

USDT Blacklist Lag Becomes a Loophole for Laundering Millions: On-Chain Proof Inside

AMLBot's Investigation
on USDT Freeze Lag



Step 1: Freeze Request (Submit Transaction)

[View on Tronscan](#) >

This transaction shows the submission of a request to freeze the target wallet. The HEX-encoded address **414049e71b23c0bad106e4e8dfd3f52a418f2a128a** corresponds to the base58 address TFq8nBxgbb9pjMw9fjT2uNRNuuHTgDdBed, confirming it as the destination wallet. **Transaction Initiated** at 2025-03-21 11:10:12 UTC — [The Submit Action](#)/ [Freeze Execution](#)

Step 2: Freeze Execution (Confirm Transaction)

[View on Tronscan](#) >

This is the confirmation of the freeze — when the transaction is executed on-chain and the freeze becomes active. It confirms the same transaction **ID: 3046** and **includes the same wallet address, indicating that it is added to the blacklist. Executed at 2025-03-21 11:54:51 UTC — 44 minutes after the submit action.**

There was a 44-minute gap between the submission and confirmation. That means even after the decision to freeze was made and submitted, there was a nearly one-hour window where the wallet was still fully active. This isn't just theoretical: both the **submit** and **confirm** actions refer to the **same transaction ID** and the **same wallet**, proving the delay and its potential for exploitation.

During this period, the wallet retained full access to **\$426,183 USDT**, meaning any fast-acting operator could have moved the funds out before the freeze took effect. This isn't a theoretical weakness. It's happening in the wild, and bad actors are watching.

Why Does the Delay Exist?

On Tron, Tether enforces freezes using a **custom multi-signature contract** (**TBPxhVAsuzoFnKyXtc1o2UySEydPHgATto**).

Verify on the Blockchain, Link:

<https://tronscan.org/#/contract/TBPxhVAsuzoFnKyXtc1o2UySEydPHgATto/transactions>

8fdd5aac...b44ac	70635013	49 days ago	ConfirmTransaction	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
759ff42f...c8e41	70635009	49 days ago	ConfirmTransaction	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
b4feadd...b1d5b	70635005	49 days ago	ConfirmTransaction	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
f66d2d4...b3697	70635002	49 days ago	ConfirmTransaction	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
c5223e2f...bc5ad	70634998	49 days ago	ConfirmTransaction	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
ae216d7...85147	70634120	49 days ago	SubmitTransaction	TYn9kGVaNbXCsdqD... ZSxmyN1	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
b94368b...cd3c9	70634107	49 days ago	SubmitTransaction	TYn9kGVaNbXCsdqD... ZSxmyN1	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
cf1a45b8...faedc	70634107	49 days ago	SubmitTransaction	TYn9kGVaNbXCsdqD... ZSxmyN1	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
132720...64629	70634105	49 days ago	SubmitTransaction	TYn9kGVaNbXCsdqD... ZSxmyN1	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓
8bec320...242c7	70634105	49 days ago	SubmitTransaction	TYn9kGVaNbXCsdqD... ZSxmyN1	SC TBPxhVAsuzoFnK... PHgATto	0 TRX	✓

Figure 1: Multi-Signature Freeze Workflow on Tron: This screenshot from the Tron blockchain shows two distinct types of smart contract transactions executed by Tether's multisig wallet that controls the blacklist: `submitTransaction()` and `confirmTransaction()` — finalizes and enforces it.

The delay between these steps opens a critical window that can be exploited by malicious actors.

The Process Involves Two Distinct Transactions:

submitTransaction() — proposes a freeze request on-chain.

confirmTransaction() — finalizes and executes the freeze after internal approval.


This workflow was likely implemented to improve internal governance and reduce the risk of unilateral actions. However, it introduces a race condition: once a freeze is suggested, it's visible on-chain, and until it's confirmed, the target wallet remains fully functional.

Tether uses a **similar setup on Ethereum**, with investigators observing delays of up to one hour between submission and confirmation.

"We've seen this multistep freeze system backfire," says Mike Tiutin, CTO at AMLBot. "It creates a dangerous gap, and criminals who monitor the blockchain can easily exploit it."

The same vulnerability exists on Ethereum. Our analysis shows that over \$28.5 million in USDT was withdrawn during the delay between submitTransaction() and confirmTransaction() steps on Ethereum. In multiple cases, wallets exploited this timing gap to move funds before blacklisting took effect. The average amount moved per wallet exceeded \$365,000, confirming that this isn't a minor flaw — it's a systemic issue across chains.

 Dataset 1: <https://drive.google.com/file/d/1JCNUA3PE6eP8HkwY5S0QABPsi1swYhpB/view?usp=drivesdk>

 Dataset 2: <https://drive.google.com/file/d/1ya4Bwj8R-uOkfn1QMQ6z9qKXAfp1cq3/view?usp=drivesdk>

A Data-Backed Look at Tether's Freeze Vulnerability

Following a deeper analysis of Tether's on-chain behavior, AMLBot's team uncovered the broader scale of this vulnerability: **\$49.6 million** was withdrawn during freeze delay windows on Tron blockchain.

170 out of 3,480 wallets (4.88%) on Tron blockchain exploited the lag before getting blacklisted. Each of these wallets made **2–3 transfers during the delay**, withdrawing: **Average: \$291,970/ Median: \$65,370.**

What's in the Data?

