یازدهمین همایش سالانه
بانکداری نوین و
نظام‌های پرداخت
پژوهشکده پولی و بانکی
بانک مرکزی جمهوری اسلامی ایران
بانک مرکزی جمهوری اسلامی ایران
شرکت ملی انفورماتیک
زیست بوم بانکداری هوشمند؛ حکمرانی دیجیتال و نظارت فنّاورانه
تهران، مرکز همایش‌های بین‌المللی برج میلاد ـ ۵ و ۶ آذر ۱۴۰۳
ISC

شناسایی انواع ریسک‌های رمزدارایی‌ها در ایران و راهکارهایی جهت تنظیم‌گری مناسب آنها

صادق صابری[۱]

چکیده

در این مقاله به بررسی و شناسایی انواع ریسک‌های مرتبط با رمزدارایی‌ها در سطح ایران و جهان پرداخته شده است. رمزدارایی‌ها که شامل انواع رمزارزها و توکن‌های بی‌همتا هستند، به عنوان یکی از جدیدترین فناوری‌های مالی در دهه اخیر، فرصت‌ها و تهدیدهای جدیدی را برای سرمایه‌گذاران، دولت‌ها و کاربران به همراه آورده‌اند. با توجه به ارزش بالای بازار جهانی این دارایی‌ها و توسعه سریع فناوری‌های مرتبط، ریسک‌های قابل‌توجهی از جمله تقلب‌ها و کلاهبرداری‌ها، پرداخت‌های غیرقانونی، ریسک‌های نظام مالی و پولی، ریسک‌های امنیت سایبری و ریسک‌های مرتبط با ارائه‌دهندگان خدمات رمزدارایی در این حوزه قابل‌مشاهده است.

در بخش دیگری از مقاله، چالش‌های تنظیم‌گری رمزدارایی‌ها در سطح بین‌المللی و ایران بررسی شده است. در حالی که کشورهای مختلف رویکردهای متفاوتی در مواجهه با این چالش‌ها دارند، در ایران به دلیل شرایط خاص اقتصادی و سیاسی، ریسک‌های اختصاصی نیز پدید آمده است. از جمله این ریسک‌ها می‌توان به امکان رصد شدن آدرس کیف‌پول‌های ارائه‌دهندگان خدمات رمزدارایی ایرانی، اختلال در بازار ارز و حساب‌های اجاره‌ای اشاره کرد.

در نهایت با معیار قرار دادن نوع تنظیم‌گری رمزدارایی‌ها در کشورهای پیشرو، راهکارهایی را جهت مقابله با ریسک‌های مذکور در سطح تنظیم‌گری ارائه می‌شود. تخصصی نمودن تنظیم‌گری برای هر دسته از ریسک‌ها، همکاری و مشورت با سایر مراکز و نهادهای دولتی، قضایی و انتظامی، و نیز استفاده از توانمندی‌های نهاد خودتنظیم‌گر از جمله توصیه‌های مهمی است که می‌تواند به کاهش اثرات منفی و افزایش بهره‌وری از فرصت‌های موجود در حوزه رمزدارایی‌ها منجر شود.

واژه‌های کلیدی: تنظیم‌گری رمزدارایی، ریسک‌های رمزدارایی‌ها، کلاهبرداری، پول‌شویی، ارائه‌دهندگان خدمات رمزدارایی، نهاد خودتنظیم‌گر

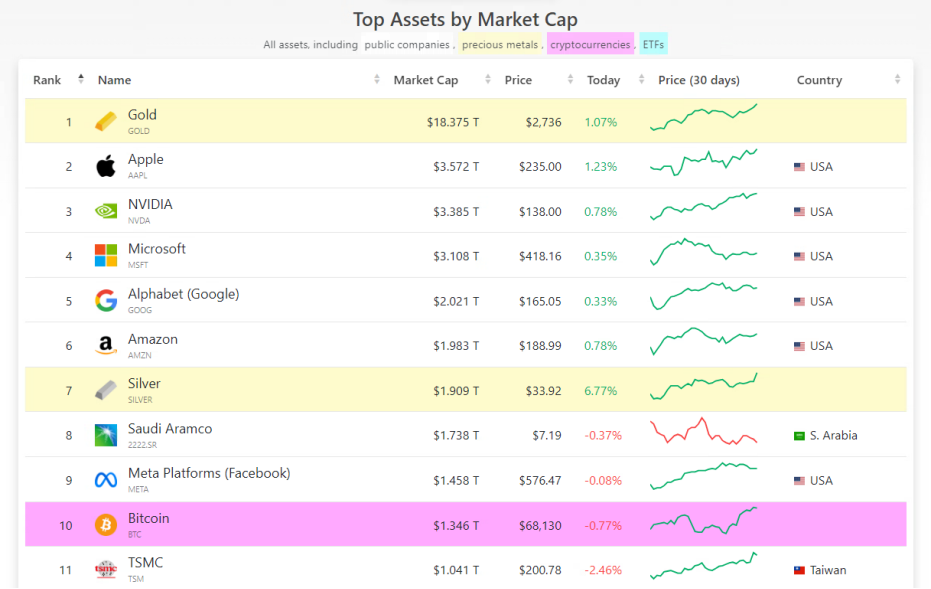
طبقه‌بندی JEL: K22، K24، G28، L86، O33

[۱] مدیر سابق آکادمی بلاکچین ققنوس، مدرس و مشاور حوزه رمزدارایی در اتاق بازرگانی تهران، sadeghsaberi@gmail.com

۱ مقدمه

رمزدارایی[1] نوعی دارایی دیجیتال است که از فناوری رمزنگاری برای تأمین امنیت تراکنش‌ها، کنترل ایجاد واحدهای جدید و تأیید انتقال دارایی‌ها استفاده می‌کند. برخلاف ارزهای سنتی که توسط دولت‌ها یا بانک‌های مرکزی کنترل می‌شوند، رمزدارایی‌ها به‌طور معمول غیرمتمرکز[2] و بر فناوری بلاکچین[3] مبتنی هستند. بلاکچین یک «فناوری دفتر کل توزیع شده»[4] است که تمام تراکنش‌های انجام شده را به صورت شفاف و تغییرناپذیر ثبت می‌کند. (Congressional Research Service, 2023)

رمزدارایی‌ها که خود شامل انواع مختلفِ «رمزارز»[5]، «توکن‌های بی‌همتا»[6]، «توکن‌های مبتنی بر دارایی‌های فیزیکی»[7] و ... هستند (Antonovici, 2024)، به عنوان یکی از جدیدترین و نوآورانه‌ترین فناوری‌های مالی در سال‌های اخیر، توجه بسیاری از افراد و نهادها را به خود جلب کرده‌اند، به‌گونه‌ای که در حال حاضر ارزش کل بازار رمزارزها، بیش از ۲/۳ هزار میلیارد دلار، و بیت‌کوین[8] به تنهایی با حجم بازار بیش از ۱/۳ هزار میلیارد دلار، دهمین دارایی ارزشمند جهان است. همچنین ارزش کل بازار NFTها بیش از ۷۰ میلیارد دلار برآورد می‌شود.



شکل ۱ . بیت‌کوین، دهمین دارایی ارزشمند جهان (CompaniesMarketCap, 2024)

---

[1] Crypto-asset

[2] Decentral

[3] Blockchain

[4] Distributed ledger Technology (DLT)

[5] Cryptocurrency

[6] Non-Fungible Token (NFT)

[7] Asset-backed Tokens

[8] Bitcoin (BTC)

باگسترش میزان سرمایه در بازار رمزدارایی و افزوده شدن تعداد فعالان آن (شامل ناشران توکن‌ها، توسعه‌دهندگان، سرمایه‌گذاران، ارائه‌دهندگان خدمات، کاربران و ...)، به همان نسبت تهدیدات و چالش‌های جدید و قابل‌ملاحظه‌ای به وجود آمده و فرصت‌های تقلب[1] و کلاهبرداری[2] نیز افزایش یافته و ریسک‌های متعددی برای مردم و دولت‌ها پدید آمده است.

۲ انواع ریسک‌های رمزدارایی

۱.۲ ریسک‌های مشترک با سایر کشورهای جهان

تراکنش‌های اغلب رمزدارایی‌ها به دلیل استفاده از بلاکچین‌های عمومی، ذاتاً شفاف و قابل‌ردیابی است، با این وجود مجرمان برای انجام فعالیت‌های غیرقانونی خود از رمزدارایی‌ها استفاده می‌کنند، چرا که رمزدارایی‌ها امکان تراکنش‌های مالیِ بین‌المللی، با سرعت بالا، بدون واسطه و با کارمزد بسیار پایین را فراهم می‌نمایند.

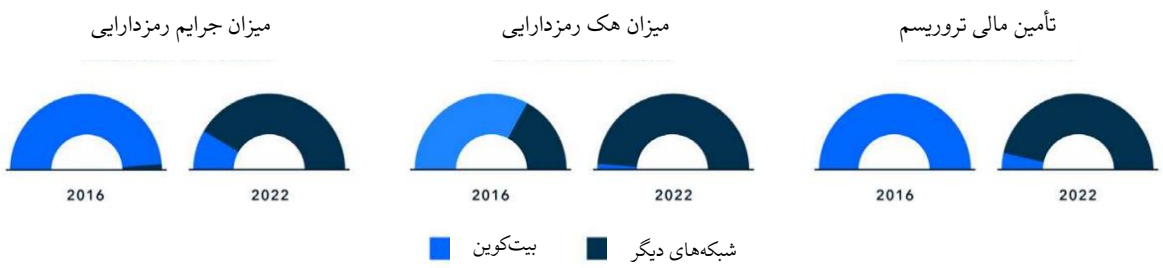
حتی سقوط شدید قیمت رمزدارایی‌ها در اواخر سال ۲۰۲۱، برخلاف انتظارها تأثیر قابل‌توجهی بر کاهش ارزش دلاری جرایم مرتبط با رمزدارایی در سال ۲۰۲۲ نداشت. مطابق داده‌های (TRM Labs, 2023) حداقل ۷/۸ میلیارد دلار با استفاده از توکن‌های پانزی[3] یا هرمی، و ۳/۷ میلیارد دلار از طریق هک‌های امنیتی در سال ۲۰۲۲ سرقت و حدود ۱/۵ میلیارد دلار در بازارهای غیرقانونی مواد مخدر غیرقانونی مبادله شده است. در همین سال مطابق داده‌های (Chainalysis, 2024)، حدود ۳۰ میلیارد دلار پول‌شویی به وسیله رمزدارایی‌ها برای انواع جرایم، از قبیل جرایم سنتی و آنلاین انجام شده است (نه فقط آن‌هایی که ذاتاً به اکوسیستم رمزدارایی گره خورده‌اند).

