هجوم ایرانیان به بازار رمزارزها در بحبوحه تنش‌های ژئوپلیتیکی

اقدامات تحریمی بین‌المللی، ماشین جنگی روسیه را مختل می‌کند

تألیف: تیم چینالیسیس (Chainalysis)
ترجمه: سپهر هاشمی
تاریخ: ۰۳ اسفند ماه ۱۴۰۳

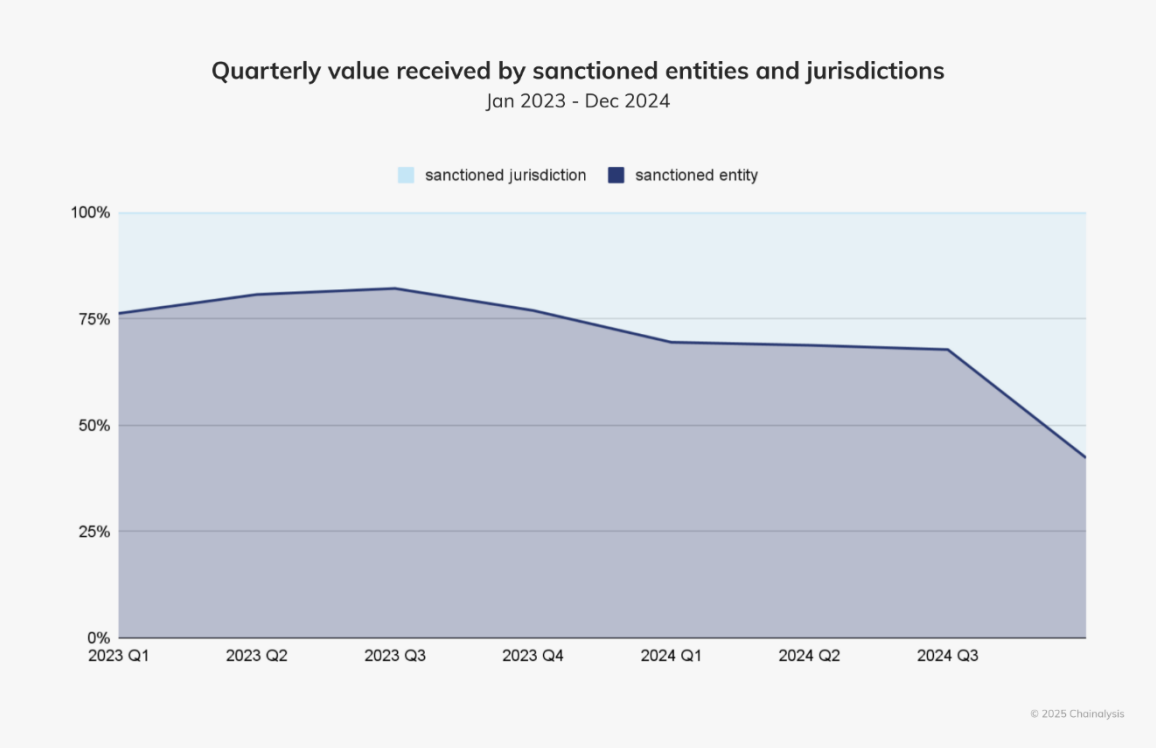
این مقاله در تاریخ ۱۹ فوریه ۲۰۲۵ مصادف با ۱ اسفند ۱۴۰۳ منتشر شده است. منبع

مقدمه

در سال ۲۰۲۴، تحریم‌ها هم در دامنه و هم در استراتژی تغییر کردند و منعکس‌کننده تحولی گسترده در فعالیت‌های غیرقانونی درون‌زنجیره‌ای در واکنش به افزایش تنش‌های ژئوپلیتیکی بودند. ازآنجایی‌که نهادهای تحریم‌شده به کانال‌های مالی جایگزین مانند رمزارز روی می‌آورند، دفتر کنترل دارایی‌های خارجی (OFAC) خزانه‌داری ایالات متحده تلاش‌های خود را برای از بین بردن زیرساخت‌های مالی حامی دولت‌های تحریم‌شده تشدید کرده و از بانکداری سنتی فراتر رفته است. ایالات متحده و متحدانش به هدف قرار دادن اقتصاد جنگی روسیه ادامه دادند، درحالی‌که اقدامات علیه سپاه پاسداران انقلاب اسلامی ایران تشدید شد و تعهدی عمیق‌تر به مهار هرگونه تأمین مالی تحت حمایت دولت‌ها[1] را نشان داد.

نهادها و حوزه‌های قضایی تحریم‌شده در سال ۲۰۲۴، ۱۵.۸ میلیارد دلار رمزارز دریافت کرده‌اند که حدود ۳۹٪ از کل تراکنش‌های غیرقانونی رمزارز را تشکیل می‌دهند. در مجموع، OFAC تعداد ۱۳ دستور تحریم صادر کرد که شامل آدرس‌های رمزارزی می‌شد (کمی کمتر از سال ۲۰۲۳) اما همچنان در رده دومین رقم بالا در هفت سال گذشته بود.

برخلاف سال‌های قبل، حوزه‌های قضایی تحریم‌شده سهم بی‌سابقه‌ای از کل فعالیت‌های مربوط به تحریم‌ها را در مقایسه با نهادهای فردی به خود اختصاص دادند و تا پایان سال ۲۰۲۴، نزدیک به ۶۰٪ مبلغ را در اختیار داشتند، همانطور که در تصویر زیر می‌بینیم:



تصویر ۱: مبلغ دریافتی فصلی توسط نهادها و حوزه‌های قضایی تحریم شده

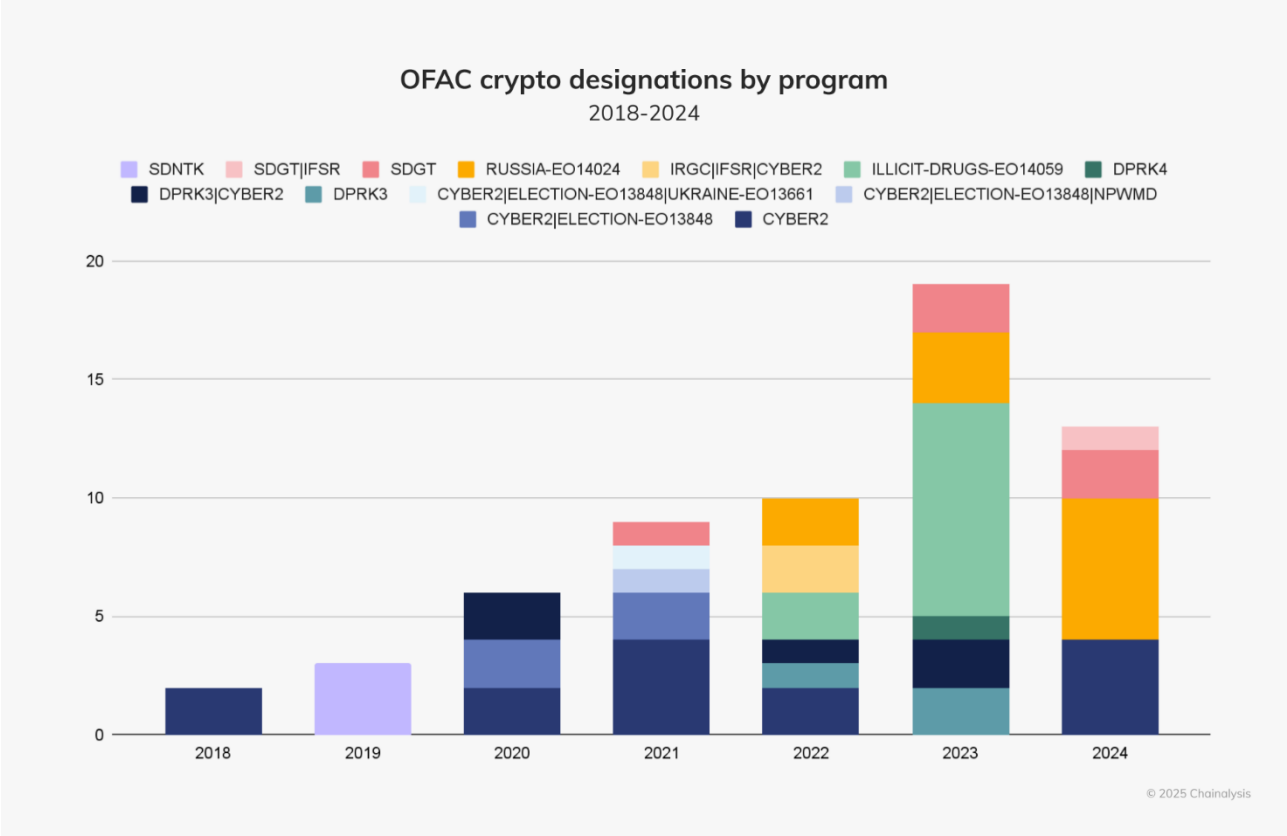
[1] State-backed financing

این تغییر تا حد زیادی ناشی از افزایش استفاده ایران از رمزارز بود. همانطور که در ادامه بررسی خواهیم کرد، صرافی‌های متمرکز ایرانی افزایش چشمگیری هم در استفاده و هم در خروج سرمایه داشتند و الگوهای تراکنش نیز نشان‌دهنده فرار سرمایه[1] بودند. این امر نشان‌دهنده روندی گسترده‌تر در میان ساکنان حوزه‌های قضایی تحریم‌شده است که به رمزارز به عنوان یک سیستم جایگزین در محیط‌های اقتصادی محدود روی می‌آورند.

تحریم‌ها در سال ۲۰۲۴ زیرساخت‌های مالی اصلی را هدف قرار دادند

در سال ۲۰۲۴، تحریم‌های OFAC مربوط به رمزارز از هدف قرار دادن افراد و گروه‌های کوچک فراتر رفت و مستقیماً زیرساخت‌های مالی حامی فعالیت‌های غیرقانونی را هدف قرار داد. اگرچه که تحریم‌های جدید کمتری در رابطه با رمزارز صادر شد، اما ردپای مالی نهادهای هدف همچنان قابل توجه باقی ماند.

