicable law.

This Report does not fulfill any obligations of conducting proper internal risk assessments and/or decision-making processes. Due to the potentially high-risk nature (e.g., crime-related) of some information used in our analysis, such information may not be disclosed to the recipient. Scorechain services are delivered "as is," with all existing faults and deficiencies, without warranty of any kind. To the fullest extent permissible under law, Scorechain, along with its affiliates and their respective licensors and service providers, expressly disclaims any warranties, whether express, implied, statutory, or otherwise, including all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, as well as any warranties that might arise from the course of dealing, performance, usage, or trade practices.

Further, Scorechain makes no warranties or representations that the services will meet your requirements, achieve any intended results, be compatible with any other software, applications, systems, or services, operate without interruption, adhere to any performance or reliability standards, or be error-free, nor does it warrant that any errors or defects can or will be corrected.

Under applicable law, neither Scorechain nor any of its service providers shall be liable for any use or inability to use the services for:

A. any action or alleged action, or any lack of action or alleged lack of action, not amounting to intentional misconduct as determined by a final, non-appealable judgment by a competent court;

B. lost profits, costs of substitute goods or services, loss of data, loss of goodwill, business interruption, computer failure or malfunction, or any other consequential, incidental, indirect, exemplary, special, or punitive damages;

C. direct damages exceeding in total the amount actually paid by you for the services;

D. any claims from third parties, whether based on statute, contract, tort, or otherwise.

The aforementioned limitations apply irrespective of whether such damages arise from breach of contract, tort (including negligence), or any other cause, and regardless of whether such damages were foreseeable or Scorechain was advised of the possibility of such damages. They also cover any losses caused by the failure of the services to accurately identify participants in blockchain transactions or assess the levels of associated risks such as fraudulent activity, and you acknowledge and agree that you do not rely on the services for such determinations.