

Stablecoin Issuer Freeze Risk: A User-Centric Risk Management Framework

An Enterprise Framework for Stablecoin Asset Risk Identification,
Attribution Analysis, and Incident Response

By BlockSec

Preface

Stablecoins, represented by USDT and USDC, have become essential infrastructure for an increasing number of global enterprises engaged in payments, settlement, cross-border transfers, and treasury management. At the same time, enterprise risk awareness around stablecoins still tends to focus on private-key security and theft prevention, while a different category of risk — one with arguably greater operational impact — receives far less attention: the risk of being frozen by the stablecoin issuer.

It is important to note that stablecoin issuers are not the only actors capable of freezing user digital assets, including stablecoins. Centralized exchanges can restrict account trading and withdrawals; custodians can limit asset access for compliance or risk-control reasons; cross-chain bridges and wrapped-asset administrators (such as BitGo, the custodian for WBTC) may suspend transfers or redemptions of certain mapped assets; and courts, regulators, and law enforcement agencies can effectively freeze assets by directing these centralized control points. The Coinbase user agreement explicitly states that Coinbase may suspend accounts, suspend the sending of digital assets, or terminate transactions, while the Tether and Paxos terms expressly reserve the right to freeze relevant stablecoins where required by law or risk-control considerations.

For enterprises, however, freezes by stablecoin issuers carry particular significance. Even an enterprise that adopts a self-custody architecture and keeps no assets on exchanges may still lose normal control over its stablecoins simply because it holds an asset whose issuance and management remain centralized — including USDT issued by Tether and USDC issued by Circle. Both Tether and Circle

have explicit blacklist mechanisms in their stablecoin contract code, and Tether's legal documentation expressly states that it may freeze Tether Tokens where required by applicable law or where Tether deems it prudent.

This whitepaper focuses on the issue enterprises most need to confront directly: how stablecoin issuer freezes happen, why enterprises are easily exposed, how to prevent freezes, and how to identify root causes and engage with the issuer once a freeze has occurred.

Executive Summary

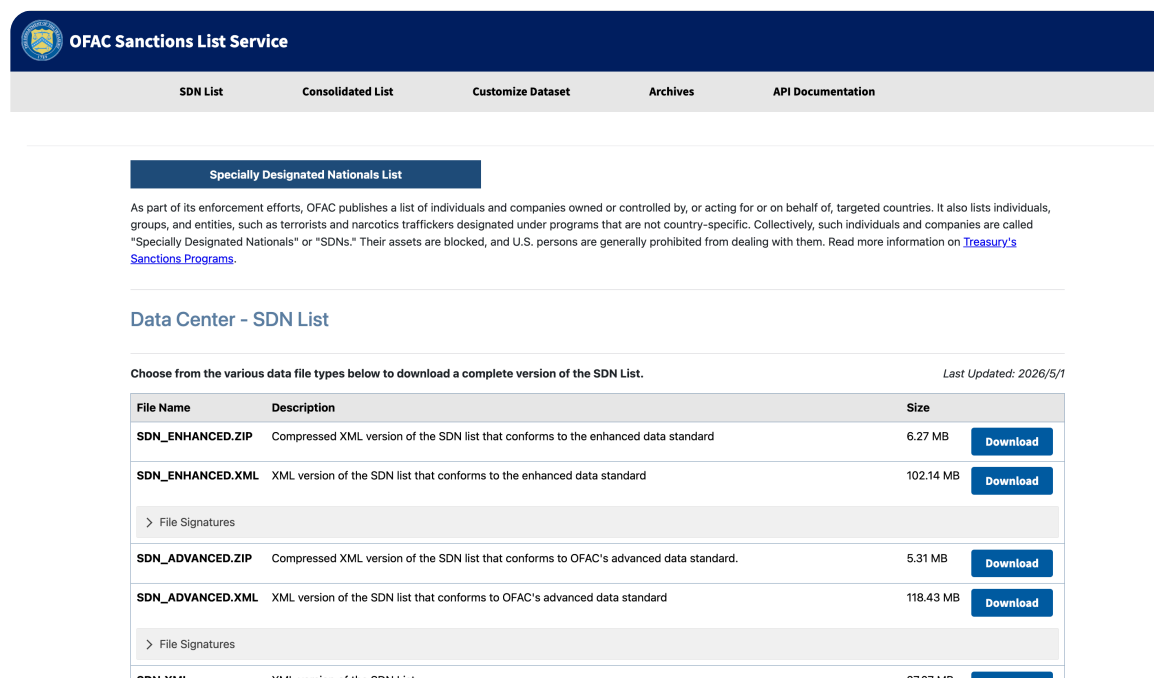
Stablecoin issuer freezes are not isolated incidents; they are an integral part of how centralized stablecoin systems are designed. Tether's legal terms expressly state that Tether may freeze a user's Tether Tokens (typically USDT) where required by applicable law or where Tether, in its own judgment, deems it prudent to do so. Both the Tether and Circle stablecoin smart contracts also expose administrative capabilities such as blacklisting (transaction restriction), and Paxos's terms similarly state that its compliance function must follow lawful orders to freeze access to assets it issues, including its U.S. dollar stablecoins.

Based on publicly available information, issuer freezes typically cluster around the following scenarios:

- Law enforcement, judicial, and regulatory requests;
- Sanctions list hits or sanctions-adjacent risk;
- High-risk fund flows linked to fraud, theft, money laundering, or terrorist financing;
- Proactive or semi-proactive measures taken during certain technical migrations, changes in chain support, or major risk events.

In 2023, Tether announced a voluntary freeze policy targeting newly listed addresses on the SDN List (the U.S. OFAC's Specially Designated Nationals and Blocked Persons List), and has since publicly disclosed multiple instances of cooperating with law enforcement to freeze funds related to terrorist financing or to sanctioned exchanges. Circle, when discontinuing support for USDC on the Flow

chain, also explicitly conducted freezes and balance snapshots.



