AMERICAN SELL-OUT

The Trump Family Crypto Firm Sold Tokens to Dozens of Suspicious Buyers Who Interacted with a Large Money-Laundering Platform, an Iranian Crypto Exchange, and Even North Korean Hackers

Accountable.US

EXECUTIVE SUMMARY

In recent months, press reports have discussed numerous foreign entanglements involving President Trump and his family's crypto ventures, including a multi-billion dollar deal with a U.A.E.-backed investment fund, investments from Chinese-born crypto billionaire Justin Sun, and a $25 million deal with the Dubai-based DWF Labs, which is run by a former Russian crypto CEO.

Now, Accountable.US reveals that the Trump family sold $WLFI tokens to a variety of highly suspicious entities with connections to North Korea, Iran, and a known money-laundering platform Tornado Cash, as well as one user who engaged with a purported Russian "Ruble-backed sanctions evasion tool."

- On Inauguration Day, Trump family cryptocurrency venture World Liberty Financial Inc. sold 600,000 of its $WLFI tokens valued at $10,000 to cryptocurrency trader "Shryder.eth." That user, Shryder.eth, appears to have made at least 55 transactions with a wallet now-sanctioned by the Treasury Department's Office of Foreign Asset Control (OFAC) for being associated with the Lazarus Group, **a notorious North Korean state-sponsored hacking team.**

    - Following the Lazarus Group Transactions, Shryder.eth was blocked from certain mainstream crypto services like Uniswap, which has stated that it only blocks wallets "owned or associated with clearly illegal behavior like: sanctions, terrorism financing, hacked or stolen funds," and other illicit activities.

    - The Lazarus Group was sanctioned by the first Trump administration in 2019 and was added to the Trump FBI's "Cyber Most Wanted List" in 2020. Also around 2019, Lazarus began targeting crypto companies and conducting hundreds of millions of dollars in successful or attempted hacks. Previously, Lazarus was behind the massive "WannaCry 2.0" attack, which affected at least 150 countries and shut down 300,000 computers—notably, the U.K.'s National Health Service emergency and intensive care services were "crippled" and the agency lost $112 million.

- In October 2024, World Liberty Financial sold nearly 3,500 $WLFI tokens to a crypto user who has deposited over $26,000 on **Iran's largest crypto exchange (NoBitex.ir)** that has facilitated sanctions violations—the same user appears to control a highly active pro-Iran X.com account, with one X repost saying U.S. warships "will sleep on the ocean floor."

- Since February 2, 2025, World Liberty Financial has sold user "0x9009" over 10,000 $WLFI tokens; this same user has also used the A7A5 crypto token – **A Russian "Ruble-backed sanctions evasion tool"** – whose creators were sanctioned by the US Government in August 2025.

- Additionally, World Liberty Financial sold $WLFI tokens to at least 62 users who also used TornadoCash, **a crypto mixing service that the Justice Department alleged helped criminals and hackers, including Lazarus Group, "launder more than $1 billion of illicit assets."** The Biden administration sanctioned Tornado Cash in 2022, but the Trump administration lifted the sanctions in March 2025.

Well after the initial World Liberty Financial token sale ended, on September 5, 2025, World Liberty disclosed that they had "blacklisted" just five accounts for "high risk exposure." Given the late hour of this disclosure, Americans must ask whether this effort was done to comply with the law, or to cover for sales to potential bad actors over the previous year.

Ultimately, the question remains - why did the Trump family crypto firm take money from people with open and obvious connections to enemies of the United States, and the network that enables those enemies and other criminals to launder billions of dollars?

TABLE OF CONTENTS

NORTH KOREA

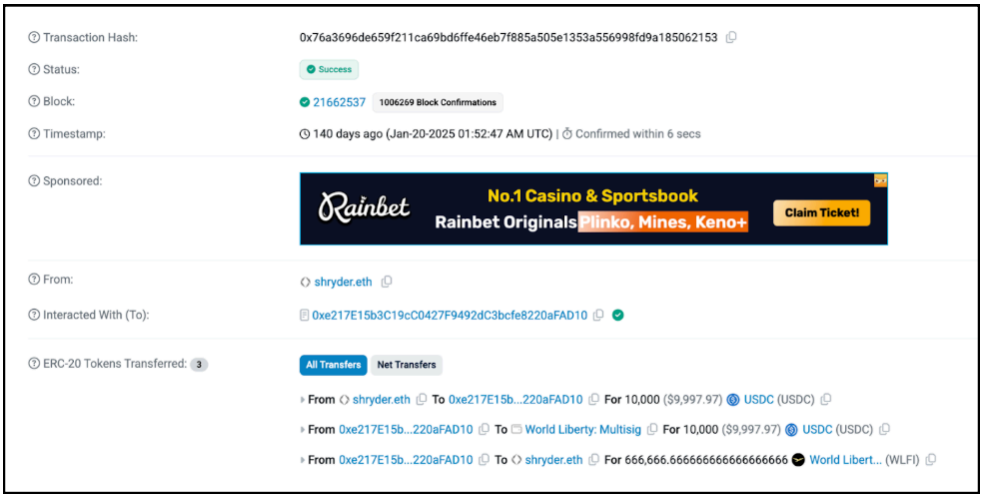
ON INAUGURATION DAY, WORLD LIBERTY FINANCIAL TOOK $10,000 FROM A CRYPTOCURRENCY TRADER WHO HAS TRANSACTED WITH NORTH KOREAN STATE-SPONSORED HACKERS AND WHO WAS BANNED FROM OTHER MAINSTREAM CRYPTO PLATFORMS LIKE UNISWAP AND OPENSEA; THEY THEN SENT HIM AN ADDITIONAL $47 AS PART OF A JUNE 2025 PROMOTIONAL GIVEAWAY.

On January 20, 2025, User "Shryder.eth" Purchased Over 600,000 $WLFI Tokens Directly From World Liberty Financial For $10,000.

Shryder.Eth Is The Ethereum Name Service Username For Token Address 0x4642D9D9A434134CB005222eA1422e1820508d7B. [Etherscan, accessed 06/09/25]

- **Ethereum Name Service Names Are Like URLs For Ethereum Addresses.** "The Ethereum Name Service or ENS is the decentralized naming protocol that is built on the Ethereum blockchain. It adheres to open-source standards and is based on a set of decentralized smart contracts that translate blockchain addresses into human-readable names. You can share your ENS name instead of a long, hard to remember crypto address." [Ethereum Name Service, accessed 06/09/25]

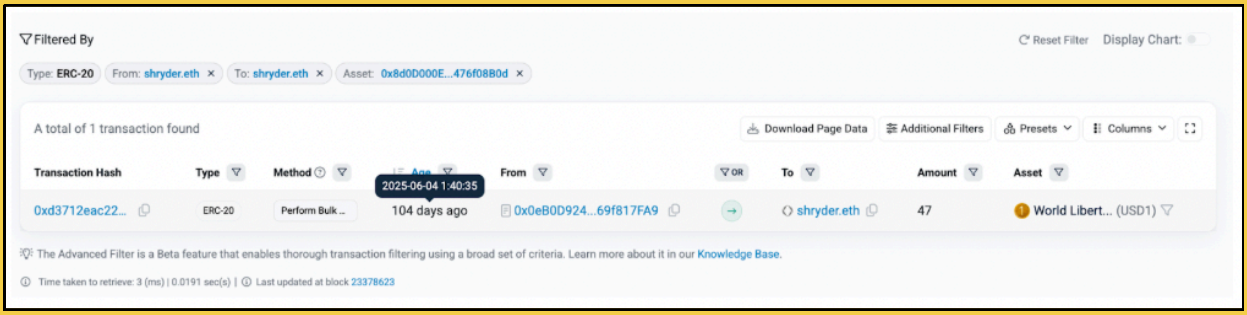
On January 20, 2025, Crypto User Shryder.eth Purchased 666,666.666 $WLFI Tokens From World Liberty Financial, For $10,000 In USDC Cryptocurrency.



[Ethereum Transaction Hash 0x76a3696de659f211ca69bd6ffe46eb7f885a505e1353a556998fd9a185062153, 01/20/25]

- **"WLFI Tokens And Use Of The WLF Protocol And Governance Platform Are Offered And Sold Solely By World Liberty Financial, Inc. Or Its Affiliates."** [World Liberty Financial, accessed 06/09/25]

On June 4, 2025, User "Shryder.eth" Received 47 $USD1 Stablecoins From World Liberty Financial As Part Of Their Airdrop To Early $WLFI Tokenholders.



