正本

中華民國證券投資信託暨顧問商業同業公會　函

地址：10459台北市中山區長春路145號3樓
承辦人：吳佩桂
電話：(02)2581-7288#209
傳真：(02)2581-7388
電子信箱：Bianca.Wu@sitca.org.tw

104
台北市中山區南京東路3段77號3樓之1

受文者：大宇國際證券投資顧問股份有限公司

發文日期：中華民國115年6月23日
發文字號：中信顧字第1150053029號
速別：普通件
密等及解密條件或保密期限：
附件：如文

主旨：函轉金融監督管理委員會證券期貨局檢送有關美國財政部外國資產管制辦公室(OFAC)制裁伊朗多家數位資產交易所及其高階主管等相關資料，請會員公司依說明二、三辦理，請查照。

說明：

一、依據金融監督管理委員會證券期貨局115年6月18日證期(券)字第1150346825號函辦理。

二、請持續關注及更新相關制裁資訊，注意相關交易之風險，並採取適當控管措施。如發現疑似洗錢或資恐(資武擴)之情形，應向法務部調查局申報。

三、對於依「資恐防制法」第4條第1項或第5條第1項指定制裁之個人、法人或團體，應依同法第7條規定辦理。

正本：本公會各投信會員公司、本公會各投顧會員公司
副本：

理事長 尤路文

檔　號：
保存年限：

金融監督管理委員會證券期貨局　書函

機關地址：106237臺北市大安區新生南路1段85號
承辦人：鄭先生
電話：02-27747266

受文者：中華民國證券投資信託暨顧問商業同業公會（代表人尤昭文）

發文日期：中華民國115年6月18日
發文字號：證期(券)字第1150346825號
速別：普通件
密等及解密條件或保密期限：
附件：如文(附件1 115UJ05059_1_18100424351.pdf、附件2 115UJ05059_2_18100424351.pdf、附件3 115UJ05059_3_18100424351.pdf)

主旨：檢送美國財政部外國資產管制辦公室(OFAC)制裁伊朗多家數位資產交易所及其高階主管等相關資料，請轉知所屬會員依說明二、三辦理，併請副本收文者配合辦理，請查照。

說明：

一、依據駐美國代表處經濟組115年6月3日經美字第1150000605號函副本辦理。

二、請持續關注及更新相關制裁資訊，注意相關交易之風險，並採取適當控管措施。如發現疑似洗錢或資恐(資武擴)之情形，應向法務部調查局申報。

三、對於依「資恐防制法」第4條第1項或第5條第1項指定制裁之個人、法人或團體，應依同法第7條規定辦理。

正本：中華民國證券商業同業公會（代表人陳俊宏）、中華民國期貨業商業同業公會（代表人詹正恩）、中華民國證券投資信託暨顧問商業同業公會（代表人尤昭文）、中華民國會計師公會全國聯合會（代表人張威珍）、中華民國虛擬通貨商業同業公會(代表人鄭光泰)
副本：臺灣證券交易所股份有限公司（代表人林修銘）、財團法人中華民國證券櫃檯買賣中心（代表人簡立忠）、臺灣期貨交易所股份有限公司（代表人吳自心）、臺灣集中保管結算所股份有限公司（代表人林丙輝）、元大證券金融股

裝　訂　線

中華民國證券投資信託暨顧問商業同業公會 （代表
1150053029　115/06/18

份有限公司（代表人吳杰）(均含附件) 115/06/18 10:10:10

裝

訂

線

U.S. DEPARTMENT OF THE TREASURY

Economic Fury Targets Iran's Largest Digital Asset Exchange for Terror Finance and Sanctions Evasion

June 2, 2026

WASHINGTON—Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated **Nobitex**, Iran's largest digital asset exchange, along with three other Iranian digital asset exchanges, as part of Economic Fury and the Trump Administration's efforts to eliminate the threat posed by the Iranian regime.

"While Iran's economy is in free fall, the regime has chosen to co-opt digital asset technologies for its own corrupt agenda, including evading sanctions and transferring wealth out of the country. Iran's current economic chaos is proof that President Trump's maximum pressure campaign has been a success," said **Secretary of the Treasury Scott Bessent.** "As promised, Treasury will continue to follow the money in support of Economic Fury, whether it is through the banking system or through digital assets, to prevent the regime from developing a nuclear weapon."