OFAC Sanctions List Service

[SDN List](#) [Consolidated List](#) [Customize Dataset](#) [Archives](#) [API Documentation](#)

Specially Designated Nationals List

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked, and U.S. persons are generally prohibited from dealing with them. Read more information on [Treasury's Sanctions Programs](#).

Data Center - SDN List

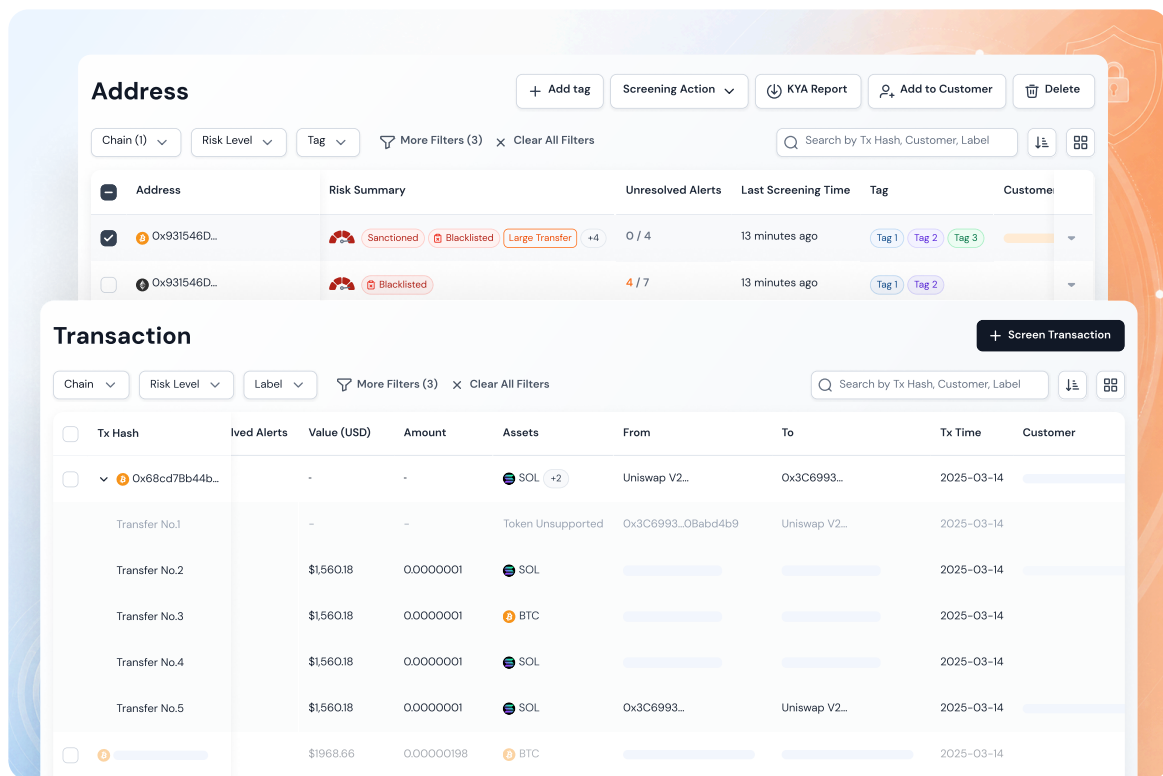
Choose from the various data file types below to download a complete version of the SDN List. Last Updated: 2026/5/1

File Name	Description	Size	
SDN_ENHANCED.ZIP	Compressed XML version of the SDN list that conforms to the enhanced data standard	6.27 MB	Download
SDN_ENHANCED.XML	XML version of the SDN list that conforms to the enhanced data standard	102.14 MB	Download
> File Signatures			
SDN_ADVANCED.ZIP	Compressed XML version of the SDN list that conforms to OFAC's advanced data standard.	5.31 MB	Download
SDN_ADVANCED.XML	XML version of the SDN list that conforms to OFAC's advanced data standard	118.43 MB	Download
> File Signatures			
SDN XML	XML version of the SDN list	27.07 MB	Download

Screenshot of the OFAC SDN List Webpage

For enterprises, the difficulty is not simply detecting that a freeze has occurred. The harder questions are: why was the freeze imposed, which batch of assets triggered the risk, has the contamination spread to the main treasury pool, and how should the company prepare materials to engage with the issuer? OFAC itself has stated that the digital currency addresses it publicly lists are typically not exhaustive — meaning enterprises that rely solely on whether an address appears on a public list are likely doing too little.

BlockSec believes that, in the stablecoin era, enterprise treasury security management must evolve from “safeguarding assets” to “managing asset availability.” Toward that end, BlockSec offers the following services:



Phalcon Compliance

- Through Phalcon Compliance, freeze-oriented KYT and KYA scanning capabilities that help enterprises identify risk across addresses, transaction paths, counterparties, and treasury pools, providing effective preventive control;
- Through its Treasury Security Management service, helping enterprises establish layering, segregation, monitoring, attribution, communication, and governance mechanisms to effectively isolate financial risk;
- After a freeze occurs, helping clients identify the cause, scope the impact, and engage with the stablecoin issuer.

Chapter 1

Why Stablecoin Freezes Are Becoming a Treasury Security Issue

1.1 Enterprises Increasingly Rely on Stablecoins for Payments, Settlement, and Treasury Management

Stablecoins are gradually evolving from a trading medium internal to crypto markets into critical infrastructure for enterprise payments, settlement, and capital movement.

The total market capitalization of stablecoins now exceeds USD 310 billion globally, indicating that a substantial liquidity base has formed. In recent years, alongside the rollout of stablecoin-related legislation, the use of stablecoins in cross-border payments has grown significantly, and a growing number of enterprises are turning to them to address pain points around transaction fees and settlement speed.

