AMLBot

Tether Freeze Gap Becomes Laundering Loophole for Criminals

An Analytical Report

How Criminals Take Advantage of USDT Blacklisting Lag on Tron and Ethereum

Tether's USDT stablecoin is usually perceived as a compliance-friendly instrument in the crypto industry, with the company using its ability to freeze suspicious wallets as per law enforcement requests. However, AMLBot's Forensics Team finds a critical vulnerability: a significant lag between the initiation of a freeze and its on-chain enforcement – a delay that has already enabled the movement of over $78 million in USDT across Tron and Ethereum.

This delay originates from Tether's multi-signature contract setup on both Tron and Ethereum, transforming what should be an immediate compliance action into a window of opportunity for illicit actors. This delay between a freeze request and its on-chain execution creates a critical attack window, allowing malicious actors to front-run enforcement and move or launder funds before the freeze takes effect. Freeze delays like this can be exploited by hacker groups, insiders, or anyone with real-time monitoring tools and knowledge of how the freeze mechanism works. Such tools may have already been developed to automate the laundering process during the freeze delay window. It's possible to build a parser bot that monitors the blockchain for freeze request patterns and immediately alerts wallet owners — providing them just enough time to transfer their funds before the freeze is enforced.

This study explores how the freeze process works, why it's exploitable, documenting real-world cases where the delay enabled criminals to move millions before enforcement.

What was Discovered

Let's look at one concrete example.

Wallet Address: **TFq8nBxgbb9pjMw9fjT2uNRNuuhTgDdBed** on the Tron blockchain was flagged for blacklisting by Tether at **11:10:12 UTC**, but the freeze wasn't executed until **11:54:51 UTC on the same day** — a **44-minute delay.**

Verification Link

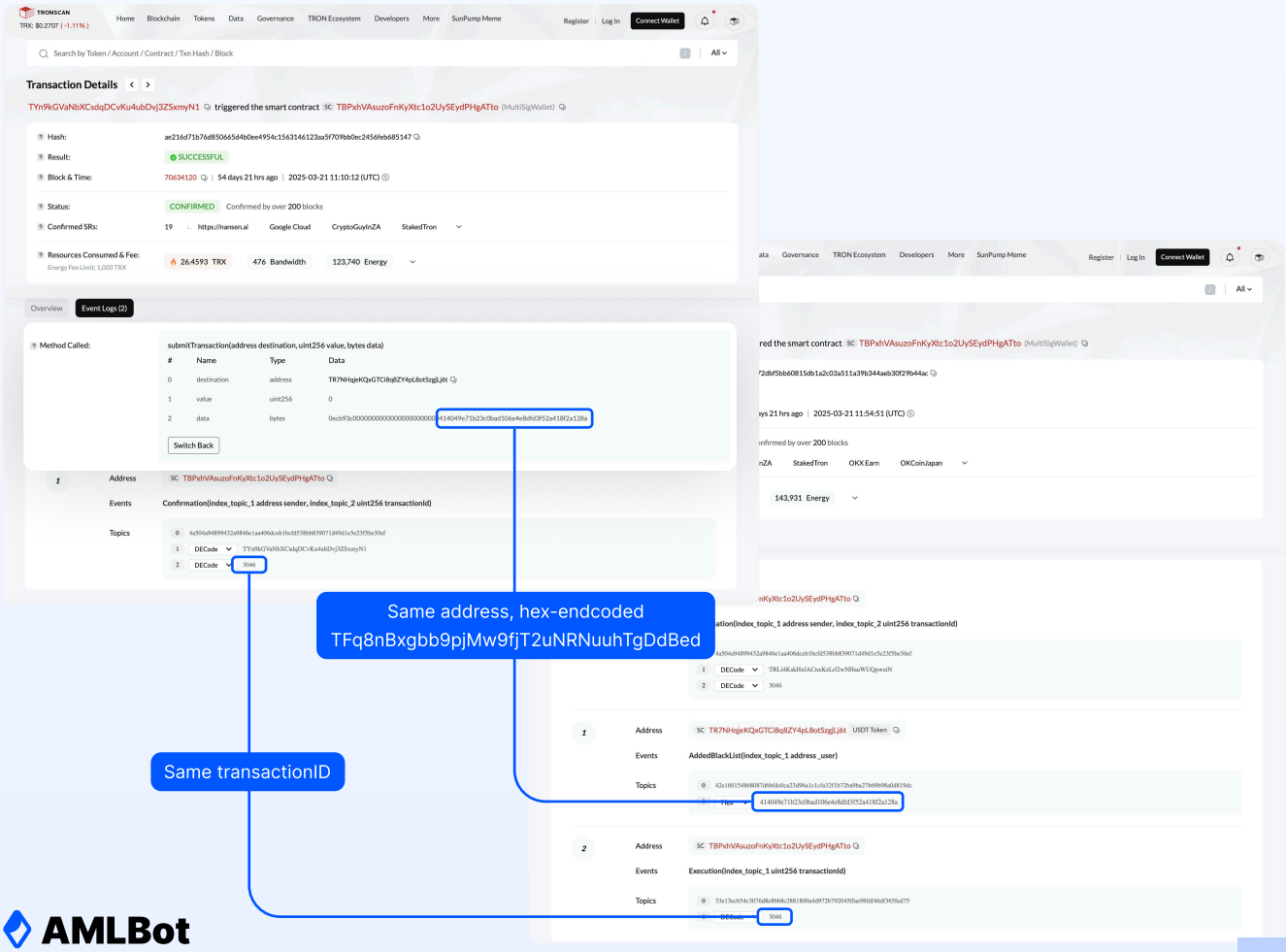
Submit https://tronscan.org/#/transaction/ae216d71b76d850665d4b0ee4954c1563146123aa5f709bb0ec2456feb685147/event-logs

