March 12, 2026

EXCHANGE PROFILE

Nobitex

Entity type:
Decentralized exchange

Year established:
2017

Volume:
USD 5 billion from 2025 – March 2026

Founder:
Amir Rad

Base of operations:
Iran

Sanctions details:
Not directly sanctioned; however, sanctioned individuals are directly affiliated with and transact with Nobitex

Background

Nobitex is Iran's largest digital asset platform and the central hub of the country's crypto ecosystem, with approximately USD 5 billion in observed volume from 2025 to the present. It serves both as a retail gateway for ordinary Iranians seeking access to foreign currency and as a key component of Iran's financial infrastructure, facilitating cross border value transfers outside traditional banking channels.

Given its scale, reach, and integration into Iran's economy, Nobitex is one of the most consequential exchanges operating within a comprehensively sanctioned jurisdiction. In a country largely cut off from the global financial system, the platform plays a significant role in enabling liquidity, settlement, and capital movement.

Nobitex also employs sophisticated operational techniques to manage liquidity, reduce transaction costs, and obscure the origin and destination of customer funds when interacting with global services. These behaviors are common for exchanges operating in heavily sanctioned environments. Details regarding aspects of these operational methods became public following a hack and leak operation in 2025, offering rare insight into how a major exchange adapts to sustained sanctions pressure.

Understanding Nobitex is essential to understanding how crypto functions within Iran's broader economic and geopolitical strategy during periods of escalation and conflict.

2025 hack showed Nobitex inner workings

In June 2025, Israel-linked hacking group Predatory Sparrow breached Nobitex, resulting in the loss of approximately USD 90 million in digital assets. TRM's on-chain analysis following the breach showed rapid movement of compromised funds across chains, along with defensive repositioning of assets. Shortly after the breach, attackers published Nobitex's internal source code, configuration files, and system documentation.

The leaked materials exposed a complex internal architecture that prioritized liquidity, operational resilience, and obfuscation. Nobitex operated a multi-tier custody model with distinct hot wallet, warm wallet, and cold wallet layers, each governed by separate services and APIs. Asset movement depended on orchestration logic across internal services, approval flows, and automated routing rules. Notably, the documents revealed Nobitex had designed infrastructure to discreetly process high-value, VIP transactions for politically connected or high-risk clients — establishing rules distinct from those for general users.

The hack revealed how ownership records, withdrawal logic, and internal ledger reconciliation were distributed across both on and off-chain systems. While this design mirrors patterns used by global exchanges, the Nobitex implementation showed additional layers specifically designed to minimize the impact of sanctions and external monitoring. Additionally, Nobitex explicitly outlines in the documents that the structures are designed to defeat US regulatory bodies.

In the aftermath of the hack, incoming transaction volumes dropped by more than 70% year over year. However, Nobitex resumed service in stages beginning in late June, aided in part by reserves held in bitcoin, including funds consolidated from previously dormant mining-linked wallets.

TRM analysis of on-chain data shows that a newly created bitcoin address associated with the exchange received approximately USD 2.7 million from more than 100 previously dormant mining-linked wallets over a 10-day period following the June 2025 hack. These wallets had accumulated rewards in 2021 and 2022 and had not previously transferred funds. The majority of upstream flows appear to trace back to two large global mining pools, EMCD and ViaBTC. The timing of this activity — immediately after the incident and shortly before withdrawals were reportedly restored — suggests the funds were likely mobilized to help the exchange survive a period of acute operational stress.

Leadership links to the Iranian regime

TRM analysis reveals that Seyed Mohammad Aghamir likely plays a senior leadership role within Nobitex's blockchain and transaction infrastructure, based on open-source reporting, sanctions records, and analysis of leaked internal Nobitex source code following the June 2025 breach.

Open source information consistently identifies Aghamir as Nobitex's blockchain lead, while US Treasury sanctions designations confirm his senior role within Iran's cyber governance apparatus. This assessment is strengthened by review of internal Nobitex code and documentation released by the Predatory Sparrow hack, which revealed centralized control over high-value and VIP transaction flows and identified oversight functions that align with Aghamir's publicly reported role. Many senior Nobitex executives have familial and/or personal ties to Iranian officials at the highest levels of the regime.

Little is known about Nobitex's CEO and founder Amir Rad aside from his educational background and position with the exchange.