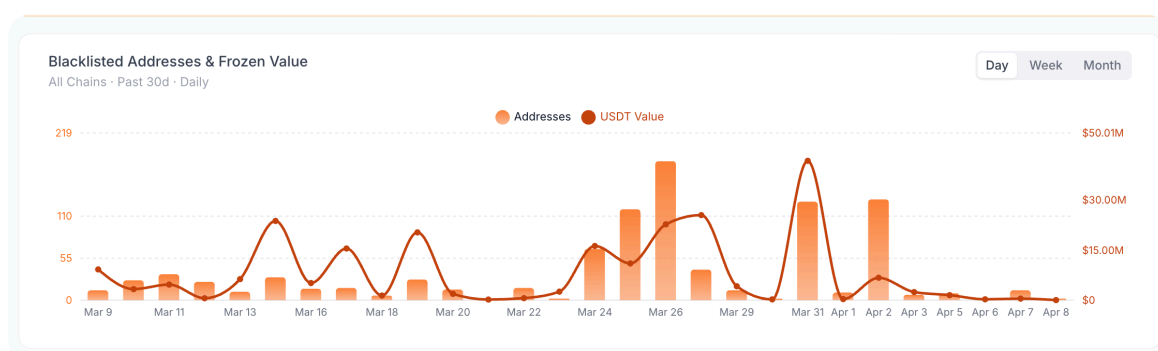
Once stablecoins take on the role of operational liquidity for an enterprise, the relevant risk is no longer simply “do we still hold the coins,” but rather “can we still transfer them, still pay with them, still move them” — that is, whether the wallet holding the stablecoins has been blacklisted or frozen.

1.2 Enterprise Understanding of On-Chain Asset Security Often Stops at “Theft Prevention”

When discussing on-chain security, many enterprises immediately think of private keys, multi-signature, MPC, hot/cold separation, and custody security. These controls are, of course, important, but they primarily address the questions of “who controls the address” and “how do we prevent assets from being stolen or sent in error.”

Stablecoin issuer freezes belong to a different category of risk: the private key remains under the enterprise’s control, yet the token itself becomes restricted in circulation and availability because the issuer exercises control at the contract, redemption, or chain-support layer.

According to BlockSec’s statistics, as of April 8, 2026, Tether had frozen 962 wallet addresses over the trailing 30 days — 835 on Tron and 127 on Ethereum — representing a total frozen amount of USD 228 million. Freeze risk warrants the same level of attention from enterprises as theft risk.



<https://blocksec.ai/usdt-freeze>

1.3 A Compliance Issue and a Treasury Security Issue

Stablecoin freezes are first and foremost a compliance issue. Issuer freeze actions are typically tied to sanctions, law enforcement cooperation, high-risk fund flows, abnormal counterparties, or other compliance-related risk. For enterprises, building strong compliance identification and risk screening — including continuous KYT (Know Your Transaction) and KYA (Know Your Address) scanning — is the foundational means of reducing the probability of being frozen and preventing high-risk funds from entering the treasury system in the first place.

Stablecoin freezes are not, however, only a compliance issue. Once a wallet address that holds core operational liquidity is frozen, the enterprise's ability to make stablecoin payments, perform settlements, and move funds is constrained — and the operational impact can be severe. Freezes are therefore equally a treasury security issue: enterprises must not only prevent risk from entering the system, but also implement more sophisticated treasury management, wallet layering, risk segregation, and real-time monitoring mechanisms to limit the impact of freeze events on overall treasury operations.

Chapter 2

Who Can Freeze Your Crypto Assets, and Why This Paper Focuses on Issuer Freezes

2.1 Freezes Do Not Originate Solely from Stablecoin Issuers

When an enterprise holds assets on-chain, potential sources of restriction extend well beyond stablecoin issuers.

- Centralized exchanges can restrict account access and the withdrawal, transfer, and trading of assets within those accounts. Binance, for example, expressly reserves the right in its Terms of Service to suspend or terminate accounts, and its Help Center documents that withdrawals may be paused for risk-control, identity-verification, wallet-maintenance, or network-upgrade reasons.
- Payment institutions and custodial payment platforms may also impose restrictions on cryptocurrency transactions, sales, and settlement. PayPal's cryptocurrency terms, for instance, expressly permit it to place a hold on related transactions or sale proceeds.

- Decentralized exchanges, cross-chain bridges, and wrapped-asset administrators — i.e., on-chain DApps — can also affect asset availability within their respective scope. A nuance worth flagging: a DEX typically cannot freeze a user's self-custodied wallet directly, but its operator can restrict access to the official front-end for specific addresses or assets. Uniswap Labs, for example, has publicly stated that it may impose interface-layer restrictions in response to legal and risk-control requirements. For cross-chain bridges and wrapped assets, users may hold the relevant token in their wallet, but minting, burning, release, and redemption typically still rely on the control logic of the bridge or its administrators — the wrapped-token-transfer mechanism described in Wormhole's official documentation is a representative example.

In short, the “freeze” an enterprise faces is not a single phenomenon. It can manifest as account-level restrictions, front-end restrictions, restrictions on bridged assets, or direct issuer-level restrictions on stablecoin addresses.

2.2 Why This Paper Focuses on Stablecoin Issuer Freezes

Although freezes have many possible sources, this paper focuses on stablecoin issuer freezes because their impact on self-custodied on-chain assets is the most direct. Many enterprises mistakenly assume that “keeping coins off exchanges” will spare them from freezes, but the public materials and source code of Tether and Circle make clear that centralized stablecoins, by their very design, can be controlled or restricted by their issuers.

For enterprises that use stablecoins for payments, settlement, and treasury management, issuer freezes are therefore not a peripheral concern but a core operational risk.