در میان دلایل احتمالی، جهش کیفیِ رمزدارایی‌ها از تسلط بیت‌کوین به سمت پدیده چند-زنجیره‌ای[4] است که تهدیدات نوینی را به وجود آورده است. به عنوان مثال، در سال ۲۰۲۲، حدود ۲ میلیارد دلار از طریق حملات به پل‌های[5] «زنجیره‌ـ متقاطع»[6] که امکان انتقال رمزدارایی‌ها از یک شبکه بلاکچین به شبکه بلاکچین دیگر (مثلاً از شبکه اتریوم[7] به شبکه سولانا[8]) را فراهم می‌کند، به سرقت رفت. همچنین جابجایی وجوه در شبکه‌های بلاکچین مختلف، به عنوان بخشی از استراتژی‌های پول‌شویی جهت پنهان‌سازی مبدأ و مقصد درآمدهای غیرقانونی، به شدت افزایش یافته است. (TRM Labs, 2023)

دوران چند-زنجیره‌ای به طور کلی تأثیر گسترده‌ای بر توزیع حجم فعالیت‌های غیرقانونی رمزدارایی‌ها داشته است، به طوری که سهم بیت‌کوین از ۹۷٪ در سال ۲۰۱۶ به ۱۹٪ در سال ۲۰۲۲ کاهش یافته است. در سال ۲۰۱۶، دو

[1] Fraud
[2] Scam
[3] Ponzi
[4] Multi-chain
[5] Bridge
[6] Cross-Chain
[7] Ethereum (ETH)
[8] Solana (SOL)

سوم حجم هک‌های ارزهای دیجیتال مربوط به بیت‌کوین بود؛ اما در سال ۲۰۲۲، این رقم به کمتر از ۳٪ کاهش یافت، در حالی که اتریوم (۶۸٪) و شبکه هوشمند بایننس[1] (۱۹٪) این حوزه را تحت سلطه قرار دادند. همچنین در حالی که بیت‌کوین در سال ۲۰۱۶ ارز انحصاری برای تأمین مالی تروریسم بود، تا سال ۲۰۲۲ تقریباً به طور کامل با دارایی‌های موجود در شبکه بلاکچین ترون[2] جایگزین شد که ۹۲٪ این فعالیت‌ها را شامل می‌شد.



شکل ۲ . تغییر رویکرد فعالیت‌های غیرقانونی از شبکه بلاکچین بیت‌کوین به سایر زنجیره‌ها (TRM Labs, 2023)

با در نظر گرفتن شرایط جدید حاکم بر دنیای رمزدارایی‌ها، انواع ریسک‌هایی که در صورت نبود تنظیم‌گری مناسب در کشور، می‌تواند سرمایه‌های مردم یا کشور را دچار آسیب‌های جبران‌ناپذیر نماید، به شرح زیر است:

۱.۱.۲ ریسک‌های ذاتی و سیستماتیک

قبل از ورود به معرفی ریسک‌های رمزدارایی‌ها، در قدم صفر، ریسک‌های ذاتی آنها برشمرده می‌شود. رمزدارایی‌ها مانند هر پدیده دیگر، فارغ از استفاده‌های گوناگونی که از آنها می‌شود، به شکل ذاتی و سیستماتیک، مزایا و ریسک‌های خاص خود را دارند. این ریسک‌ها شامل موارد زیر است:

۱.۱.۱.۲ *برگشت‌ناپذیر بودن تراکنش‌ها*

از مزایای بلاکچین و رمزدارایی‌ها، رفع مشکل «چند بار خرج کردن»[3] دارایی‌های دیجیتال و نیز غیرقابل جعل بودن تراکنش‌ها است. ولی در ازای به دست آمدن این مزایا، یک واقعیت را باید در مورد آنها پذیرفت و آن این‌که وقتی تراکنشی انجام شد، حتی به آدرس اشتباه، به هیچ عنوان دیگر قابلیت بازگرداندن تراکنش و رفع ایراد وجود ندارد. اصولاً اگر امکان برگشت تراکنش وجود داشت، دیگر هیچ تراکنشی قابل اعتماد نبود. (Casino, 2019)

[1] Binance Smart Chain (BNB)

[2] Tron (TRX)

[3] Double Spending Problem

۲.۱.۱.۲ امکان از دست دادن کیف‌پول غیر حضانتی[1]

تا زمانی که صاحب رمزدارایی، موجودی خود را در کیف‌پول غیر حضانتی نگاه می‌دارد، خود آن شخص مسئول صفر تا صد نگهداری از دارایی‌های خویش است، زیرا در این فضا هیچ واسطه‌ای از جمله بانک، برای نگهداری از پول و دارایی وجود ندارد.

کیف‌پول غیر حضانتی به کیف‌پول‌هایی گفته می‌شود که کلید خصوصی آن در دست خود شخص دارنده رمزدارایی است و هر زمان که بخواهد می‌تواند به آن دسترسی داشته باشد. این کیف‌پول‌ها تنوع بسیار زیادی دارند و از امنیت بالایی برخوردارند. در کیف‌پول‌های غیر حضانتی یا کلید خصوصیِ[2] آن شامل ۶۴ کاراکتر تصادفی از اعداد و حروف در اختیار کاربر قرار می‌گیرد و یا یک عبارت بازیابی[3] شامل ۱۲ یا ۲۴ به نمایندگی از همان کلید خصوصی. کاربر باید کلید خصوصی یا عبارت بازیابی را در یک جای امن نگهداری نماید تا در صورت هرگونه رخداد غیرمترقبه (مانند حذف شدن نرم‌افزار کیف‌پول از گوشی یا رایانه، سرقت شدن یا گم شدن یا خراب شدن گوشی یا رایانه یا کیف‌پول سخت‌افزاری) که موجب عدم دسترسی کاربر به کیف‌پول خود شود، وی بتواند به کمک آن کلید خصوصی یا عبارت بازیابی، مجدداً به کیف‌پول خود دسترسی پیدا کند. در صورتی که کلید خصوصی یا عبارت بازیابی گم شده باشد، دیگر امکان دسترسی کاربر به کیف پول غیرممکن خواهد بود و در نتیجه تمام رمزدارایی‌های خود را از دست خواهد داد. (Weichbroth, 2023)

۲.۱.۲ کلاهبرداری‌ها[4] و تقلب‌ها[5]

کلاهبرداری و تقلب را می‌توان به عنوان فریبی که منجر به ضرر می‌شود، در نظر گرفت. تقلب می‌تواند در هر کجا و در هر میزانی رخ دهد، از سرقت چند دلار در زندگی روزمره مصرف‌کنندگان تا کلاهبرداری‌های پیچیده شرکتی که منجر به از دست رفتن میلیاردها دلار در رمزدارایی‌ها می‌شود. با توجه به حجم و انواع کلاهبرداری‌ها و تقلب‌هایی که در فضای رمزدارایی رخ داده است و متأسفانه همچنان رخ می‌دهد، به نظر می‌رسد که تقریباً همه روش‌های قدیمی، در فضای رمزدارایی‌ها به کار گرفته شده‌اند (TRM Labs, 2023). با این حال، برخی از انواع تقلب‌ها در میان کلاهبرداران دنیای رمزدارایی‌ها محبوب‌تر هستند، عبارت‌اند از:

۱.۲.۱.۲ انتشار، عرضه و تبلیغات رمزدارایی‌های پانزی یا هرمی

طرح‌های پانزی یا هرمی پیش از خلق رمزدارایی‌ها نیز وجود داشتند، ولی قرار گرفتن این طرح‌ها در کنار رمزدارایی‌ها، توانست سرعت انتشار و میزان کلاهبرداری‌های از این جنس را به شدت افزایش دهد. در این روش ممکن است که کلاهبردار تا مدتی سود قول داده شده را از طریق پول وارد شده توسط قربانیان جدید، به نفرات قبلی بدهد. اما پس از مدتی که ورود پول به مجموعه کاهش یافت، کلاهبردار به هدف خود رسیده است و با حجم عظیمی

---

[1] Non-Custodial Wallet

[2] Private Key

[3] Recovery Phrase

[4] Scam

[5] Fraud

از پول فرار می‌کند. در طرح پانزی جذب زیرمجموعه الزامی نیست، اما در یک طرح با سیستم هرمی باید حتماً این کار انجام شود. (Jason Scharfman, 2023)

نبود نظارت مناسب می‌تواند به افزایش کلاهبرداری‌ها و طرح‌های پانزی مبتنی بر رمزدارایی‌ها منجر شود. برای مثال، کلاهبرداری پلاس‌توکن[1] یک پروژه کلاهبرداری بزرگ در چین بود که به صورت طرح پانزی منتشر شده بود و به دلیل عدم تنظیم‌گری مناسب در چین، موفق شد در سال‌های ۲۰۱۸ و ۲۰۱۹، حدود ۲,۶ میلیون کاربر را فریب دهد. البته در آن زمان، پلیس محلی چین حدوداً معادل ۱۴ میلیارد دلار، بیت کوین، اتریوم و دیگر رمزدارایی‌ها را ضبط کرد. (Akolkar, 2024)

همچنین می‌توان به یک کلاهبرداری بسیار معروف در ایران به نام «کینگ‌مانی»[2] و رمزارز آن KIM اشاره نمود که در سال ۲۰۱۹ با ترکیب فضای رمزدارایی با طرح پانزی، در سایه نبود نهاد تنظیم‌گر و قوانین به‌روز، توانست یکی از بزرگ‌ترین کلاهبرداری‌های تاریخ ایران را رقم بزند. پرونده کینگ‌مانی بیش از ۴۰۰۰ شاکی به ارزش ۱۰۷ میلیون یورو داشت. در سال ۲۰۲۱ وزارت اطلاعات ایران اعلام نمود که گردانندگان کینگ مانی دستگیر شده‌اند. اوایل سال ۲۰۲۴ نیز رأی دادگاه در قبال متهمان پرونده صادر گردید و ایشان محکوم به حبس طویل‌المدت و پرداخت معادل یورویی مطالبات شاکیان با احتساب ارزش ریالی ارز مذکور شدند. (ایزک‌شیریان، ۱۴۰۳)

۲.۲.۱.۲ انتشار، عرضه و تبلیغات رمزدارایی‌های غیرقابل فروش

یکی دیگر از ریسک‌ها، انتشار و عرضه رمزدارایی‌های است که قرارداد هوشمند[3] آنها، طوری کدنویسی شده است که کاربران تنها می‌توانند آنها را خریداری نمایند، ولی اطلاع ندارند که امکان فروش بسته است. بدین ترتیب قیمت این رمزدارایی‌ها در ابتدا فقط بالا و بالاتر می‌رود و هیچ‌گاه نمودار قیمتی آنها نزولی نمی‌شود. در نهایت تیم توسعه‌دهنده‌ی این رمزدارایی‌ها بعد از جمع‌آوری مبالغ از قربانیان، با دسترسی بالاتری که دارند، کل آن رمزدارایی را به صورت دفعی یا تدریجی می‌فروشند و قیمت آن را به صفر می‌رسانند. بهترین مثال این استراتژیِ کلاهبردارانه، رمزارز «اسکوئید گیم»[4] است. (TRM Labs, 2022)

