

An abstract network diagram in the top right corner, consisting of numerous blue and red dots connected by thin lines, forming a complex web of connections.

Garantex Payout Scheme Revealed. At Least \$25M Paid Out, More to Follow

Investigation

An abstract network diagram in the bottom right corner, similar to the one in the top right, featuring blue and red dots connected by lines, representing a complex network structure.

Key highlights

- Global Ledger has identified new Garantex wallets on Bitcoin and Ethereum that had accumulated **over \$34 million** worth of crypto to continue processing customer **payouts**, despite sanctions.
- At least **~\$25 million** worth of crypto has **already been paid out** to Garantex ex-users.
- The data suggests that payouts are only in their initial phase: over **88% of ETH** is still held **in reserve**.
- Wallets used for payouts and reserves have direct exposure to **CEXs** ranked in the **top 10 on CoinMarketCap**.
- We mapped the payout system and mechanisms that make these payouts possible despite sanctions. The structure of fund flows shows **deliberate layering**: reserves → mixers/protocols → aggregation wallets → obfuscating cross-chain hops → final payout wallets.
- Ethereum payouts rely heavily on **cross-chain** obfuscation, with transfers via Across protocol, Relay.link, and Unit.

Global Ledger identified new Garantex wallets and reconstructed its payout system

On July 30, 2025, Garantex's official Telegram channel [announced](#) that they are starting payouts in BTC and ETH. The [Global Ledger](#) team has traced its payout wallets.

We have traced **over 3200 ETH** (~\$9.6 million at the time of investigation) and **more than 260 BTC** (~\$24+ million) to reconstruct its payout system and the operational schemes that sustain it.

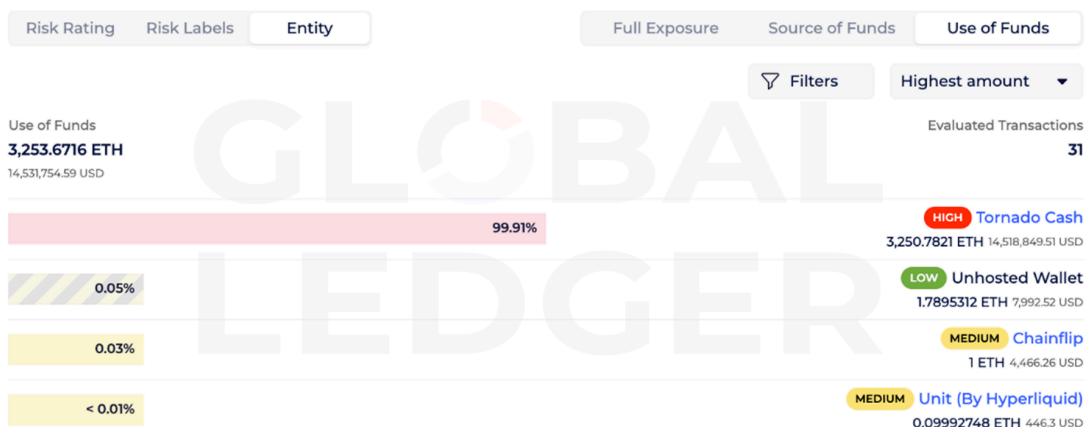
Garantex's wallet **0xbc6...5de77** accumulated a total of 3256 ETH in a single day on 06.03.2025 when Garantex's servers were [seized](#).

Garantex Untouched Reserves

Read the full investigation [here](#).

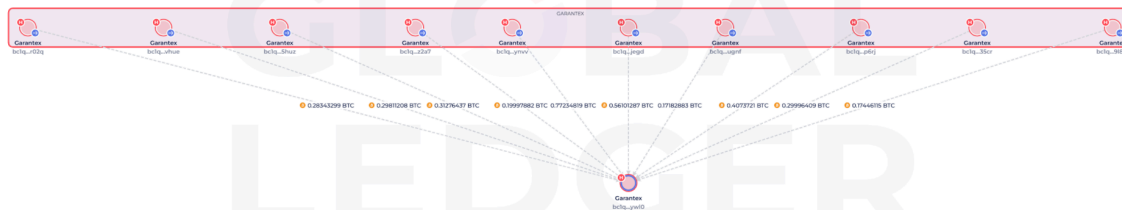
Shortly after, **99.91%** of these funds were **transferred to the Tornado Cash mixer**.

GLOBAL LEDGER Garantex transfers 99.91% of ETH reserves to Tornado Cash to obfuscate trails



Around **15.88 BTC** in Bitcoin reserves that had been dormant since 2022 began to be **consolidated** on March 17, 2025.

Dormant Garantex BTC reserves start moving on Mar 17, 2025



Notably, **2.2 BTC** were traced to the **TRON** network. On May 8, one of the paths led to **Grinex**, a service that launched operations shortly after the Garantex funds were blocked and has announced support for Tether (USDT) transactions starting from May 7.

Grinex: One More Garantex's Exchange Discovered by Global Ledger

Read the full investigation [here](#).