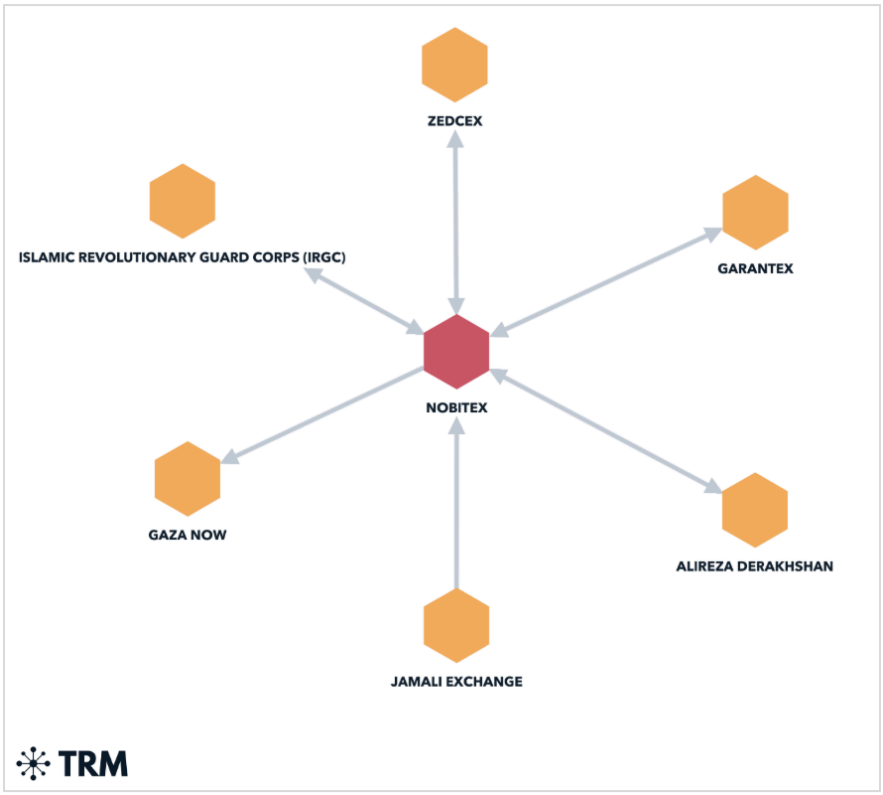
Operational model and on-chain footprint

Since 2019, TRM has observed Nobitex process tens of billions of dollars in total transaction volume, serving millions of users and supporting activity across Bitcoin, Ethereum, TRON, and other major networks. For many Iranian users, Nobitex represents the primary on-ramp and off-ramp between local currency systems and global crypto markets.

Over time, Nobitex has emerged as a recurring nexus point in blockchain tracing connected to Iranian regime linked activity.

Nobitex has emerged in TRM analysis as a recurring nexus point for Iranian regime-linked crypto activity, including flows associated with entities connected to the Islamic Revolutionary Guard Corps (IRGC), recently sanctioned exchange Zedcex, and regime financiers Alireza Derakhshan and Arash Estaki Alivand.

Nobitex plays a critical role as a node in a larger shadow economy of sanctioned countries and entities and the tools they create to access foreign currencies, using crypto as a settlement rail. Offshore networks and domestic Iranian exchanges like Nobitex work together — shell companies, brokers, Russian and Venezuelan intermediaries, and Chinese suppliers form one broader ecosystem.



Nobitex has extensive on-chain exposure to other sanctioned entities such as Russian exchange Garantex, BitPapa and cross-border settlement platform A7, as well as foreign terrorist organizations Hamas (through sanctioned fundraising network Gaza Now) and Palestinian Islamic Jihad (PIJ).

Law enforcement and regulatory response

- Nobitex is Iran's largest domestic cryptocurrency exchange and is subject to broad US, EU, and UK sanctions by virtue of Iran's status as a comprehensively sanctioned jurisdiction — meaning transactions involving Nobitex carry sanctions exposure regardless of any specific entity designation.
- On February 14, 2024, the United States Treasury sanctioned entities connected to Iran's central bank digital currency (CBDC) program, but did not sanction Nobitex itself.
- In June 2025, Israel's NBCTF issued Administrative Seizure Order ASO22/25 targeting two Nobitex-associated cryptocurrency wallets (0x53b9B72DC6f96Eb4B54143B211B22e2548e4cf5c and 0xE3740C1B2FcDA407027E2c80906306604E5260e7),designating them as entities of interest related to terrorism financing.