Chapter 3

Why Stablecoin Issuers Freeze

3.1 The Control Properties of Centralized Stablecoins

The reason centralized stablecoins can be frozen is, fundamentally, that they are not fully decentralized native assets. They are issued, redeemed, and administered through smart contracts by a specific legal entity. To take the leading examples: Circle's public stablecoin contracts and design documentation explicitly expose roles and capabilities such as blacklist, pause, mint, and burn; Tether's code likewise contains functions such as `addBlackList` that allow the issuer to blacklist accounts holding USDT.

At the same time, this control profile is being further institutionalized by emerging regulatory frameworks. The U.S. GENIUS Act expressly requires permitted payment stablecoin issuers to fulfill AML and sanctions compliance obligations and to maintain the technical capability to comply with lawful orders, with its definition of a "lawful order" clearly encompassing measures such as seize, freeze, burn, and prevent transfer. Hong Kong's stablecoin regulatory framework similarly imposes AML/CFT, risk management, redemption, and regulatory cooperation obligations on licensed issuers.

Given these two layers of properties, enterprises must abandon the assumption that “as long as I control the private key, no third party can affect my assets.” Issuer freezes are not an incidental capability — they are part of the institutional design of this asset class.

3.2 Common Issuer Freeze Scenarios

Public terms and case examples indicate that issuer freezes generally cluster around the following scenarios.

The first is law enforcement, judicial, and regulatory requests. Tether’s Law Enforcement Requests Policy describes how it handles information requests from law enforcement agencies worldwide and requires appropriate legal process. This is also the most often overlooked source: Tether may freeze an address pursuant to a request from law enforcement, judicial, or regulatory authorities, and such requests typically begin with a victim’s report.

The second is sanctions list hits and sanctions-adjacent risk. The OFAC Frequently Asked Questions explain that OFAC may add digital currency addresses to the SDN identifier fields, and explicitly note that these listings are typically not exhaustive. In 2023, Tether publicly announced that it would voluntarily freeze newly listed SDN wallet addresses, and would also freeze previously listed addresses that had not yet been frozen. In other words, with respect to SDN-listed wallet addresses, Tether will act proactively to freeze.

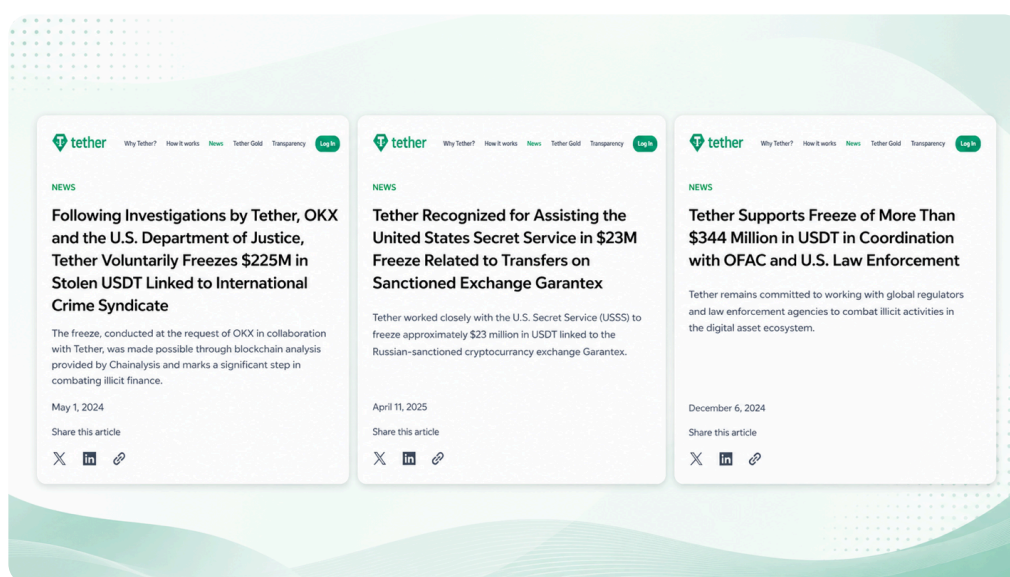
The third is high-risk funds related to fraud, theft, money laundering, or terrorist financing. Tether has publicly disclosed multiple instances of cooperating with U.S. law enforcement to freeze related funds, including funds associated with terrorist financing and funds tied to the sanctioned exchange Garantex.

The fourth is technical migrations or changes in chain support. When Circle discontinued USDC support on the Flow chain, it announced that it would freeze remaining assets and conduct a balance snapshot. Tether's Supported Protocols page likewise states that Tether no longer issues or honors redemption obligations on certain blockchains. For enterprises operating primarily on mainstream chains, this scenario can generally be set aside.

3.3 Patterns Reflected in the Public Record

Reviewing publicly verifiable materials, several patterns are consistently observable. First, law-enforcement-cooperation freezes are the most readily verifiable from outside the issuer. Across Tether's public news releases and policy disclosures, many freeze cases are tied to law-enforcement coordination, sanctions enforcement, or anti-fraud cooperation.

Second, proactive risk control is also a real phenomenon — particularly in the SDN context, where Tether has publicly committed to voluntarily freezing newly listed addresses.



Tether News Screenshot

Third, issuers do not look only at “whether an address precisely matches a public list.” OFAC has expressly stated that its public digital currency addresses “are unlikely to be exhaustive,” which means that, in practice, risk identification frequently extends to associated transaction paths, upstream and downstream relationships, and broader risk exposure.

Chapter 4

Why Enterprises Are Exposed to Issuer Freeze Risk

4.1 Address and Counterparty Risk Is Not Visible

Many enterprises have a reasonable understanding of their counterparties' off-chain identities, yet have little visibility into their on-chain addresses, related address clusters, or historical interactions. The OFAC mechanism itself reflects the principle that risk identification depends not solely on "is the address on a sanctions list," but also on on-chain analysis of digital currency addresses and related identifying information to assess risk exposure. Issuers and service providers, when conducting risk control, similarly do not focus only on whether an enterprise "subjectively believes its business is normal" — they place greater weight on on-chain risk exposure to illicit actors.