[Etherscan.io - shryder.eth, accessed 09/16/25]

- **The Airdrop Of World Liberty Financial's Then-New $USD1 Stablecoin (Valued At $1 Each) Was Designed To "Reward Initial Supporters, Increase Liquidity For USD1, And Stress-Test The Project's Token Distribution Mechanism Under Live Market Conditions."** "World Liberty Financial, a DeFi venture part-owned by a trust of US President Donald Trump, has kicked off a new airdrop campaign targeting early backers. On June 4, the blockchain analytics platform Lookonchain confirmed that the project began distributing $47 worth of its USD1 stablecoin to wallets that participated in the WLFI token sale. The airdrop, approved by community vote weeks earlier, aims to reward initial supporters, increase liquidity for USD1, and stress-test the project's token distribution mechanism under live market conditions. Meanwhile, market observers believe the firm selected the $47 figure to honor Trump's designation as the 47th President of the United States. This symbolic gesture adds a political and cultural layer to what would otherwise be a standard reward mechanism." [Crypto Slate, 06/04/25]

Previously, In 2022, Shryder.eth Appears To Have Transacted With "LAZARUS Group" A North Korean State-Sponsored Hacking Group.

Timestamp	Sender	Receiver	Currency	Amount
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:33:40	LAZARUS Group (0x098)	Shryder.eth	$CASH	9

Timestamp	Sender	Receiver	Currency	Amount
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:34:33	LAZARUS Group (0x098)	Shryder.eth	$CASH	9

Timestamp	Sender	Receiver	Currency	Amount
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9
2022-03-30 23:35:37	LAZARUS Group (0x098)	Shryder.eth	$CASH	9

After The 2022 Transactions With LAZARUS Group, Shryder.eth Was Blocked From Using Certain Mainstream Cryptocurrency Services Like Uniswap.

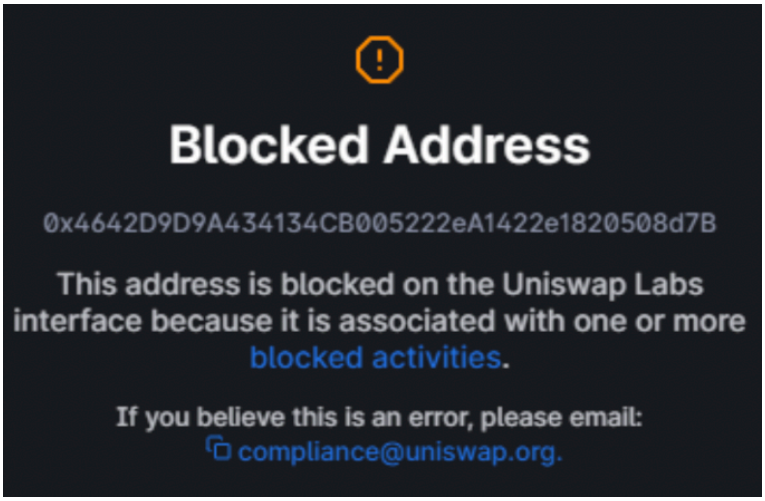
The X.com Account "Shryder1337" Has Suggested That They Control Shryder.eth.

[X.com Post from Shryder1337, 04/02/22]

The X.com Account "Shryder1337" Has Suggested That They Control The Crypto Address Associated With Shryder.eth.

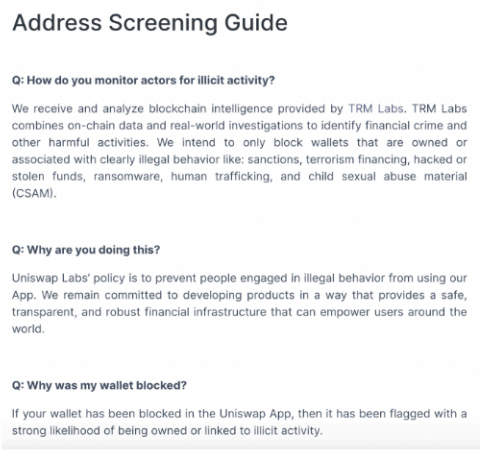
[X.com Post from Shryder1337, 04/21/22]

On April 21, 2022, @Shryder1337 Posted On X.com That They Were Blocked By Uniswap Labs And OpenSea, Two Major Mainstream Cryptocurrency Platforms.



[X.com Post from @Shryder1337, 04/21/22]

- **As Of October 2022, Uniswap Labs Said They Only Blocked "Wallets That Are Owned Or Associated With Clearly Illegal Behavior Like: Sanctions, Terrorism Financing, Hacked Or Stolen Funds, Ransomware, Human Trafficking, And Child Sexual Abuse Material (CSAM)."**



Address Screening Guide

Q: How do you monitor actors for illicit activity?

We receive and analyze blockchain intelligence provided by TRM Labs. TRM Labs combines on-chain data and real-world investigations to identify financial crime and other harmful activities. We intend to only block wallets that are owned or associated with clearly illegal behavior like: sanctions, terrorism financing, hacked or stolen funds, ransomware, human trafficking, and child sexual abuse material (CSAM).

Q: Why are you doing this?

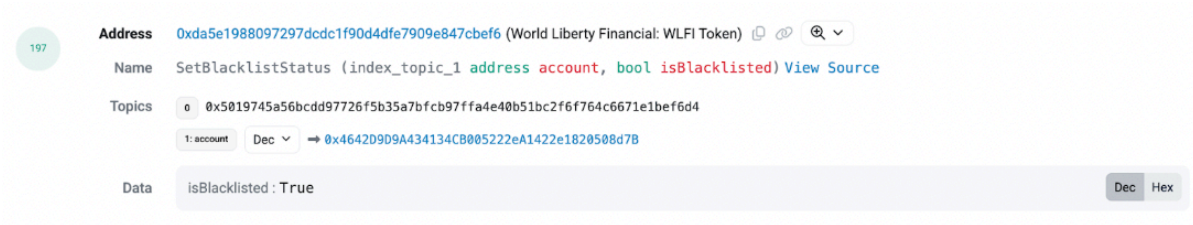
Uniswap Labs' policy is to prevent people engaged in illegal behavior from using our App. We remain committed to developing products in a way that provides a safe, transparent, and robust financial infrastructure that can empower users around the world.

Q: Why was my wallet blocked?

If your wallet has been blocked in the Uniswap App, then it has been flagged with a strong likelihood of being owned or linked to illicit activity.

[Uniswap Labs Address Screening Guide, 10/07/22 (via Internet Archive)]

It Wasn't Until August 31, 2025 That World Liberty Financial Appears To Have Blacklisted Shryder.ETH From Interacting With The $WLFI Token.



197

Address 0xda5e1988097297dcdc1f90d4dfe7909e847cbef6 (World Liberty Financial: WLFI Token)

Name SetBlacklistStatus (index_topic_1 address account, bool isBlacklisted) View Source

Topics 0 0x5019745a56bcdd97726f5b35a7bfcb97ffa4e40b51bc2f6f764c6671e1bef6d4

1: account Dec → 0x4642D9D9A434134CB005222eA1422e1820508d7B

Data isBlacklisted : True Dec Hex

[Etherscan.io Tx 0xf128f4aa0bdde67ed35cba628932b004a37807566d71a11baff30b741df4da90 - Logs, 08/31/25]

- **On September 5, 2025, World Liberty Financial Disclosed They Had Blacklisted 272 Addresses, Including Just 5 For "High-Risk Exposure;" It Is Unclear Under Which Parameter Shryder.ETH Was Added To The Blacklist.**

WLFI @worldlibertyfi · Sep 5

3/

Breakdown of the 272:

• 215 (≈79.0%) tied to a phishing attack—we stepped in preemptively to stop hackers from draining funds and are working with the rightful owners to secure/move assets.

• 50 (≈18.4%) owners reported compromise via support; we blacklisted at their request to help protect/recover funds.

• 5 (≈1.8%) flagged for high-risk exposure (security risk under review).

