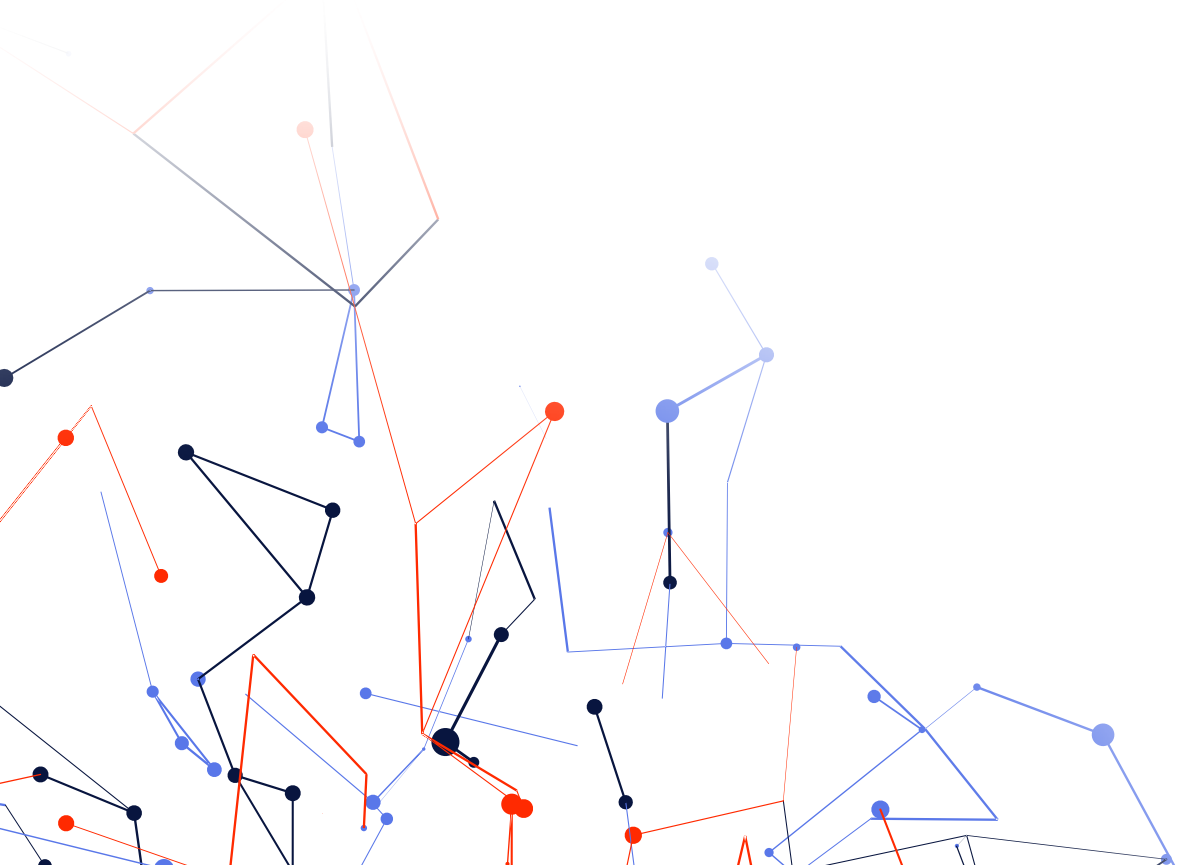
GLOBAL LEDGER

Garantex Exposure

To Top Crypto Entities



Key Highlights

- In 2024, Garantex processed **over $14.52 billion** worth of ETH, USDT, and USDC.
- Licensed VASPs processed **~57% of these funds** in 2024, while entities without licences account for 29.7%.
- **$6.51 billion** was sent to/from VASPs holding EU licences. They account for **78.8%** of all licensed entities' exposure.
- Research shows that **licensed entities are a primary target for Garantex**. This might be due to their popularity, high trading volumes, and access to bank accounts, enabling them to cash out funds into fiat.
- Garantex exposure is complex to identify, as it relies on different tactics to avoid detection. Their main goal is to **overload and outrun compliance officers.**
- Any bad actor can use these tactics to evade detection. Still, with extra effort, this behaviour **can be detected and labelled.**

Prehistory

On March 6, 2025, the U.S. Secret Service, in cooperation with international law enforcement agencies took down the website of the Russian crypto exchange Garantex. Tether took a stand against it by blocking Garantex wallets holding over 2.5 billion rubles (about $28 million).