Off-chain documentation can be falsified, but on-chain fund flows cannot. The transparency, public visibility, and immutability of blockchain make it possible for fund flows from illicit entities to be identified and traced through professional on-chain anti-money-laundering platforms.

What this means is: a counterparty viewed as “normal” by the enterprise may, in the eyes of an issuer or an on-chain AML system, sit in an address cluster with significant interactions with high-risk services, sanctioned entities, or anomalous fund networks. The relevant risk arises not only from explicit sanctions designations but also from on-chain interactions tied to fraud, terrorist financing, ransomware, hacking, darknet markets and trading, drug trafficking, human trafficking, and other illicit activities.



Risk Of On-Chain Interactions with Illicit Activities

For example, if an enterprise’s counterparty uses an address linked to North Korean hacking activity, the issuer may still freeze related funds even if that address is not currently on a sanctions list, because it may form part of a network involved in money laundering, hacking proceeds, or sanctioned activity. Enterprises therefore need the capability to trace and identify these latent high-risk interaction paths, rather than relying solely on explicit list-based information.

4.2 Funding Sources and Historical Paths Are Not Visible

When an enterprise receives a stablecoin payment, the relevant risk does not necessarily originate from the immediate sender — it may stem from a much earlier point in the historical path. OFAC has expressly stated that its publicly listed addresses are typically not a complete list, and so checking only whether the current address is on a list is insufficient to reconstruct whether a batch of assets has earlier-stage risk exposure.

In many cases, the source of funds may involve multi-hop transactions: for example, a stablecoin transfer may first pass through an address controlled by a sanctioned actor, after which laundered funds eventually arrive at the enterprise's address. This kind of "historical contamination" is not easy to identify, because freeze risk is not driven solely by the current transaction but spans multiple transaction layers. Once historically contaminated assets enter the main operations pool, consolidation pool, or reserve pool, what was "per-receipt risk" can escalate into "main-pool availability risk." Enterprises must therefore continuously monitor fund flows and understand the lifecycle trajectory of their funds, rather than relying on a single point-in-time compliance check at the moment of each transaction.

4.3 Wallet and Treasury Pool Architecture Is Inadequate

If an enterprise's treasury architecture has no layering, the impact surface of an issuer freeze expands significantly. Once a particular asset on a particular address or chain becomes unavailable, whether the enterprise can isolate the impact and maintain business continuity depends largely on the extent to which its funds are commingled.

For example, a company that has not implemented funds layering — keeping all assets concentrated in a single primary wallet on a single chain — exposes itself to the risk that, the moment that wallet has any interaction with a high-risk address, the entire wallet and treasury pool become exposed to potential freezing. The impact would extend across the company's operations, not merely a single transaction. Once that wallet is frozen, all dependent payments, settlements, and capital movements are constrained.

Enterprises should therefore design a sensible treasury pool architecture, using layering and segregation to limit the impact of freeze risk on the broader fund flow.

4.4 Lack of Continuous Monitoring and Systematic Governance

Risk is not static. OFAC lists are updated, new law-enforcement information and case tags continue to emerge, and on-chain criminal activity evolves rapidly. Risk identification is a continuous process, not a one-time event.

If an enterprise screens funds only once at receipt, with no ongoing monitoring, review, or update process, then funds that appear “normal” at intake can later expose freeze risk. A payment may pass intake screening today, only to be retroactively at risk because the on-chain sanctions list is updated or new illicit addresses appear in the transaction path. To prevent this, enterprises deploying KYT (Know Your Transaction) systems should pay close attention to real-time monitoring capabilities and conduct regular reviews and updates of treasury pools and wallet addresses.

Chapter 5

BlockSec's Methodology for Freeze Risk Identification and Attribution

5.1 Enterprises Cannot Rely on "Is the Address on a Public List" Alone

OFAC's FAQ confirms both that addresses can be added to the SDN identifier fields and that those listings are typically not exhaustive; the FAQ for OFAC's search tool likewise clarifies that digital currency addresses can only be searched by exact match within the "ID #" field.

What this means is that public-list screening is only a baseline control. It can help an enterprise identify high-risk addresses that have already been explicitly listed, but it cannot fully answer the more important question: is this batch of assets associated with a high-risk actor, sanctions path, or major case?

5.2 Four Dimensions of Freeze Risk Identification

BlockSec decomposes issuer-freeze risk identification into four dimensions.

The first is address risk: whether the address itself already carries publicly known high-risk markers, sanctions identifiers, or anomalous tags. OFAC's digital-currency-address mechanism provides the foundational external reference at this layer.

The second is path risk: the high-risk actors, services, or paths the address has interacted with before and after entering the enterprise treasury. Tracing such interactions cannot be limited to direct counterparties — it should extend to multi-hop tracing of the counterparty's own funding sources.

The third is behavioral risk: enterprises should not focus on a single address in isolation, but should also examine whether the counterparty controls multiple related addresses, exhibits historical anomalies, or shows clearly abnormal transaction behavior such as fund splitting. The fourth is treasury-pool risk: whether risky assets have already entered the main treasury pool, whether they have been commingled with normal assets, and whether they may continue to spread through consolidation and outbound flows.

5.3 Core Questions in Freeze Event Attribution

When a freeze has already occurred, what an enterprise typically needs to answer is not the generic question “why were we frozen,” but a series of more specific questions:

- Which address or batch of assets triggered the risk;
- Whether the risk originates upstream, downstream, or from historical contamination;
- Whether the freeze stems from a direct high-risk identifier hit or from exposure detected via associated paths;
- Whether the risk has spread into the main treasury pool;
- Which addresses and transactions require focused explanation.