• 1 (≈0.4%) suspected of misappropriation of other holders' funds; under thorough internal review.

60 128 754 224K

[X.com Post from @worldlibertyfi, 09/05/25]

IN 2019, THE FIRST TRUMP ADMINISTRATION SANCTIONED THE LAZARUS GROUP, AN ELITE NORTH KOREAN STATE-SPONSORED HACKING GROUP, AND ADDED LAZARUS TO ITS "CYBER MOST WANTED LIST" IN 2020.

2019: The First Trump Administration's Office of Foreign Assets Control Announced Sanctions Against The Lazarus Group And Two of Its Sub-Groups As "North Korean State-Sponsored Malicious Cyber Groups."

September 2019: During The First Trump Administration, The Treasury Dept.'s Office of Foreign Assets Control (OFAC) Announced Sanctions Against The Lazarus Group And Two Of Its Sub-Groups As "North Korean State-Sponsored Malicious Cyber Groups." "Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the global cyber security private industry as 'Lazarus Group,' 'Bluenoroff,' and 'Andariel' as agencies, instrumentalities, or controlled entities of the Government of North Korea pursuant to Executive Order (E.O.) 13722, based on their relationship to the Reconnaissance General Bureau (RGB)." [U.S. Department of the Treasury, 09/13/19]

- **The Treasury Dept. Also Designated Two Sub-Groups Of Lazarus Group, Bluenoroff And Andariel, Which Respectively Earn Illicit Revenue To Circumvent Global Sanctions Against The DPRK And Conduct Malicious Cyber Operations On Foreign Entities.** "Also designated today are two sub-groups of Lazarus Group, the first of which is referred to as Bluenoroff by many private security firms. Bluenoroff was formed by the North Korean government to earn revenue illicitly in response to increased global sanctions. [...] The second Lazarus Group sub-group designated today is Andariel. It focuses on conducting malicious cyber operations on foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses, as well as the defense industry." [U.S. Department of the Treasury, 09/13/19]

- **The Treasury Department Stated That Lazarus Group Was Created By The North Korean Government And "Targets Institutions Such As Government, Military, Financial, Manufacturing, Publishing, Media, Entertainment, And International Shipping Companies, As Well As Critical Infrastructure."** "Lazarus Group targets institutions such as government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations. Created by the North Korean Government as early as 2007, this malicious cyber group is subordinate to the 110th Research Center, 3rd Bureau of the RGB." [U.S. Department of the Treasury, 09/13/19]

- **Although North Korea Has Never Admitted Being Behind The Lazarus Group, The Nation Is "Thought To Be The Only Country In The World Using Its Hacking Powers For Financial Gain."** "North Korea has never admitted being behind the Lazarus Group, but is thought to be the only country in the world using its hacking powers for financial gain." [BBC, 03/09/25]

The U.S. Treasury Department Calls The Lazarus Group "A State-Sponsored Cyber Hacking Group Of The Democratic People's Republic Of Korea (DPRK)." "Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Sinbad.io (Sinbad), a virtual currency mixer that serves as a key money-laundering tool of the OFAC-designated Lazarus Group, a state-sponsored cyber hacking group of the Democratic People's Republic of Korea (DPRK)." [U.S. Department of the Treasury, 11/29/23]

The U.S. And Its Allies Have Accused The Lazarus Group Of "Carrying Out Dozens Of Hacks In Recent Years To Fund The Regime's Military And Nuclear Development." "Experts say the infamous hacking team is working nearly 24 hours a day - potentially funnelling the money into the regime's military development. [...] The US and allies accuse the North Koreans of carrying out dozens of hacks in recent years to fund the regime's military and nuclear development." [BBC, 03/09/25]

In 2020, The First Trump Administration's FBI Added Suspected Lazarus Members To Its "Cyber Most Wanted List."

In 2020, The U.S. Added Suspected Lazarus Group Members To Its "Cyber Most Wanted List." "In 2020, the US added North Koreans accused of being part of the Lazarus Group to its Cyber Most Wanted list. But the chances of the individuals ever being arrested are extremely slim unless they leave their country." [BBC, 03/09/25]

LAZARUS GROUP HAS HEAVILY TARGETED CRYPTO COMPANIES THROUGH HUNDREDS OF MILLIONS OF DOLLARS IN HACKS AND WAS PREVIOUSLY BEHIND THE MASSIVE "WANNACRY 2.0" ATTACK—WHICH AFFECTED AT LEAST 150 COUNTRIES AND CRIPPLED PART OF THE U.K.'S NATIONAL HEALTH SERVICE—AND AN ATTEMPTED $850 MILLION HEIST FROM THE CENTRAL BANK OF BANGLADESH.

Around 2019, Lazarus Group Began Targeting Less-Secure Cryptocurrency Companies With Hundreds Of Millions Of Dollars In Successful Or Attempted Hacks.

In About 2019, Lazarus Group Began Targeting Cryptocurrency Companies, Which Have Fewer Security Measures And Fewer Safeguards Against Money Laundering. "Previously the Lazarus Group hackers targeted banks, but have in the last five years specialised in attacking cryptocurrency companies. The industry is less well protected with fewer mechanisms in place to stop them laundering the funds." [BBC, 03/09/25]

North Korea-Tied Crypto Hacks Since 2019 Include The $600 Million Ronin Bridge Attack In 2022; A $100 Million Attack On Atomic Wallet In 2023; A $41 Million Hack On UpBit In 2019; An Attempted $275 Million Theft From KuCoin. "Recent hacks linked to North Korea include:

- The 2019 hack on UpBit for $41m
- The $275m theft of crypto from exchange KuCoin (most of the funds were recovered)
- The 2022 Ronin Bridge attack which saw hackers make off with $600m in crypto
- Approximately $100m in crypto was stolen in an attack on Atomic Wallet in 2023"

[BBC, 03/09/25]

In 2023, The FBI Identified Lazarus Group As Responsible For A $41 Million Crypto Heist From Online Betting Platform Stake.com. "The FBI is issuing this release to warn the public regarding the theft of approximately $41 million in virtual currency from Stake.com, an online casino and betting platform. The FBI has confirmed that this theft took place on or about September 4, 2023, and attributes it to the Lazarus Group (also known as APT38) which is comprised of DPRK cyber actors." [Federal Bureau of Investigation, 09/06/23]

- **Headline: FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com** [Federal Bureau of Investigation, 09/06/23]

Previously, Lazarus Group Was Behind The Massive "WannaCry 2.0" Ransomware Attack, Affecting At Least 150 Countries And Shutting Down About 300,000 Computers—The Attack Cost The U.K.'s National Health Service $112 Million And "Crippled" Large Parts Of Its Intensive And Emergency Care Services.

In 2017, Lazarus Group Was Involved In The "WannaCry 2.0" Ransomware Attack, Which "Affected At Least 150 Countries Around The World And Shut Down Approximately Three Hundred Thousand Computers." "Lazarus Group was involved in the destructive WannaCry 2.0 ransomware attack which the United States, Australia, Canada, New Zealand and the United Kingdom publicly attributed to North Korea in December 2017. Denmark and Japan issued supporting statements and several U.S. companies took independent actions to disrupt the North Korean cyber activity. WannaCry affected at least 150 countries around the world and shut down approximately three hundred thousand computers." [U.S. Department of the Treasury, 09/13/19]

The Attack Cost The The U.K.'s National Health Service (NHS) $112 Million And "Crippled" Parts Of Its Network, Including One-Third Of Its Secondary Care Hospitals, Which Provide Intensive And Emergency Care, And 8% Of The U.K's General Medicare Care Services. "Among the publicly identified victims was the United Kingdom's (UK) National Health Service (NHS). Approximately one third of the UK's secondary care hospitals — hospitals that provide intensive care units and other emergency services — and eight percent of general medical practices in the UK were crippled by the ransomware attack, leading to the cancellation of more than 19,000 appointments and ultimately costing the NHS over $112 million, making it the biggest known ransomware outbreak in history." [U.S. Department of the Treasury, 09/13/19]

Lazarus And Its Sub-Group Bluenoroff Stole About $80 MIllion From The Central Bank Of Bangladesh's New York Federal Reserve Account While Attempting To Steal A Total Of $851 Million.