۲.۲.۱.۳ انتشار، عرضه و تبلیغات رمزدارایی‌های بی‌ارزش

نوع دیگری از رمزدارایی‌های کلاهبرداری، مواردی است که نه مدل کسب‌وکاری آنها مشخص است، نه پشتوانه واقعیِ فیزیکی (مانند الماس) یا غیرفیزیکی (مانند آثار هنری) دارند، نه خدمت خاصی را روی بستر بلاکچین انجام می‌دهند و نه حتی یک جامعه مخاطبِ انبوهِ غیرمتمرکز دارند که در تأیید تراکنش‌ها و ارتقای پروژه سهیم باشند. این‌گونه رمزدارایی‌ها معمولاً یا سپیدنامه ندارند و یا محتوای سپیدنامه شامل نکات فنی، اهداف توکن، نحوه اجماع، معرفی تیم سازنده و ... نیست. (Jason Scharfman, 2023)

---

[1] PlusToken

[2] King Money

[3] Smart Contract

[4] Squid Game

مثلاً رمزارز «سیف‌مون»[1] بدون هیچ مدل اقتصادی مشخص و با وعده‌ی سوددهی غیرواقعی توسط سلبریتی‌ها، بسیاری از سرمایه‌گذاران را فریب داد ولی در نهایت ارزش آن به سرعت کاهش یافت و ورشکسته شد. یک نمونه اخیر نیز مجموعه NFTهای «دنیای صلح‌آمیز»[2] بود که ادعا می‌کرد توسط دولت اوکراین هواداری شده است ولی این‌طور نبود. (Kaaru, 2023)

در ایران نیز موارد متعددی مانند رمزارزهای «بریج»[3] و «کربلا کوین» و ... بوده‌اند که در این دسته قرار می‌گیرند. به عنوان مثال در پروژه «کربلا کوین» کلاهبرداران دست روی باورهای دینی و مذهبی ایرانیان گذاشتند و با تبلیغات بسیار، رمزارز «کربلا کوین» را روشی برای مشارکت در کارهای خیر مانند اهدای وام قرض‌الحسنه و اشتغال آفرینی معرفی کردند که منجر به سوددهی برای خیّرین می‌شود. (علی‌یاری، ۱۴۰۲)

هر سه مورد اخیر از دسته کلاهبرداری‌های با هدف خروج (rugpulls) هستند و زمانی اتفاق می‌افتد که گردانندگان یک پروژه رمزدارایی، به یکباره توسعه پروژه را متوقف می‌کنند و وجوه کاربران را برای خود برداشت می‌کنند. (TRM Labs, 2023)

۴.۲.۱.۲ *قراردادهای هوشمند فریبنده*[4]

قراردادهای هوشمند فریبنده، به طور عمدی طراحی شده‌اند که کاربران را فریب داده تا مجوز انتقال رمزدارایی از کیف پول خود را به توسعه‌دهنده قرارداد هوشمند بدهد. در نظر داشته باشید که اعطای مجوز در کیف‌پول‌هایی مانند متامسک[5]، امری معمول است و ممکن است کاربر کیف پول، با قرارداد هوشمند فریبنده، مشابه سایر قراردادهای هوشمند که سالم و بدون مشکل هستند برخورد نماید، به خصوص اگر تخصص کافی برای کار در حوزه «امور مالیِ غیرمتمرکز»[6] نداشته باشد.

شناخته‌شده‌ترین نمونه این نوع قراردادها «Drainware» است، قراردادهای هوشمندی که پس از تعامل، به مهاجم اجازه می‌دهند تا رمزدارایی‌ها و NFTهای موجود در کیف پول قربانی را تخلیه کنند. توکن‌های جعلی نیز شکل دیگری از قراردادهای هوشمند فریبنده هستند. (TRM Labs, 2023)

---

[1] SafeMoon

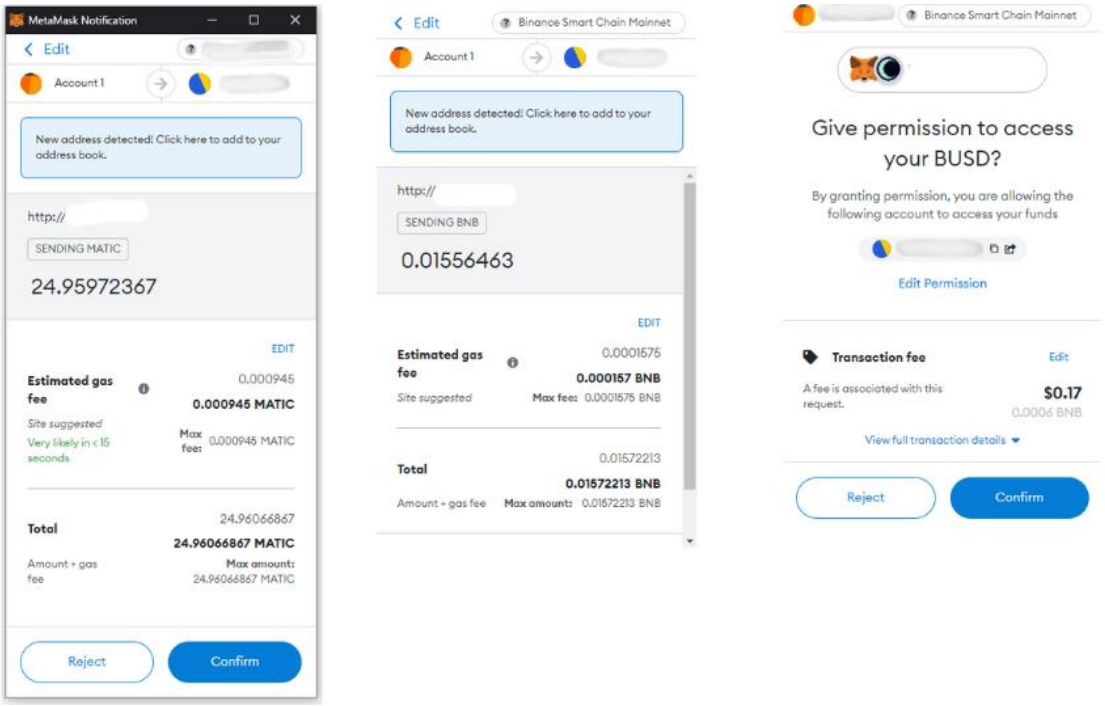
[2] Peaceful World

[3] Bridge (BRG)

[4] Deceptive Smart Contracts

[5] Metamask

[6] Decentral Finance (DeFi)



شکل ۳. نمونه‌ای از فضای اعطای مجوز برای اجرای قراردادهای هوشمند در کیف پول متامسک

افزایش چشمگیر در حملات drainware حتی منجر به ظهور «الگوهای Drainware به عنوان سرویس» (DTaaS) شده است که الگوهایی مخرب و از پیش ساخته آماده برای راه‌اندازی را همراه با یک وب‌سایت فیشینگ، ربات سرور دیسکورد و قرارداد هوشمند ارائه می‌دهد. (TRM Labs, 2023)

۲ .۱ .۲ .۵ *کلاهبرداری به وسیله مهندسی اجتماعی*[1]

در این نوع از کلاهبرداری‌ها که عناوین دیگری همچون «کلاهبرداری عاشقانه»[2] یا «کلاهبرداری قصابی خوک»[3] نیز دارد، کلاهبردار با جلب اعتماد قربانی به روش‌های مختلف به ویژه روش‌های احساسی و عاشقانه، و با دادن وعده سود فوق‌العاده سرمایه‌گذاری آغاز می‌شود. کلاهبردار که خود را به‌عنوان فردی ثروتمند یا صاحب نفوذ در نهادهای حاکمیتی یا شرکت‌های بزرگ معرفی می‌کند، پس از فریب قربانی به لحاظ احساسی و روانی، و سوءاستفاده از اعتماد او، پول‌هایش را به سرقت می‌برد و در عمل سرمایه فرد را قصابی می‌کند. به عنوان مثال در سپتامبر ۲۰۲۱، گزارش شد که چندین نفر در ونکوور کانادا قربانی کلاهبرداری‌های عاشقانه مرتبط با رمزارز شده‌اند و در مجموع بیش از ۱۰۰،۰۰۰ دلار از دست داده‌اند. (Jason Scharfman, 2023)

---

[1] Social Engineering

[2] Romance Scam

[3] Pig Butchering Scam

۲ .۱ .۲ .۶ *فیشینگ*[1]

فیشینگ شامل استفاده از ایمیل‌ها، وب‌سایت‌ها، یا پیام‌های جعلی برای فریب کاربران به منظور افشای اطلاعات حساس مانند کلیدهای خصوصی یا اعتبارنامه‌های ورود است. در فضای رمزدارایی‌ها، حملات فیشینگ ممکن است کاربرانِ کیف‌پول‌ها یا صرافی‌ها را هدف قرار دهد که منجر به سرقت وجوه می‌شود.

فیشینگ در فضای رمزدارایی‌ها عمدتاً با ایجاد صفحات وب جعلی که به لحاظ نام، آدرس و ظاهر صفحه، کاملاً مشابه صرافی‌های رمزدارایی[2] یا کیف‌پول‌های آنلاین اصلی هستند، اتفاق می‌افتد. کلاهبرداران با استفاده از روش‌های مختلف نظیر تبلیغات و مهندسی اجتماعی کاربران را فریب می‌دهند و بسیاری از آن‌ها را به سوی این صفحات می‌کشانند. پس از اینکه کاربر اطلاعات شخصی خود را در وب‌سایت جعلی وارد کرد، این اطلاعات در اختیار کلاهبرداران قرار گرفته و کل دارایی فرد قربانی ربوده خواهد شد. (Jason Scharfman, 2023)

ربات‌های معامله‌گر[3] نیز یکی دیگر از روش‌های فیشینگ محسوب می‌شود. برخی کاربران برای بهبود معاملات خود در صرافی‌های رمزدارایی، از این ربات‌ها استفاده می‌کنند ولی همه آنها دانش کدنویسی این ربات‌ها را ندارند و به همین علت از سایرین خریداری می‌نمایند. فروشنده ربات ممکن است بدون اطلاع خریدار، طوری کدنویسی کرده باشد که وقتی کاربر برای انجام معاملات خودکار با ربات وارد صرافی شده و اطلاعات حساب خود را وارد می‌کند. ربات معامله‌گر این اطلاعات را ذخیره کرده و برای فروشنده ارسال می‌نماید تا دارایی‌های کاربر را به سرقت ببرد. حملات فیشینگ در زمان رونق عرضه اولیه سکه[4] در سال ۲۰۱۷ نیز بسیار برجسته شدند. قربانیان در این حملات فیشینگ فقط مقدار رمزدارایی را از دست می‌دادند که به اشتباه به آدرس نادرست ارسال کرده بودند. با ورود NFTها به جریان اصلی بازار، مهاجمان شروع به هدف قرار دادن سرمایه‌گذاران تازه‌کار NFT کردند.