Confirm https://tronscan.org/#/transaction/8fdd5aac1f1aedfd71a72dbf5bb60815db1a2c03a511a39b344aeb30f29b44ac/event-logs

How the Freeze Delay Unfolds On-Chain

The screenshots below show two related transactions on the Tron blockchain involving the same wallet:

TFq8nBxgbb9pjMw9fjT2uNRNuuhTgDdBed — the wallet targeted for freezing.



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 blocklist. 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.

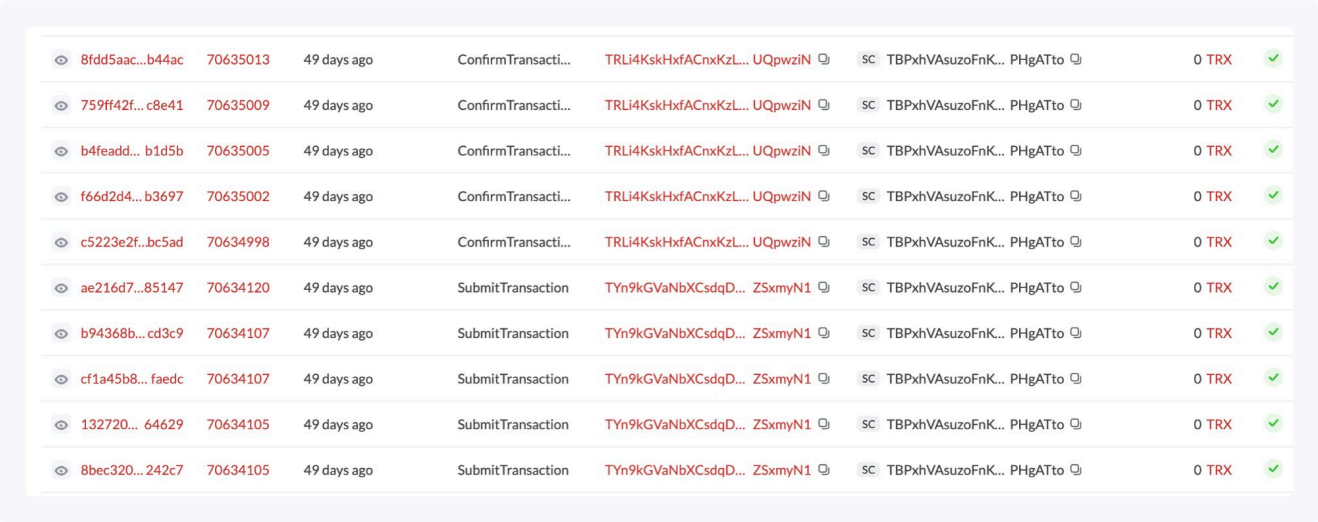
During this period, the wallet retained full access to **$426,183 USDT,** meaning any fast-acting operator could have moved the funds out before the freeze took effect. This isn't a theoretical weakness. It's happening in the wild, and bad actors are watching.