Two datasets were compiled to support this analysis:

1 **Wallet-Level Summary, showing:**

- blacklisted_address;
- tx_submit & tx_confirm;
- datetime_submit & datetime_confirm

- delay duration;
- sum_amount_out;
- tx_count_out

2 Transaction-Level Log, Listing:

- Source and Destination Wallets;
- Timestamps;
- Transferred Amounts.

 Dataset 1: https://drive.google.com/file/d/1O6FB89LiQEWJFWF_q-X_AiPhno3TgBg0/view?usp=sharing

 Dataset 2: <https://drive.google.com/file/d/1DilqhYzj793HzsRHHu1SVJNbqf834MX/view?usp=sharing>

Criminals Are Watching — And Reacting Fast

For blockchain-savvy attackers, these delays are golden. By tracking Tether's calls in real time, a fraudster can be instantly alerted that their address is being targeted. With minutes or even an hour before enforcement, they can withdraw or move funds, beating the freeze.

This turns the concept of "on-chain enforcement" into a false sense of security. The freeze may look active to observers, but it has no real effect until confirmation, something that could be delayed or even dropped.

Why It Matters

USDT is the most used stablecoin in the world, with over \$100 billion in circulation as of Q1 2025. It's widely used across CeFi, DeFi, and — critically — in illicit transactions. Tether's blacklisting capabilities are frequently cited as a safeguard for law enforcement and regulators.

But This Flaw Exposes a Dangerous Truth:

- Hackers and fraudsters can evade freezes by reacting faster than Tether's multi-sig approval.
- Investigations may be compromised when asset control is only "Pending." The reputational promise of compliance and control is weakened.

In past years, studies have shown that USDT is one of the most preferred tokens for laundering funds through mixers and high-risk exchanges. This implementation gap adds a new weapon to a criminal's toolbox.

"The Freeze Isn't Real Until It's Confirmed"

This analysis shows that Tether's on-chain enforcement mechanism, especially on Tron, contains a structural delay that weakens its role as a compliance safeguard.

What looks like active enforcement is often just the first step. Until the `confirmTransaction()` is broadcast and confirmed on-chain, the targeted wallet isn't actually frozen. This creates a false sense of security and leaves a dangerous window of opportunity for bad actors who know how to watch and react faster than enforcement can finalize.

"The enforcement looks like it's happening, but until the `confirmTransaction()` is broadcast, nothing is actually frozen."

Confirm Transaction: [View Confirm Tx >](#)

➤ Go to Event Logs → AddedBlackList – Change DECode to Hex — the same wallet appears in HEX: **414049e71b23c0bad106e4e8dfd3f52a418f2a128a**

A total of 3 event log(s)

0	Address	SC TBPxhVAsuzoFnKyXtc1o2UySEydPHgATo						
	Events	Confirmation(index_topic_1 address sender, index_topic_2 uint256 transactionId)						
	Topics	<table border="1"><tbody><tr><td>0</td><td>4a504a94899432a9846e1aa406dceb1bcfd538bb839071d49d1e5e23f5bc30ef</td></tr><tr><td>1</td><td>DECode TRLi4KskHxfACnxKzLr2wNHauWUQpwwzN</td></tr><tr><td>2</td><td>DECode 3046</td></tr></tbody></table>	0	4a504a94899432a9846e1aa406dceb1bcfd538bb839071d49d1e5e23f5bc30ef	1	DECode TRLi4KskHxfACnxKzLr2wNHauWUQpwwzN	2	DECode 3046
0	4a504a94899432a9846e1aa406dceb1bcfd538bb839071d49d1e5e23f5bc30ef							
1	DECode TRLi4KskHxfACnxKzLr2wNHauWUQpwwzN							
2	DECode 3046							
1	Address	SC TR7NHqjeKQxGTCi8q8ZY4pL8otSzglJ6t USD Token						
	Events	AddedBlackList(index_topic_1 address_user)						
	Topics	<table border="1"><tbody><tr><td>0</td><td>42e160154868087d6bfd0ca23d96a1c1cfa32f1b72ba9ba27b69b98a0d819dc</td></tr><tr><td>1</td><td>Hex 414049e71b23c0bad106e4e8dfd3f52a418f2a128a</td></tr></tbody></table>	0	42e160154868087d6bfd0ca23d96a1c1cfa32f1b72ba9ba27b69b98a0d819dc	1	Hex 414049e71b23c0bad106e4e8dfd3f52a418f2a128a		
0	42e160154868087d6bfd0ca23d96a1c1cfa32f1b72ba9ba27b69b98a0d819dc							
1	Hex 414049e71b23c0bad106e4e8dfd3f52a418f2a128a							
2	Address	SC TBPxhVAsuzoFnKyXtc1o2UySEydPHgATo						
	Events	Execution(index_topic_1 uint256 transactionId)						
	Topics	<table border="1"><tbody><tr><td>0</td><td>33e13ecb54c3076d8e8bb8e2881800a4d972b792045ffae98fd46d1365fed75</td></tr><tr><td>1</td><td>DECode 3046</td></tr></tbody></table>	0	33e13ecb54c3076d8e8bb8e2881800a4d972b792045ffae98fd46d1365fed75	1	DECode 3046		
0	33e13ecb54c3076d8e8bb8e2881800a4d972b792045ffae98fd46d1365fed75							
1	DECode 3046							