در نمودار زیر که توسط فرمان اجرایی[2] و برنامه تحریم[3] ترسیم شده است می‌توانیم ببینیم که ترکیب تحریم‌های رمزارزی OFAC در طول زمان چگونه تکامل یافته‌اند:



تصویر ۲: دستورهای OFAC توسط برنامه تحریم

---

[1] Capital Flight

[۲] منظور همان Executive Order یا دستور اجرایی رئیس جمهور ایالات متحده است.

[۳] به مجموعه قوانین، مقررات و اقداماتی اشاره دارد که توسط دولت یا سازمان‌های بین‌المللی برای اعمال فشار اقتصادی، سیاسی یا نظامی بر یک کشور یا گروه خاص اتخاذ می‌شود. در مورد ایران، برنامه‌های تحریمی مختلفی توسط ایالات متحده، اتحادیه اروپا و سازمان ملل متحد وضع شده است که هر کدام اهداف و محدودیت‌های خاص خود را دارند.

این تمرکز بیشتر در افزایش استفاده از دستور اجرایی شماره ۱۴۰۲۴ مشهود بود، در رابطه با فعالیت‌های مضر خارجی مشخص‌شده از دولت فدراسیون روسیه، که به برنامه غالب برای تحریم‌های مرتبط با رمزارز تبدیل شد، زیرا ایالات متحده و متحدانش تلاش‌ها برای تضعیف زیرساخت مالی روسیه را تشدید کردند. تلاش‌های تحریمی در درجه اول بر شبکه‌های تسهیل‌کننده فرار از تحریم‌ها، جرایم سایبری، و تدارکات نظامی متمرکز بودند.

اقدامات اساسی هدف قرار دادن فعالیت رمزارز روسیه

در سال ۲۰۲۴، آژانس‌های غربی مجموعه‌ای از سرکوب‌های اساسی را علیه نهادهای رمزارزی مرتبط با روسیه که نقش‌های کلیدی در حمایت از اقتصاد جنگی روسیه، فعالیت‌های سایبری غیرقانونی، و شبکه‌های جنایی سازمان‌یافته ایفا می‌کردند، آغاز کردند.

۲۳ آگوست ۲۰۲۴

OFAC شرکت KB Vostok OOO، یک تولیدکننده پهپاد[1] روسی که برای نیروهای روسیه در اوکراین پهپاد تأمین می‌کرد را به‌عنوان بخشی از اقدامی گسترده‌تر علیه تقریباً ۴۰۰ نهاد حامی زنجیره تأمین نظامی روسیه تحریم کرد. مانند OKO Design Bureau، یکی دیگر از تولیدکنندگان پهپاد که اخیراً با ردپای درون‌زنجیره‌ای کوچک‌تری تحریم شده بود، شرکت KB Vostok نیز درخواست کمک‌های مالی رمزارزی کرد و احتمالاً فروش پهپادهای خود با رمزارز را آسان کرده است.

تحلیل‌های درون‌زنجیره‌ای ما نشان داد که یک عامل از سمت KB Vostok تعداد ۱۶ تراکنش از ۲۴ تراکنش آدرس‌های رمزارزی تحریم‌شده‌ی KB Vostok را به خود اختصاص داده است و مقادیر انتقال‌یافته در تراکنش‌ها نیز با قیمت پهپادهای آنها[2] مطابقت دارد. این عامل نزدیک به ۴۰ میلیون دلار معامهل کرده و از چندین آدرس سپرده در صرافی تحریم‌شده روسی به نام گارانتکس[3] که بیش از ۱۰۰ میلیون دلار رمزارز تحت مدیریت دارد استفاده کرده است، که این مورد نشان‌دهنده‌ی دخالت احتمالی شبکه تدارکات نظامی روسیه است.

۱۹ سپتامبر ۲۰۲۴

پلیس جنایی فدرال آلمان[4] زیرساخت ۴۷ صرافی رمزارزی روسی‌زبان بدون احرازهویت را در عملیات «تبادل نهایی» توقیف کرد. این پلتفرم‌ها که فاقد پروتکل‌های احراز هویت مشتری بودند، برای پرداخت‌های باج‌افزاری، تراکنش‌های دارک‌نت، و فرار از تحریم‌ها مورد سوء استفاده قرار می‌گرفتند.

تحلیل ما از پلتفرم‌های هدف نشان‌دهنده‌ی فعالیت‌های گسترده غیرقانونی است. بسیاری از آنها جریان‌های ورودی قابل‌توجهی از بازارهای دارک‌نت، وجوه سرقتی، و نهادهای تحریم‌شده دریافت

---

[1] UAV

[2] به نام اسکلپل - Scalpel

[3] Garantex

[4] BKA

کرده‌اند که نشان‌دهنده‌ی ادغام عمیق آنها در اکوسیستم جرایم سایبری است. این خدمات همچنین اتباع روسیه را قادر ساخته است تا از تحریم‌ها فرار کنند و رمزارز را به بانک‌های تحریم‌شده روسی واریز/برداشت کنند. علی‌رغم استفاده از سرورهای مستقر در آلمان، این صرافی‌ها در درجه اول با تنظیمات زبان پیش‌فرض به زبان روسی و گزینه‌های تراکنش فیات مرتبط با بانک‌های تحریم‌شده مانند اسبربانک[۱] برای ارائه خدمات به کاربران روسی فعالیت کرده‌اند.

۲۶ سپتامبر ۲۰۲۴

OFAC صرافی رمزارز کریپتکس[۲] مستقر در روسیه و اپراتور آن، سرگئی سرگیویچ ایوانوف[۳] را به جرم پولشویی وجوه مرتبط با فروشگاه‌های کلاهبرداری، باج‌افزار و بازارهای دارک‌نت تحریم کرد. صرافی کریپتکس از سال ۲۰۱۸ بیش از ۵.۸۸ میلیارد دلار تراکنش داشت و به عنوان واسطه مالی برای بازیگران غیرقانونی عمل کرد. همزمان، FinCEN[4] صرافی بدون احرازهویت PM2BTC که بیش از ۱ میلیارد دلار تراکنش داشت را به عنوان نگرانی اصلی پولشویی تحت قانون مبارزه با پولشویی روسیه معرفی کرد. این تحریم‌ها بخشی از عملیات Endgame، یک تلاش گسترده و هماهنگ بین مقامات ایالات متحده و اروپا برای از بین بردن فعالان مالی جرایم سایبری بود. نیروهای انتظامی هلند و ایالات متحده دامنه‌ها و زیرساخت‌های مربوطه را توقیف کردند، درحالی‌که وزارت امور خارجه ایالات متحده جایزه ۱۰ میلیون دلاری برای اطلاعات منجر به دستگیری ایوانوف صادر کرد. علاوه بر این، نیروهای انتظامی هلند، با پشتیبانی چینالیسیس و تتر، ۷ میلیون یورو از وجوه این صرافی را توقیف کردند.

صرافی کریپتکس، صرافی PM2BTC، و شرکت UAPS که یک پردازشگر پرداخت است که توسط ایوانوف اداره می‌شد و در درجه اول به فروشگاه‌های کلاهبرداری خدمات ارائه می‌کرد - میلیاردها دلار تراکنش را برای مجرمان سایبری، از جمله گروه‌های باج‌افزار و فروشگاه‌های کلاهبرداری، مدیریت کردند. تحلیل‌های درون‌زنجیره‌ای ما نشان می‌دهد که فقط در سال ۲۰۲۴، شرکت UAPS بیش از ۹۷ میلیون دلار به صرافی کریپتکس ارسال کرده است که نشان‌دهنده روابط مالی عمیق آنهاست.

۰۴ دسامبر ۲۰۲۴

آژانس ملی جنایی[۵] بریتانیا یک شبکه پولشویی چند میلیارد دلاری روسی‌زبان را در عملیات خنثی‌سازی از بین برد و این اقدام منجر به دستگیری ۸۴ نفر و توقیف بیش از ۲۰ میلیون یورو وجه

---

[1] Sberbank
[2] Cryptex
[3] Sergey Sergeevich Ivanov
[4] FinCEN مخفف عبارت Financial Crimes Enforcement Network یا شبکه اجرای جرایم مالی است. این سازمان یک دفتر زیرمجموعه وزارت خزانه‌داری ایالات متحده آمریکا است که نقشی حیاتی در مبارزه با جرایم مالی، هم در داخل کشور و هم در سطح بین‌المللی، ایفا می‌کند.
[5] NCA

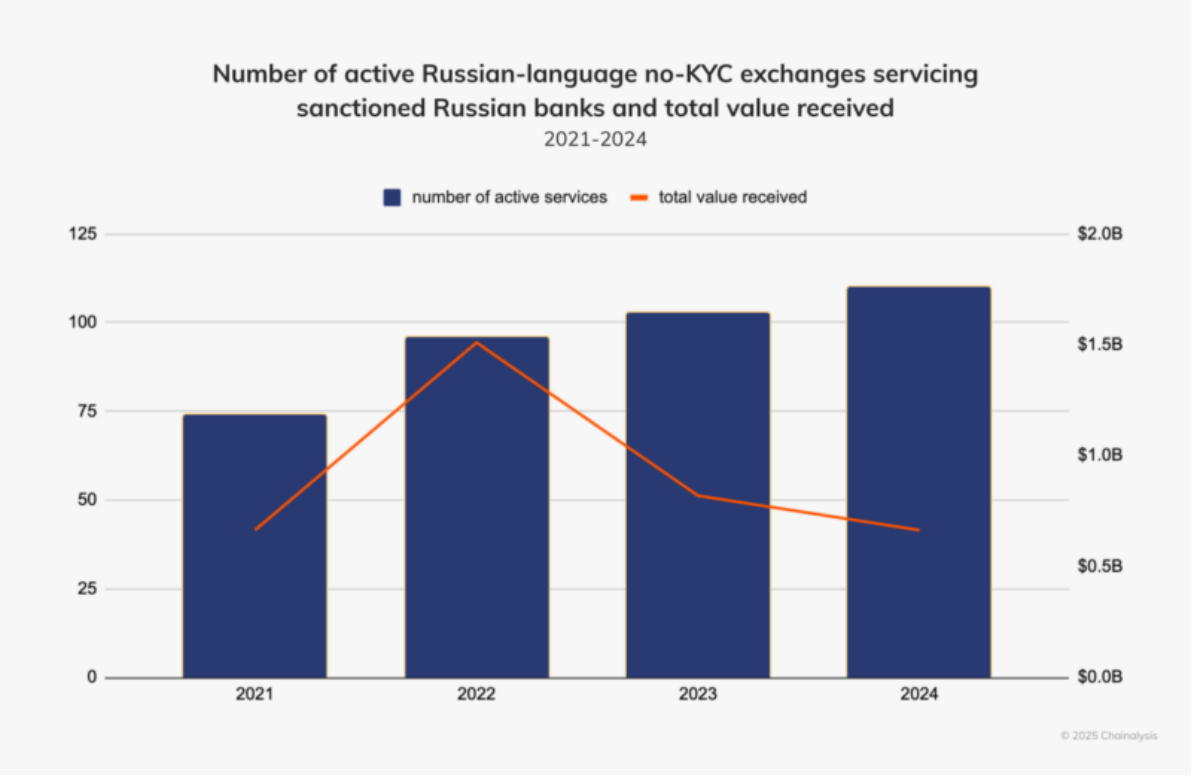
نقد و رمزارز شد. شبکه‌های Smart و TGR، وجوه را برای نخبگان روسی، مجرمان سایبری و سندیکاهای جنایی سازمان‌یافته پولشویی می‌کردند.