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	ConfirmTransacti...	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX
759ff42f... c8e41	70635009	49 days ago	ConfirmTransacti...	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX
b4feadd... b1d5b	70635005	49 days ago	ConfirmTransacti...	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX
f66d2d4... b3697	70635002	49 days ago	ConfirmTransacti...	TRLi4KskHxfACnxKzL... UQpwziN	SC TBPxhVAsuzoFnK... PHgATto	0 TRX
c5223e2f...bc5ad	70634998	49 days ago	ConfirmTransacti...	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, it creates a dangerous gap, and criminals who monitor the blockchain can easily exploit it." - AMLBot's Data and Forensics Team***

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. This occurred across a time frame spanning **November 28, 2017 to May 12, 2025.** 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.

Example of the Addresses That Avoided the Freeze Due to the Delay

blacklisted_address	tx_submit	tx_confirm	datetime_submit	datetime_confirm	delay (datetime_diff)	amount_withdrawn (during delay)
THy2dVfuPpdtSTXq571omBRnfXjpp78Von	ebf2326780479e92a0de7d72eaff0bb96fa0a5679bac2894eb7ebef03aabc806	5786956dd217533d8c7965bd1dbf9c2e49c47de9b93804c3d9195e0a5c12aa09	2025-05-12 16:15:15	2025-05-12 20:20:39	4:05:24	51886.08
TX39XnXfwabE2YhHnpcq4xhtrV1YhvDDg8	1788461a751f40cc396172110c82a0ed3dfe75bd378019a834f65455aca92e11	1d45f73f7c2879c2e3fb6ec4cb11ae0726d7f2c24bc78f706af62348e3ed4f6c	2025-05-12 16:01:45	2025-05-12 20:20:36	4:18:51	244076
TR6Z4GG2VuJCKbQV4pSYfrWHQVheq3cApc	5fb9ce909c44d77086a5df37b99b1d5c6b91e1ff1ea5053a5cdad2e6354f463b	fa840e5051d6afc6be1454ac428b95c9d1557e7645c55230d4a5fbcfe7439cf0	2025-05-09 11:25:06	2025-05-09 18:32:12	7:07:06	100
TXxCay7MF5apyCxGHvVC7ZSnMPNs39f3Aj	65f6585fb0d23e2301bafd37599a83c333d3d7af6c0b33181e8c60ddc4fd31d6	6369df3bc343dd9d5074b3b1fee3b327703c9919617b9bf778e627d4fa82e6d8	2025-05-07 13:10:54	2025-05-08 22:20:39	1 day, 9:09:45	616390
TD7pNjjV8h443FwD7BMLvE4jAwnSacfUNs	69f8e2a19a7bd84f94f533b96ca29a6efd3f432d7942b233cd6f9d0e87beb30e	d245d9864e54e93dd657dc24a17e26924e370e1761ebca94bcc30561d47521d4	2025-05-07 13:10:51	2025-05-08 22:20:39	1 day, 9:09:48	566
TFQGgsQXAVQuzafwMRMJerU1RWBDSXzS3G	68245fd560b9eac9334337d3a6b3d6b9b50b64039557ce77ffcf4de0b9749d39	7f1d4325517df1521bf5dfba5fc1b9cea68a3ba874eb86db83100520c8f40ecf	2025-05-08 12:35:45	2025-05-08 14:05:57	1:30:12	134125.1928

blacklisted_address	tx_submit	tx_confirm	datetime_submit	datetime_confirm	delay (datetime_diff)	amount_withdrawn (during delay)
TNUDtJPHYFomM3JtH5CpPEaJ2uSckST6g2	c5b291d7cd799a132433646b7e77b836bfe309c4fba638a3ae9048cc5feddfc7	b42cf454ce7ba8b8dcb12aefac343d365ff8a5a7895205fb9b068f16dece2752	2025-05-08 12:35:42	2025-05-08 14:05:51	1:30:09	130747.8273
TWUsSHYkXvgwoEwsVbwXPeF2XDcAqXMrjk	afbbd648b5fa659dfc1f3c63e5db10c2dca5ba538d617ec58d7e9cae55b3125a	e7dd17d10567699e83a0d28436f5be17f1cfd725ad2b6c147837e000f33f3d1f	2025-05-08 12:35:39	2025-05-08 14:05:48	1:30:09	261226.0615
TNxyvisLQ3zSqyJKuntxUasgwHPX66MfNR	d2bd1366695221be6d3cccfe6a875c845f076c919baa54fa863c7f68c279f7d9	0105693931c6e1fb4a1c9b9b8154b525c8e36b86f1c44a6aa2b59dc308f26bd1	2025-05-08 12:35:36	2025-05-08 14:05:45	1:30:09	140053.7523

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**

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 $150 billion in circulation as of May 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.”***