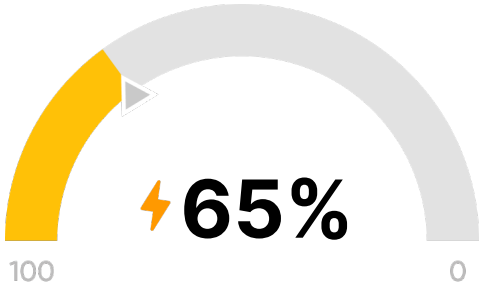
AML Risk Report

document ID 6515ECBCEB7B1522711966:000D08BDB4323D0
From 28.09.2023 21:14
Report Generation Block Height 809780
whoer.net
Fast mode

BTC Address	**3HQBsRNJcnzk4kcGxMabFMqD6Ud23T5eUd**
Balance	**0.00 (~$0.00)**
Sanction lists	**Sanction free**



Medium Risk

Balance

Total balance	**$0.00 • 0.00 BTC**
Total recieved	**$113.91 • 0.00263673 BTC**
Total spent	**$113.91 • 0.00263673 BTC**

Info

First change of balance	**7 Jan 2022 22:25 (UTC)**
Last change of balance	**7 Jan 2022 22:46 (UTC)**
Number of transactions	**2**

Danger

66.2% Gambling

⚠ Suspicious sources

24.6% Exchange | High Risk

Trusted sources

0.1% Other

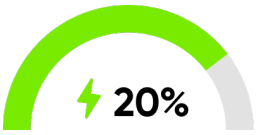
0.4% Payment Management

0.1% Wallet

8.4% Exchange

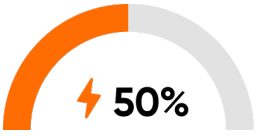
What is a Risk Score

Risk Score is a metric that estimates the likelihood that an address/transaction is related to illegal activities. The value can range from **High Risk** (max. 100%) to **Low Risk** (min. 0%).



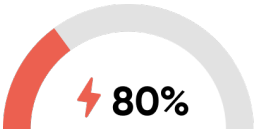
Low Risk

Transfer from the wallet should be safe.



Risk Zone

From 50% and above, there is a chance that transfers from this wallet can be blocked by centralized cryptocurrency exchanges (such as Binance, Huobi, etc.) or other reputable cryptocurrency businesses.



Extreme Danger

Transfers from this wallet have a big chance of being blocked.

Whoer Identifies 42 Money Laundering Risk Sources:

Danger

- **Child Exploitation**

  Persons associated with child exploitation.

- **Dark Market**

  Coins associated with illegal activities.

- **Special Measures**

  Entities or addresses identified by FinCEN as being of "primary money laundering concern". Countermeasures include recordkeeping, reporting requirements, and restrictions on fund transfers and account management.

  The scope may extend to similar authorities in other countries or jurisdictions as they are implemented.

- **Dark Service**

  Coins related to child abuse, terrorist financing or drug trafficking.

- **Enforcement action**

  The entity is subject to proceedings with legal authorities.

- **Fraud Shop**

  An entity that sells various types of data, including personal information, credit card information, and stolen accounts.

  Fraudulent transactions usually differ from darknet markets in their behavior, such as constant replenishment of deposits and no incoming transactions to customers.

- **Fraudulent Exchange**

  Exchanges involved in exit scams, illegal behavior, or whose funds have been confiscated by government authorities.

- **Gambling**

  Coins associated with unlicensed online games.

- **High-Risk Jurisdiction**

  The jurisdiction that is listed on the the FATF's non-cooperative list, has extensive malicious cryptocurrency activity or lacks a sophisticated regulatory environment.

  Including countries such as Iran, Venezuela, Albania and Democratic People's Republic of Korea, also known as North Korea.

- **Illegal Service**

  Coins associated with illegal activities.

- **Illicit Actor/Organization**

  An organization or physical person who directly or indirectly participates in various forms of illegal activity.