On February 24, 2025, the EU imposed sanctions against an infamous Russian crypto exchange "closely associated with EU-sanctioned Russian banks." This move followed earlier actions by other authorities. In 2022, the US Office of Foreign Assets Control designated Garantex, and in 2023, the United Kingdom added it to its sanction notice.

Garantex has already become a haven for bad actors, facilitating illicit activities and "wilfully disregard[ing]" AML and CTF requirements.

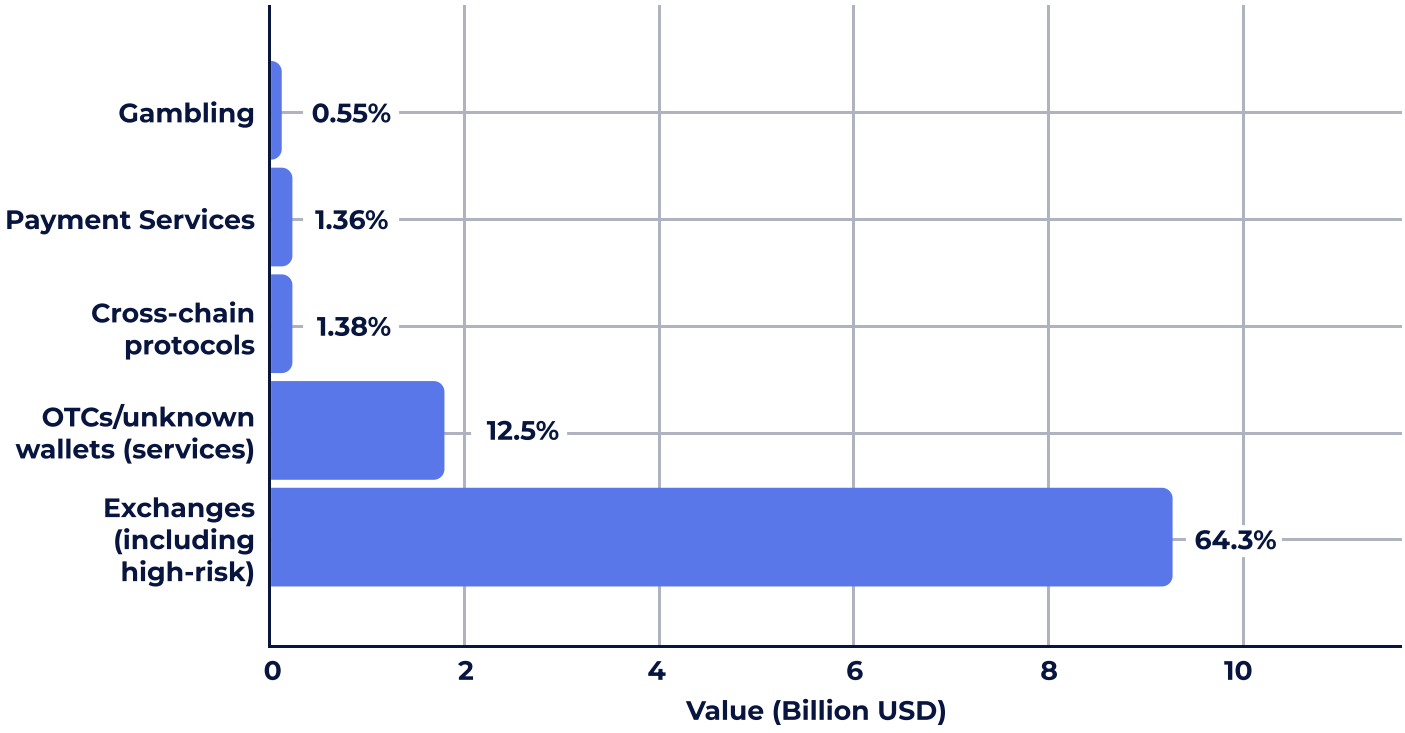
Global Ledger dove into the data and discovered its significant exposure to prominent, licensed, and regulated entities, further underscoring the risks associated with its operations.