فیشینگ روش‌های متعدد دیگری نیز دارد. به عنوان مثال کلاهبرداری‌های ایمیل تجاری[5] که در آن کلاهبرداران خود را به عنوان یک کسب‌وکار یا سازمان قانونی جا می‌زنند تا کارمندان یا شرکای کسب‌وکار را فریب داده که با به خطر افتادن حساب‌های ایمیل متعلق به کارمندان صرافی‌ها، ارائه‌دهندگان کیف پول، منجر به سرقت وجوه یا داده‌های حساس می‌شود. در سال ۲۰۲۲، BEC به دلیل خسارات گزارش شده توسط قربانیان به مرکز شکایت جرم اینترنتی FBI[6]، معادل ۲/۷ میلیارد دلار (رمزدارایی و پول فیات) را شامل شد. (TRM Labs, 2023)

۲ .۱ .۲ .۷ *کلاهبرداری‌های جعل هویت*[7]

در این روش، کلاهبرداران خود را نماینده صرافی‌های رمزدارایی یا پشتیبان کیف پول جا می‌زنند تا کاربرانِ ناآگاه را فریب داده و رمزدارایی آنها را به آدرس‌های کلاهبردار ارسال کنند یا اطلاعات حساس را افشا کنند. کلاهبرداران خبره

---

[1] Phishing

[2] Crypto Exchange

[3] Trading Bots

[4] Initial Coin Offering (ICO)

[5] Business email compromise (BEC)

[6] FBI's Internet Crime Complaint Center (IC3)

[7] Impersonation Scams

در این روش، معمولاً چند روز یا چند هفته بعد از دریافت اطلاعات حساس کاربر، برای تخلیه حساب یا کیف‌پول اقدام می‌کنند تا خود را از مظان اتهام دور نگاه دارند. (Jason Scharfman, 2023)

۸. ۲. ۱. ۲ دستکاری بازار[1]

دستکاری بازار می‌تواند شامل طرح‌های مختلفی باشد که برای تأثیرگذاری مصنوعی بر قیمت یک رمزدارایی طراحی شده‌اند. این طرح‌ها می‌تواند شامل طرح‌های پامپ و دامپ[2] یا تبلیغ غیرمجاز[3] باشد. در دسامبر ۲۰۲۲، کمیسیون بورس و اوراق بهادار ایالات‌متحده[4]، مدیران Alameda Research و صرافی رمزدارایی FTX را به دستکاری در قیمت رمزدارایی FTT (رمزدارایی اختصاصی صرافی FTX) به وسیله خرید مقادیر زیادی در بازار آزاد برای بالا بردن قیمت آن متهم کرد. (TRM Labs, 2023)

- طرح‌های پامپ و دامپ

شامل خرید هماهنگ یک ارز دیجیتال یا توکن برای افزایش مصنوعی قیمت آن است و پس از رسیدن قیمت به یک سطح خاص، فروش هماهنگ انجام می‌شود. این امر منجر به سقوط قیمت شده و سرمایه‌گذاران بی‌خبر را با ضررهای قابل‌توجهی مواجه می‌کند.

هزاران اتاق گفتگوی آنلاین در بخش تاریک وب و همچنین کانال‌های عمومی در تلگرام به طرح‌های پامپ و دامپ اختصاص داده شده‌اند که برخی از آنها تا چهار میلیون عضو دارند. سازمان‌دهندگان کانال‌های تلگرام ممکن است سیگنال‌های معاملاتی را چند دقیقه پس از اینکه خودشان معامله کرده‌اند به دیگر اعضای گروه ارائه دهند. این کار به رهبران گروه اجازه می‌دهد تا به قیمت زیان دیگر اعضا سود کنند، اعضایی که به اشتباه تصور می‌کنند با خرید یا فروش توکن مربوطه بر اساس دستورالعمل‌های سازمان‌دهندگان سود خواهند برد.

طرح‌های پامپ و دامپ تا حدود ۱۲۰ میلیارد دلار حجم سالانه در بازارهای رمزنگاری را تشکیل می‌دهند. تحلیل مبتنی بر موقعیت جغرافیایی نشان داد که ایالات‌متحده منبع اصلی این طرح‌هاست و پس از آن ایران قرار دارد. (TRM Labs, 2023)

- تبلیغ غیرمجاز

وقتی فردی یک رمزدارایی یا دارایی مجازی دیگری را که به عنوان توکن اوراق بهادار[5] تعریف شده است تبلیغ نماید، بدون اعلام آنکه از طرف ناشران آن، پول دریافت کرده است، به این عمل «تبلیغ غیرمجاز» گفته می‌شود. در هفت سال گذشته، چندین شخصیت مشهور به دلیل نقض قوانین تبلیغ غیرمجاز هنگام تبلیغ یک ICO توسط کمیسیون بورس و اوراق بهادار آمریکا (SEC) جریمه شده‌اند.

---

[1] Market Manipulation

[2] Pump & Dump

[3] Touting

[4] The U.S. Securities and Exchange Commission

[5] Security Token

در اکتبر ۲۰۲۲، کمیسیون بورس و اوراق بهادار آمریکا، معروف‌ترین سلبریتی زن آن زمان آمریکا را به دلیل تبلیغ یک «توکن اوراق بهادار» که توسط EthereumMax عرضه و فروخته شده بود، بدون افشای این که به او ۲۵۰ هزار دلار برای این کار پرداخت شده بود، متهم کرد. وی برای تسویه این اتهامات ۱,۲۶ میلیون دلار به عنوان جریمه، استرداد درآمد و بهره پرداخت کرد. در ایران نیز متأسفانه طی سال‌های اخیر، موارد بسیار زیادی از چنین تبلیغات غیرمجازی توسط سلبریتی‌ها در شبکه‌های اجتماعی مختلف دیده شده که تا کنون برخورد قانونی نشده است. (TRM Labs, 2023)

۹.۲.۱.۲ رانت دسترسی به اطلاعات دسته‌اول[1]

به استفاده از اطلاعات غیرعمومی برای خرید رمزدارایی یا دیگر دارایی‌های مجازی قبل از اعلام لیست شدن در صرافی‌ها و کسب سود از افزایش قیمت پس از اعلام خبر، مربوط می‌شود.

طبق تحقیقات اختصاصی شرکت Argus Inc که در زمینه تحلیل معاملات داخلی رمزدارایی‌ها فعالیت می‌کند، تنها در سال ۲۰۲۲ حدود ۲۴ میلیون دلار از توکن‌های ERC20 به رانت دسترسی به اطلاعات دست‌اول مرتبط بوده است و حداقل ۵,۵ میلیون دلار سود برای معامله‌گران ایجاد کرده است. بسیاری از این کیف پول‌ها در سال ۲۰۲۳ نیز همچنان فعال بوده‌اند. امکان انجام این نوع از کلاهبرداری در صرافی‌های متمرکز[2] بسیار بیشتر از صرافی‌های غیرمتمرکز[3] است.

در ژوئن ۲۰۲۲، یکی از کارمندان سابق یک بازار NFT به عنوان اولین فرد به اتهام کلاهبرداری در ارتباط با طرحی برای سوءاستفاده از رانت دسترسی به اطلاعات دست‌اول در مورد اینکه کدام NFTها قرار است در صفحه اصلی صرافی نمایش داده شوند، متهم شد. پس از آن افراد دیگری نیز با اتهامات مشابه روبرو شدند. (TRM Labs, 2023)

۱۰.۲.۱.۲ کلاهبرداری تحت عنوان اجاره ماینر[4]

این مدل از کلاهبرداری، لزوماً ارتباط مستقیم با رمزدارایی‌ها ندارد، بلکه با جمع‌آوری سرمایه کاربران برای ماینینگ ابری[5] تحت عنوان اجاره ماینر و ارائه سود ماینینگ به کاربر، بدون نیاز به خرید دستگاه‌های گران قیمت ماینر و مشکلات فراوان راه‌اندازی آن و اختصاص یک فضای مناسب برای ماینرها، انجام می‌گیرد. در اغلب مواقع اصلاً هیچ ماینری در کار نیست و فقط در پنل کاربر، اعدادی به عنوان میزان درآمد در روز نمایش داده می‌شود. اما همین که کاربر بخواهد درآمدهای خود را دریافت نماید، هیچ مبلغی به او پرداخت نمی‌شود. بدین ترتیب فرد کلاهبردار مبالغ زیادی را جمع‌آوری کرده و بعد از مدتی فرار می‌کند. (اسماعیلی، ۱۴۰۲)

---

[1] Insider Trading

[2] Centralized Exchanges (CEX)

[3] Decentralized Exchanges (DEX)

[4] Miner

[5] Cloud Mining

۳.۱.۲ پرداخت‌های غیرقانونی

بخش مهمی از ریسک‌های رمزدارایی‌ها مربوط به پرداخت‌های غیرقانونی و مجرمانه برای مقاصدی از جمله رشوه به مقامات فاسد یا حوزه‌های قضایی و ... است. صندوق بین‌المللی پول در مقاله‌ای در سال ۲۰۲۲ این‌گونه بیان می‌کند: «به تجربه ثابت شده است که استفاده بیشتر از رمزدارایی، با فساد بیشتر و کنترل‌های سرمایه شدیدتر مرتبط است.» که نشان می‌دهد رمزدارایی‌ها ممکن است برای انتقال درآمدهای غیرقانونی یا دور زدن فرایندهای کنترل‌های سرمایه از سمت نهادهای دولتی و بین‌المللی استفاده شود. (Alnasaa et al, 2022)

۱.۳.۱.۲ اخاذی[1]

اخاذی با رمزدارایی می‌تواند اشکال مختلفی داشته باشد. در ساده‌ترین شکل آن، شامل افراد تهدید قربانیان خود و مطالبه پرداخت رمزدارایی می‌شود. معمولاً هم به این شکل است که ابتدا یک گروه هکری، به روش Ransomware به مراکز حساس دولتی یا شرکت‌های بزرگ، حمله امنیتی می‌کند و اطلاعات حساس آنها را رمزگذاری یا سرقت می‌نماید، سپس اقدام به اخاذی و مطالبه مبالغ هنگفتی به شکل رمزدارایی می‌کند. (TRM Labs, 2023)

در سال ۲۰۲۳، کارمند سابق یک شرکت فناوری مستقر در نیویورک به دلیل سرقت فایل‌های شرکت و مطالبه تقریباً ۲ میلیون دلار برای بازگشت آن‌ها، به شش سال زندان محکوم شد. در ایران هم گروه هکری موسوم به IRleaks توانست از طریق حمله به برخی نهادهای حکومتی، هسته اصلی سیستم بانکی (سرقت اطلاعات حساس مشتریان ۲۰ بانک کشور) و شرکت‌های شاخصی مانند اسنپ‌فود، تپسی و اتاقک، مبالغ چند میلیون دلاری را از طریق بیت‌کوین اخاذی نماید در قبال آن‌که اطلاعات را به بیرون درز ندهد. (راه پرداخت، ۱۴۰۳)