Over 88% of Garantex's ETH payout reserves are unspent. Payouts are just starting to roll out

Key numbers:

- 0.01% (46.15 ETH) is the volume of processed payouts.
- ~6.38% (~204.48 ETH) transferred to multiple centralized exchanges.
- < 0.01% (~1.13 ETH) transferred to Grinex through centralized exchanges and cross-chain protocols.
- ~5% (~160 ETH) transferred to multiple centralized exchanges and after — to cross-chain protocols. Preliminary, this volume is a preparation for the second iteration of payouts.

We got some on-chain details from Garantex customers

One of the Garantex customers has shared with us limited information on ETH payouts during a conversation:

Роман

last seen recently



August 1

Здоров, подскажи, тебе гара реально все битки вернула? или у тебя эфир был

10:44 PM ✓✓

здоров, эфир был

10:47 PM

весь эфир вернули, битков не было

10:47 PM

капец ну ты красавчик

10:48 PM ✓✓

прошел селфи видео всю историю да?

10:48 PM ✓✓

да, всё сделал, видосик заснял кошелёк распечатал, отправил

10:48 PM

примерно через 12 часов зачислили

10:48 PM

бля сказка просто

10:49 PM ✓✓

дыа, сам в шоке полном сидел

10:49 PM

думал затянется на пару недель

10:49 PM

а я сижу на иглах уже второй день, то же самое все сделал и говорят ждите

10:49 PM ✓✓

ну раз выплачивают, то думаю нет смысла волноваться

10:49 PM

да бля это жесь, я рассчитывал на эту выплату ,обещали и пипец

10:50 PM ✓✓

слушай а можешь скинуть скрин хотя бы что получил чтобы я хоть спал спокойно

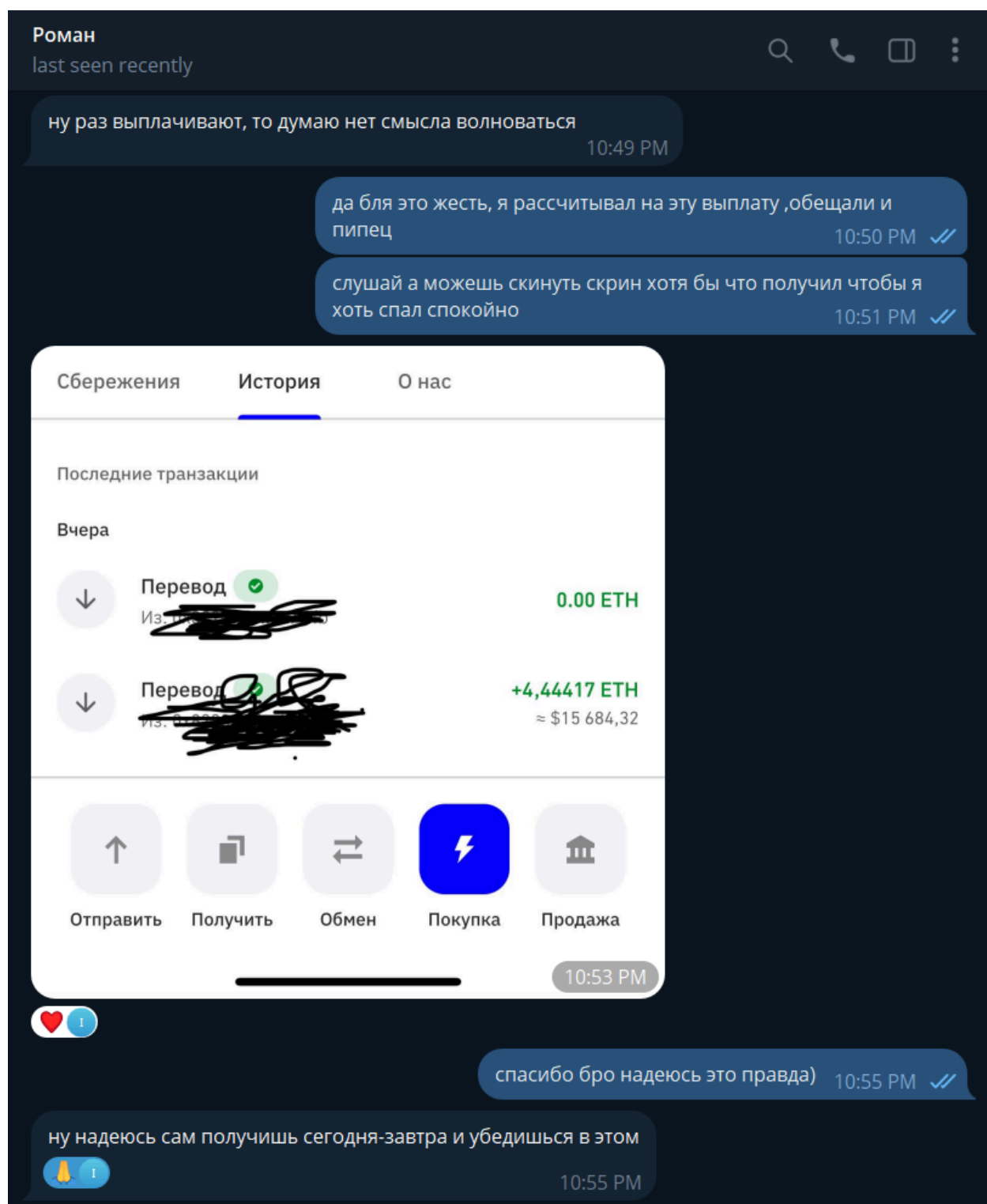
10:51 PM ✓✓

Сбережения

История

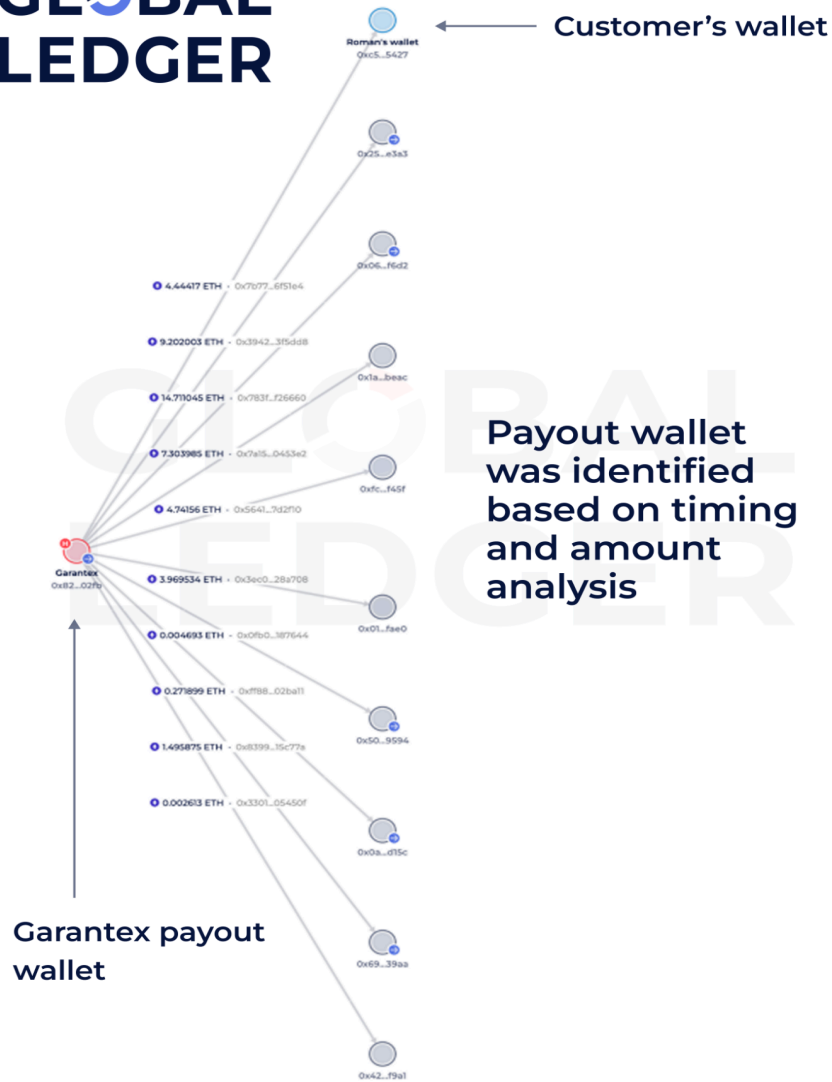
О нас





Although the original snapshot from the self-hosted wallet app was hidden, we have revealed a transaction based on a timing and amount analysis and, as a result, a payout wallet: 0x822...c02fb:

GLOBAL LEDGER



Over 20% from the Garantex payout wallet sent to one of the top CEXs

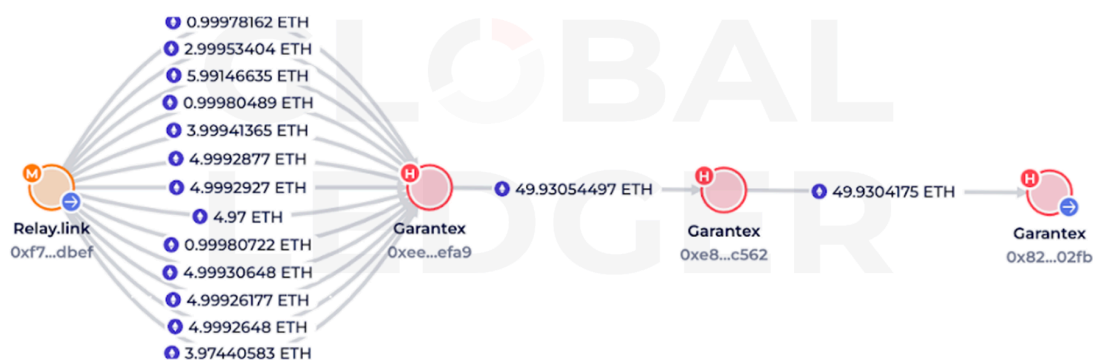


Counterparty analysis of the identified Garantex wallet

Garantex relies heavily on cross-chain protocols to hide its trail

Tracing back from the identified wallet, we identified originating transactions with a total of ~50 ETH from the [Relay.link](#) bridge.