Lazarus And Its Sub-Group Bluenoroff Stole About $80 Million From The Central Bank Of Bangladesh's New York Federal Reserve Account—The Groups Attempted to Steal A Total Of $851 Million, But An Error Revealed Their Activities To Bank Personnel. "Also designated today are two sub-groups of Lazarus Group, the first of which is referred to as Bluenoroff by many private security firms. [...] According to cyber security firms, typically through phishing and backdoor intrusions, Bluenoroff conducted successful operations targeting more than 16 organizations across 11 countries, including the SWIFT messaging system, financial institutions, and cryptocurrency exchanges. In one of Bluenoroff's most notorious cyber activities, the hacking group worked jointly with Lazarus Group to steal approximately $80 million dollars from the Central Bank of Bangladesh's New York Federal Reserve account. By leveraging malware similar to that seen in the SPE cyber attack, Bluenoroff and Lazarus Group made over 36 large fund transfer requests using stolen SWIFT credentials in an attempt to steal a total of $851 million before a typographical error alerted personnel to prevent the additional funds from being stolen." [U.S. Department of the Treasury, 09/13/19]

Lazarus Group Was "Directly Responsible" For The 2014 Cyber Attacks Against Sony Pictures Entertainment. "Lazarus Group was also directly responsible for the well-known 2014 cyber-attacks of Sony Pictures Entertainment (SPE)." [U.S. Department of the Treasury, 09/13/19]

- **The Attacks Were Retaliation Against Sony For Its Movie "The Interview," A Satire Of The DPRK's Leader, And Included Malware, Stolen Confidential Data, And Threats Against Sony Executives And Employees.** "In November 2014, the conspirators launched a destructive attack on Sony Pictures Entertainment (SPE) in retaliation for the movie "The Interview," a farcical comedy that depicted the assassination of the DPRK's leader. The conspirators gained access to SPE's network by sending malware to SPE employees, and then stole confidential data, threatened SPE executives and employees, and damaged thousands of computers." [The U.S. Department of Justice, 09/06/18]

IN 2025, THE LAZARUS GROUP MADE "THE LARGEST HEIST IN CRYPTO HISTORY," A $1.5 BILLION HACK OF CRYPTO EXCHANGE BYBIT, PROMPTING SEN. ELIZABETH WARREN (D-MA) TO DEMAND ANSWERS FROM THE TRUMP ADMINISTRATION AND WARN OF WEAK CRYPTO SAFEGUARDS IN THE PENDING GENIUS ACT, WHICH SHE CALLED "'A SUPERHIGHWAY FOR DONALD TRUMP'S CORRUPTION.'"

In 2025, The Lazarus Group Made "The Largest Heist In Crypto History," Successfully Converting At Least $300 Million In A "Record-Breaking" $1.5 Billion In Funds…

March 2025: In What Was Called "The Largest Heist In Crypto History," The Lazarus Group Successfully Converted At Least $300 Million Of A "Record-Breaking" $1.5 Billion Heist From The Bybit Crypto Exchange Into Unrecoverable Funds. "Hackers thought to be working for the North Korean regime have successfully converted at least $300m (£232m) of their record-breaking $1.5bn crypto heist to unrecoverable funds. The criminals, known as Lazarus Group, swiped the huge haul of digital tokens in a hack on crypto exchange ByBit two weeks ago. Since then, it's been a cat-and-mouse game to track and block the hackers from successfully converting the crypto into usable cash." [BBC, 03/09/25]

- **Headline: How the largest heist in crypto history happened** [BBC, 03/10/25]

…Prompted By Lazarus Group's Heist, Senate Banking Committee Ranking Member Elizabeth Warren (D-MA) Demanded Information From Trump's Treasury Secretary And Attorney General On Their Responses To "A Dangerous Escalation In North Korea's Use Of Crypto Theft To Evade Sanctions And Fund Its Weapons Programs"…

May 2025: Prompted By Lazarus Group's $1.5 Billion Hack, Sen. Elizabeth Warren (D-MA), Ranking Member Of The Senate Banking Committee, And Sen. Jack Reed (D-RI), Sent A Letter To Treasury Sec. Scott Bessent And Attorney General Pam Bondi Requesting Information On Trump Administration Efforts To Combat North Korea's "Increasingly Aggressive And Frequent Cyber-Attacks." "U.S. Senators Elizabeth Warren (D-Mass.), Ranking Member of the Senate Banking, Housing, and Urban Affairs Committee, and Jack Reed (D-R.I.), sent a letter to Secretary of the Treasury Scott Bessent and Attorney General Pam Bondi requesting information on efforts to combat increasingly aggressive and frequent cyber-attacks by ransomware groups based in North Korea. In February, the Lazarus Group, a hacker syndicate backed by the North Korean government, stole approximately $1.5 billion in digital currency from Bybit, a popular cryptocurrency exchange." [U.S. Senate Committee on Banking, Housing, And Urban Affairs, 05/19/25]

The Senators Called Lazarus Group's Attack "A Dangerous Escalation In North Korea's Use Of Crypto Theft To Evade Sanctions And Fund Its Weapons Programs — A Direct Threat To U.S. National Security And Global Stability." "In the letter, the senators warn the attack marks a dangerous escalation in North Korea's use of crypto theft to evade sanctions and fund its weapons programs — a direct threat to U.S. national security and global stability. 'In the wake of this attack—the 'largest crypto theft of all time'—we write to request information regarding your efforts to combat increasingly aggressive and frequent cyber-attacks by ransomware groups based in North Korea,' wrote the senators." [U.S. Senate Committee on Banking, Housing, And Urban Affairs, 05/19/25]

The Senators' Letter Said, "'North Korea Relies On Cryptocurrency Theft To Subvert U.S.-Led International Sanctions And To Undermine The Security Of The United States,'" Adding, "'These Stolen Assets Have Helped Keep The Regime Afloat And Supported Continued Investments In Its Nuclear And Conventional Weapons Programs.'" "They continued: 'North Korea relies on cryptocurrency theft to subvert U.S.-led international sanctions and to undermine the security of the United States and our Indo-Pacific allies… These stolen assets have helped keep the regime afloat and supported continued investments in its nuclear and conventional weapons programs. Reports suggest there are potentially thousands of North Korean-affiliated crypto hackers around the globe.'" [U.S. Senate Committee on Banking, Housing, And Urban Affairs, 05/19/25]

…Sen. Warren's Demands Came As Senate Republicans Were Advancing The GENIUS Act, Stablecoin Legislation "With Few Guardrails And Inadequate National Security Protections"—Sen. Warren Separately Said The Bill Would "'Create A Superhighway For Donald Trump's Corruption.'"

The Senators' Inquiry Came As Senate Republicans Were Trying To Advance The GENIUS Act, Legislation That Would "Dramatically Expand The Stablecoin Market With Few Guardrails And Inadequate National Security Protections." "The senators press the agencies on how they are responding to the evolving tactics of North Korean hackers and what tools they need to prevent future attacks. This comes as Senate Republicans attempt to advance the GENIUS Act — legislation that, as currently drafted, would dramatically expand the stablecoin market with few guardrails and inadequate national security protections." [U.S. Senate Committee on Banking, Housing, And Urban Affairs, 05/19/25]

- **June 11, 2025: The Senate Voted To End Debate On The GENIUS Act, Bringing The Bill One Step Closer To A Final Vote In The Senate.** "The Senate voted Wednesday to advance legislation setting up a regulatory framework for payment stablecoins, bringing the crypto bill one step closer to a final vote in the upper chamber. Eighteen Democrats voted with almost every Republican to end debate on an updated version of the GENIUS Act." [The Hill, 06/11/25]