۲.۳.۱.۲ پرداخت رشوه[2]

چندین مورد پر سروصدا از رشوه ثابت شده یا ادعایی مربوط به رمزدارایی وجود داشته است. در سال ۲۰۲۱، سم بنکمن‌ـ‌فرید[3]، بنیانگذار یکی از بزرگترین صرافی‌های رمزارزی در دنیا با نام FTX، ظاهراً در ازای آزادسازی حساب‌های شرکت خود در چین که حاوی بیش از ۱ میلیارد دلار رمزدارایی بوده است، رشوه ۴۰ میلیون دلاریِ رمزدارایی به مقامات چینی داده است. در مثالی دیگر در سال ۲۰۲۲، وزارت دادگستری ایالات‌متحده دو افسر اطلاعاتی چینی را به تلاش برای رشوه دادن به یک کارمند دولت ایالات‌متحده ۶۱۰۰۰ دلار در قالب بیت‌کوین جهت سرقت اسناد مربوط به تحقیقات در مورد غول فناوری چینی با نام هواوی[4] متهم نمود. (Cohen, 2023)

۳.۳.۱.۲ تجارت غیرقانونی

تجارت غیرقانونی شامل خریدوفروش انواع کالاها و خدمات غیرقانونی است. در حالی که اکثریت قریب به اتفاق تجارت غیرقانونی همچنان از ارز فیات[5] مانند دلار آمریکا استفاده می‌کنند، رمزدارایی‌ها ارز ترجیحیِ تبادلات مالی

---

[1] Extortion

[2] Bribery

[3] Sam Bankman-Fried

[4] Huawei

[5] Fiat Money

در بازارهای سیاه[1]، انجمن‌های جرم سایبری[2] و ... است. در این بازارها ممکن است تجارت مواد مخدر، معامله کالاهای سرقت شده، قاچاق انسان و اعضای بدن، استخدام قاتل و زورگیر، ارائه خدمات جرایم سایبری مانند هاستینگ ضدگلوله[3]، حملات DDoS، بات‌نت به عنوان سرویس[4]، حملات اسپم[5] و... انجام شود. (TRM Labs, 2023)

۴.۳.۱.۲ استفاده برای فعالیت‌های جاسوسی[6]

فعالیت‌های جاسوسی می‌تواند شامل انتقال مخفی وجوه برای حمایت از جمع‌آوری اطلاعات یا عملیات مخفی دیگر باشد. رمزدارایی‌ها می‌توانند یک روش دور از انظار و امن برای انتقال وجوه فراهم کنند و به یک گزینه جذاب برای بازیگران دولتی یا غیردولتی درگیر در جاسوسی تبدیل شوند. در سال ۲۰۲۲، ایران چهار جاسوس اسرائیل را که ادعا می‌شد مبالغی را به صورت رمزدارایی دریافت نموده‌اند، دستگیر کرد. (Sengupta, 2022)

۵.۳.۱.۲ فرار از کنترل‌های صادراتی[7]

فرار از قوانین کنترل صادرات شامل استفاده از رمزدارایی‌ها برای دور زدن کنترل‌های گمرکی و محدودیت‌های صادرات کالاها یا فناوری‌های خاص است. افراد می‌توانند از رمزدارایی‌ها برای تسهیل پرداخت‌های اقلام ممنوعه استفاده کنند و از سیستم‌های مالی سنتی که ممکن است چنین تراکنش‌هایی را علامت‌گذاری یا مسدود کنند، دور بزنند. در مطالعه‌ای در سال ۲۰۱۹ مشخص گردید رمزدارایی‌ها به طور گسترده توسط بازرگانان چینی جهت دور زدن قوانین کنترلی استفاده می‌شود. (Hu, 2019)

۴.۱.۲ بر هم زدن نظام مالی و پولی کشورها

رمزدارایی‌ها می‌توانند به روش‌های زیر، به عنوان یک چالش جدی برای نظام مالی و پولی کشورها عمل کنند:

۱.۴.۱.۲ عملیات پرداخت با استفاده از رمزدارایی‌ها و تهدید حاکمیت ارز ملی

استفاده از رمزدارایی‌ها به عنوان ابزار پرداخت، می‌تواند حاکمیت مالی و پولی کشور را تهدید کند. معاملات انجام‌شده با رمزدارایی‌ها جهت خریدوفروش هر دارایی دیگر مانند ملک، خودرو، طلا و ... موجب تضعیف ارز ملی می‌شود. این‌گونه معاملات در کشورهای با نرخ تورم بالا، بیشتر اتفاق می‌افتد، چرا که افراد نمی‌خواهند با نگهداری پول نقد، درگیر ریسک کاهش دارایی خود شوند. مثلاً در نیجریه، استفاده از رمزدارایی‌ها برای معاملات بزرگ به دلیل کاهش ارزش نایرا[8] و محدودیت‌های شدید بانکی افزایش یافته و موجب کاهش تسلط بانک مرکزی بر پول ملی شده است. (Johnson, 2023)

---

[1] Darknet markets (DNMs)

[2] Cybercrime Forums

[3] Bulletproof Hosting

[4] Botnet As a Service

[5] Spam Attacks

[6] Espionage

[7] Export Control Evasion

[8] Nigerian Naira

یا به عنوان مثال مرکزی با نام «خانه رمزارز ایران» که در سال ۲۰۲۴ در مجتمع تجارت جهانی فردوسی (مرکز خریدوفروش طلا، سکه و ارز) فعالیت می‌کرد، از سوی مراجع انتظامی پلمب شد، زیرا به دفعات و با مبالغ بالا از رمزدارایی‌ها به عنوان ابزار پرداخت جهت خریدوفروش رمزدارایی با سکه، ارز و طلا، برای خود و سایر کسبه استفاده می‌کرده است. (علی‌پور، ۱۴۰۳)

۲.۴.۱.۲ *نوسانات قیمتی زیاد*

از آنجا که حجم بازار بیش از ۹۹ درصد رمزدارایی‌ها بسیار کوچک است، بنابراین با ورود یا خروج سرمایه‌های بسیار خرد، امکان تغییرات قیمت با نوسان بالا در آنها بسیار زیاد است. به‌گونه‌ای که در مدت چند دقیقه امکان رشد قیمت ۱۰۰۰ درصدی یا سقوط قیمت ۹۹ درصدی وجود دارد و بارها رخ داده است. این نوسانات شدید قیمت می‌تواند به عدم ثبات در بازارهای مالی کشور منجر شود و خطر بحران‌های اقتصادی را افزایش دهد.

۳.۴.۱.۲ *پول‌شویی*[1]

پول‌شویی باعث افزایش میزان کلی فعالیت‌های غیرقانونی در اکوسیستم می‌شود زیرا تمام تراکنش‌هایی که در جهت شستشوی پول انجام می‌شوند، خودشان نیز غیرقانونی هستند. این فرایند شامل پردازش وجوهی است که از فعالیت‌های مجرمانه به دست آمده‌اند تا منشأ غیرقانونی آن‌ها را پنهان کند. پول‌شویی به کمک رمزدارایی‌ها یکی از چالش‌های مهم در دنیای مالی دیجیتال است. در این روش‌ها از ویژگی‌های خاص رمزدارایی‌ها، مانند ناشناسی و انتقال سریع، سوءاستفاده می‌شود. برخی از روش‌های متداول پول‌شویی با رمزدارایی‌ها عبارت‌اند از: (Elliptic, 2024)

- **مبادله‌های مستقیم:** پولشویان از صرافی‌های رمزدارایی برای تبدیل ارزهای فیات به رمزدارایی‌ها و برعکس استفاده می‌کنند. در این روش، فرد پول آلوده را به رمزدارایی تبدیل می‌کند و سپس آن را در صرافی‌های مختلف مبادله می‌کند تا ردیابی دشوار شود.
- **میکسرها**[2]**:** میکسرهایی مانند «تورنادو ـ کش»[3] به کاربران اجازه می‌دهد تا رمزدارایی‌های خود را با رمزدارایی دیگران ترکیب کنند تا منشأ آن قابل‌ردیابی نباشد. این سیستم‌ها با مخلوط کردن تراکنش‌ها، تراکنش‌های خروجی را از تراکنش‌های ورودی جدا می‌کنند.
- **انتقال از طریق کیف‌پول‌های ناشناس:** کیف‌پول‌های دیجیتالی که نیاز به احراز هویت ندارند یا امکان ساخت چندین آدرس دارند، برای پنهان کردن هویت افراد مورد استفاده قرار می‌گیرند.
- **پلتفرم‌های مالی غیرمتمرکز:** این پلتفرم‌ها به دلیل نبود واسطه‌ها و نظارت مرکزی، زمینه مناسبی برای پول‌شویی فراهم می‌کنند. در DeFi، تراکنش‌ها به صورت همتا به همتا و بدون دخالت نهادی انجام می‌شوند.
- **خریدوفروش NFT:** یکی از روش‌های جدید پول‌شویی خریدوفروش NFTها است. افراد می‌توانند NFTها را با قیمت‌های غیرواقعی خریداری یا بفروشند تا منابع مالی مشکوک را قانونی جلوه دهند.

---

[1] Money Laundering

[2] Mixers

[3] Tornado-Cash

- **استفاده از رمزارزهای حریم خصوصی[1]:** رمزارزهایی مانند مونرو و زی‌کش به‌گونه‌ای هستند که برخلاف سایر رمزارزها، نه مبلغ تراکنش‌ها مشخص است و نه معلوم است که مبالغ از کجا می‌آیند و به کجا می‌روند. بنابراین تراکنش‌های روی شبکه‌های رمزارزهای خصوصی قابل ردگیری نیستند.

۲ .۱ .۴ .۴ تأمین مالی گروه‌های تروریستی

شناسایی طرفین انتقال پول به وسیله رمزدارایی‌ها، کار چندان آسانی نیست و در برخی موارد اصلاً امکان‌پذیر نیست. در نتیجه رمزدارایی‌ها می‌توانند به ابزاری برای تأمین مالی فعالیت‌های تروریستی غیرقانونی تبدیل شوند که امنیت ملی را تهدید نماید. کمپین‌های جمع‌آوری کمک مالی برای خانواده‌های داعش که در اردوگاه‌های بازداشت در شمال شرقی سوریه نگهداری می‌شوند، یکی از عوامل مهم استفاده از ارز دیجیتال در میان داعش و حامیان آن بوده است. (TRM Labs, 2023)

۲ .۱ .۴ .۵ فرار مالیاتی[2]

نبود مقررات دقیق برای شفافیت در معاملات رمزدارایی‌ها می‌تواند منجر به فرار مالیاتی گسترده شود، که این امر به کاهش درآمدهای دولت و افزایش فشار بر سایر منابع درآمدی منجر خواهد شد. به عنوان مثال، در ایالات‌متحده، برخی از سرمایه‌گذاران رمزدارایی‌ها از روش‌های پیچیده برای فرار از مالیات‌های خود استفاده می‌کنند و این امر باعث شده تا دولت برای شناسایی این معاملات دست به ایجاد مقررات بیشتری بزند (Iacurci, 2021).