~50 ETH sent to Garantex payout wallet from the bridge



Using this bridge's public [explorer](#), we identified incoming transactions from three Arbitrum addresses:

- 0xdb2...A83a3
- 0x314...1e028
- 0xfa0...79a06

These addresses have been used solely to obscure the trail of the funds. A review of incoming transactions shows that all came from the Optimism network via the [Across](#) protocol bridge.

To find the origin chain, we used a public [Arbiscan](#) explorer. Here is an example of how it works. The sender address on the origin chain can be found in the input data section of the transaction page using the decoder feature:

| # | Name | Type | Data |
|---|----------------------------|---------|---|
| 0 | relayData.depositor | bytes32 | 0x00000000000000000000000000000006... 1 |
| 0 | relayData.recipient | bytes32 | 0x000000000000000000000000000000f... 16 |
| 0 | relayData.exclusiveRelayer | bytes32 | 0x00000000000000000000000000000003... d |
| 0 | relayData.inputToken | bytes32 | 0x00000000000000000000000000000004... 6 |
| 0 | relayData.outputToken | bytes32 | 0x00000000000000000000000000000008... 1 |

[Switch Back](#)
[View In Decoder](#)

`relayData.depositor` field represents the ABI-encoded address, and by removing extra zeroes, we determine the address in a standard Ethereum format: `0x6ef...469C1`.

To determine the chain the funds were sent from, we checked the `relayData.originChain` field in the same section.

| | | | |
|---|-------------------------|---------|----|
| 0 | relayData.originChainId | uint256 | 10 |
|---|-------------------------|---------|----|

Chain ID 10 corresponds to the Optimism network, as defined by the Across protocol's chain ID [mapping](#).

Across Documentation

Ctrl K

V4 Developer Docs

REFERENCE

Supported Chains

Fees in the System

Actors in the System

Security Model and Verification

Tracking Events

RELAYERS

Running a Relay

Relayer Nomination

RESOURCES

Release Notes

Developer Support

Bug Bounty

Mainnet Chains

| Name | Chain ID |
|---------------------------------|----------|
| Aleph Zero | 41455 |
| Arbitrum | 42161 |
| Base | 8453 |
| Blast | 81457 |
| BNB Smart Chain | 56 |
| Ethereum | 1 |
| Ink | 57073 |
| Lens | 232 |
| Linea | 59144 |
| Lisk | 1135 |
| Mode | 34443 |
| Optimism | 10 |
| Polygon | 137 |

There are also three addresses in **Optimism** that participated in the cross-chain transfer of ~50 ETH:

- 0x6ef...469C1
- 0x178...8fA51
- 0xEA6...57A45

These addresses were also used for a single purpose — to send the assets between the chains and obfuscate the trail. But this time they were all leading **back to Ethereum** via the Across protocol [spoke pool](#).

We identified addresses on Ethereum using the same method described above, this time with a corresponding chain ID 1.

```
0 relayData.depositor bytes32 0x0000000000000000000000000000000000000000000000000000000000000000 8
```

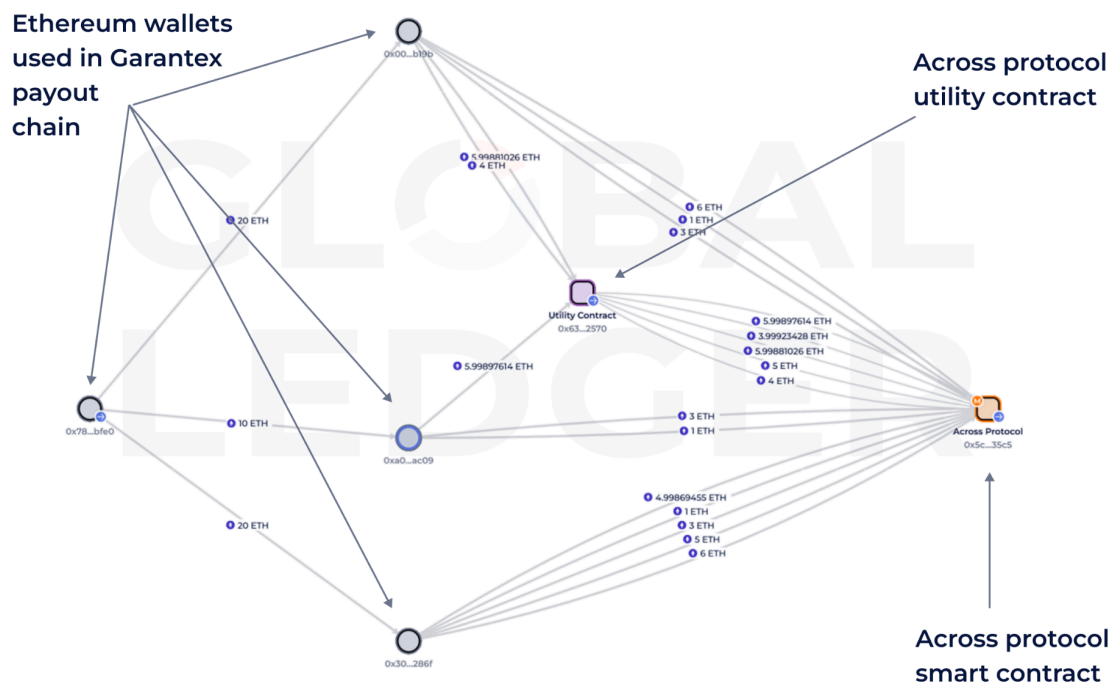
For the transfer between the Ethereum and Optimism chains, Garantex also used three addresses:

- 0x30f...4286f
- 0xa04...5ac09
- 0x007...0b19b

The following graph illustrates the combined total of 50 ETH contributed by all three wallets. After deducting transaction fees and cross-chain service costs, 49.9304175 ETH was ultimately transferred to the payout wallet 0x822...c02fb, which the user provided. The funds arrived the same day — July 30, 2025 — within just six hours of the first outgoing transaction from the wallet 0x782...6bfe0 (leftmost on the graph below).

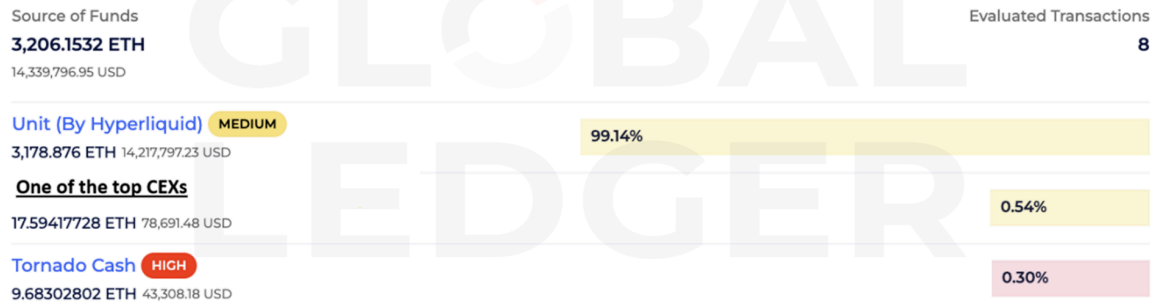
**GLOBAL
LEDGER**

Garantex uses cross-chain protocol to hide trails

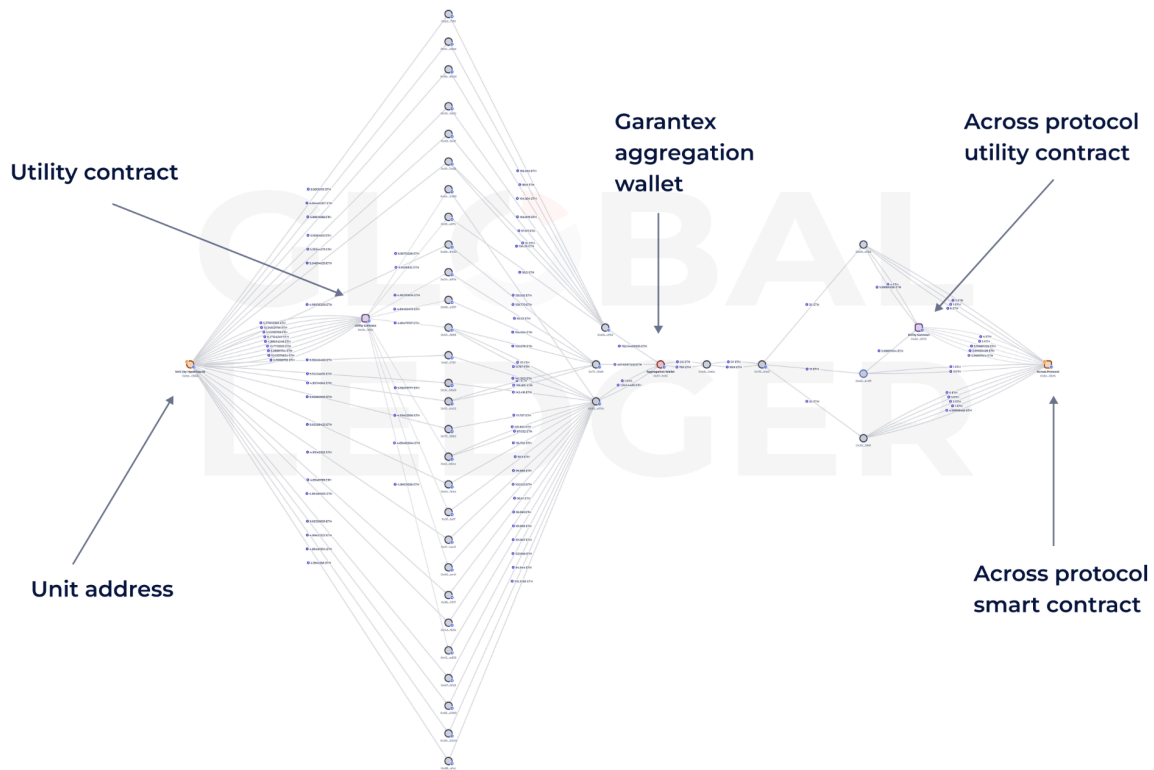


By tracing the incoming transactions to the wallet that sent 50 ETH, we identify a structure leading back to what is believed to be a single aggregation wallet for Garantex's Ethereum funds: 0x3f5...81cd2, which has accumulated **3,206.15 ETH**. 99.1% of the funds in this wallet originate from the Unit's wallet.