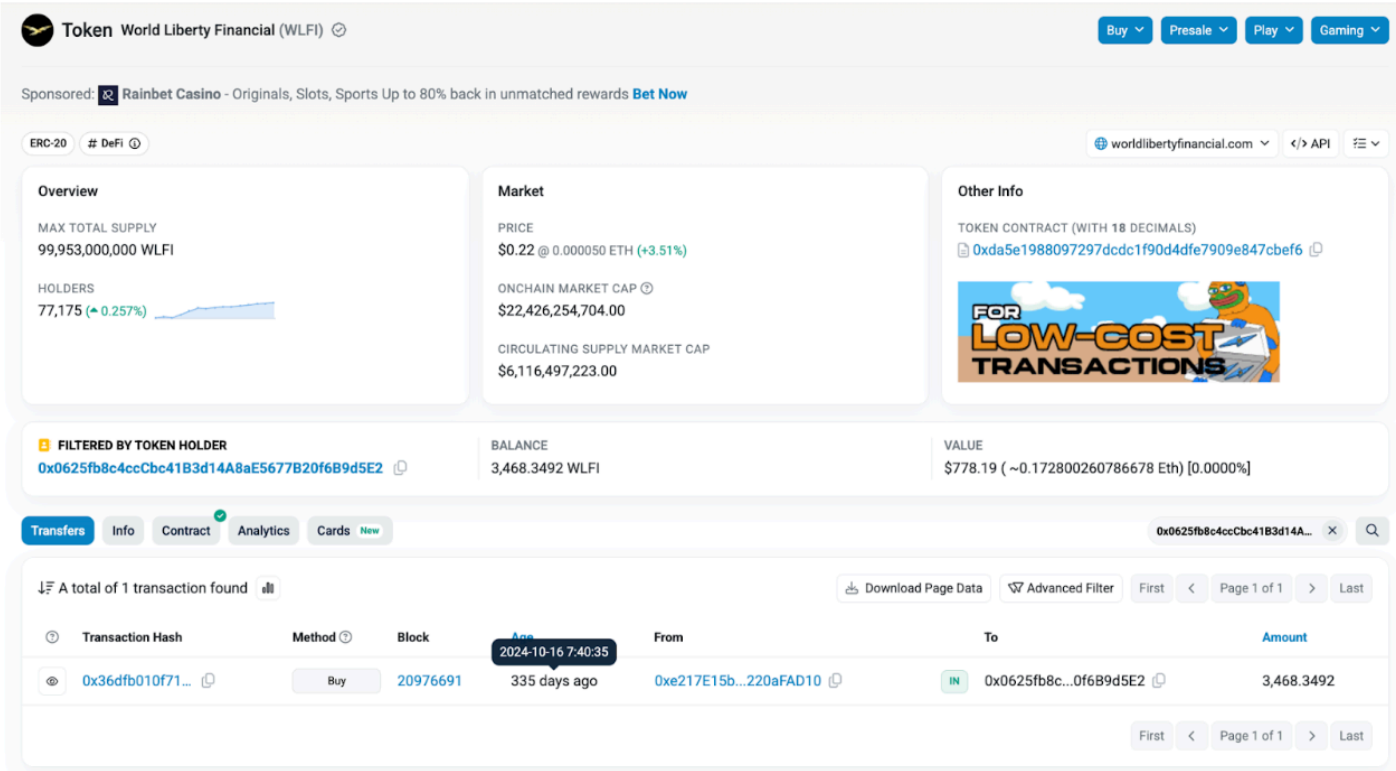
Sen. Warren Said The GENIUS Act Would "'Create A Superhighway For Donald Trump's Corruption'" And Critics Warned It Could "Enable Corruption, Screw Over Taxpayers, And Potentially Destabilize The Economy "On its face the bill, which has advanced with bipartisan support, purports to offer a regulatory framework for the expansion of "stablecoins," a form of crypto pegged to an existing, recognized asset — in many cases the U.S. dollar. In reality, it could enable corruption, screw over taxpayers, and potentially destabilize the economy. […] No one has been more outspoken on the failings of the GENIUS Act than Sen. Elizabeth Warren (D-Mass.), who told Rolling Stone ahead of key votes that the bill would 'create a superhighway for Donald Trump's corruption.'" [Rolling Stone, 06/12/25]

IRAN

IN OCTOBER 2024, WORLD LIBERTY FINANCIAL SOLD NEARLY 3,500 $WLFI TOKENS TO A CRYPTO USER WHO HAS DEPOSITED OVER $26,000 ON IRAN'S LARGEST CRYPTO EXCHANGE, WHICH HAS FACILITATED SANCTIONS VIOLATIONS; THE SAME USER APPEARS TO CONTROL A HIGHLY-ACTIVE PRO-IRAN X ACCOUNT, WITH ONE X REPOST SAYING U.S. WARSHIPS "WILL SLEEP ON THE OCEAN FLOOR."

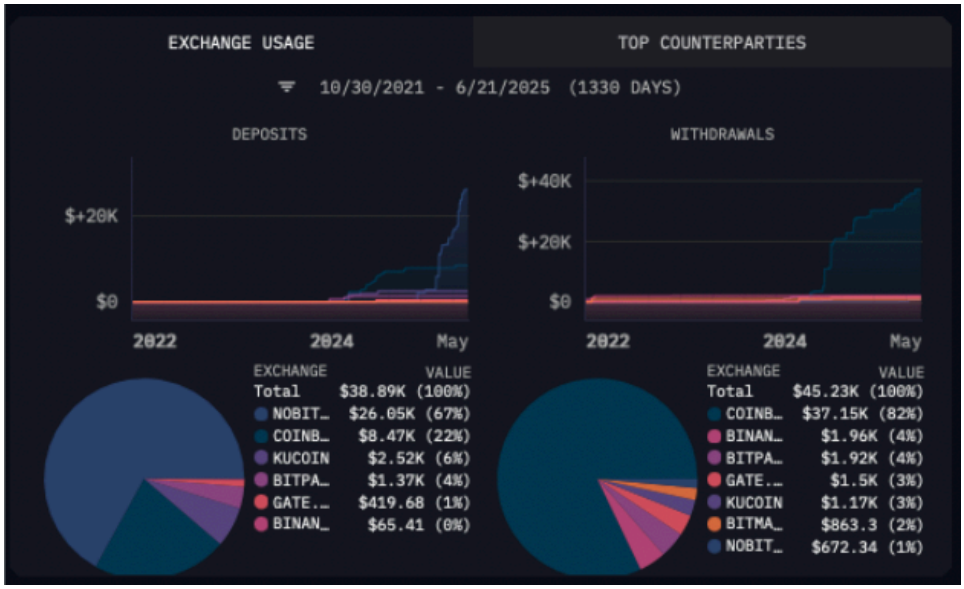
Crypto User "0x062" Holds Over 3,400 In $WLFI Tokens And Has Made Over $26,000 In Deposits To Nobitex.ir, Which Is Iran's Largest Crypto Exchange, Has Been Linked To "A Range Of Illicit Actors," And Has Facilitated Sanctions Violations.

On October 16, 2024, Crypto User 0x0625fb8c4ccCbc41B3d14A8aE5677B20f6B9d5E2 (0x062) Purchased 3,468.3492 In $WLFI Tokens From World Liberty Financial.



[Etherscan, accessed 06/23/25]

0x062 Has Made Over $26,000 In Deposits On Nobitex And Over $672 In Withdrawals From Nobitex.ir Since 2021:



[Arkham, accessed 06/23/25]

0x062 Has Transferred Thousands Of Dollars Worth Of Cryptocurrency To A Nobitex.ir Deposit Wallet In 2025 Alone:

TRANSFERS | SWAPS | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
2 weeks ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.224	ETH	$557.18
3 weeks ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.21	ETH	$548.19
1 month ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.545	ETH	$1.44K
1 month ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.362	ETH	$907.45
1 month ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.636	ETH	$1.57K
1 month ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.268	ETH	$704.66
1 month ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	1	ETH	$2.67K
2 months ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.108	ETH	$224.05
2 months ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.328	ETH	$600.79
2 months ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.39	ETH	$698.37
2 months ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.842	ETH	$1.33K
3 months ago	0x0625fb8c4ccCbc41B3d14A8…	Nobitex.ir Deposit (0xa2B)	0.0769	ETH	$120.88

[Arkham, accessed 06/23/25]