این عملیات تلاش هماهنگ‌شده‌ی بین‌المللی‌ای بود که شامل سازمان‌هایی از بریتانیا، اتحادیه اروپا و ایالات متحده، از جمله OFAC، DEA و FBI می‌شد. OFAC برای اعمال فشار و سخت‌گیری بیشتر ۴ نهاد و ۵ فرد مرتبط با شبکه TGR را تحریم کرد، از جمله موسس شبکه TGR جورج راسی[1] و همکارانش که از طریق ساختارهای شرکتی در بریتانیا، امارات متحده عربی، تایلند و ایالات متحده به تسهیل پردازش تراکنش‌های غیرقانونی می‌پرداختند. OFAC همچنین کیف‌پول‌های رمزارزی مرتبط ببا اعضای شبکه TGR را شناسایی کرد، از جمله یک کیف‌پول متعلق به فرد تحریم‌شده خاجی مراد دالگاتویچ ماگومدوف[2] که بیش از ۲۰۰ میلیون دلار وجوه غیرقانونی را پردازش کرده بود.

شبکه‌های Smart و TGR در ۳۰ کشور فعالیت می‌کردند و وجوه غیرقانونی را از طریق تبادل پول نقد به رمزارز جابجا می‌کردند و پرداخت‌های باج‌افزار، فرار از تحریم‌ها و قاچاق مواد مخدر را تسهیل می‌کردند. طبق گفته سازمان NCA، شبکه Smart به طور مستقیم عملیات‌های جاسوسی روسیه را تأمین مالی می‌کرد و وجوه گروه باج‌افزاری Ryuk را پولشویی می‌کرد.

صرافی‌های بدون احرازهویت روسی به فعالیت خود ادامه می‌دهند

علی‌رغم اقدامات اجرایی که بازیگران اصلی را مختل می‌کند، صرافی‌های جدیدِ بدون‌احرازهویت از دل همان برندهای تعطیل‌شده‌ی قبلی با نام و برند جدید ظاهر می‌شوند:



تصویر ۳: تعداد و حجم دریافت‌شده‌ی صرافی‌های روسی‌زبان فعال و بدون‌احرازهویت که به بانک‌های تحریمی روسی خدمات می‌دهند

[1] George Rossi
[2] Khadzhi Murat Dalgatovich Magomedov

در حالی که تعداد صرافی‌های فعال بدون‌احرازهویت افزایش یافته اند، همانطور که صرافی‌های کوچک تازه‌کار و برندهای تازه شکاف ناشی از تعطیلی برند را پر می‌کنند، جریان‌های ورودی به‌صورت کلی کاهش یافته‌اند که نشان‌دهنده‌ی تأثیر مخرب اقدامات تحریمی امریکایی و بین‌المللی است.

مهم است توجه داشته باشیم که اگرچه این پلتفرم‌ها به زبان روسی فعالیت می‌کنند و به بانک‌های تحریم‌شده روسی خدمات می‌دهند، اما اغلب فاقد جزئیات ثبت یا تأسیس هستند که تعیین حوزه قضایی واقعی آنها را دشوار می‌کند.

همانطور که سازمان‌های اجرای قانون دیدگاه بیشتری درباره این شبکه‌ها به دست می‌آورند، مختل‌سازی‌های بعدی بیشتر برای مهار جریان‌های مالی حامی جرایم سایبری، قاچاق مواد مخدر و عملیات دولتی تحریم‌شده رخ خواهند داد. کنترل‌ها و ابزارهای سطح صنعت رمزارز مانند چینالیسیس می‌توانند به مشارکت‌کنندگان در اکوسیستم رمزارز این امکان را بدهند تا به صورت لحظه‌ای افشا شدن خود را پایش کنند و به جلوگیری از نفوذ وجوه غیرقانونی به سیستم‌های مالی مشروع کمک کنند.

حوزه‌های قضایی تحریم‌شده دنبال مسیرهای پرداخت جایگزین منجمله رمزارزها هستند

همزمان با تشدید محدودیت‌های غربی، کشورهای تحریم‌شده به رمزارزها و سیستم‌های مالی جایگزین برای حفظ تجارت و دسترسی به سرمایه روی می‌آورند. به ویژه روسیه و ایران که روابط مالی خود را با کشورهای بریکس (برزیل، روسیه، هند، چین، و آفریقای جنوبی) عمیق کرده‌اند تا مکانیزم‌های پرداخت خارج از دلار آمریکا و شبکه‌های بانکی سنتی را توسعه دهند. اعضای بریکس امکان ایجاد یک ارز دیجیتال مشترک را بررسی کرده‌اند، در حالی که روسیه برای تسویه‌حساب‌های تجاری با چین و هند تلاش بر استفاده از Stablecoinها و CBDC به جای دلار آمریکا داشته است.

در میان فشار مالی فزاینده از تحریم‌های غربی، روسیه در پاییز گذشته قانونی را تصویب کرد که استخراج رمزارزها را قانونی می‌کند و اجازه استفاده از رمزارز برای پرداخت‌های بین‌المللی را می‌دهد، که این اقدام به خودی خود تغییری چشمگیر از موضع قبلی مبنی بر ممنوعیت کامل رمزارزها است. این تغییر سیاست استراتژیک با هدف کاهش فشار مالی تحریم‌های غربی و امکان تجارت جهانی با استفاده از رمزارزها اتخاذ شده است.

علی‌رغم حفظ ممنوعیت پرداخت‌های داخلی با رمزارز، روسیه همچنان یکی از کشورهای برتر در شاخص پذیرش جهانی رمزارز در فهرست مندرج در وبسایت چینالیسیس است. حتی قبل از این قانون‌گذاری، بانک‌هایی مانند روس‌بانک[1] شروع به آزمایش تراکنش‌های مرزی مبتنی بر رمزارز کرده بودند. در حال حاضر بانک مرکزی روسیه تلاش‌هایی را برای ادغام رمزارز در سیستم مالی کشور که تحت نظر تنظیم‌گران است پیش برده است.

[1] Rosbank

سنجش فعالیت مشروع رمزارز در حوزه‌های قضایی تحریم‌شده

در حالی که استفاده از رمزارز در حوزه‌های قضایی تحریم‌شده ممکن است با تامین مالی غیرقانونی تحت کنترل دولت‌ها مرتبط باشد، همچنین نشان‌دهنده‌ی یک خط حیاتی مالی مهم برای شهروندان عادی است که با مشکلات اقتصادی تحت رژیم‌های محدودکننده مواجه هستند. بسیاری از افراد و کسب‌وکارها در این مناطق برای حفظ ارزش دارایی، انتقال وجوه به سرتاسر دنیا و دور زدن کنترل‌های مالی تحمیل شده توسط دولت به رمزارزها – حجم پذیرش رمزارز که ما در ایران شناسایی کرده‌ایم و در ادامه به تفصیل بررسی خواهیم کرد.

از نظر رگولاتوری، تمایز بین فرار از تحریم‌های هدایت شده توسط دولت و استفاده فردی تصادم کمی دارد، زیرا تحریم‌های گسترده تقریباً تمام تعاملات مالی بین اشخاص آمریکایی و نهادهای موجود در حوزه‌های قضایی تحریم‌شده را، صرف نظر از قصد و نیت معامله، ممنوع می‌کند. بااین‌حال، هنگام بررسی تأثیر گسترده‌تر رمزارزها در این دست اقتصادها، مهم است تشخیص دهیم که افراد و کسب‌وکارها اغلب بدون نیت اعمال غیرقانونی به رمزارزها روی می‌آورند که نشان‌دهنده‌ی تنش بین اجرای ملاحظات مالی و بشردوستانه است.

علاوه‌براین، پلتفرم‌های غیرمتمرکز علی‌رغم تحریم‌ها همچنان فعالیت می‌کنند که اینها نیز اقدامات اجرایی را پیچیده می‌کنند. برخلاف موسسات مالی سنتی، این شبکه‌ها را نمی‌توان به راحتی ضبط یا تعطیل کرد، که البته نیازمند رویکردی گسترده‌تر در سطح اکوسیستم برای انطباق با قوانین است. همانقدر که اجرای دستورات قانونی و تحریمی ادامه می‌یابد، رسیدگی به ریسک‌های تحریم به صورت کلی، از طریق همکاری بین دولت‌ها، ابزارهای انطباق مانند چینالیسیس، و ارائه‌دهندگان خدمات دارایی‌های مجازی[1] برای مدیریت ریسک تأمین مالی غیرقانونی در عین حفظ دسترسی مشروع به رمزارزها حیاتی خواهد بود.