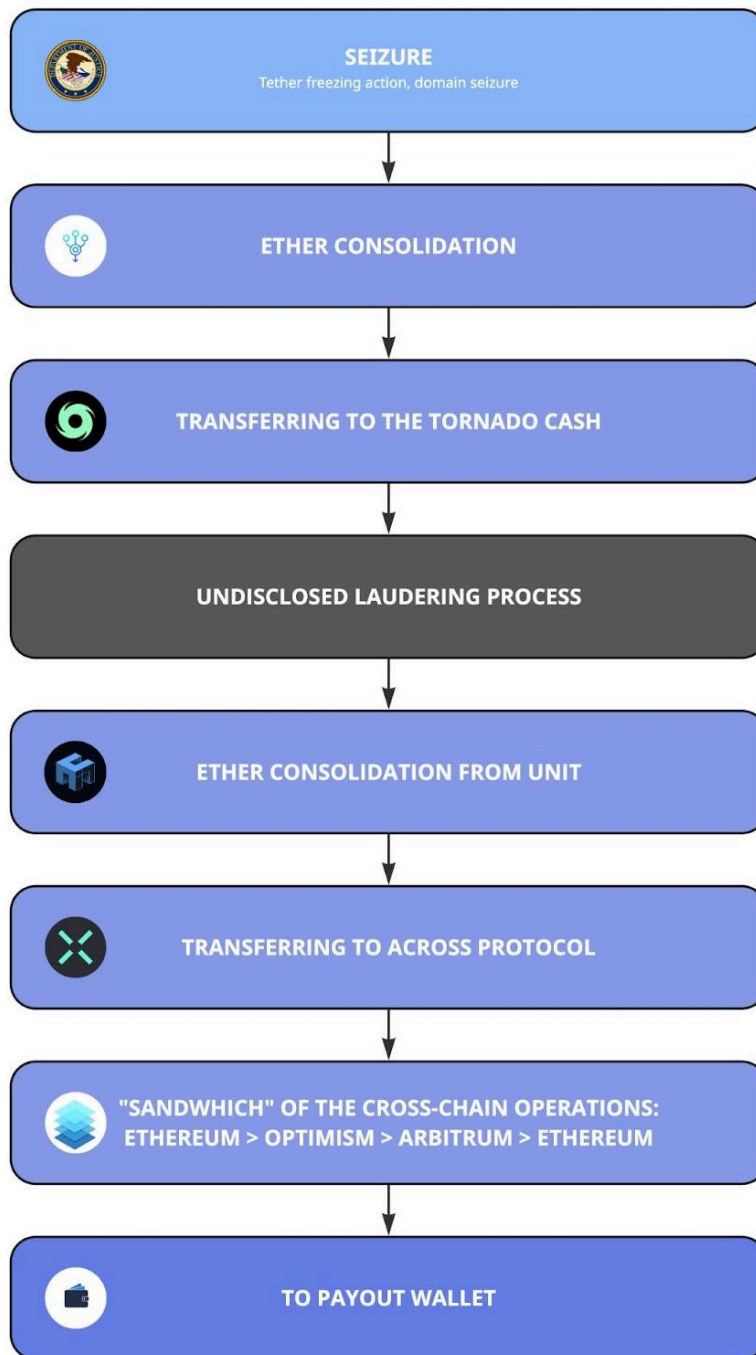
GLOBAL LEDGER 99% of funds come to Garantex aggregation wallet from DeFi protocol



Here is the flow — from Unit via a series of intermediary wallets to the Garantex aggregation wallet, and the first bridge entry. *(Only the first outgoing transactions from Unit are shown to provide a clearer overview):*



The image below shows how the scheme operated — from the moment of seizure to the identified payout wallet:



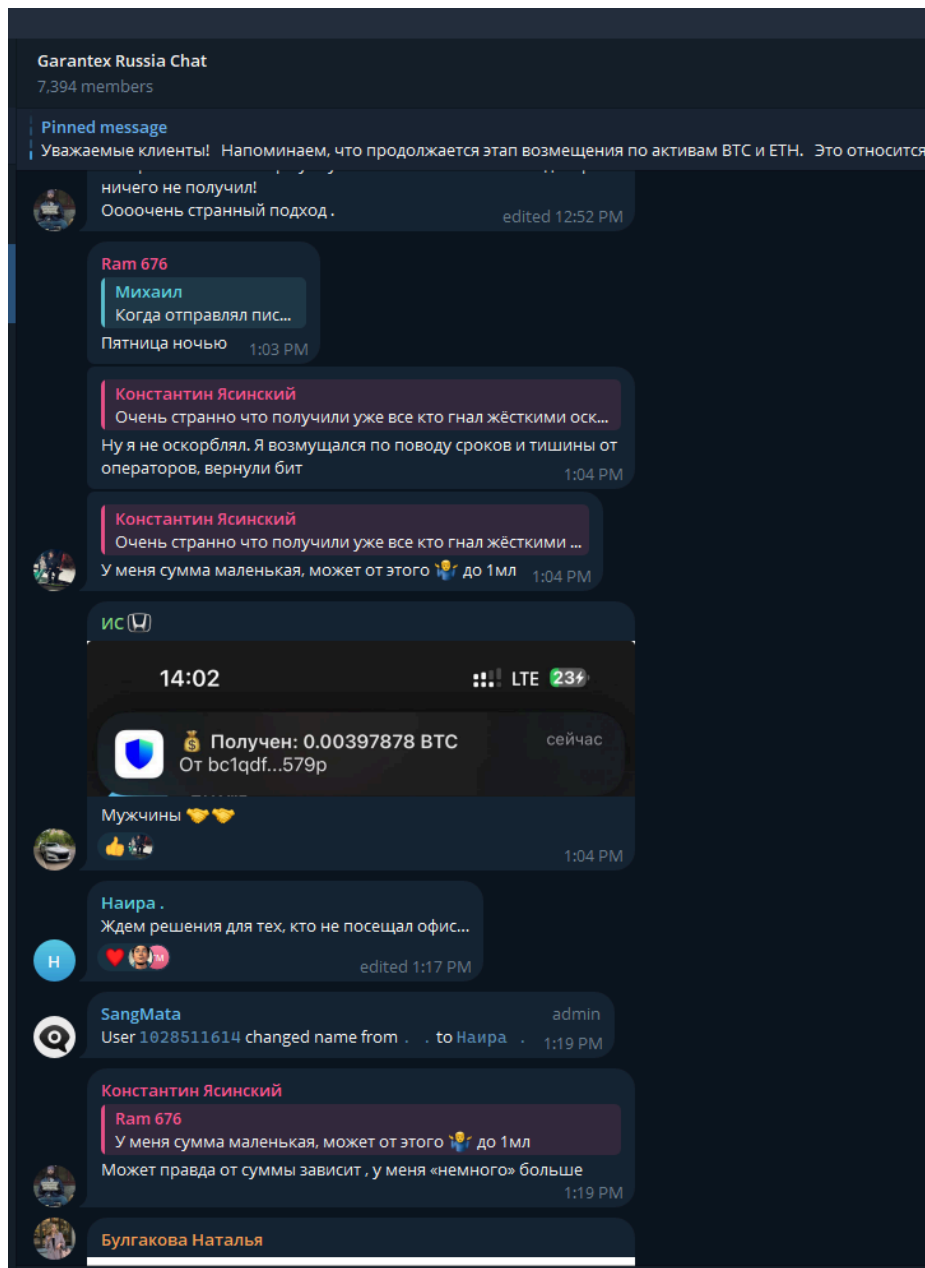
Bitcoin payout wallets lead to one of the largest CEXs

Key numbers:

- *We have identified payout wallets with a balance of 45.82 BTC.*
- *Two other wallets still hold a total of 24.52 BTC after the alleged payouts.*
- *All these wallets are linked to a payout aggregation wallet, which has received 192.63 BTC and currently holds a balance of 6.27 BTC.*
- *Several source wallets had direct exposure to one of the largest CEX's deposit address, with transaction "change" consistently redirected to it.*



We have identified payout wallets with a balance of 45.82 BTC in total and two wallets that still hold a total of 24.52 BTC

In the same Garantex-associated channels, we noticed several users mentioning that their BTC had been returned:



Even though the sending wallet was hidden we identified the Garantex BTC payout wallet using timing and amount analysis: bc1qd...l579p.

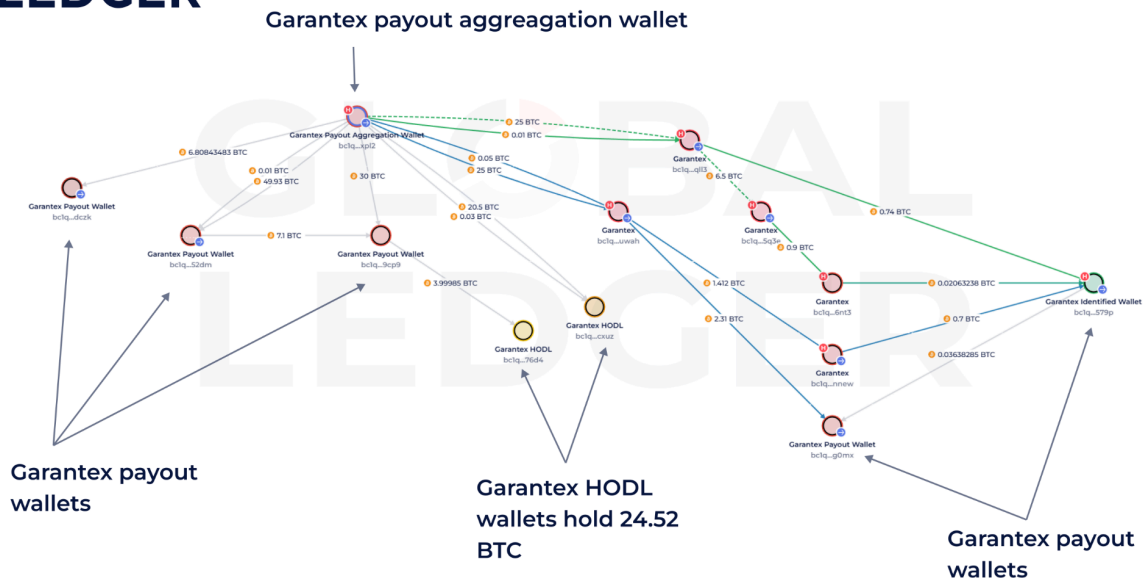
Another ex-customer who had received BTC shared a snapshot that helped us identify another Garantex BTC payout wallet: bc1q0...hnnew.