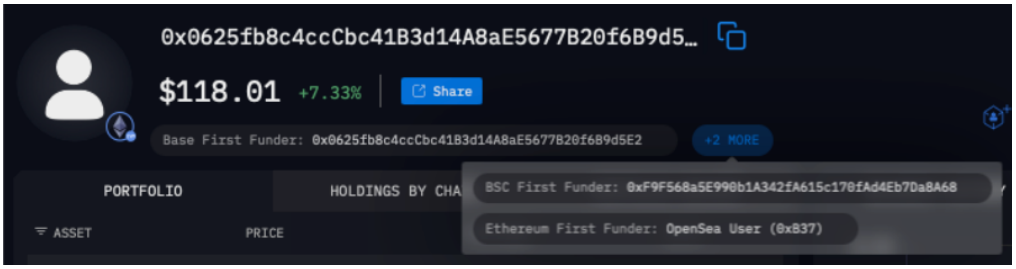
June 2025: Nobitex, "Iran's Largest Cryptocurrency Exchange," Lost $90 Million In A "Major Hack" Conducted By A Pro-Israel Hacker Group. "Nobitex, Iran's largest cryptocurrency exchange, suffered a major hack on 18 June. Elliptic has so far identified over $90 million sent from Nobitex wallets to hacker addresses. It comes after pro-Israel hacker group Gonjeshke Darande ('Predatory Sparrow') issued a warning claiming that they had conducted cyberattacks against Nobitex and pledged to publish its source code on 18 June. Nobitex's website remains inaccessible at the time of writing." [Elliptic, 06/18/25]

Due To Sanctions Against Iran And Iranian Entities, Nobitex Has "Become The Go-To Platform For Iranian Users Seeking Access To Global Crypto Markets." "Nobitex is the largest cryptocurrency exchange in Iran and a central pillar of the country's digital asset ecosystem. Operating in a heavily sanctioned environment, it has become the go-to platform for Iranian users seeking access to global crypto markets, facilitating the majority of on-chain exchange activity originating in the country." [Chainalysis, 06/18/25]

Nobitex Has Been Linked "To A Range Of Illicit Actors" And Has Facilitated Transactions With "Sanctioned Pro-Hamas Media Outlet, Gaza Now, A Pro-Al-Qaeda Propaganda Channel; Sanctioned Russian Crypto Exchanges," And Others. "Past on-chain analysis has linked Nobitex to a range of illicit actors, including wallets affiliated with IRGC-affiliated ransomware operators, and entities tied to Houthi and Hamas-affiliated networks as identified by the National Bureau for Counter Terror Financing (NBCTF) of Israel. As we see in the Chainalysis Reactor graph below, the platform has also facilitated transactions with sanctioned pro-Hamas media outlet, Gaza Now, a pro-al-Qaeda propaganda channel; sanctioned Russian crypto exchanges, Garantex and Bitpapa; and many other illicit operators." [Chainalysis, 06/18/25]

0x062 Was First Funded By 0xb37 And The Two Accounts Appear To Share The Same Unique Binance Deposit Wallet…

0x062's First Ethereum Funder Address Was OpenSea User 0xb37, Whose Full Address Is 0xB37B9e1d07F4180f0C705fE0C1C141Ee1b22eA5b:



[Arkham, accessed 06/23/25]

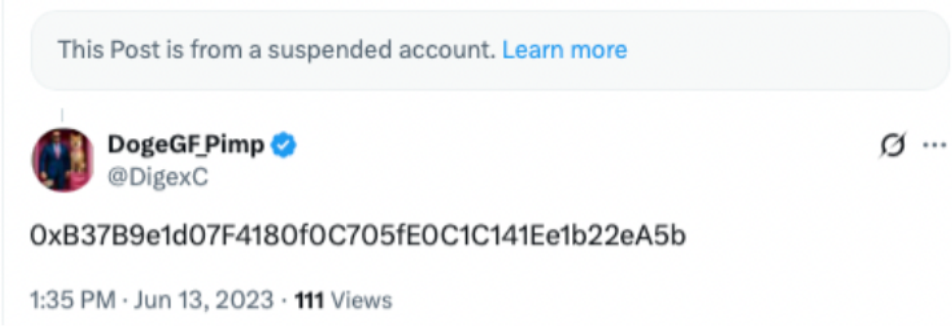
As Of June 23, 2025, 0x062 And 0xB37 Have Made 20 Transactions Valued At Over $2,200—Additionally, Both 0x062 And 0xB37 Share The Same Address On Binance, Which Provides A "Unique 'Deposit Address'" For Each User:

[Arkham, accessed 06/23/25]

- **Binance Users' Deposits Are Directed To A "Unique 'Deposit Address.'"** "When you deposit assets into your Binance account, your funds are directed to a unique 'deposit address' that Binance manages for you. Your Binance deposit address is distinct from addresses in self-custodial wallets like Trust Wallet, Metamask, etc. In a self-custodial wallet, users hold their wallet's private keys, thus fully controlling their funds. However, when you deposit funds on a centralized platform like Binance, we manage the wallets and the deposited funds on your behalf." [Binance, accessed 06/23/25]

…0xb37 Which Appears To Be Controlled By X Account @DigexC, Who Has Reposted Many Pro-Iran Items, Including "I Stand With Iran," "Boom Boom Tel Aviv" And "Let The U.S. Enter [The Israel-Iran War]… Their Warships Will Sleep On The Ocean Floor."

June 2023: X User @DigexC Posted The Same Crypto Address 0xB37B9e1d07F4180f0C705fE0C1C141Ee1b22eA5b, In Response To A Now-Unavailable Post:



[X Post by @DigexC, 06/13/23, accessed 06/23/25]

On X, @DigexC Has Reposted Many Pro-Iran Posts, Including Those Saying "Boom Boom Tel Aviv," "I Stand With Iran," And "Let The U.S. Enter [The Israel-Iran War]… Their Warships Will Sleep On The Ocean Floor":

[X Profile for @DigexC, accessed 06/23/25]

[X Profile for @DigexC, accessed 06/23/25]

[X Profile for @DigexC, accessed 06/23/25]

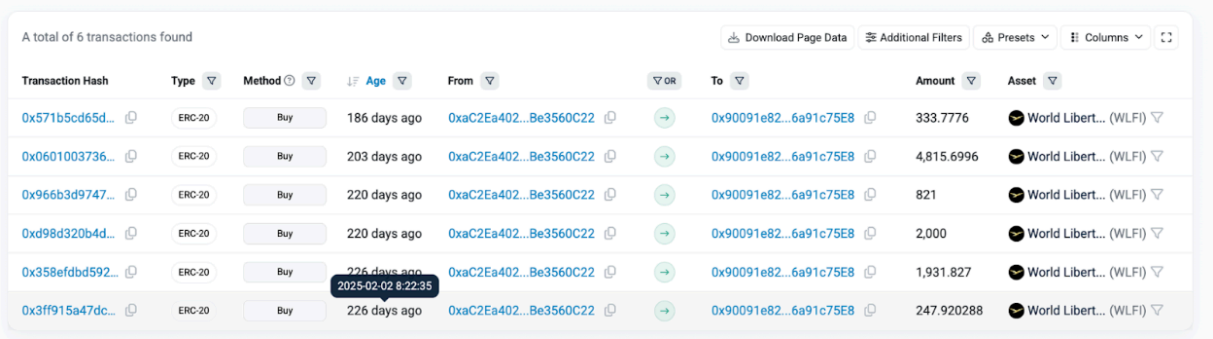
[X Profile for @DigexC, accessed 06/23/25]

[X Profile for @DigexC, accessed 06/23/25]

RUSSIA

SINCE FEBRUARY 2, 2025, WORLD LIBERTY FINANCIAL HAS SOLD USER "0X9009" OVER 10,000 $WLFI TOKENS; THIS SAME USER HAS ALSO USED THE A7A5 CRYPTO TOKEN – A RUSSIAN "RUBLE-BACKED SANCTIONS EVASION TOOL" – WHOSE CREATORS WERE SANCTIONED BY THE US GOVERNMENT IN AUGUST 2025.

Starting On February 2, 2025, Address 0x90091e824c79F090be63f5575F4e7156a91c75E8 Began Buying $WLFI Tokens, Which At The Time Were Only Available For Purchase Directly From World Liberty Financial; The User Ultimately Purchased 10,150 $WLFI Tokens.