Nobitex has provided significant support to the regime, processing more than 50 percent of all Iranian digital asset inflows in 2025 and facilitating payments tied to Iran's terrorist activities, sanctions evasion efforts, and Islamic Revolutionary Guard Corps (IRGC)-linked transactions, including activity associated with IRGC-affiliated ransomware actors. Nobitex also helped the Central Bank of Iran access hundreds of millions of dollars in stablecoins used to prop up the plummeting value of the Iranian rial, while enabling regime insiders to access international digital asset exchanges and evade sanctions across multiple jurisdictions. Following the commencement of U.S. combat operations in Iran, Nobitex played a role in protecting and moving assets and funds out of Iran to shield regime wealth despite internet blackouts. OFAC today also designated **Amir Hossein Rad**—Nobitex's chairman, co-founder, and former CEO—as well as numerous other Nobitex leaders and officials.

Today's action is being taken pursuant to the counterterrorism authority, Executive Order (E.O.) 13224, as amended, as well as E.O. 13902, which targets persons operating in Iran's financial sector, among other economic sectors. It continues the robust sanctions campaign in support of Economic Fury and in furtherance of the strategy outlined in the President's National Security Presidential Memorandum 2 (NSPM-2), instituting a campaign of maximum economic pressure on Iran. For more information on sanctions risk associated with Iranian digital asset exchanges, please see FAQ 1250 and FAQ 1257. Additionally, the U.S. Department of State's Rewards for Justice (RFJ) program is offering a reward of up to $15 million for information leading to the disruption of the financial mechanisms of Iran's IRGC and its various branches. More information is available on the RFJ website.

ECONOMIC FURY DELIVERS MAXIMUM PRESSURE ON IRAN

The Treasury Department is maintaining maximum pressure on Iran and targeting the regime's ability to generate, move, and repatriate funds. Treasury is aggressively advancing Economic Fury and has disrupted tens of billions of dollars' worth of revenue from being otherwise accessible to the Iranian regime and its proxies. This includes actions that have led to the freezing of nearly half a billion dollars in regime-linked cryptocurrency. In addition, Treasury has cracked down on Tehran's global shadow banking networks; designated networks supplying weapons and other military components to Iran; sanctioned a corrupt Iraqi official who has facilitated the sale of oil along with Iran-backed militias operating in Iraq; taken numerous actions against Iran's terrorist proxies; and targeted shadow fleet vessels, companies, and other entities that sustain Iran's illicit oil industry.

Through the blockade, the Trump Administration is directly targeting the regime's primary revenue stream. Any person or vessel facilitating the illicit trade of oil or other commodities, through covert trade or financial channels, risks exposure to U.S. sanctions.

Treasury will continue to vigorously target both traditional sanctions evasion schemes and the exploitation of digital assets while continuing to freeze funds stolen from the Iranian people. Treasury is also prepared to take action against any foreign company supporting illicit Iranian commerce, including airlines, and, as necessary, may impose secondary sanctions on foreign financial institutions that facilitate Iran's activities.

Additionally, Treasury recently warned of the sanctions risk associated with complying with Iranian demands for passage through the Strait of Hormuz such as "toll" payments, including payments made via fiat currency, digital assets, offsets, informal swaps, or other in-kind payments such as nominally charitable donations, and providing sensitive vessel information. On May 27, 2026, Treasury designated Iran's so-called "Persian Gulf Strait Authority," an IRGC-linked scheme to extort international shipping seeking to transit the Strait of Hormuz.

IRANIAN DIGITAL ASSET EXCHANGES: A TOOL FOR REGIME INSIDERS

Nobitex processed over 50 percent of all Iranian digital asset inflows in 2025 and has provided significant support to the Iranian regime. The company has facilitated a significant number of digital asset transactions linked to the IRGC, including transactions for wallets associated with IRGC-affiliated ransomware actors. For example, Nobitex has been used by OFAC-designated IRGC operatives. Nobitex allows Iranian regime insiders to access international digital asset exchanges and enables sanctions evasion across numerous jurisdictions.