Without answers to these questions, the enterprise has little foundation on which to build subsequent communication and remediation.

5.4 Why Attribution Capability Determines the Effectiveness of Subsequent Communication

An issuer freeze does not necessarily preclude a productive dialogue, but the precondition for effective communication is that the enterprise itself first understands clearly what happened. Both Tether and Circle provide official support and ticketing channels; however, an enterprise that can only assert in general terms that “we are conducting normal business,” without clearly identifying key addresses, transactions, timelines, and risk sources, will struggle to construct a targeted explanatory framework.

In BlockSec’s view, attribution capability is therefore not a value-add — it is a prerequisite for engaging with issuers.

Chapter 6

How BlockSec Helps Enterprises Prevent and Manage Issuer Freeze Risk

6.1 Phalcon Compliance: KYT Capability Tailored to Freeze Risk

In stablecoin issuer freeze risk management, what enterprises need is not simply the ability to “check an address,” but the capability to maintain continuous visibility into risk. To that end, Phalcon Compliance can serve as the day-to-day KYT capability layer for enterprises, helping them maintain ongoing visibility across four dimensions — addresses, paths, counterparties, and treasury pools — and elevating one-off address checks into continuous risk monitoring.

In practice, this capability is particularly well-suited to deployment at several key control points: before receipt, to assess whether to accept funds from a specific address; before consolidation, to assess whether to merge a particular batch of assets into the main pool; before outbound transfers, to assess whether to send funds to a higher-risk counterparty;

and on a recurring basis, to re-examine whether the historical risk exposure of held assets has changed. This approach is consistent with the continuously updated nature of OFAC's sanctions data: risk control is not a one-time validation, but ongoing monitoring.

6.2 Treasury Security Management Service: Governance Capabilities for Enterprises

Tools alone help enterprises “see” the problem, but actually reducing freeze risk requires translating identification capability into organizational mechanisms and treasury architecture. With issuer freezes as the central risk, BlockSec's Treasury Security Management service places greater emphasis on the following governance actions:

- Wallet and treasury-pool layering, to reduce the probability of risk spreading from peripheral addresses into the main pool;
- Stablecoin exposure management, to avoid concentrating critical operating liquidity in a single issuer or a single chain version;
- Risk segregation mechanisms, to separately manage high-risk batches, watchlist batches, and main operating batches;
- Routine screening and review, embedding intake, consolidation, outbound, and held-asset re-examination into standard operating procedures;
- Freeze-incident response plans, defining escalation paths, materials preparation, and external communication protocols before a risk event occurs.

This methodology does not promise that an enterprise “will never be frozen.” It aims to reduce risk exposure, contain the spread of contamination, and improve incident response efficiency.

6.3 BlockSec's Value Proposition

BlockSec's positioning is not solely that of an on-chain risk-identification tool provider, nor is it limited to running a one-off review only after a freeze occurs. More precisely, BlockSec's role spans three layers:

- Through Phalcon Compliance, helping enterprises "see" freeze risk clearly;
- Through the Treasury Security Management service, helping enterprises convert risk identification into governance capability;
- After a freeze has occurred, helping clients identify the cause, scope the impact, prepare materials, and engage with the stablecoin issuer.

Chapter 7

How BlockSec Supports Enterprises That Have Already Been Frozen

7.1 Quickly Identify the Cause of the Freeze

When a freeze has occurred, the enterprise first needs to determine: is this in fact an issuer freeze? Typical indicators include the inability to transfer a specific stablecoin out of an address while the address still holds native gas assets normally, or other assets in the same address remain unaffected while a specific stablecoin alone is restricted.

The simplest approach is to scan the address in BlockSec's AML system and check whether it has been flagged as "Blocked". <https://app.blocksec.com/phalcon/compliance>

Once a freeze is confirmed, the enterprise should immediately notify upstream and downstream parties to halt further transfers to the address.

At this stage, BlockSec's role is to help the client rapidly trace back across three dimensions — address, transaction, and path — and to clarify, to the extent possible, where the trigger was, whether the issue is point-level or pool-level, whether the risk originates upstream or from historical contamination, and whether there is clear sanctions-related or case-related exposure.

7.2 Quickly Determine the Scope of Impact

After the cause is clarified, the second step is to determine the scope of impact. Enterprises typically need to know:

- Which addresses have already been affected;
- Which batches of assets have been contaminated or need to be isolated;
- Whether the main consolidation pool, operations pool, and reserve pool are subject to collateral impact;
- Which business paths will be interrupted or delayed as a result.

The objective at this step is to prevent a freeze from escalating into a broader treasury disruption.

7.3 Assistance in Assembling Communication Materials

Before contacting a stablecoin issuer, the enterprise typically needs to prepare a complete, clear, and verifiable set of materials. With Tether as an example, its official support channel allows users to submit tickets, problem descriptions, and attachments; its Law Enforcement Requests Policy also makes clear that, for matters involving freezes or information requests, Tether processes these in accordance with applicable legal procedures.