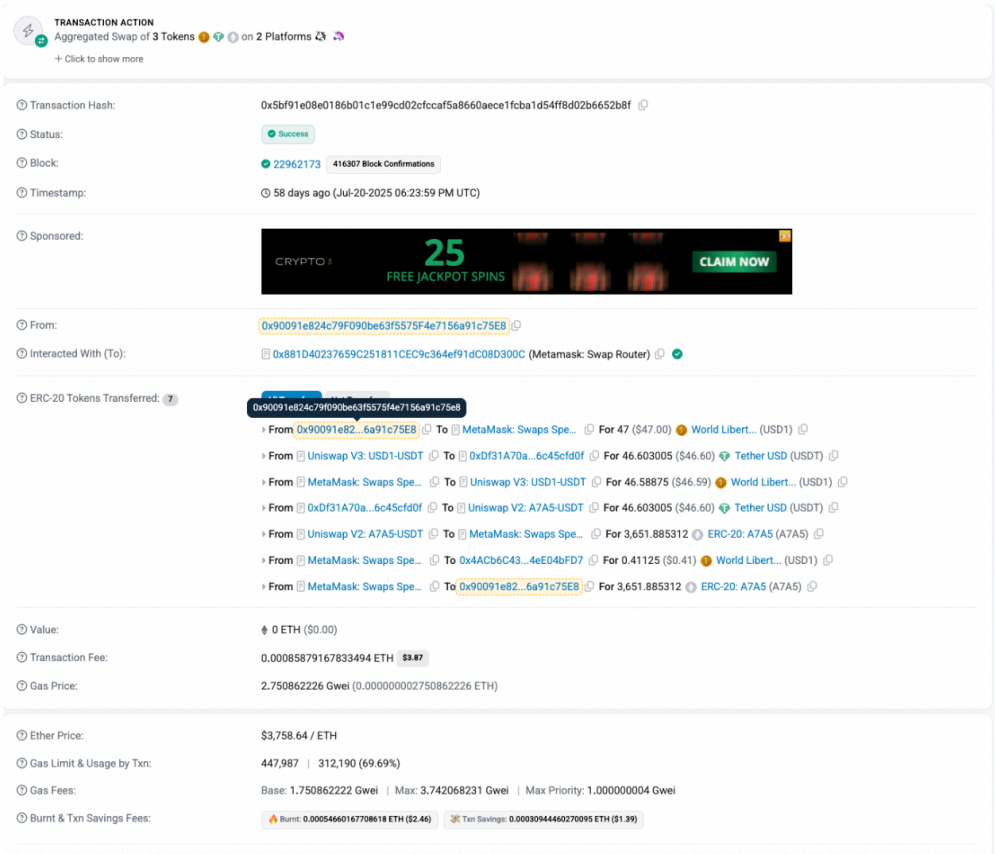
[Etherscan.io – Address 0x90091e824c79F090be63f5575F4e7156a91c75E8, accessed 09/16/25]

On June 4, 2025, Address 0x90091e824c79F090be63f5575F4e7156a91c75E8 Received 47 $USD1 Stablecoins From The World Liberty Financial Team As Part Of An Airdrop.

[Etherscan.io – Address 0x90091e824c79F090be63f5575F4e7156a91c75E8, accessed 09/16/25]

- **The Airdrop Of World Liberty Financial's Then-New $USD1 Stablecoin (Valued At $1 Each) Was Designed To "Reward Initial Supporters, Increase Liquidity For USD1, And Stress-Test The Project's Token Distribution Mechanism Under Live Market Conditions."** "World Liberty Financial, a DeFi venture part-owned by a trust of US President Donald Trump, has kicked off a new airdrop campaign targeting early backers. On June 4, the blockchain analytics platform Lookonchain confirmed that the project began distributing $47 worth of its USD1 stablecoin to wallets that participated in the WLFI token sale. The airdrop, approved by community vote weeks earlier, aims to reward initial supporters, increase liquidity for USD1, and stress-test the project's token distribution mechanism under live market conditions. Meanwhile, market observers believe the firm selected the $47 figure to honor Trump's designation as the 47th President of the United States. This symbolic gesture adds a political and cultural layer to what would otherwise be a standard reward mechanism." [Crypto Slate, 06/04/25]

On July 20, 2025, Address 0x90091e824c79F090be63f5575F4e7156a91c75E8 Swapped Their 47 $USD1 Tokens Through A Series Of Transactions Which Ultimately Resulted In Them Receiving Approximately 3,651 $A7A5 Tokens In Return.



[Etherscan.io - Tx 0x5bf91e08e0186b01c1e99cd02cfccaf5a8660aece1fcba1d54ff8d02b6652b8f, 07/20/25]

- **The A7A5 Crypto Token Has Been Called A "Ruble-Backed Sanctions Evasion Tool."** [TRM Labs, 8/15/25]

- **A7A5 Was Reportedly "Created By A7 LLC, Which Assists Russian Businesses Impacted By Western Sanctions To Make Cross-Border Payments."** "A7A5 is a Ruble-backed stablecoin launched in Kyrgyzstan in January 2025, and available on the TRON and Ethereum blockchains. As described in a June 2025 report by the Centre for Information Resilience, A7A5 was created by A7 LLC, which assists Russian businesses impacted by western sanctions to make cross-border payments. A7 was sanctioned by the UK in May 2025 and by the EU in July 2025." [Elliptic Research, 07/28/25]

- **The United States Sanctioned The Entities Behind The A7A5 Token On August 15, 2025.** "On August 14, 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced actions targeting the founder and co-owners of the previously sanctioned cryptocurrency exchange Garantex, one of its successor platforms Grinex, and the ruble-backed A7A5 token. The designations mark the latest step in a multi-year effort to dismantle a sanctions-evasion infrastructure that has facilitated the laundering of ransomware proceeds, darknet market revenues, and other illicit transactions since at least 2019." [TRM Labs, 8/15/25]

TORNADO CASH

WORLD LIBERTY FINANCIAL HAS INTERACTED WITH DOZENS OF USERS THAT ALSO USED THE TORNADO CASH MONEY LAUNDERING PLATFORM.

Tornado Cash Is A Cryptocurrency Mixing Service That The Department Of Justice Alleges Has Helped Criminals And Hackers "Launder More Than $1 Billion Of Illicit Assets."

Tornado Cash Is A Service That Allows Users To "Send And Receive Cryptocurrency Anonymously." "Launched by Roman Storm and Roman Semenov on Ethereum in 2019, Tornado Cash allows users to send and receive cryptocurrency anonymously, without exposing their wallet history. Unlike centralized mixers, Tornado Cash operates entirely onchain through immutable smart contracts, meaning no central party controls the funds." [CoinTelegraph, 05/07/25]

- **"The Justice Department Has Alleged That Criminals, Including Lazarus Group, A U.S.-Sanctioned North Korean Cybercrime Organization, Used Tornado Cash To Launder More Than $1 Billion Of Illicit Assets."** [Wall Street Journal, 03/24/25]

Tornado Cash Was Under Sanction By The US Treasury Department's Office Of Foreign Asset Control (OFAC) From August 8, 2022 Until President Trump Lifted The Sanctions On March 21, 2025.

On August 8, 2022, The United States Government Sanctioned Tornado Cash. "Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash, which has been used to launder more than $7 billion worth of virtual currency since its creation in 2019." [US Department of the Treasury - Press Release, 08/08/22]

- **Specifically, Tornado Cash Was Sanctioned For Providing Material Support Or Assistance For Foreign Behavior "That Is Reasonably Likely To Result In, Or Has Materially Contributed To, A Significant Threat To The National Security, Foreign Policy, Or Economic Health Or Financial Stability Of The United States."** "Tornado is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain." [US Treasury Department - Press Release, 08/08/22]

- **The Sanctions Specifically Included A List Of Addresses On The Ethereum Blockchain.** [US Department of the Treasury – SPECIALLY DESIGNATED NATIONALS LIST UPDATE, 08/08/22]

In November 2024, The 5th Circuit Court Of Appeals Ruled That OFAC "Exceeded Its Statutory Authority By Sanctioning Immutable Smart Contracts Created By Tornado Cash." "On November 26, 2024, the United States Court of Appeals for the Fifth Circuit issued a landmark decision holding that the Treasury Department's Office of Foreign Assets Control ("OFAC") exceeded its statutory authority by sanctioning immutable smart contracts created by Tornado Cash. While the decision leaves several legal issues open and is still subject to appeal by the Treasury Department, it has significant implications for the use of the International Emergency Economic Powers Act ("IEEPA") to regulate certain decentralized finance (DeFi) technologies." [Mayer Brown, 12/03/24]

On March 21, 2025, The Trump Administration Removed Economic Sanctions Against Tornado Cash. "WASHINGTON — Based on the Administration's review of the novel legal and policy issues raised by use of financial sanctions against financial and commercial activity occurring within evolving technology and legal environments, we have exercised our discretion to remove the economic sanctions against Tornado Cash as reflected in Treasury's Monday filing in Van Loon v. Department of the Treasury." [US Department of the Treasury - Press Release, 03/21/25]

While Tornado Cash Was Under Sanction, Many Reputable Crypto Companies Refused To Do Business With Tornado Cash Users.