  It is often associated with such risky topics as darknet markets, fraudulent transactions, extremist financing and hacking.

- **Mixer**

  Coins that passed through a mixer to make tracking difficult or impossible. Mixers are mainly used for money laundering.

- **Ransom**

  Coins obtained through extortion or blackmail.

- **Sanctions**

  Sanctioned entities.

- **Scam**

  Coins that were obtained by deception.

- **Stolen Coins**

  Coins obtained by hijacking someone else's cryptocurrency.

- **Terrorism Financing**

  Entities associated with terrorism financing.

- **Online Pharmacy**

  Entities specializing in the illicit sale of unapproved or prescription medication. Comparable to darknet markets, but may operate on both dark and clear web, warranting a separate classification.

- **Malware**

  Addresses linked to harmful programs, including cryptojackers, which exploit host computers for mining purposes. Other malware types include clippers, botnets, trojans, and DDoS campaigns.

Suspicious sources

- **ATM**

  Coins obtained via cryptocurrency ATM operator.

- **DEX**

  The blockchain application that facilitates cryptocurrency and token trading through automated smart contracts.

  Trades on the decentralized platform are peer-to-peer and have no third party or central authority other than the smart contract that executes the trades, making it a popular money laundering tool among malicious actors.

- **Exchange | High Risk**

  An entity becomes high-risk based on the following criteria:

  No KYC: Requires absolutely no customer information before allowing any level of deposit/ withdrawal, or makes no attempt to verify that information.

  Criminal Connections: Criminal charges against the legal entity in connection with AML/CFT violations.

  Impact: High exposure to risky services such as darknet markets, other high-risk exchanges, or blending is defined as a service whose direct high-risk exposure differs by one standard deviation from the average of all identified exchanges over a 12-month period.

  Jurisdiction: based in a jurisdiction with weak AML/CFT measures.

  Unlicensed: Does not have any specific license to trade cryptocurrencies.

- **Infrastructure as a Service**

  The organization that offers computing and information services, including but not limited to VPNs, VPS and domain registrations.

  It could potentially represent a payment to privacy-focused providers that could be used for illicit purposes, but at the same time could represent a payment to completely legitimate business provider.

- **Lending Contract**

  The blockchain application that allows users to peer-to-peer lend and borrow crypto assets peer-to-peer without interacting with a third party or central authority.

- **Liquidity Pools**

  Smart contracts where tokens are locked up to provide liquidity.

- **P2P Exchange | High Risk**

  The organization does not have any special license to conduct business related to the provision of cryptocurrency exchange services, when participants exchange directly with each other, without intermediaries.

  It also includes entities that are licensed but located in listed jurisdictions, are listed as non-cooperating companies by the FATF, or do not provide KYC for large-value transactions, making them attractive for money laundering.

- **Privacy Protocol**

  A protocol or entity that uses privacy features, such as zero-knowledge proofs, to provide users with privacy features.

  Ensuring transparency of transactions, but at the same time, the addresses of counterparties remain hidden.

  This feature is the default behavior of many privacy-protecting cryptocurrencies such as Monero and Secret, meaning that gaining access to these assets does not necessarily mean that funds have been mixed or deliberately obfuscated.

- **Smart Contract**

  Blockchain functionality that functions like a self-executing contract, with the terms of the agreement between buyer and seller written directly into lines of code, executable without the need for a third party.

- **Token Smart Contract**

  The crypto asset that is built on another blockchain and that can be sent and received using a crypto wallet.

  There are various technical standards of agreed rules that guide the design, development, behaviour and operation of the given token.

- **Unnamed Service**

  The category refers to currently unidentified clusters that exhibit the behavior expected of a service, by a large number of addresses and transactions.

Trusted sources

- **Exchange**

  The organization allows users to buy, sell and trade cryptocurrencies by holding trading licenses that include the following aspects of the services:
  — Depository, brokerage or other related financial services that provide exchange services where participants interact with a central party.

  And does not include:
  — Licenses for non-specific financial services and jurisdictions included in the FATF non-cooperative list.