From a practical standpoint, enterprises should prioritize preparing the following types of information:

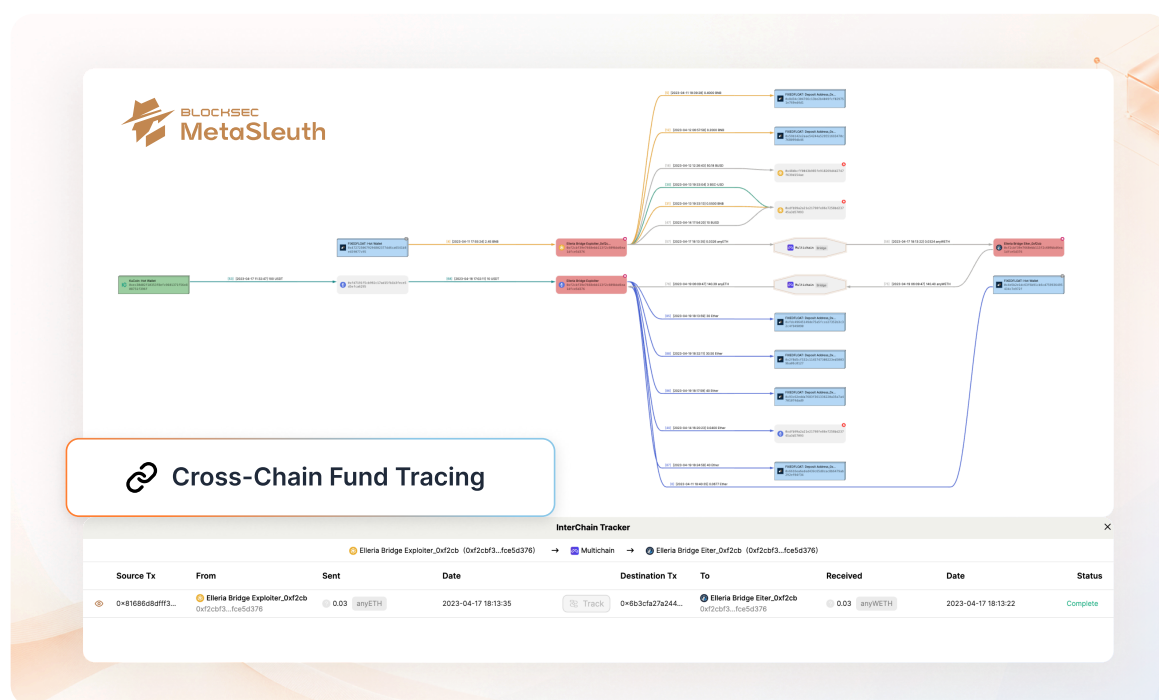
- Baseline factual information: affected addresses, affected chains, affected tokens, affected amounts, and the time the freeze was first observed;
- Key transaction information: critical Tx around the freeze, principal upstream sources and downstream destinations, and associated addresses;
- Business context: descriptions of the use of funds, transaction context, principal counterparties, orders or contracts, payment vouchers, chat records, and similar evidence;
- Explanatory materials: an event timeline, a fund-flow summary, and other questions the enterprise wishes to clarify.

In practice, after the enterprise submits materials to the issuer, follow-up handling typically centers on a few core questions: whether the freeze is connected to a formal law-enforcement or judicial request, the jurisdiction or case type to which the freeze corresponds, and what additional facts or supporting documentation will be required next. Tether's public policies state that it relies on appropriate legal process when handling such requests, which means enterprises should focus their continued engagement on the nature of the case, the originating authority, the supplementary materials needed, and the proper communication channel. If the matter clearly involves criminal investigation, an enforcement order, or cross-border judicial assistance, counsel should be brought in early; BlockSec can assist in this process.

7.4 Engagement Support with the Stablecoin Issuer

After a freeze, many enterprises find that the problem is not a lack of materials but the inability to assemble those materials into a clear, coherent explanatory narrative. Building on its on-chain analysis results, BlockSec can help clients articulate more clearly the likely cause of the freeze, the source of risk, the scope of impact, and the control actions already taken — supporting more targeted communication between the client and the stablecoin issuer.

It is important to emphasize that BlockSec's value is not in making decisions on the issuer's behalf, but in helping clients translate complex on-chain transactional behavior into a structured explanation that can be communicated and understood.



MetaSleuth

In a freeze event, communication is not simply about “submitting materials.” It hinges on whether the enterprise can clearly explain the cause of the freeze, the key time windows, and the source and destination of the funds. This is precisely the core value of professional on-chain analysis. Leveraging MetaSleuth, BlockSec can visually trace and reconstruct the complete fund flow within key time windows, identify principal upstream sources, downstream propagation paths, related address clusters, and anomalous nodes — helping the enterprise produce a more precise path-level explanation.

Equally important for the enterprise is comprehensive evidence preservation and a robust compliance workflow. If the enterprise can provide clear business context, orders or contracts, payment records, address-attribution explanations, an internal-response timeline, and a continuous record of KYT/KYA risk control, it is in a much stronger position to demonstrate that it has not knowingly participated in high-risk activity, or that it took prompt control measures upon detecting anomalies.

Beyond on-chain attribution analysis, BlockSec can also help clients translate complex on-chain facts into clearer, more explainable, and more communicable explanatory materials.

In more complex cases, BlockSec can also coordinate with attorneys who hold relevant overseas qualifications and have experience with digital-asset cases: BlockSec provides the on-chain attribution, fund-path analysis, and technical explanation, while counsel addresses the procedural requirements of the specific jurisdiction and supports the client through subsequent communication. This combined “technical analysis + legal coordination” approach is generally far more effective than the piecemeal submission of fragmented information.

7.5 Post-Incident Review and Governance Improvement

Once the freeze incident has been resolved, what matters most is the post-mortem: how did the risk first enter the treasury system, which control points failed to function, and which fund paths should have been identified at an earlier stage? Enterprises should specifically examine whether the impact was amplified by inadequate high-risk-address detection, blind spots in historical paths, fund commingling, excessive concentration in a single stablecoin, or the absence of continuous monitoring. Truly effective governance improvement is therefore not about adjusting the wallet structure or appending an emergency response plan; it requires building a routine, ongoing address-scanning and monitoring mechanism that covers address screening, transaction monitoring, historical path analysis, and continuous early warning. Only in this way can an enterprise transform the lessons of a single freeze incident into long-term treasury resilience, rather than reverting to reactive handling the next time risk arises.