As a vehicle for sanctions evasion, and in particular its previous connection to the Central Bank of Iran, Nobitex has contributed to the repression of the Iranian people and reportedly enables the Iranian government to conduct warrantless surveillance of Iranian civilians at a time of mass government repression. In addition, two of Nobitex's co-founders are close associates of former Supreme Leader of Iran Ayatollah Ali Khamenei's family. OFAC is designating Nobitex pursuant to E.O. 13224, as amended for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the IRGC and pursuant to E.O. 13902 for operating in the financial sector of the Iranian economy.

Amir Hossein Rad (Rad) is Nobitex's chairman, co-founder, and former CEO. In June 2025, he helped Nobitex, which previously allowed the Iranian regime to evade sanctions and transfer wealth out of the country, to reconstitute its operations following a $90 million hack of the company on June 18, 2025. OFAC is designating Rad pursuant to E.O. 13224, as amended for being a leader or official of Nobitex and pursuant to E.O. 13902 for operating in the financial sector of the economy of Iran.

Seyed Mohammad Ali Aghamir Mohammad Ali (Ali Aghamir) is a Nobitex co-founder and a member of the Kharrazi family. The Kharrazi family is part of Supreme Leader Khamenei's inner circle. OFAC is designating Ali Aghamir pursuant to E.O. 13224, as amended for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to, or in support of, Nobitex.

Seyed Mohammad Aghamir Mohammad Ali (Mohammad Aghamir) is a Nobitex co-founder and blockchain lead for the company. He is member of the Kharrazi family. OFAC is designating Mohammad Aghamir pursuant to E.O. 13224, as amended for being a leader or official of Nobitex.

Seyed Ali Khoee (Khoee) is the current CEO of Nobitex and previously served as its director of product and marketing. OFAC is designating Khoee pursuant to E.O. 13224, as amended for being a leader or official of Nobitex.

Wallex is Iran's second-largest digital asset exchange by volume and received 12 percent of all Iranian digital asset inflows in 2025. It additionally has facilitated numerous transactions linked to the IRGC.

Bitpin is an Iranian digital asset exchange. It received 10 percent of all Iranian digital asset inflows in 2025 and has processed millions of dollars' worth of transactions, including for transactions linked to the IRGC. Furthermore, Bitpin's investors have reportedly been linked to Iranian efforts to evade U.S. sanctions.

Ramzinex is a digital asset exchange based in Tehran. Founded in 2018, Ramzinex has processed over $2.45 billion in transactions, including for transactions linked to the IRGC and a financial institution backed by the Iranian government, and has been used for sanctions evasion.

OFAC is designating Wallex, Bitpin, and Ramzinex pursuant to E.O. 13902 for operating in the financial sector of the Iranian economy.

SANCTIONS IMPLICATIONS

All property and interests in property of the persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of blocked persons.

Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons. OFAC may impose civil penalties for sanctions violations on a strict liability basis. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities involving designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated or blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person. Non-U.S. persons are also prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. Individuals located in the U.S. or abroad who provide information about sanctions violations to FinCEN's whistleblower incentive program may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, or to submit a request, please refer to OFAC's guidance on Filing a Petition for Removal from an OFAC List.

Click here for more information on the persons designated and any property identified as blocked property today.

第 5 頁，共 5 頁

2026/6/22 上午10:12 線上_1150053029_

檔　號:
保存年限:

駐美國代表處經濟組 函

地址：4201 Wisconsin Avenue, N.W.,
Washington D.C. 20016, U.S.A.
承 辦 人：張旨華
聯絡電話：1-202-686-1691
電子郵件：chhchang@sa.moea.gov.tw

受文者：金融監督管理委員會

發文日期：中華民國115年6月3日
發文字號：經美字第1150000605號
速別：普通件
密等及解密條件或保密期限：
附件：如文（fc71d3_1150000605R1.pdf、fc71d3_1150000605R2.pdf）

主旨：有關美國執行經濟怒火行動，制裁伊朗最大之數位資產交易所，指控其被用於恐怖主義融資與規避制裁事，報請鑒察。

說明：

一、美財政部本(115)年6月2日就旨案發布新聞稿略以：

(一)美財政部外國資產管制辦公室(OFAC)當(2)日將伊朗最大之數位資產交易所Nobitex及其他三家伊朗數位資產交易所(Wallex、Bitpin、Ramzinex)列入制裁名單，此係「經濟怒火」(Economic Fury)行動之一部分，亦是川普政府為消除伊朗政權構成之威脅而採取之措施。