تورنادوکش با وجود تحریم‌ها و اقدامات قانونی همچنان زنده است

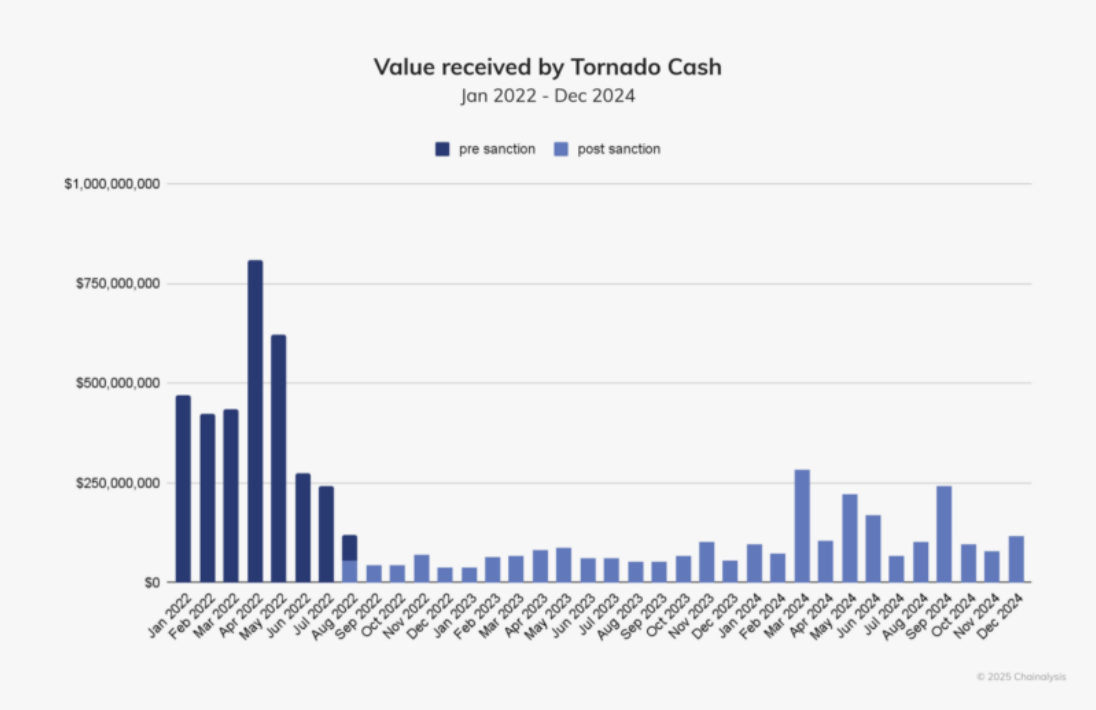
همانطور که قبلاً اشاره کردیم، میکسر رمزارزی مشهور به نام تورنادوکش نمونه بارزی از چالش‌هایی است که قانون‌گذاران در اجرای تحریم‌ها علیه پلتفرم‌های غیرمتمرکز با آن روبرو هستند. تورنادوکش علی‌رغم تحریم‌های OFAC، اقدامات قانونی، و حتی دستگیری توسعه‌دهندگان آن همچنان به پردازش تراکنش‌های غیرقانونی ادامه می‌دهد.

این پلتفرم که در سال ۲۰۲۲ توسط OFAC به دلیل تسهیل پولشوییِ بیش از ۴۵۵ میلیون دلار از وجوه سرقت شده -عمدتاً مرتبط با گروه لازاروس کره شمالی- تحریم شد، تعطیل کردن زیرساخت اصلی‌اش ظاهراً دشوار است. در آگوست ۲۰۲۳، دادستان‌های آمریکایی آقای رومن سمنوف[2]، یکی از بنیانگذاران تورنادوکش را به توطئه برای پولشویی و نقض تحریم‌ها متهم کردند. در همین حال،

[1] VASP
[2] Roman Semenov

مقامات هلندی تیز الکسی پرتسف[1]، یکی دیگر از بنیانگذاران این پلتفرم را در سال ۲۰۲۴ محکوم کردند و او را به بیش از پنج سال زندان محکوم کردند.

اگرچه تورنادوکش در ابتدای زمانی که صفحه وب آن آفلاین شد با کاهش تقریباً ۹۰٪ در حجم تراکنش‌ها مواجه شد، اما قراردادهای هوشمند غیرمتمرکز آن امکان ادامه فعالیت را فراهم کردند. در سال ۲۰۲۴، جریان‌های ورودی در مقایسه با سال قبل ۱۰۸٪ افزایش یافتند که روند بازگشت را که اولین بار در گزارش سال ۲۰۲۴ جرایم رمزارزی منتشر شده است ادامه داد.



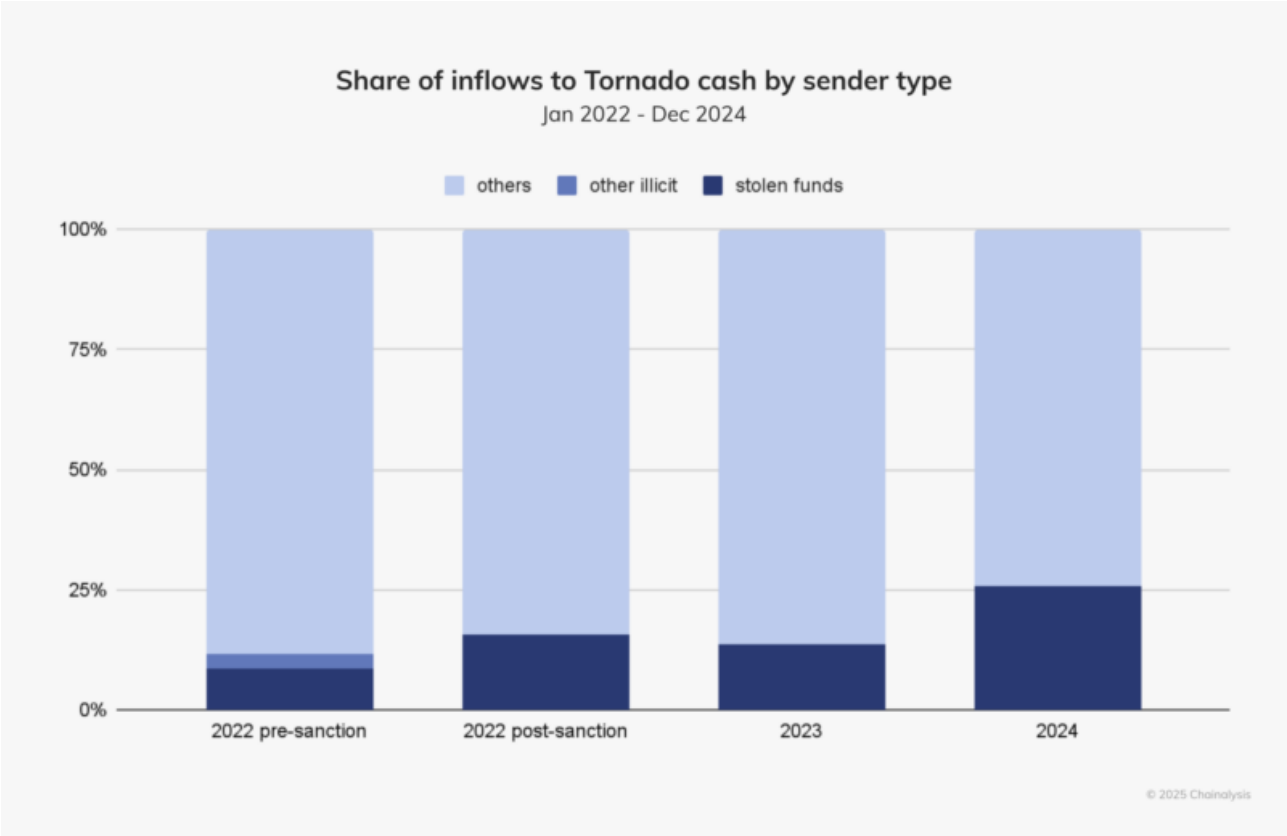
تصویر ۴:حجم تراکنش‌های دریافت‌شده توسط تورنادوکش

اگرچه جریان‌های ورودی هنوز به سطوح قبل از تحریم بازنگشته‌اند، اما تورنادوکش همچنان صدها میلیون دلار تراکنش را در هر ماه پردازش می‌کند.

وجوه سرقتی موجب احیای تورنادوکش می‌شوند

همانطور که در تصویر زیر می‌بینیم، افزایش استفاده از تورنادوکش در سال ۲۰۲۴ عمدتاً ناشی از وجوه سرقتی بود که به بالاترین حد سه ساله رسید و ۲۴.۴٪ از کل جریان‌های ورودی را تشکیل می‌داد:

[1] Alexey Pertsev



تصویر ۵: سهم جریان‌های ورودی به تورنادوکش بر اساس نوع فرستنده

یکی از مهم‌ترین حوادثی که موجب این جریان‌های ورودی شد، هک پل HECO[1] بود که مهاجمین در آن حمله‌ی سایبری معادل ۱۴۵ میلیون دلار ارز ETH را از طریق تورنادوکش برای شستشوی این مبلغ منتقل کردند.

از سال ۲۰۱۹، چینالیسیس ارتباط بیش از ۲۵٪ از وجوه پردازش شده از طریق تورنادوکش به فعالیت‌های غیرقانونی را کشف کرده است که گروه لازاروس در صدر فهرست آن است. مهم است در نظر داشته باشیم که اگرچه تورنادوکش بدون شک نقش عمده‌ای در پولشویی وجوه سرقتی داشته است، اما میکسرهای رمزارزی مانند تورنادوکش ابزارهایی برای صرفاً فعالیت مجرمانه نیستند. به‌عنوان مثال، ویتالیک بوترین، یکی از بنیانگذاران اتریوم علناً اعلام کرد که از تورنادوکش برای ناشناس‌سازی کمک مالی به اوکراین پس از حمله گسترده روسیه در سال ۲۰۲۲ استفاده کرده است که نشان می‌دهد چگونه این سرویس‌ها می‌توانند برای حریم خصوصی مالی در زمینه‌های مشروع نیز استفاده شوند.

چالش‌های منحصربه‌فردی در اِعمال قانون بر پلتفرم‌های غیرمتمرکز ظاهر می‌شوند

برخلاف سرویس‌های متمرکز که می‌توانند ضبط یا تعطیل شوند، تورنادوکش از طریق قراردادهای هوشمند در یک شبکه بلاکچین غیرمتمرکز فعالیت می‌کند که اِعمال قانون را بسیار دشوارتر می‌کند.

[1] HECO Bridge

درحالی‌که شفافیت بلاکچین به مقامات امکان می‌دهد جریان‌های غیرقانونی را ردیابی کنند، تنظیم‌گرها از سویی دیگر قدرت محدودی برای برچیدن واقعی زیرساخت غیرمتمرکز دارند.