در ایران نیز روش‌های مختلفی برای فرار مالیاتی با استفاده از رمزارزها استفاده می‌شود. به عنوان مثال در معاملات، به جای جابجایی ریال، رمزدارایی جابجا می‌شود.

۲ .۱ .۵ هک‌ها[3] و ریسک‌های امنیتی[4]

سرقت بزرگترین محرک جرایم رمزدارایی‌هاست. این شامل طیف گسترده‌ای از تخلفات است، از هک و سوءاستفاده گرفته تا سرقت. در مجموع، مطابق بررسی Crystal Blockchain از سال ۲۰۱۱ تا انتهای سال ۲۰۱۹، نزدیک به ۱۵/۵ میلیارد دلار رمزدارایی به روش‌های مختلف مورد سرقت قرار گرفته است (CoinTelegraph, 2019). از سال ۲۰۲۰ تاکنون (حدود ۵ سال) به طور متوسط سالانه مبلغ ۲/۵ میلیارد دلار سرقت رمزدارایی انجام شده که در صورت جمع همه این مبالغ، به عدد باورنکردنی ۲۳ میلیارد دلار می‌رسیم. (TRM Labs, 2023)

هک‌ها را می‌توان به دو دسته حملات قراردادهای هوشمند و حملات زیرساختی تقسیم کرد. گروه اول شامل سوءاستفاده از کد و حملات پروتکلی است؛ در حالی که گروه دوم شامل سرقت کلیدهای خصوصی و تعویض سیم‌کارت، در میان موارد دیگر است. سال ۲۰۲۲ بزرگترین سال ثبت شده برای هک‌ها و سوءاستفاده‌های رمزدارایی‌ها بود و حدود ۳,۷ میلیارد دلار در بیش از ۱۷۵ حادثه به سرقت رفت، یعنی به صورت میانگین هر هک بیش از ۲۰ میلیون دلار در هر حادثه. نزدیک به ۹۰ درصد از ۳,۷ میلیارد دلار سرقت شده در این سال از طریق

---

[1] Privacy Coins

[2] Tax Evasion

[3] Hacks

[4] Cybersecurity

حملات زیرساختی و سوءاستفاده از باگ‌های داخل کد انجام شد. رایج‌ترین نوع حمله در سال ۲۰۲۲، سوءاستفاده از باگ‌های داخل کد بود که ۵۷ حادثه را شامل می‌شد. در سال ۲۰۲۳ مجموع میزان مبالغ هک شده با حدود ۳۰ درصد کاهش، به رقم ۱/۸ میلیارد دلار رسید. (TRM Labs, 2023)

حملات علیه پروژه‌های DeFi (مالی غیرمتمرکز) در سال ۲۰۲۲ نسبت به حملات علیه اهداف CeFi (مالی متمرکز) بیشتر و مخرب‌تر بودند، به‌طوری که تقریباً ۸۰٪ از تمام وجوه سرقت شده، معادل ۳ میلیارد دلار، شامل قربانیان DeFi بود و ۹ مورد از ۱۰ حمله بزرگ به پروژه‌های DeFi رخ داد. (TRM Labs, 2023)

۱.۵.۱.۲ حملات قراردادهای هوشمند[1]

قراردادهای هوشمند برنامه‌های کامپیوتری با قابلیت اجرای خودکار هستند که در بلاکچین ذخیره شده و برای اتوماسیون اجرای تراکنش‌ها استفاده می‌شوند. در حملات قراردادهای هوشمند، هکرها به دنبال بهره‌برداری از اشکالات یا آسیب‌پذیری‌های این قراردادها هستند تا رمزدارایی‌ها را مورد سرقت قرار دهند، داده‌ها را دستکاری کنند یا عملکرد سرویس را مختل نمایند. (TRM Labs, 2023)

- سوءاستفاده از کد[2]

در این روش به کد قرارداد هوشمند پروژه حمله می‌شود و به مهاجم اجازه می‌دهد بدون مجوز وجوه را از پروتکل‌های DeFi خارج کند. این نوع سوءاستفاده‌ها به دلیل اشتباهات و خطاهای کدنویسی تسهیل می‌شوند، مانند ارتباط با ابزارهای شخص ثالث کنترل‌نشده، مشکلات کنترل دسترسی و اشکالات منطقی. از مجموع ۱,۴ میلیارد دلار سرقت شده از طریق سوءاستفاده از کد در سال ۲۰۲۲، حدود ۹۰٪ به دلیل مشکلات احراز هویت، اعتبارسنجی نادرست و مشکلات تأیید امضا بوده است. در فوریه ۲۰۲۲، پل Wormhole متعلق به سولانا هدف حمله‌ای قرار گرفت که منجر به سرقت بیش از ۳۰۰ میلیون دلار از پروتکل DeFi شد. (Kolakowski, 2022)

- حملات پروتکل[3]

حملات پروتکل نقاط ضعف موجود در پروتکل اصلی یا منطق تجاری یک سیستم ارائه‌دهنده خدمات رمزدارایی را هدف قرار می‌دهند. اگرچه این نوع حملات یکی از رایج‌ترین انواع حملات در سال ۲۰۲۲ بود، اما میانگین آسیب وارد شده توسط هر حمله‌ی پروتکل نصف سایر هک‌ها بود. در اکتبر ۲۰۲۲، پروژه Sovryn، که گفته می‌شود اولین پروتکل DeFi بر روی بیت‌کوین است، هدف حمله قرار گرفت که منجر به از دست رفتن تقریبی ۱ میلیون دلار شد. در این حمله، هکر از یک آسیب‌پذیری در قیمت‌گذاری سوءاستفاده کرد و یک وام فوری اجرا کرد. (TRM Labs, 2023)

[1] Smart Contract Attacks

[2] Code Exploits

[3] Protocol Attacks

۲.۵.۱.۲ *حملات زیرساختی*[1]

حملات زیرساختی سیستم‌ها، پلتفرم‌ها یا خدماتی را که از ایجاد، تبادل یا ذخیره رمزدارایی‌ها پشتیبانی می‌کنند، هدف قرار می‌دهند. این نوع حملات معمولاً با استفاده از حملات سایبری سنتی یا سوءاستفاده‌ها انجام می‌شوند. تکنیک‌ها شامل سرقت کلید خصوصی یا عبارت بازیابی و تعویض سیم‌کارت هستند. (TRM Labs, 2023)

- سرقت کلید خصوصی[2]

مخرب‌ترین نوع حملات زیرساختی، سرقت کلید خصوصی یا عبارت بازیابی است که به مهاجم اجازه می‌دهد کنترل کیف پول قربانی را به دست گیرد و آن را خالی کند. سرقت کلید خصوصی یا عبارت بازیابی در سال ۲۰۲۲ حدود ۱٫۵ میلیارد دلار از وجوه دزدیده شده، یعنی ۸۵ درصد از کل حملات زیرساختی، را شامل می‌شد. سایر انواع حملات زیرساختی مانند حملات جلویی و دستکاری DNS، حدود ۲۵۰ میلیون دلار از وجوه دزدیده شده را در سال ۲۰۲۲ به خود اختصاص دادند. در مارس ۲۰۲۲، پل Ronin مورد حمله قرار گرفت که منجر به از دست رفتن بیش از ۶۰۰ میلیون دلار شد. (Tidy, 2022)

- تعویض سیم‌کارت[3]

تعویض سیم‌کارت شامل ربودن شماره تلفن قربانی برای احراز هویت جعلی و انتقال وجوه از حساب او است. در سال ۲۰۲۲، یک مرد اهل فلوریدا به دلیل حمله تعویض سیم‌کارت در سال ۲۰۱۸ به ۱۸ ماه زندان محکوم شد. این حمله به همدستان او اجازه داد تا شماره تلفن قربانی را سرقت کرده و بیش از ۲۳ میلیون دلار ارز دیجیتال را به صورت جعلی از کیف پول او منتقل کنند. (U.S. Attorney's Office, 2022)

۶.۱.۲ ریسک‌های مرتبط با ارائه‌دهندگان خدمات رمزدارایی[4]

حدود ۱۵ الی ۱۹ میلیون نفر ایرانی در بازار رمزدارایی فعال هستند که حدود ۱۰ الی ۱۲ میلیون نفر از آنها از خدمات پلتفرم‌های ارائه‌دهنده خدمات رمزدارایی (VASP) یا همان صرافی‌های متمرکز ایرانی استفاده می‌کنند و باقی افراد یا از صرافی‌های متمرکز خارجی و یا از صرافی‌های غیرمتمرکز استفاده می‌نمایند. (Okoth, 2024)

نکته قابل‌توجه این است که بیشترین میزان گردش مالی و در عین حال کمترین میزان شکایات قانونی در فضای رمزدارایی‌ها، مربوط به همین پلتفرم‌های ارائه‌دهنده خدمات رمزدارایی است. دلیل استقبال بیشتر مردم از پلتفرم‌های متمرکز، سادگی کاربری، کارمزد پایین و از همه مهم‌تر ارائه خدمات «حضانت دارایی»[5] است که باعث می‌شود کاربران با کمترین میزان دانش از فضای رمزدارایی و بلاکچین، دیگر درگیر ساخت کیف‌پول و نگرانی‌های مربوط به از دست دادن پول خود نمی‌شوند.

---

[1] Infrastructure Attacks

[2] Private Key Theft

[3] SIM Swapping

[4] Virtual-Assets Service Provider (VASP)

[5] Custody

مشکل اصلی دقیقاً از همین‌جا آغاز می‌شود که شرکت‌های ارائه‌دهنده خدمات رمزدارایی، علاوه بر ارائه خدمت معاملات رمزدارایی، خدمات دیگری از جمله انتقال پول، حضانت دارایی، استیکینگ[1]، سبدگردانی و را هم انجام می‌دهند و نظام مالی کشور را درگیر ریسک‌های متعددی می‌نمایند. بخشی از ریسک‌ها عبارت‌اند از:

۱.۶.۱.۲ *عدم رعایت اصل امانت‌داری توسط ارائه‌دهندگان خدمات رمزدارایی*

در صرافی‌های رمزارزیِ متمرکز، کاربران علاوه بر مبادله رمزدارایی‌های خود، می‌توانند موجودیِ رمزدارایی و موجودی ریالی خود را در داخل صرافی نگهداری نمایند (صرافی نقش «امین دارایی» را نیز پیدا می‌کند). اغلب افراد به علت عدم آگاهی کافی از خطرات آن، همین کار را می‌کنند و رمزدارایی‌های خود را به کیف پول شخصی منتقل نمی‌نمایند که این امر باعث ایجاد ریسک‌های متعددی می‌شود.