(二)美財長貝森特(Scott Bessent)表示，伊朗經濟正處自由落體式下滑，該政權選擇利用數位資產技術實現其腐敗目的，包括規避制裁以及將財富轉移出境。伊朗當前之經濟混亂證明，川普總統極限施壓政策取得成功。美財

政部將持續追蹤支持「經濟怒火」行動之資金流向，無論該等資金是透過銀行系統或數位資產，以阻止伊朗政權發展核武。

(三)Nobitex大力支持伊朗政權，包括：

1、處理伊朗在2025年超過50%之數位資產流入，並促成與伊朗恐怖活動、規避制裁以及與伊斯蘭革命衛隊(IRGC)等相關交易(包括與IRGC附屬勒索軟體組織有關之活動)之支付。

2、協助伊朗中央銀行取得數億美元穩定幣，以用於支撐暴跌之伊朗貨幣-里亞爾，同時使伊朗政權內部人士能使用國際數位資產交易所，規避多個司法管轄區之制裁。

3、在美國對伊朗發動軍事行動後，網路中斷下，Nobitex仍參與保護與轉移資產及資金出境之工作，以保護伊朗政權之財富。

(四)OFAC本日另將Nobitex董事長、聯合創始人兼前首席執行官Amir Hossein Rad及其他多名Nobitex領導人與官員列入制裁名單。

(五)本日行動係依據反恐授權之第13224號行政命令以及針對在伊朗金融領域及其他經濟領域活動人員之第13902號行政命令，對伊朗施加最大經濟壓力。

(六)有關伊朗數位資產交易所相關制裁風險之更多資訊，請見常見問題1250 (https://ofac.treasury.gov/faqs/1250)與1257 (https://ofac.treasury.gov/faqs/1257)。

(七)美國務院提供「正義獎賞」(RFJ)計畫懸賞高達1500萬美元，獎勵提供有助於破壞伊朗伊斯蘭革命衛隊及其各分支機構金融機制之資訊者。詳情請見RFJ網站(https://rewardsforjustice.net/rewards/islamic-revolutionary-guard-corps/)。

(八)美財政部近日警告稱，倘滿足伊朗通過荷姆茲海峽之要求，如支付「通行費」，無論以任何形式支付，包括以法定貨幣、數位資產、抵銷交易、非正式互換或其他實物支付方式，如名義上之慈善捐款，以及提供敏感船舶資訊，恐面臨制裁風險。(詳附件OFAC針對滿足伊朗通過荷姆茲海峽要求面臨制裁風險之警告，包括金融機構須注意之各類支付方式以及海事服務提供業者對船舶之盡職調查等)

(九)制裁的影響：

1、上述受制裁實體在美國境內或由美國公民持有或控制之所有財產及財產權益均被凍結，並須向美國OFAC報告。

2、由一名或多名被制裁人員直接或間接、單獨或合計擁有50%或以上權益(股權)之實體亦被凍結。

3、除獲OFAC頒發特定許可授權或取得豁免，依OFAC規定，禁止美國公民或在美國境內(或過境)者進行涉及被凍結人員任何財產或財產權益之所有交易。

4、違反美國制裁可能導致美國人與外國人遭受民事或刑事處罰。OFAC可依據嚴格責任原則對違反制裁之行為處以民事處罰。OFAC《經濟制裁執行指南》提供更多

OFAC執行美國經濟制裁之資訊。

5、金融機構與其他人員可能因參與涉及被制裁人員之某些交易或活動而面臨制裁風險，這些禁令包括禁止金融機構或其他人員對任何被制裁人員提供或捐贈資金、貨物或服務；或禁止金融機構或其他人員接受任何被制裁者提供之捐贈資金、貨物或服務。

6、非美國公民亦被禁止唆使或共謀唆使美國公民故意或無意違反美國制裁，以及從事任何規避美國制裁之行為。身處美國境內或境外之個人，倘向美財政部金融犯罪執法局(FinCEN)之舉報人獎勵計劃提供有關違反制裁之資訊，且該資訊達成成功執法行動，致使罰款金額超過100萬美元，舉報人可能有資格獲得獎勵。