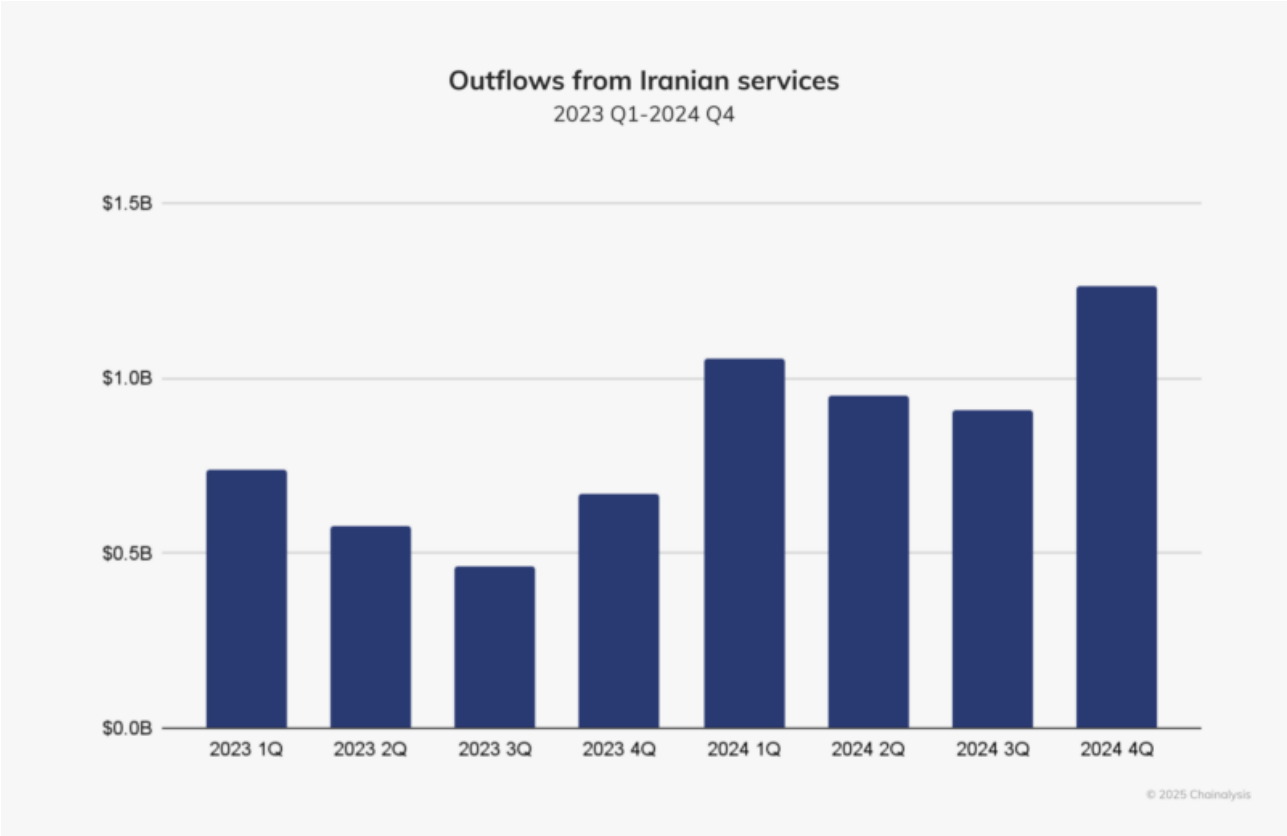
در ۲۶ نوامبر ۲۰۲۴، یک دادگاه ایالات متحده حکم کرد که OFAC در تحریم آدرس‌های قرارداد هوشمند تورنادوکش از اختیارات خود پا را فراتر گذاشته است. این تصمیم سؤالات گسترده‌تری را در مورد محدودیت‌های اجرای قانون علیه پروتکل‌های دیفای ایجاد می‌کند و بر نیاز به همکاری بین‌المللی و انطباق قوی در سطح پروتکل و خدمات تأکید می‌کند. این صنعت قطعاً در چند سال گذشته گام‌هایی در زمینه انطباق برداشته است، که در ادامه به تفصیل به آن خواهیم پرداخت.

پرونده تورنادوکش، رقص ظریف بین نوآوری، حریم خصوصی مالی، و انطباق با مقررات در پروتکل‌های غیرمتمرکز را نشان می‌دهد. همانقدر که دیفای در سطح جهانی گسترش می‌یابد، توسعه‌دهندگان باید فشار فزاینده‌ای را برای پیاده‌سازی محافظه‌هایی که از فعالیت‌های غیرقانونی جلوگیری می‌کنند و در عین حال موارد استفاده قانونی را برای حریم خصوصی حفظ می‌کنند، پیش ببرند. تضمین انطباق با مقررات بدون مخاطره‌ی اخلاقیات عدم‌تمرکز و حریم خصوصی، یک چالش فراگیر برای صنعتی است که بر پایه فناوری غیرمتمرکز ساخته شده است. نظارت پیشگیرانه و کاهش ریسک، با تکامل انتظارات نظارتی ضروری است. تیم چینالیسیس به صورت لحظه‌ای راه‌حل‌هایی را برای کمک به رفع این چالش‌ها ارائه می‌دهد.

در بحبوحه تنش‌های ژئوپلیتیکی، رمزارز امکان خروج سرمایه را در ایران فراهم می‌کند

از زمان تصرف سفارت ایالات متحده در تهران در سال ۱۹۷۹، ایالات متحده محدودیت‌های مالی گسترده‌ای را بر ایران اعمال کرده است. علی‌رغم تحریم‌ها، دسترسی به سیستم مالی بین‌المللی به دلیل ثبات و نقدینگی که ارائه می‌دهد، برای ایران بسیار مهم است. در کشورهایی مانند ایران که ارز ملی بی‌ثبات و بی‌ارزش شده‌اند، عدم توانایی تعامل با بانک‌های جهانی تحرک مالی را به شدت محدود می‌کند و افراد و کسب‌وکارها را به جستجوی جایگزین‌ها سوق می‌دهد.

در سال ۲۰۲۴، سرویس‌های ایرانی سهم بسیار بیشتری از فعالیت‌های مربوط به تحریم‌ها را به خود اختصاص دادند که ناشی از افزایش بی‌اعتمادی به دولت و بی‌ثباتی ژئوپلیتیکی مداوم بود.



تصویر ۶: جریان‌های خروجی سرویس‌های ایرانی

در سال ۲۰۲۴، خروجی‌ها با حدود ۷۰ درصد افزایش سالانه به ۱۸.٤ میلیارد دلار رسید.

درحالی‌که پذیرش رمزارزها در این مناطق اغلب در درجه اول از دریچه فرار از تحریم‌ها دیده می‌شود، این همچنین بازتاب گسترده‌تری از نیاز اساسی به ابزارهای مالی قابل اعتماد در اقتصادهایی است که از سیستم بانکداری جهانی جدا شده‌اند.

کنترل دولت و خروج سرمایه

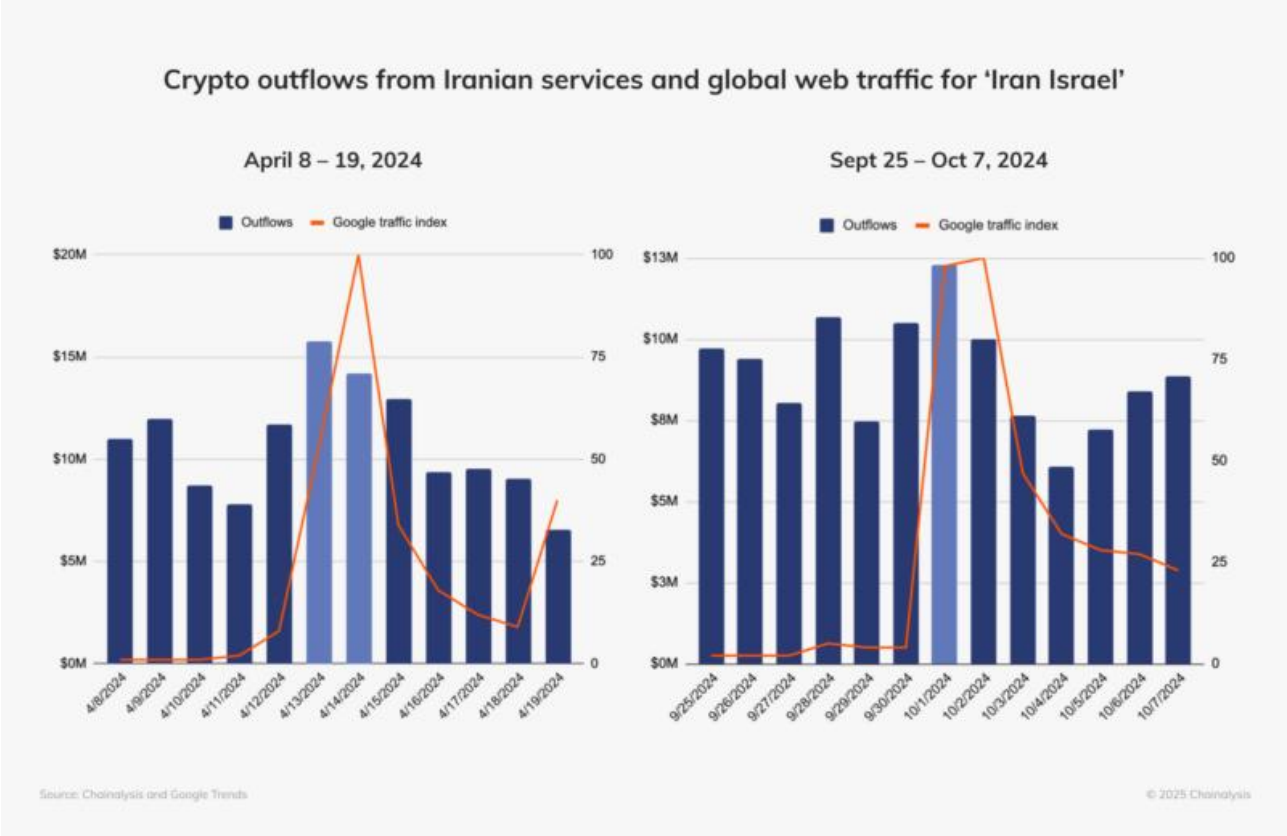
دولت ایران کنترل گسترده‌ای بر سیستم مالی کشور، از جمله زیرساخت‌های رمزارزی دارد. این واقعیت به شکل خاصی در دسامبر ۲۰۲۴ آشکار شد، زمانی که مقامات (بانک مرکزی ایران) به‌طور ناگهانی برداشت‌ها از صرافی‌های ایرانی را در پاسخ به کاهش بی‌سابقه ارزش ریال ایران متوقف کردند. این اقدام نشان داد که دولت قادر است به میل خود جریان‌های مالی را برای جلوگیری از خروج سرمایه محدود کند - نگرانی فزاینده‌ای است درحالی‌که تورم در حدود ۴۰٪تا۵۰٪ است و ریال به روند نزولی خود ادامه می‌دهد. از زمانی که ایالات متحده در سال ۲۰۱۸ از برجام خارج شد و تحریم‌هایی را علیه نفت ایران اعمال کرد، این ارز تقریباً ۹۰ درصد از ارزش خود را از دست داده است و کاهش ارزش آن در بحبوحه افزایش تنش در سال ۲۰۲۳ و ۲۰۲۴ سریع‌تر شده است.