Crypto Currency Exchange OKX "Declared That Any Accounts On The OKX Exchange Found To Be Interacting With Tornado Cash Would Be Terminated." ""In an announcement aimed at reinforcing financial integrity and improving compliance measures with international sanctions, OKX CEO Star Xu declared that any accounts on the OKX exchange found to be interacting with Tornado Cash would be terminated. The announcement comes in response to escalating concerns about Tornado Cash, a decentralized mixing service that enables users to obfuscate the origin and destination of their cryptocurrency transactions. While Tornado Cash is popular among privacy-conscious users, malicious actors to launder stolen funds." [Cointelegraph, 08/09/24]

Crypto Platform dYdX "Blocked User Accounts That Previously Interacted With Tornado Cash, In Line With… US Sanctions." "Derivatives protocol dYdX confirmed on Thursday morning that it blocked user accounts that previously interacted with Tornado Cash, in line with new US sanctions. dYdX added in a blog post that it is working with a "compliance vendor" that flagged certain accounts that had received funds from the Tornado Cash app." [The Block, 08/27/22]

The Front End Developers For Decentralized Exchange Uniswap "Blocked 253 Wallet Addresses Linked To Illicit Financial Activities… After The U.S. Government Imposed Sanctions On Tornado Cash." "Decentralized exchange Uniswap has appeared to block 253 wallet addresses linked to illicit financial activities on its front end after the U.S. government imposed sanctions on Tornado Cash earlier this month… Uniswap has partnered with TRM Labs to screen and monitor suspicious financial activities, including those related to mixing service Tornado Cash." [Forkast, 08/23/22]

World Liberty Financial Sold Tokens To At Least 62 Users That Also Used TornadoCash.

$WLFI Buyer Address	$WLFI Tokens Held	# of Tornado Cash Transactions
0x48d21dc6bbf18288520e9384aa505015c26ea43c	1,613.50	2
0xf0b4fb521eee7561e746a2e01ef933c5a2225809	4,068.50	2
0xb9b8ef61b7851276b0239757a039d54a23804cbb	341,491	15
0x601c6d9eff76ae8cd7bff5fc4900f20f6f80734f	666,133	3

$WLFI Buyer Address	$WLFI Tokens Held	# of Tornado Cash Transactions
0x6b0ea34cc854316dd8784502ff85c1cb24f800b4	10,000	1
0x0f48669b1681d41357eac232f516b77d0c10f0f1	101,022.90	1
0x9be0acd94d6772fbeba3779efb0fc9f3bf02a22c	227,435.50	2
0xb1998487b4cd187b4c4d1ad81a957ccbc10a0f85	1,325.30	2
0x605a4eb7ca3e7c0b3af9ae557938210cad0a2800	170,557	2
0x653d63e4f2d7112a19f5eb993890a3f27b48ada5	25,743	6
0x73f2e04f047931e85b62e4f2652b156199000e14	3,240.30	1
0x63f35fc30690ed1111a2bfb75034b1ef41821c66	400,000	1
0x01974549c9b9a30d47c548a16b120b1caa7b586c	1,333,333.30	5
0xa06ad2e0339375124d255f1fab201964ef707e18	200,010,755.60	1
0x8aae84404661e3c015284b20b74c7a62ed29907e	525.5	3
0xcda1a0ecd7d25b49ecbf0eec1f45f0b7fb59961b	3,421,880	2
0x3cfd366e74601bf1db379912889262e071e8c63a	13,614.10	2
0x750171933e5ad548250712b077ce295a9ab8ffeb	162,398.90	1
0x8474c4397048101501981993679 3ddc210a0050e	16,545	160
0xe2616b431eb9bf550f12c197778c2830ee89a368	43,136.70	1
0x2d64f6539dda515322254d617d0cb14b754cdcf5	200	1
0x6e0fc44cce1b49323185138217649b5e8996a159	7,334.25	3
0x3b3d4c951b39540c06d1f64c74d8b970d645c35e	40,000	3
0x8e631b065c1730275f67ae4db637e37d49b736bb	7,171.50	1
0x98a24753360f40b72478ae5b8411224bfa18b3f5	5,390.50	1
0x5336cd70cad7e4f36f3d6463a0bee3dcdb59c7c5	1,999,175.20	1

$WLFI Buyer Address	$WLFI Tokens Held	# of Tornado Cash Transactions
0x44017a895f26275166b1d449bcb1573fd324b456	100,000	15
0x25ad2667b19e866109c1a93102b816730a6aec3f	19,707	2
0x4ea4d86c2dcadb881bccaad5d28a14b80d6aa1ef	108,680	25
0x11c73ae24a15679dc2baa5a7e8b5b1bbb4b66d94	139,730.60	1
0x1350804da29d56eb3ec41189d8a7168fc017401a	211,713.10	2
0x50dce8e2f9be12016a0fb62a0e7630904213514b	3,333,333.30	2
0xb718727e7c8a4646d41d8b0be5e8e2c028b9efaa	458,157	6
0x29b9d8b112f97b637c134579b9d10a4f4fcac7ec	2,136,053.30	4
0xefe1047333fbae3b39ccdb568f30f54d78ac1d4c	20,000	1
0x223ce9110f7e678467d30fb132640a5bee090697	680,212.70	1
0xd3799da7d9700630d4e1c34b5ba87808b6de250f	100,200	1
0x47361b03a95842340cd4d272f434082c68a264f9	44,580,934	3
0x846e49ece01ac637f57c2fdf3effe476b7001190	1,038,798.60	1
0xa7255773acc951850348e4885e8e6433d8101980	201,884.60	1
0x1cf0cbb9f563529d5c6617bb5c37557c6338d4f9	9,122.90	2
0x5f561eb8b4380886bd3bbdc87fb4c28c0353b71a	114,062.60	1
0x8d2b0632b1efd1af43f61fe3f11a0fa2daf65eef	665,707.20	1
0xd881b4d076812ce4d4d8a09257e2ad994e373898	20,000	1
0xbb0244016a4dcb20c499b50e740083cfbb6c2f78	87,980.70	6
0x2bdbe765972927916b0081d6cbfcd40c0e1c1043	20,469.70	1
0x46282a19f843e50faac7ec6a1195c323484aaf2a	1,167,676.50	1
0x67c1bb9d5408655bacd89773f5534d039bfa765a	25,600	3

$WLFI Buyer Address	$WLFI Tokens Held	# of Tornado Cash Transactions
0x0f769e9fe7430b04d2173ba65e093917475852b5	2,356,856	1
0xdfc4fbbdd9c47c7976febb14b1d37c7f85fe299d	7,030.20	1
0xca810f64a0bbc8498dd0d714113c8518feeb8d29	67,463.90	3
0xc3fc2cc59b5cfa56b884ec3ad0096e6bf63ebea8	52,349	1
0x51242c532f9f93b15f3d0e009ee50a364c0bd59a	199,600	2
0xe0cef207b3fa3ce8af09d800c6ef7d25341ba245	1,000.20	1
0x7ff32570f8527fa84e927bcc557c62671a7d5c51	6,783,170.10	2
0xddffaafc75f0e8fe8c1453f590b71869d921599c	8,667.80	1
0x9af8a033f02ec1368d6c30e2f72c8c1098e55437	1,150.90	1
0xf6fe1654cebf900f59ca191d2ab9f87655c0c6ad	14,003.80	1
0xe5859cbc7a5c954d33480e67266c2bbc919a966e	336,743	1
0x5cf3727953eddbe34d295c2957884427bdf3a680	471,669.60	1
0xa858b62061e014686e1a5ba57e88516ae64271fa	338,000	1
0xc78ee2dc3574a6e50874efae87fd2b1d2f67b50e	17,504.80	1