7.6 What On-Chain Data Reveals About Unfreeze Outcomes

According to on-chain statistics from BlockSec's USDT Freeze Tracker, as of April 9, 2026, Tether had unfrozen 69 addresses on Ethereum and Tron over the trailing 30 days, corresponding to approximately USD 29.03 million in unfrozen funds. The data is based on public on-chain events on Ethereum and Tron and is tracked in real time by BlockSec.

For enterprises, this means that, although freeze events tend to come with significant urgency and uncertainty, they do not necessarily translate into permanent loss of access.

In a number of cases, if the enterprise can promptly identify the cause of the freeze, recognize the fund paths within the relevant time window, prepare comprehensive background materials, and engage continuously with the issuer or relevant authorities, there is meaningful scope for the case to advance — and, in some cases, for assets to be unfrozen.

Chapter 8

How Enterprises Should Build a Treasury Security Management System for Issuer Freezes

8.1 From “Safeguarding Assets” to “Managing Asset Availability”

In the stablecoin era, enterprise treasury security should not be designed solely around “whether assets will be lost.” Equally important, in a multi-chain, multi-counterparty, multi-business-path, and dynamically evolving sanctions environment, is whether the enterprise can continuously maintain identifiable and isolatable risk, transferable funds, and recoverable assets following a freeze.

8.2 Four Capabilities Enterprises Should Possess

At a minimum, enterprises should possess four foundational capabilities:

Risk Identification Capability — continuous identification of address, path, counterparty, and treasury-pool risk. Risk Segregation Capability — layered management that separates high-risk batches and watchlist batches from main operating funds. Freeze Attribution and Communication Capability — rapid reconstruction of cause, timeline, and impact scope after a risk event, producing materials suitable for external communication. Continuous Governance Capability — translation of individual case experience into improvements in policy, process, and architecture, reducing the probability of recurrence.

8.3 BlockSec's Position

BlockSec's view is that what enterprises truly need in the stablecoin era is not a set of isolated list-screening actions. Rather, what is needed is an end-to-end treasury security management system covering the pre-event, in-event, and post-event phases. Within that system, Phalcon Compliance addresses the problem of "seeing risk"; the Treasury Security Management service addresses the problem of "containing risk"; and attribution and communication support during freeze events addresses the problem of "how to restore order after risk has materialized."

Appendix A Enterprise Freeze Risk Self-Assessment Checklist

Enterprises can use the following questions for a quick self-assessment:

- Do you clearly know your stablecoin exposure ratio in the main operating funds, broken down by issuer?
- Have you separated receipt, consolidation, operations, and reserve funds from any potentially contaminated funds?
- Do you perform screening at intake?
- Do you continuously monitor held assets and key wallet addresses?
- Do you check only whether addresses appear on public lists, or focus only on direct interaction risk, while ignoring multi-hop risk?
- Can you produce, within one hour, the principal sources and key transactions for any given batch of stablecoins?
- Have you established unified escalation procedures, materials templates, and communication paths for freeze events?
- Are you over-reliant on a single issuer, single chain version, or single liquidity channel?
- Can you quickly determine the impact scope after a freeze occurs?

Multiple negative answers above generally indicate that meaningful governance gaps remain in your defenses against issuer freeze risk.

Appendix B Freeze Incident Emergency Checklist

When an enterprise suspects a stablecoin issuer freeze, the following actions should be prioritized:

- Immediately confirm whether only specific stablecoins are affected.
- Halt further inbound, consolidation, and outbound transfers for the affected address to prevent contamination spread.
- Lock down key addresses, key Tx, key timestamps, and recent abnormal inbound/outbound transfers.
- Distinguish between an issuer freeze, a platform freeze, or a chain migration / service-discontinuation event.
- Immediately assess whether the main operations pool, consolidation pool, and reserve pool may be collaterally affected.
- Stand up a unified internal response group across finance, security, risk, and legal.
- Use on-chain analysis to produce an address list, transaction list, timeline, and risk-path narrative.
- Prepare structured materials for engagement with the issuer and submit them through official channels.
- After the incident is contained, review fund paths, segregation design, and process control gaps.

Source List

The following are the principal first-party and official sources used in this whitepaper:

- Tether Legal — Tether’s official legal terms covering freezing, suspension, and termination of service.
- Tether Introduces New Policy to Strengthen Ecosystem Security — Tether’s official announcement of its voluntary freeze policy for newly listed SDN addresses.
- Tether Law Enforcement Requests Policy — Tether’s official law-enforcement-request handling page.
- Tether Acknowledged by U.S. Authorities for Freezing \$1.6M Connected to Terrorism Financing — Tether announcement on its freeze cooperation in terrorism financing cases.
- Tether Recognized for Assisting the United States Secret Service in \$23M Freeze Related to Garantex — Tether announcement on assistance with sanctioned-exchange-related freezes.
- Tether Supported Protocols — Tether’s official supported-protocols page, indicating chains where issuance and redemption obligations no longer apply.
- Circle stablecoin-evm repository — Circle’s official public repository for its EVM-compatible stablecoin contracts.
- Circle stablecoin-evm design docs / Pausable logic — Circle’s public design documentation and code, covering pause, blacklist, and related capabilities.

- Circle USDC on Flow manual migration process — Circle Help Center documentation describing the freeze-and-snapshot arrangements when Flow chain support was discontinued.
- OFAC FAQ 562 / 563 / 594 — OFAC official FAQs on the identification of digital currency addresses within the SDN List, their non-exhaustive nature, and exact-match requirements in the search tool.
- OFAC Sanctions List Service — OFAC's official list-download service, documenting the continuous-update nature of sanctions data.
- Coinbase User Agreement / Account restriction materials — Coinbase's official user agreement and Help Center documents describing how a centralized platform may restrict accounts or asset transfers.
- Paxos Terms and Conditions – Illegal Activity — Paxos's official terms regarding the freezing of asset-backed tokens it issues pursuant to lawful orders.