یکی از این ریسک‌ها عدم رعایت اصل امانت‌داری توسط ارائه‌دهندگان خدمات رمزدارایی است. زیرا به مرور این مبالغ زیاد شده و صاحبان صرافی‌ها را به فکر استفاده از رمزدارایی‌های کاربران در بازارهای موازی و یا حتی مصرف آنها در شبکه‌های قمار می‌اندازد. در این مدت، ارائه‌دهنده خدمات به نوعی «خالی فروشی» انجام می‌دهد. به عنوان مثال صرافی QuadrigaCX که در سال‌های ۲۰۱۶ تا ۲۰۱۸، بزرگترین کارگزار مبادله رمزدارایی در کانادا بود، مبلغ ۲۵۰ میلیون دلار از دارایی‌های کاربران خود را وارد قمار نموده بود. (OSC, 2020)

۲.۶.۱.۲ *پلمب شدن یا ورشکستگی ارائه‌دهندگان خدمات رمزدارایی*

به دلایل مختلف این امکان وجود دارد که یک ارائه‌دهنده خدمات رمزدارایی ورشکسته شود یا توسط نهادهای قضایی و انتظامی، تعطیل و پلمب گردد. در چنین شرایطی اگر از قبل، راهکارهای جایگزین برای عودت مال به کاربران صرافی برنامه‌ریزی نشده باشد، با توجه به نوسانات شدید بازار رمزدارایی، امکان رسیدن ضررهای بسیار بزرگ به کاربران وجود دارد. بنابراین باید تمهیداتی جهت حفاظت از حقوق مصرف‌کنندگان تدوین و اجرایی شود.

این اتفاق در ایران با «صرافی کریپتولند[2]» رخ داد. این صرافی که در سال ۲۰۱۷ کار خود را آغاز نموده بود، خیلی سریع تعداد کاربران خود را افزایش داد. در سال ۲۰۱۹ توکن بومی صرافی خود با نام «بریج[3]» را ایجاد و منتشر نمود و کلاهبرداری به شیوه مورد اشاره در بند ۳ـ۲ـ۱ـ۲ را انجام داد. در سال ۲۰۲۱ فعالیت این پلتفرم توسط مراجع قضایی متوقف و اموال آن (اموال مردم) بلوکه شد و تا مدت‌ها مردم نتوانستند به سرمایه‌های خود دست پیدا کنند. (مناجاتی‌پور، ۱۴۰۲)

۳.۶.۱.۲ *فرار صاحبان ارائه‌دهندگان خدمات رمزدارایی*

یکی دیگر از خطرات، فرار صاحبان کارگزاران مبادله رمزدارایی از کشور است. رمزدارایی‌ها به دلیل ماهیت دیجیتالی خود، امکان جابجایی سریع و آسانی را دارند و طی کمتر از یک دقیقه می‌توان بدون دخالت هیچ واسطه‌ای، موجودی کیف پول را به هر کجای دنیا منتقل کرد، یا اینکه در کیف پول صاحبان صرافی، با فرار ایشان، از کشور خارج شود. از آنجا که مبالغ حضانت شده توسط صرافی‌ها، می‌تواند چندین هزار میلیارد تومان باشد، در فضای بدون نهاد

---

[1] Staking

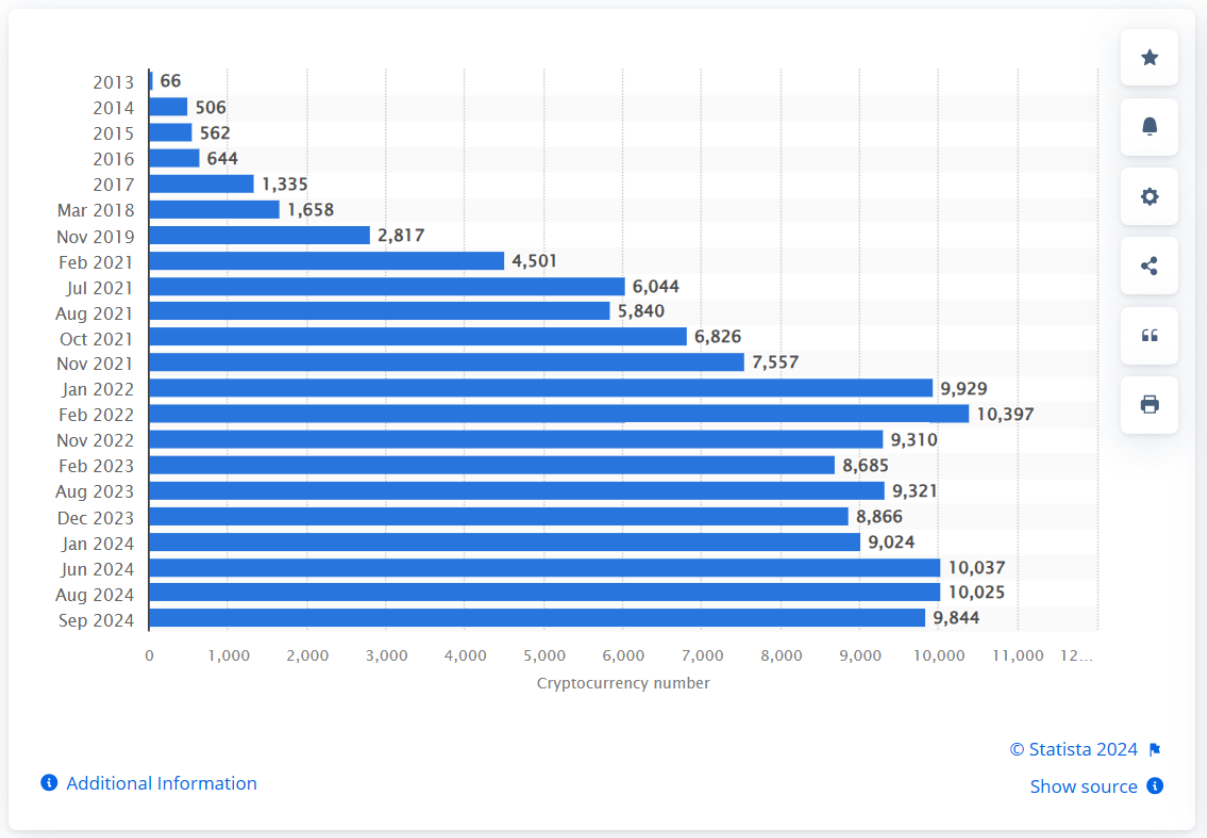
[2] Cryptoland

[3] Bridge (BRG)

تنظیم‌گر، ریسک فرار آنها بسیار بالاست. به عنوان مثال در سال ۲۰۲۱ بنیانگذار صرافی ترکیه‌ای تودکس[1] با بیش از ۳۹۱ هزار کاربر و با ۲ میلیارد دلار سرمایه‌ی کاربران، از این کشور فرار کرد.

۴.۶.۱.۲ لیست کردن رمزدارایی‌های بی‌ارزش[2]

تا انتهای سپتامبر ۲۰۲۴ حدود ۱۰ هزار رمزارز قابل معامله در صرافی‌های دنیا وجود دارد. مرجعی برای نمایش تعداد کل NFTها در بازارهای مختلف وجود ندارد ولی تعدادشان اگر بیشتر از تعداد رمزارزها نباشد، کمتر نیست. بسیاری از این رمزدارایی‌ها فقط برای کلاهبرداری ساخته شده‌اند، نه توکنومیکس درستی دارند و نه تیم متخصص و مطرحی روی آنها کار می‌کند. اگر ارائه‌دهندگان خدمات رمزدارایی دقت لازم را در لیست کردن رمزدارایی نداشته باشند و صرفاً براساس ترندهای روز، موارد نامناسب را به فهرست رمزدارایی‌های قابل معامله خود اضافه نمایند، کاربران خود را در معرض خطر قرار می‌دهند. (Statista, 2024)



شکل ۴ . نمودار میله‌ای تعداد رمزارزهای قابل معامله در صرافی‌های دنیا از سال ۲۰۱۳ تا انتهای سپتامبر ۲۰۲۴

[1] Thodex

[2] Shitcoin

۲ .۱ .۶. ۵ ارائه تسهیلات با توثیق رمزدارایی کاربران

چند سالی است در دنیا خدمات وام‌دهی و ارائه تسهیلات با توثیق رمزدارایی توسط VASPها انجام می‌شود. اخیراً در ایران نیز ارائه‌دهندگان خدمات رمزدارایی و برخی پلتفرم‌های همکار آنها از جمله «ونسی» این خدمت را به لیست خدمات خود اضافه نموده‌اند و بدون مجوز بانک مرکزی ج.ا.ا، با دریافت توثیق رمزدارایی، وام و تسهیلات ارائه می‌دهند. (حاتمی، ۱۴۰۳)

با توجه به ماهیت پر نوسان رمزدارایی‌ها، این موضوع ریسک بالایی را برای کاربران و نیز نظام پولی و بانکی کشور ایجاد می‌نماید. مثلاً در سال ۲۰۲۲، یکی از بزرگترین پلتفرم‌های وام‌دهی رمزدارایی در آمریکا به نام سلسیوس[1] با مشکلات مالی روبرو شد و توانایی بازپرداخت وام‌های خود را از دست داد، که باعث زیان‌های گسترده برای وام‌گیرندگان و سرمایه‌گذاران شد (Roush, 2022).

۲ .۱ .۶. ۶ خدمات بازارهای دوطرفه با ضرایب بالا مانند بازارهای آتی[2]

در این‌گونه معاملات، در واقع رمزدارایی معامله نمی‌شود، بلکه کاربران قراردادهای پیش‌بینی خود از صعودی یا نزولی بودن بازار را با ضرایب ۲x تا ۱۰۰ x با دیگران خریدوفروش می‌نمایند. این مدل بازارها، جدا از ایرادات فقهی، می‌توانند به راحتی باعث از دست رفتن کل سرمایه کاربران شوند. مثلاً زمانی که کاربر اهرم[3] ۱۰۰x می‌گذارد، کافی است بازار فقط به اندازه یک درصد برخلاف جهت مورد نظر وی حرکت نماید تا سرمایه استفاده شده در این معامله به طور کامل از دست برود یا اصطلاحاً لیکوئید[4] شود.

۲ .۱ .۶. ۷ نحوه نگهداری از رمزدارایی کاربران در کیف‌پول‌های گرم و سرد

با توجه به مبالغ هنگفتی که ارائه‌دهندگان خدمات رمزدارایی که نزد VASPها به امانت است، نحوه نگهداری نامناسب آنها می‌تواند بسیار خطرآفرین باشد. مثلاً برخی از آنها ممکن است کیف‌پول سرد[5] (کیف‌پول سخت‌افزاری) نداشته باشند و فقط از کیف‌پول گرم[6] استفاده کنند که ریسک هک شدن و سرقت رمزدارایی‌ها بسیار بالا می‌رود. برخی دیگر امکان دارد کیف‌پول اصلی خود را چند امضایی کرده باشند.