二、檢送美財政部新聞稿及OFAC發布之警告如附件，併請卓參。

正本：經濟部國際貿易署
副本：財政部、金融監督管理委員會、交通部(均含附件) 2026/06/04 08:02:06

2026/6/22 上午10:12 線上_1150053029_

OFAC ALERT

Sanctions Risks of Iranian Demands for Strait of Hormuz Passage

May 1, 2026

The Office of Foreign Assets Control (OFAC) is aware of Iranian threats to shipping and demands for "toll" payments to receive safe passage through the international Strait of Hormuz. These demands may include several payment options, including fiat currency, digital assets, offsets, informal swaps, or other in-kind payments, such as nominally charitable donations made to the Iranian Red Crescent Society, Bonyad Mostazafan, or Iranian embassy accounts. OFAC is issuing this alert to warn U.S. and non-U.S. persons about the sanctions risks of making these payments to, or soliciting guarantees from, the Iranian regime for safe passage. These risks exist regardless of payment method.

U.S. persons and U.S.-owned or -controlled foreign entities are generally prohibited under U.S. sanctions from engaging in transactions with the Government of Iran, including the provision or receipt of services, unless exempt or authorized by OFAC. U.S. sanctions also generally prohibit U.S. persons from engaging in transactions with Iran's Islamic Revolutionary Guard Corps (IRGC), which is sanctioned pursuant to several authorities, including nonproliferation and counterterrorism sanctions, and is a designated Foreign Terrorist Organization. U.S. persons are also generally prohibited from engaging with Iranian digital asset exchanges, which are considered blocked Iranian financial institutions under U.S. sanctions.

Additionally, non-U.S. persons may risk exposure to sanctions for engaging in transactions with the Government of Iran and the IRGC that are not otherwise exempt or authorized for U.S. persons. This risk to non-U.S. persons includes secondary sanctions on participating foreign financial institutions, which could prohibit or restrict such foreign financial institutions' access to the U.S. financial system. Non-U.S. persons engaging with blocked Iranian digital asset exchanges may also risk sanctions for operating in or supporting the sanctioned Iranian financial sector. Further, non-U.S. persons could face civil and criminal enforcement liability should such payments cause U.S. persons, such as insurers, reinsurers, and financial institutions, to violate sanctions.

Please see FAQ 1249 for more information on sanctions risk for paying tolls to the Government of Iran and the IRGC, and FAQs 1250 and 831 on engaging with Iranian digital asset exchanges and the Iranian financial sector.

Maritime industry participants involved with vessels calling at Iranian ports face significant sanctions risk under multiple sanctions authorities targeting Iran's shipping sector and ports, and OFAC will continue to aggressively target Iran's main revenue-generating sectors, in particular its petroleum and petrochemical sectors, under

2026/6/22 上午10:12 線上_1150053029_

Executive Order 13902 and other sanctions authorities. Vessels of all nations entering or leaving Iranian ports and coastline are also subject to U.S. Central Command's impartial naval blockade, and OFAC authorizations do not supersede the authorities of all other U.S. government agencies and departments, including U.S. Central Command.

MARITIME SERVICE PROVIDERS

OFAC strongly encourages all maritime service providers to conduct enhanced due diligence on any vessels attempting to transit the Strait of Hormuz to ensure that such vessels have not engaged in any sanctionable conduct involving Iran, which could expose the service provider to sanctions risk. Service providers should carefully review all available information for red flags, including voyage planning or actual transits through Iranian territorial waters. Service providers should ask counterparties for details on who they coordinated with to transit the Strait of Hormuz and if any safe passage fees were or will be paid to Iran. For more information about Iran's use of obfuscation techniques in maritime shipping, please see OFAC's Sanctions Advisory: Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion.

Mariners are encouraged to coordinate with U.S. authorities:

Fifth Fleet Battle Watch
+1-813-529-7430
cusnc.bwc.mil@us.navy.mil

NAVCENT NCAGS
+1-813-529-7108 (Primary/Watch Desk)
+973-3986-4800 (Alternate)
m-ba-navcent-ncags@us.navy.mil
m_ba_navcent_ncags_ice@us.navy.mil

OFAC
Office of Foreign Assets Control

OFAC Compliance Hotline
ofac.treasury.gov/ofac-compliance-hotline