رمزارز، برای بسیاری از ایرانیان، نشان‌دهنده‌ی یک سیستم مالی جایگزین است و افزایش استفاده از صرافی‌های رمزارزی ایرانی نشان می‌دهد که افراد و مؤسسات بیشتری برای حفاظت از ارزش دارایی و دور زدن محدودیت‌های مالی به رمزارز روی می‌آورند. بررسی دقیق‌تر این خروجی‌ها نشان می‌دهد که فعالیت ایرانی‌ها لزوماً ناشی از فعالیت‌های مالی غیرقانونی یا فعالیت‌های تحت

حمایت دولت ایران نیستند، بلکه ناشی از بی‌اعتمادی عمیق شهروندان ایرانی به حاکمیت و نیاز مبرم به انتقال وجوه به خارج از کشور است.

نقاط عطف ژئوپلیتیکی، خروجی رمزارز را در ایران افزایش می‌دهد

در دوره‌های زمانی تشدید بی‌ثباتی ژئوپلیتیکی که شامل ایران نیز می‌شوند، دریافتیم که خروجی رمزارز از صرافی‌های ایرانی افزایش یافته است - به ویژه در روز یا بلافاصله پس از وقوع درگیری‌ها.

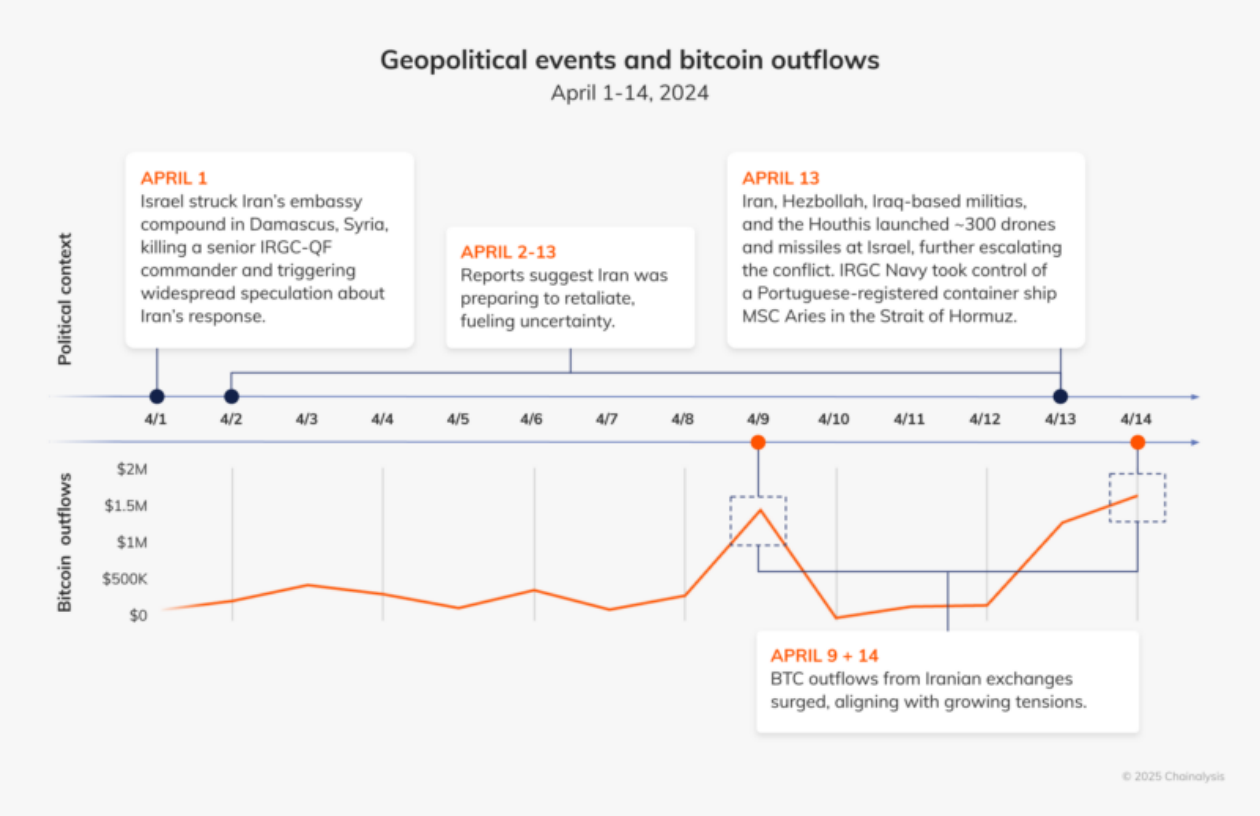


تصویر ۷: جریان‌های خروجی از سرویس‌های ایران و ترافیک وب جهانی برای کلیدواژه «ایران اسراییل»

دیتای گوگل ترندز[1] این ارتباط را تقویت می‌کند و اوج‌های جهانی در جستجوی «ایران اسرائیل» در ۱۴ آوریل و ۱ اکتبر را نشان می‌دهد - تاریخ‌هایی که با تشدید درگیری همسو هستند. این الگو با تحولات مالی گسترده‌تر در ایران مطابقت دارد که در آنجا نرخ بازار موازی ریال در پاسخ به تحولات سیاسی و نظامی به شدت نوسان پیدا می‌کند.

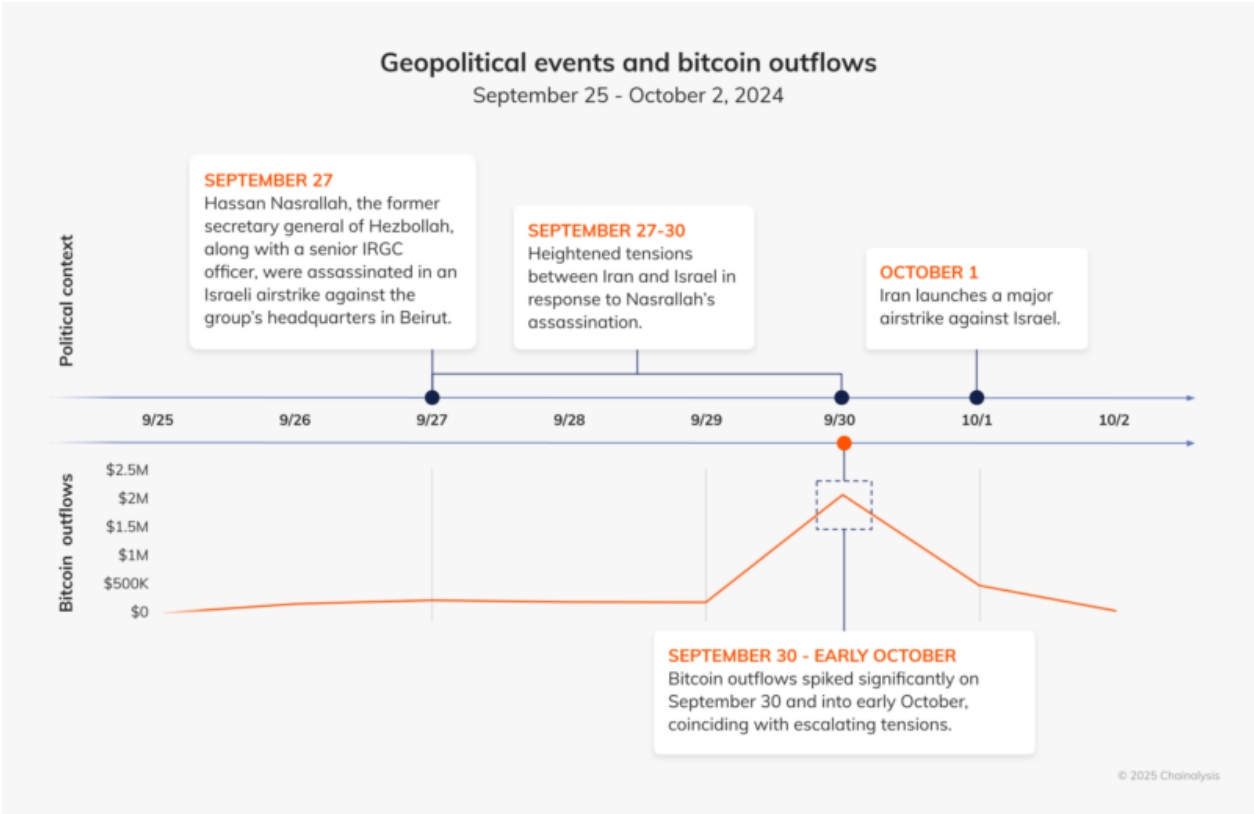
نکته جالب اینجاست که درحالی‌که افزایش خروجی‌ها در همه دارایی‌ها، از جمله Stablecoinها مشاهده شد، حجم بسیار بالاتری را در بیتکوین مشاهده کردیم. جدول زمانی زیر خروجی بیتکوین را در رابطه با رویدادهای کلیدی ژئوپلیتیکی نشان می‌دهد:

[1] Google Trends



تصویر ۸: رویدادهای ژئوپلیتیکی و جریان‌های خروجی بیتکوین – ۱ تا ۱۴ آوریل ۲۰۲۴

اوج خروجی‌های بیتکوین در زمانی رخ داد که مشخص شد ایران احتمالاً اقدام به پرتاب موشک خواهد کرد. همین اتفاق در چند روز پس از رویدادها، همانطور که در بالا در تاریخ‌های ۹ و ۱۴ آوریل ۲۰۲۴ می‌بینیم -و به‌طور مشابه در اواخر سپتامبر و اوایل اکتبر ۲۰۲۴- رخ داد.