  They represent the most important and most used category of entities in the cryptocurrency industry, accounting for 90% of all funds sent through these services.

- **ICO**

  The organization that crowdfunds its project by selling their newly minted cryptocurrency to investors in exchange for fiat currency or more common cryptocurrencies such as Bitcoin and Ether.

  There are many legitimate examples of these offerings, but also many cases where bad actors raise funds through ICOs, then they take the money and disappear.

- **Marketplace**

  Coins that were used to pay for legal activities

- **Merchant Services**

  The entity that allows businesses to accept payments from their customers, also known as payment gateways or payment processors.

  It often faciliates conversions to local fiat currency and clearing the funds into the merchant's bank account.

- **Miner**

  Coins mined by miners and not forwarded yet.

- **Other**

  Coins obtained through airdrops, token sales or other means.

- **P2P Exchange**

  The entity is licensed to conduct a business that is specific to providing cryptocurrency exchange services where participants exchange directly with each other, without a middleman.

  It does not include non-specific financial services licenses and jurisdictions that are on the non-cooperative FATF list.

- **Payment Processor**

  Coins associated with payment services.

- **Seized Assets**

  Crypto assets seized by the government.

- **Wallet**

  Coins stored in verified wallets.

- **Bridge**

  Entities enabling the transfer of value across different blockchains. These connections allow the movement of assets without trading them, differentiating bridges from decentralized exchanges.

- **NFT Platform - Collection**

  Assemblages of NFTs on platforms dedicated to their issuance, trade, and sale. Classified by their real-world purpose, despite similarities to smart contracts or decentralized exchanges.

Disclaimer

This Report is for information purpose only and is valid on the date of its issuance.

Whoer does not give any express or implied warranty to the validity of any Report after the date of its' issuance.

Whoer takes all steps necessary to provide an independent, up-to-date analysis and accurate information in the Report.

Whoer is not liable for any changes in assumptions and updates to this report in case of new facts or circumstances occurring after the date of the Report or facts that were not known to Whoer at the time of generation of this Report.

Any decision taken by the recipient of this Report is made solely on their own risk. The liability of Whoer is hereby excluded to the fullest extent permitted by the applicable law.

The Report does not discharge any obligation of proper internal risk assessment and/or decision making process. Certain information, due to high risk (e.g. crime related), used for analysis, may not be able to be disclosed to the recipient. Whoer services are provided to you "as is" and with all faults and defects without warranty of any kind. To the maximum extent permitted under applicable law, Whoer, on its own behalf and on behalf of its affiliates and their respective licensors and service providers, expressly disclaims all warranties, whether express, implied, statutory or otherwise, with respect to Whoer services, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and warranties that may arise out of course of dealing, course of performance, usage or trade practice.

Without limitation to the foregoing, Whoer provides no warranty or undertaking, and makes no representation of any kind that the services will meet your requirements, achieve any intended results, be compatible or work with any other software, applications, systems or services, operate without interruption, meet any performance or reliability standards or be error free or that any errors or defects can or will be corrected.

To the fullest extent permitted by applicable law, in no event will Whoer services, or any of its respective service providers, have any liability arising from or related to your use of or inability to use the services for:

a) any act or alleged act, or any omission or alleged omission, that does not constitute wilful misconduct by Whoer, as determined in a final, non-appealable judgment by a court of competent jurisdiction;

b) lost profits, cost 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 in amounts that in the aggregate exceed the amount actually paid by you for the services;

d) any third-party claims (whether based in statute, contract, tort or otherwise).

The foregoing limitations:

a) will apply whether such damages arise out of breach of contract, tort (including negligence) or otherwise and regardless of whether such damages were foreseeable or Whoer was advised of the possibility of such damages; and

b) include any loss caused by the failure of the services to correctly identify participants in blockchain transactions or the levels of any associated risks such as fraudulent activity, and you acknowledge AND AGREE THAT YOU DO NOT RELY ON THE SERVICES FOR SUCH PURPOSES.