Garantex processed $14.5B+ worth of crypto in 2024

Over 2024, Garantex processed more than $14.52 billion worth of these cryptocurrencies:

- **ETH — $112,771,909**
- **USDT (ERC-20/TRC-20) — $64,820,007**
- **USDC (ERC-20) — $14,335,583,547.**

Top 5 Types of Garantex Counterparties in 2024



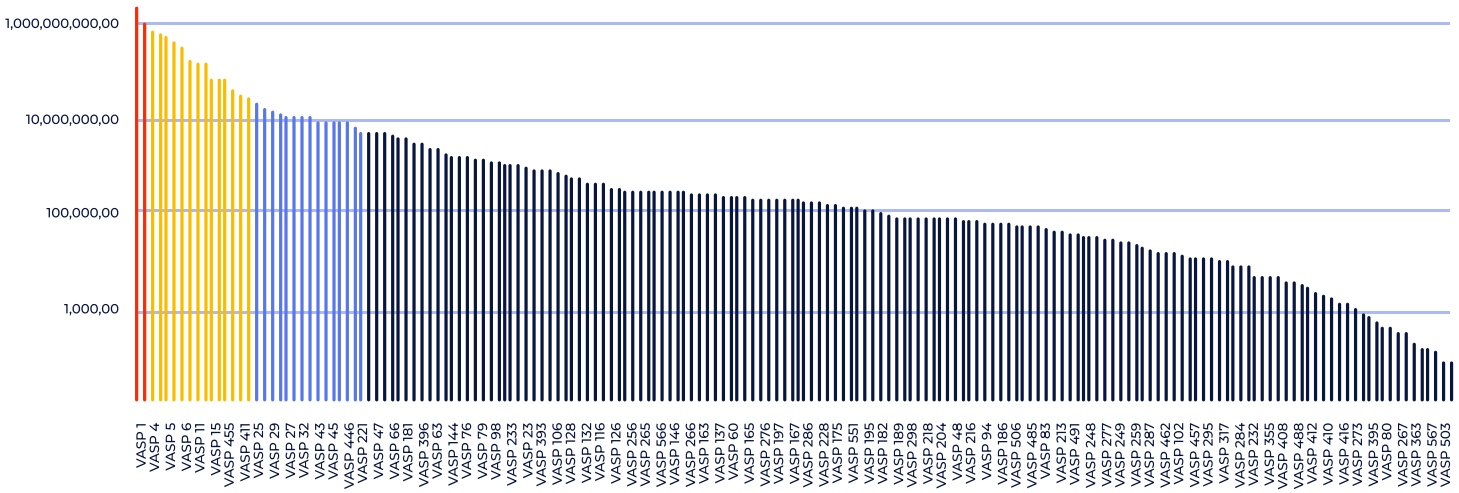
*** Out of all Garantex exposure in ETH, USDT, USDC**

Licensed VASPs processed ~57% of Garantex funds in 2024. Unlicensed account for ~29.7%

Over $11.76 billion was sent to/from 567 VASPs.

177 licensed entities (31.2% out of all VASPs) processed the biggest part of it — approximately **$8.26 billion**. This is about 70.2% of what all VASPs processed and about 57% of all funds processed by Garantex in 2024).

177 Licensed VASPs Processed $8.26B of Garantex Funds



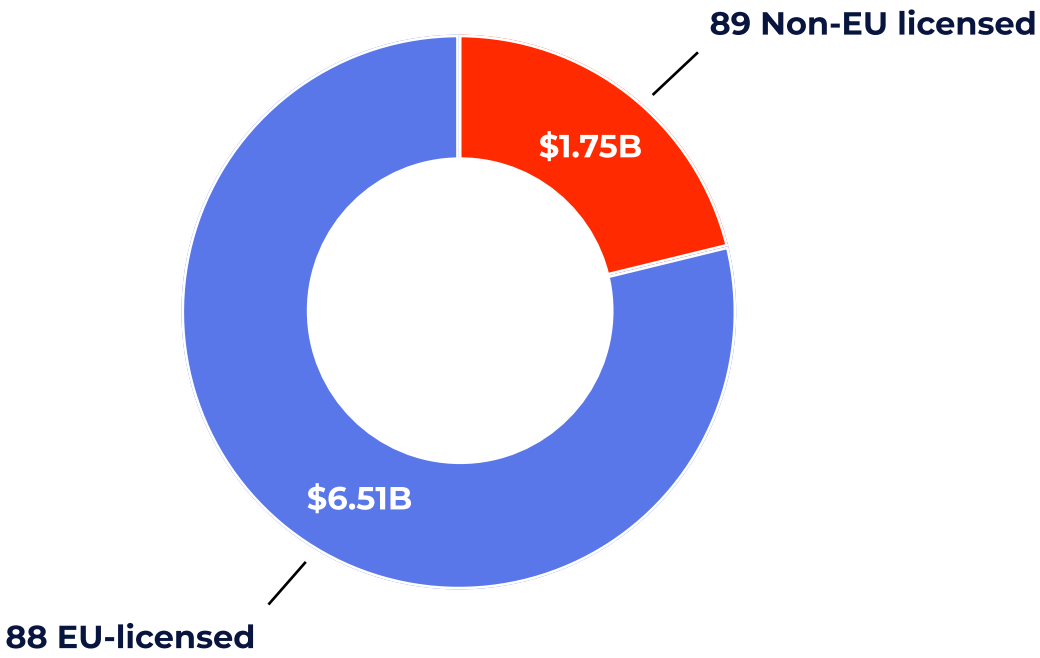
- 1 VASP with total exposure of >$2B
- 1 VASP with total exposure of >$1B
- 24 entities with total exposure of >$10M
- 28 entities with total exposure of >$1M