تصویر ۹: رویدادهای ژئوپلیتیکی و جریان‌های خروجی بیتکوین – ۲۵ سپتامبر تا ۲ اکتبر ۲۰۲۴

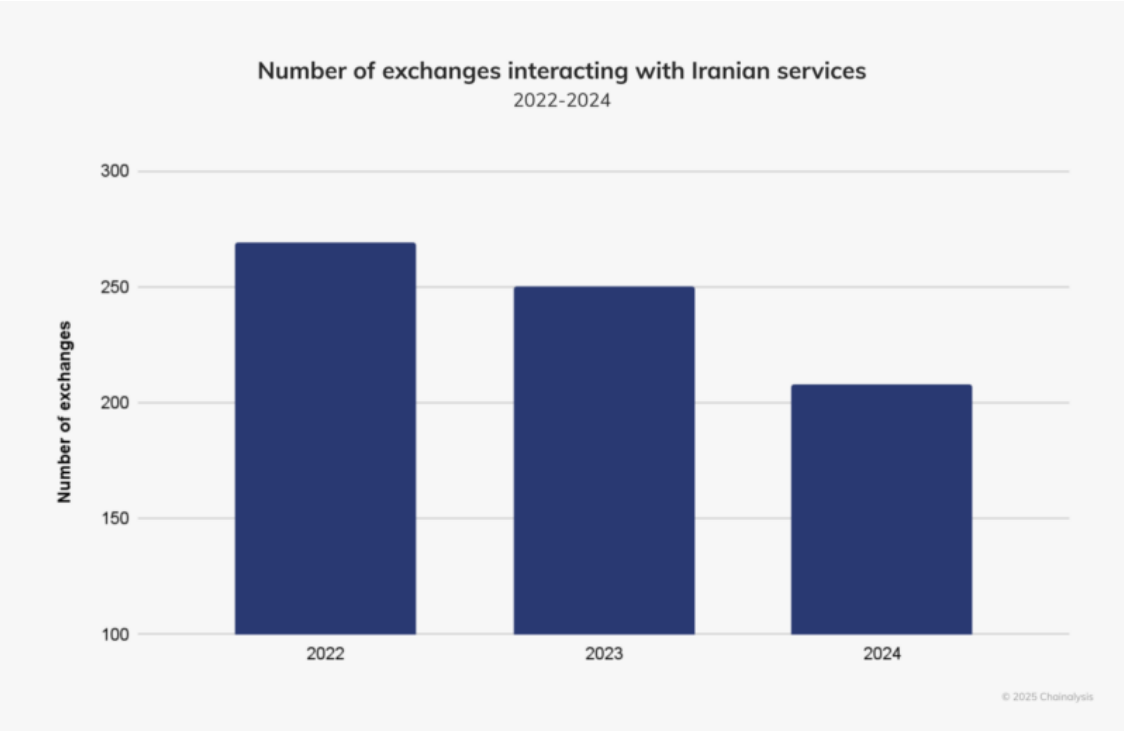
این امر نشان می‌دهد که نگرانی عمومی فزاینده‌ای در مورد درگیری‌های ژئوپلیتیکی در رفتار مالی منعکس شده است و افراد برای محافظت در برابر عدم‌اطمینان ژئوپلیتیکی یا اقتصادی به رمزارز روی می‌آورند. با تشدید فشار تحریم‌ها و ادامه‌ی عدم‌اطمینان اقتصادی ایران، تقاضا برای رمزارز احتمالاً بالا خواهد ماند.

نقش بیتکوین در زمان‌های عدم‌اطمینان

درحالی‌که این روندها در ایران مشهود و ملموس است، الگوهای مشابهی را در سطح جهانی در زمان‌های جنگ، آشفتگی اقتصادی یا سرکوب دولت نیز مشاهده کرده‌ایم. ماهیت مقاوم در برابر سانسور و خودحضانتی بیتکوین، آن را به گزینه‌ای جذاب در هنگام بحران تبدیل می‌کند. برخلاف دارایی‌های سنتی، بیتکوین را می‌توان به هر جایی در دنیا منتقل کرد، در درون زنجیره به عنوان ذخیره ارزش در برابر بی‌ثباتی نگهداری کرد، و فقط به نگهداری عبارات بازیابی بسنده کرد - که در شرایطی که افراد ممکن است نیاز به فرار کردن داشته باشند، انعطاف‌پذیری مالی را ارائه می‌دهد. این امر بیتکوین را به‌طور منحصربه‌فردی برای کسانی که در حوزه‌های قضایی تحریم‌شده با بی‌ثباتی ژئوپلیتیکی و محدودیت‌های مالی روبرو هستند، مناسب می‌کند.

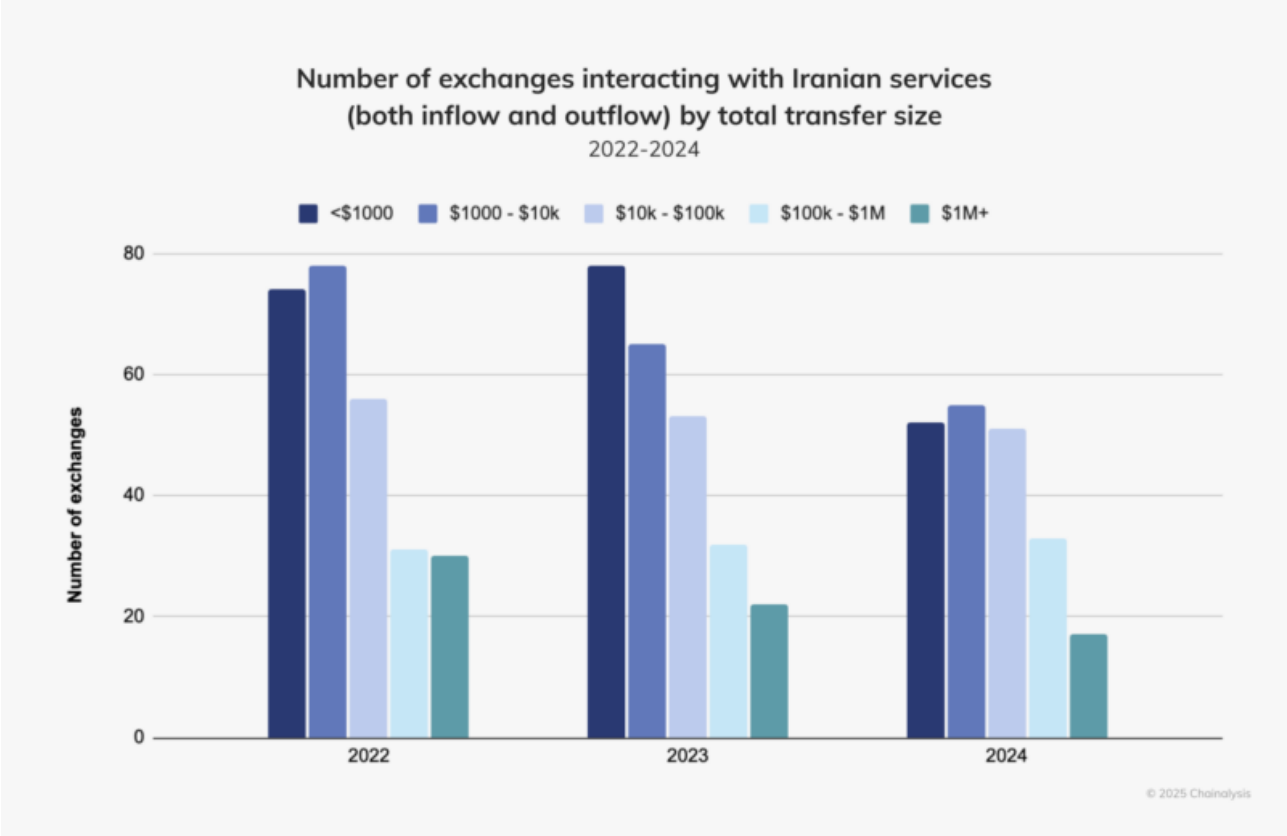
نگاه به آینده: انطباق جامع در سطح اکوسیستم

اگرچه بسیاری از ایرانیان برای خروج سرمایه به رمزارز تکیه کرده‌اند، برنامه‌های انطباق با مقررات در سراسر اکوسیستم جهانی رمزارزها این راه‌ها را می‌بندند. با قرار گرفتن انطباق در مرکز توجه، تعداد صرافی‌های در حال تعامل با سرویس‌های ایرانی هر سال کاهش می‌یابد به شکلی که بین سال‌های ۲۰۲۲ تا ۲۰۲۴ حدود ۲۳٪ کاهش داشته است.



تصویر ۱۰: تعداد صرافی‌های در حال تعامل با سرویس‌های ایرانی از ۲۰۲۲ تا ۲۰۲۴

نگاهی دقیق‌تر به حجم تبادل بین پلتفرم‌های ایرانی و صرافی‌ها نشان می‌دهد که تعداد صرافی‌های در حال تعامل با صرافی‌های ایرانی در تقریباً همه گروه‌های تراکنش بین سال‌های ۲۰۲۳ و ۲۰۲۴ کاهش یافته است.



تصویر ۱۱: تعداد صرافی‌های در حال تعامل با صرافی‌های ایرانی (جریان‌های ورودی و خروجی) بر اساس حجم تبادل کلی

بیشترین کاهش در گروه زیر ۱۰۰۰ دلار (<$1000) رخ داده است که ۳۳٫۳۳٪ کاهش نسبت به سال ۲۰۲۳ را نشان می‌دهد. گروه بالای یک میلیون دلار (+$1M) نیز با ۲۲٫۷۳٪ کاهش قابل توجهی روبرو شد.