| | |
|--|--|
| Дата | Сегодня, 13:29 |
| Статус  | Выполнено |
| Отправитель |  |
| Подтверждения | 3 |

By analyzing connections between two payout wallets, we identified a direct connection between them and payout aggregation wallet bc1q6...4xpl2. The analysis of the payout aggregation wallet showed:

- The first ever transaction to this wallet was made on 28 January, 2025.
- The latest transaction to this wallet was made on 10 October, 2025.
- The total amount of received funds is 198.90 BTC.
- Its current balance is 6.27 BTC.
- We also identified other payout wallets with a total balance of 45.82 BTC:
 - bc1q6...752dm
 - bc1qp...zcxuz
 - bc1qe...5dczk
 - bc1qr...z9cp9
 - Bc1qr7...wtg0m.
- Additionally, wallets that still hold a total of 24.52 BTC appear to have accumulated those funds after the alleged payouts:
 - bc1q8...h76d4
 - bc1qp...zcxuz

Garantex BTC payout scheme



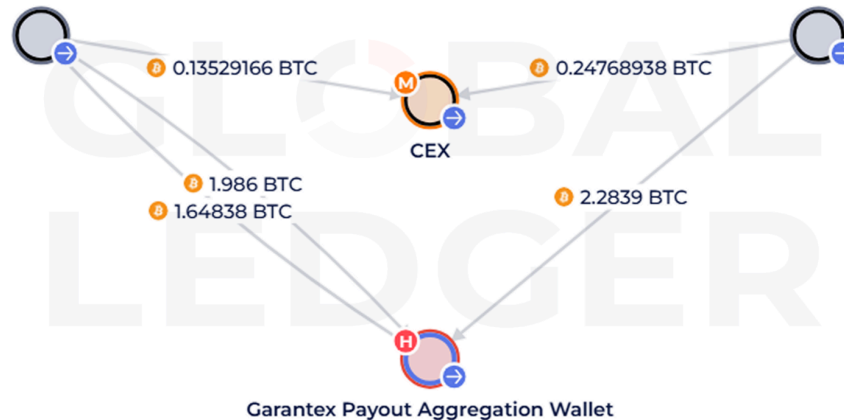
The payout aggregation wallet's traces lead to major CEXs

The payout aggregation wallet's sources of funds include CEXs, including those from the [top 10 on CoinMarketCap](#) by trading volume.

Garantex payout aggregation wallet received funds from top CEXs



We also found out that the wallets supplying the payout aggregation wallet had direct exposure to a deposit wallet of one of the largest CEX's, showing a behavioral pattern in which the "change" from supply transactions was redirected to it.



Conclusions

1. Garantex is still processing payouts despite sanctions

Even after the U.S. and EU actions, Garantex has continued distributing customer funds in BTC and ETH. The company relies on aggregation wallets and a carefully **structured payout system** to bypass restrictions.

2. Ethereum payouts rely heavily on cross-chain obfuscation

- The bulk of ETH (over 3,200 ETH) was first routed through **Tornado Cash** and **Unit**, indicating deliberate attempts to hide funds origins.
- Cross-chain transfers via the **Across protocol** and **Relay.link** were then used to move assets between Ethereum, Optimism, and Arbitrum, before reaching payout wallets.
- Only **46.15 ETH** has been distributed so far, while the majority (88%+) remains in reserve, signalling that **Ethereum payouts are still in their early stages**.

3. Bitcoin payouts are more advanced and centralised

- Two primary BTC payout wallets were identified, both linked to an **aggregation wallet** that received **198.90 BTC**.

- Additional payout and HODL wallets contain an additional **70.34 BTC**.
- Source wallets repeatedly show connections to **one of the largest CEXs**, with “change” transactions routed to its deposit address.

4. Operational behavior indicates planning and resilience

- ETH and BTC reserves that Tether could not freeze were mobilized after the March 2025 seizures.
- The structure of fund flows shows deliberate layering: reserves → mixers/protocols → aggregation wallets → obfuscating cross-chain hops → final payout wallets.
- This mirrors **classic laundering typologies** adapted for crypto environments.