Meanwhile, **390 unlicensed** VASPs (68.8% out of all VASPs) processed **$3.49 billion**. It is over 29.7% of the amount processed by all VASPs and ~20.9% of total Garantex exposure).

EU-licensed entities make up 78.8% of all licensed entities' exposure

- The research shows that **$6.51 billion** was sent to/from 88 VASPs with EU licences. They account for **78.8%** of all licensed entities' exposure.
- Meanwhile, 89 entities licensed in other jurisdictions sent/received **$1.75 billion** to/from Garantex. This is **21.2%** of the total exposure of licensed VASPs.

$6.51B Sent to/from EU-Licensed VASPs



Garantex's goal is to overload and outrun compliance officers. Exposure is complex to identify

Research indicates that licensed VASPs have become a primary target for Garantex. This might be due to these CEXs' popularity, high trading volumes, and access to bank accounts, enabling them to cash out funds into fiat.

Why haven't experienced market players noticed Garantex exposure?

The complexity of identifying Garantex exposure stems from these key factors:

1 Garantex relies on various tactics to avoid detection

It's almost never a simple deposit or withdrawal. Garantex is well aware of how blockchain analytics works and uses different tactics to avoid being detected, including:

- One-time deposit wallets
- Temporary hot wallets
- Pass-through withdrawals. Pass-through transactions mean that all funds are routed through temporary, one-time-use wallets.
- Pattern changes.

The exchange's clients consciously using Garantex for their crypto operations additionally utilize cross-chain protocols, mixers, proxy services, DeFi services, and rely on small transactions. It makes the analysis even more complicated.

2 Garantex is exploiting attribution issues

- Attribution timing/speed. Delays in processing and updating data can lead to outdated or lagging insights. This means that by the time an attribution is made, the landscape of transactions may have already changed.
- Attribution quality refers to how accurately and reliably blockchain analytics can connect transactions or addresses to specific entities/individuals.

  This might be challenging, especially for TRON due to many factors:

  - TRON transactions contain minimal metadata and lack services like ENS, making it harder to link addresses to real-world entities.
  - Designed for fast, low-cost transfers, TRON experiences high-frequency activity that can obscure illicit patterns like peel chains or mixing.
  - Transactions can be nearly free when TRX is frozen for Energy/Bandwidth, complicating behavioural analysis.
  - TRON's smart contracts are widely used by mixers, gambling platforms, and decentralized exchanges. Some privacy-enhancing smart contracts on TRON make it hard to link deposits and withdrawals, hindering tracing.
  - Unlike Ethereum, Many TRON smart contracts lack clear naming conventions, making it difficult to distinguish legitimate services from laundering schemes.
  - Its frequent role as an intermediary chain adds another layer of complexity to tracing transactions.

Any illicit actors can use this model. What can we do?

Garantex and its clients take advantage of low-quality attribution and quick processing to skirt sanctions. They pair this approach with existing blockchain analytics tools and typical compliance shortcomings.

This is not only a “Garantex problem.” Any bad actor can use these tactics to evade detection.

Still, the Global Ledger research shows that with extra effort, this behaviour can be detected and labelled.

To enhance AML/CTF efforts, the following steps could be suggested:

- Strengthen risk assessment protocols
- Apply stricter measures to review transactions
- Use advanced tools to track the movement of funds
- Enhance overall risk evaluation practices.