کاهش قابل اندازه‌گیری در تعاملات صرافی‌های رمزارزی با سرویس‌های ایرانی نشان‌دهنده‌ی تأثیر ملموس اقدامات انطباق در محدود کردن احتمال تعامل با حوزه‌های قضایی تحریم شده است. صرافی‌ها مسئولیت فزاینده‌ای برای کاهش فعالیت مالی مرتبط با مناطق تحریم شده دارند.

فشار سیاست جهانی بر ایران، خطرات مالی را افزایش می‌دهد

اقدامات ایران، ریسک انجام تجارت با اکوسیستم مالی خود را در داخل و خارج از زنجیره افزایش داده است. ایران طی ۱۲ تا ۱۸ ماه گذشته روابط اقتصادی و نظاری خود با روسیه را عمق بخشیده است -که در حال حاضر بیشترین تحریم‌ها را در جهان دارد- و پرچم‌های قرمز بیشتری را برای نهادهای نظارتی جهانی برافراشته است. ایران، به عنوان یکی از تنها سه کشور در لیست سیاه FATF (به همراه کره‌شمالی و میانمار) همچنان به دلیل ضعف کنترل‌های خود در زمینه مبارزه با پولشویی (AML) و مبارزه با تأمین مالی تروریسم (CFT) تحت ذره‌بین است. علاوه بر این، ایران به

ارائه حمایت مادی به گروه‌هایی مانند حزب‌الله و حماس ادامه می‌دهد و نگرانی‌های نظارتی و امنیت ملی را تشدید می‌کند.

در فوریه ۲۰۲۵، دولت جدید ایالات متحده صورتجلسه امنیت ملی ریاست جمهوری[1] را ارائه کرد و کمپین «فشار حداکثری» بر ایران را مجدداً برقرار کرد. این دستورالعمل، موضع‌گیری تهاجمی‌تری را در زمینه اجرای قانون الزام می‌کند و اقدامات خاصی برای وزارت دادگستری ایالات متحده از جمله موارد زیر را مشخص می‌کند:

- بررسی و تعقیب شبکه‌های مالی و تدارکاتی مرتبط با ایران، و همچنین عوامل یا گروه‌های نیابتی در داخل ایالات متحده که توسط ایران یا نیابتی‌های ایرانی حمایت می‌شوند.
- توقیف محموله‌های غیرقانونی نفت ایران.
- شناسایی دارایی‌های دولت ایران برای توقیف در ایالات متحده و خارج از کشور.
- متهم کردن و محاکمه کردن رهبران گروه‌های تروریستی تحت حمایت ایران.
- استفاده از ابزارهای جنایی، نظارتی، سایبری و اختیارات برای مختل کردن جاسوسی‌ها، فرار از تحریم‌ها، و فعالیت‌های مالی مخرب ایران.

با تداوم شدت تحریم‌های هدفمند و حوزه‌ای، همراه با سرکوب نفت و کشتیرانی ایران، وضعیت حاد باقی می‌ماند و احتمالاً تقاضا برای رمزارزها و سایر راهکارهای مالی را افزایش می‌دهد. همانطور که بازیگران تحریم‌شده به پذیرش دنیای فعال‌شده با رمزارز می‌پردازند، اجرای قانون به‌طور فزاینده‌ای به اطلاعات بلاکچین برای ردیابی جریان‌های مالی غیرقانونی، شناسایی نهادهای تحریم‌شده و کاهش احتمال تبادل با حوزه‌های قضایی محدود مانند ایران متکی خواهد بود.

تحلیل بلاکچین آینده‌ای مبتنی بر انطباق را تضمین می‌کند

فناوری‌های غیرمتمرکز چالش‌های اجرای پیچیده‌ای را ایجاد می‌کنند و انطباق در سطح پروتکل و سرویس را ضروری می‌سازند. چینالیسیس با ارائه خدمات نظارت لحظه‌ای تراکنش، پایش کیف‌پول و کنترل‌های مبتنی بر ریسک برای کمک به شناسایی و جلوگیری از احتمال تبادل با نهادهای تحریم‌شده، از صرافی‌ها، پلتفرم‌های دیفای، نهادهای نظارتی و آژانس‌های مجری قانون کمک می‌کند. با افزایش انتظارات نظارتی، اقدامات انطباق فعال برای حفظ یکپارچگی مالی و در عین حال حفظ دسترسی قانونی ضروری خواهد بود.

با استفاده از تحلیل درون‌زنجیره‌ای، سرویس‌های رمزارزی می‌توانند ریسک طرف مقابل را ارزیابی کرده و تراکنش‌های غیرقانونی را قبل از دسترسی به سیستم مالی گسترده‌تر رهگیری کنند. برنامه‌های بهبود یافته انطباق که توسط تحلیل بلاکچین پشتیبانی می‌شوند، به کاهش قابل‌اندازه‌گیری در تعاملات صرافی با نهادهای تحریم‌شده کمک کرده‌اند و اثربخشی استراتژی‌های کاهش ریسک مبتنی بر داده را نشان می‌دهند.

[1] NSPM-2

همانطور که کشورهای تحریم‌شده به دنبال کانال‌های مالی جایگزین هستند، همکاری نزدیک بین شرکت‌کنندگان اکوسیستم و همچنین شرکای بخش خصوصی و دولتی امری ضروری است. یک رویکرد مبتنی بر ریسک که بین فرار از تحریم‌های تحت هدایت دولت و خطوط حیات مالی فردی تمایز قائل می‌شود، در شکل‌دهی چارچوب‌های نظارتی عادلانه و مؤثر بسیار مهم خواهد بود. ترکیبی از نظارت تنظیم‌گرانه، همکاری در سطح صنعت، و ابزارهای پیشرفته‌ی تحلیل بلاکچین می‌تواند تضمین کند که رمزارز یک سیستم مالی قابل دوام و قانونی باقی می‌ماند و در عین حال کانال‌هایی را برای بازیگران و دولت‌های غیرقانونی حذف می‌کند.

نهادهای مرتبط با رمزارز که در سال ۲۰۲۴ تحریم شدند

جدول زیر شامل رویدادهای مختلف تحریم و اقدامات هماهنگ اجرای قانون با محوریت رمزارز است که در طول سال ۲۰۲۴ رخ داده است.

نام	دلیل تحریم	تاریخ تحریم	نوع تحریم
آرتور سونگاتوف و ایوان کوندراتیف	دو تبعه روسی متهم به ایفای نقش بازاریاب برای باج‌افزار LockBit RaaS	۲۰ فوریه ۲۰۲۴	باج‌افزار
ایلیا آندریویچ گامباشیدزه و نیکولای الکساندرویچ توپیکین	تسهیل کمپین‌های تحریف اطلاعات از طرف دولت روسیه، با استفاده از رمزارز برای تأمین مالی	۲۰ مارس ۲۰۲۴	تحریف اطلاعات و تسهیل مالی
نهادهای Netex24 و Bitpapa	کمک به ساخت یا بهره‌برداری از خدمات مبتنی بر بلاک‌چین برای تسهیل فرار احتمالی از تحریم‌ها برای اتباع روسیه	۲۵ مارس ۲۰۲۴	فرار از تحریم‌ها از طریق رمزارز
توفیق محمد سعید اللو	اپراتور حواله مستقر در سوریه که قبلاً توسط NBCTF به عنوان فردی که با عوامل حزب‌الله در زیرساخت تأمین مالی رمزارز کار کرده بود، شناسایی شده بود.	۲۶ مارس ۲۰۲۴	تأمین مالی تروریسم
غزه نو و چندین فرد مرتبط	رسانه خبری سوشال مدیا و همکاران به دلیل نقششان در جمع‌آوری پول برای حماس پس از حملات ۷ اکتبر علیه اسرائیل	۲۷ مارس ۲۰۲۴	تأمین مالی تروریسم
OKO Design Bureau و تقریباً ۳۰۰ فرد و نهاد درگیر در ماشین جنگی روسیه	تسهیل تولید سلاح روسیه و فرار از تحریم‌ها، با یک نهاد که به پذیرش رمزارز معروف است.	۱ مه ۲۰۲۴	تهیه سلاح و فرار از تحریم‌ها
دیمیتری یوریویچ خوروشف	رهبر گروه LockBit RaaS، برای توسعه و توزیع باج‌افزار	۷ مه ۲۰۲۴	باج‌افزار
یونه وانگ و افراد متعدد مرتبط با بات‌نت 911 S5	به دلیل کنترل ادعایی یک بات‌نت از رایانه‌های آلوده مرتبط با سرویس پروکسی مسکونی	۲۹ مه ۲۰۲۴	جرایم سایبری و عملیات بات‌نت

افراد مرتبط با جنبش مقاومت نوردیک	مشارکت در افراط‌گرایی خشونت‌آمیز و تروریسم، که از طریق کمک‌های مالی رمزارز تأمین می‌شود.	۱۴ ژوئن ۲۰۲۴	تأمین مالی تروریسم و افراط‌گرایی
شرکت KB Vostok OOO	یک توسعه‌دهنده پهپاد روسی که به دلیل طراحی پهپادهای مورد استفاده توسط نیروهای روسی در اوکراین شناخته شده است.	۲۱ آگوست ۲۰۲۴	توسعه تسلیحات
سرگئی سرگیویچ ایوانوف و صرافی Cryptex	پولشویی صدها میلیون دلار رمزارز برای مجرمان سایبری و فروشندگان دارک‌نت	۲۶ سپتامبر ۲۰۲۴	پولشویی و جرایم سایبری
اعضای تیم Evil Corp	توسعه و توزیع بدافزار Dridex که منجر به خسارات مالی قابل توجه در سطح جهانی شد.	۱ اکتبر ۲۰۲۴	جرایم سایبری و کلاهبرداری
شبکه‌های Smart و TGR	بهره‌برداری از شبکه‌های گسترده پولشویی روسی با ارتباط با مواد	۴ اکتبر ۲۰۲۴	پولشویی و جرایم سازمان‌یافته
سعید الجمال	سرمایه‌دار حوثی مستقر در ایران که در قاچاق اسلحه، پولشویی و حمل و نقل غیرقانونی نفت ایران با استفاده از رمزارز فعالیت دارد.	۱۹ دسامبر ۲۰۲۴	تأمین مالی تروریسم و قاچاق اسلحه