۲.۲ ریسک‌های اختصاصی ایران

با توجه به شرایط خاص حاکم بر سیاست و اقتصاد ایران، علاوه بر ریسک‌های مشترک با سایر کشورهای جهان در حوزه رمزدارایی‌ها ریسک‌های دیگری نیز وجود دارد که برخی از آنها به مراتب خطرناک‌تر از ریسک‌هایی ذکر شده تا اینجاست.

---

[1] Celsius

[2] Futures

[3] Leverage

[4] Liquid

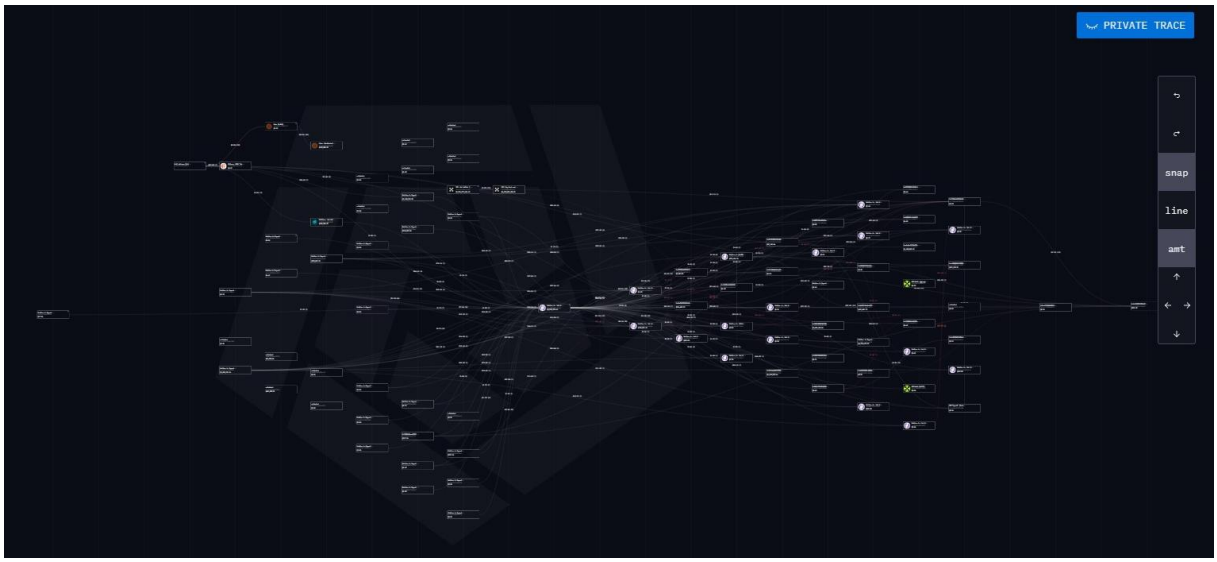
[5] Cold Wallet

[6] Hot Wallet

۱.۲.۲ ریسک‌های ناشی از فضای سیاسی ایران

۱.۱.۲.۲ رصد شدن آدرس کیف‌پول رمزدارایی‌های صرافی‌های ایرانی

با توجه به شرایط خاص کشور در برهه کنونی از یک سو و تعداد چند میلیونیِ کاربران صرافی‌های داخلی از سوی دیگر، ریسک قفل‌شدن[1] رمزدارایی‌های کاربران در کیف‌پول‌های ایشان به دلیل تگ خوردن آدرس کیف‌پول‌های صرافی‌ها وجود دارد. امروزه ابزارهای رصد بسیار پیشرفته‌ای برای تراکنش‌های رمزارزی روی بستر بلاکچین‌های مختلف وجود دارد که به دنبال شناسایی تراکنش‌ها در دنیا به خصوص موارد مربوط به صرافی‌ها هستند. پلتفرم‌های آرکام[2] و TRM Labs شرکت‌های تحلیل داده‌های بلاکچین هستند که بسیاری از آدرس‌های کیف‌پول پرمخاطب‌ترین صرافی ایرانی یعنی نوبیتکس با بیش از ۶ میلیون کاربر فعال ماهانه را شناسایی و برچسب‌گذاری کرده‌اند. (Okoth, 2024)



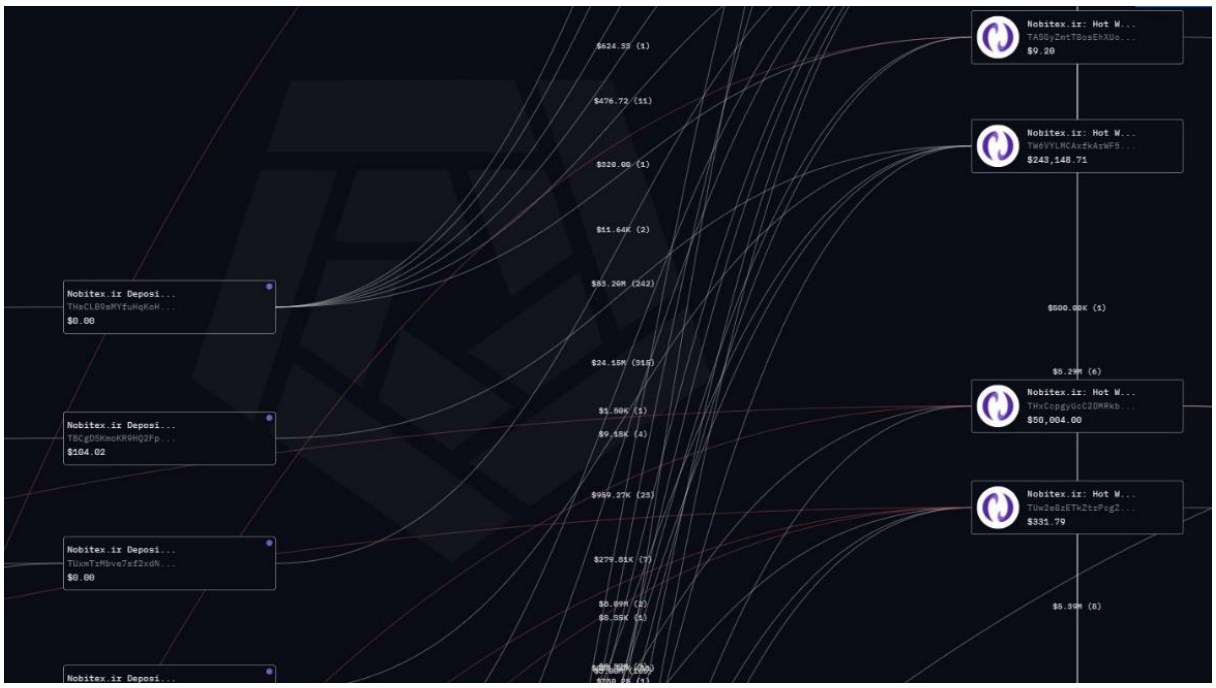
شکل ۵. نمونه‌ای از ردیابی تراکنش‌ها تا چندین مرحله قبل در نرم‌افزار آرکام، به لطف شفافیت تراکنش‌ها در بلاکچین

در ماه می ۲۰۲۴، دو سناتور برجسته آمریکایی در نامه‌ای به وزیر دفاع، وزیر خزانه‌داری و مشاور امنیت ملی، نگرانی‌های خود را در مورد دست داشتن احتمالی نوبیتکس در فعالیت‌هایی که می‌تواند پول‌شویی و تأمین مالی تروریسم برای دولت ایران را تسهیل کند، ابراز کردند. با توجه به این‌که سازمان‌هایی مانند بنیاد تتر[3] و سایر صادرکنندگان رمزارزهای بدون نوسان متمرکز بایستی مطابق با قوانین دفتر کنترل دارایی‌های خارجی وزارت

[1] Freezing
[2] Arkham
[3] Tether (USDT)

خزانه‌داری ایالات‌متحده (OFAC) عمل نمایند، ممکن است این سازمان‌ها رمزدارایی‌های کاربران را مسدود نمایند. (Okoth, 2024)

بنابراین وقتی کیف پول یک صرافی ایرانی تگ می‌خورد و شناسایی می‌شود، ریسک قفل شدن رمزدارایی‌های کاربران بسیار بالا می‌رود، به طوری که یا امکان خروج رمزدارایی از کیف‌پول برای همیشه بسته می‌شود (به عنوان مثال برای رمزارز تتر) و یا اینکه رمزداراییِ مذکور توسط هیچ کارگزار مبادله رمزداراییِ خارجی دریافت نمی‌شود. بدتر از آن اینکه کاربران صرافی‌های ایرانیِ تگ خورده پس از انتقال وجه از این صرافی به کیف‌پول‌ها و صرافی‌های بین‌المللی، با محدودیت حساب‌ها و کیف‌پول‌های خود مواجه شده و دارایی‌های دیگرشان نیز به خطر می‌افتد.



شکل ۶. نمونه‌ای از ردیابی تراکنش‌های ورودی و خروجی صرافی نوبیتکس در نرم‌افزار آرکام

۲.۱.۲.۲ *خروج سرمایه‌ها از کشور*

در شرایطی که هم کیفیت خدمات کارگزاران مبادله رمزداراییِ داخلی، پایین‌تر از رقبای خارجی آنهاست، هم ریسک ذکر شده در بند قبل، کاربر صرافی ایرانی را تهدید می‌کند، وی با مشاهده این‌که هیچ قانون و نهادی هم از حقوق وی در این شرایط حفاظت نمی‌کند، تصمیم به استفاده از خدمات صرافی‌های خارجی گرفته و سرمایه خود را به آن‌جا منتقل می‌کند. از آنجاکه به‌خاطر شرایط سیاسی کشور، ایرانیان در پلتفرم‌های معتبر خارجی امکان احراز هویت ندارند، سرمایه‌های خود را به صرافی‌های ناشناخته یا کمتر شناخته شده منتقل می‌نمایند و با این کار میزان بسیار زیادی از سرمایه‌های کشور در معرض خطر جدی قرار می‌گیرد.

۲.۲.۲ ریسک‌های ناشی از فضای اقتصادی ایران

۲.۲.۲.۱ اختلال در بازار ارز

بازار رمزدارایی‌های با ارزش ثابت که به نوعی جایگزین دلار شده‌اند (مانند تتر که هر واحد آن همواره معادل یک دلار است)، می‌تواند به بازار ارز کشور جهت دهد و باعث نوسانات شدید نرخ ارز شود. مثلاً در نیمه‌شب ۱۳ آوریل ۲۰۲۴، زمانی که بازار ارز تعطیل بود، با توجه به ۲۴*۷ بودن بازار رمزدارایی‌ها و نیز نبود سقف مجاز برای میزان در اختیار داشتن تتر، قیمت تتر به شدت افزایش یافت از حدود ۶۵ هزار تومان، به ۷۲ هزار تومان رسید.

۲.۲.۲.۲ حساب‌های اجاره‌ای

یکی از مهم‌ترین اقدامات ضد پول‌شویی که ارائه‌دهندگان خدمات رمزدارایی بایستی در زمان ثبت‌نام کاربران انجام دهند، «احراز هویت»[1] کامل آنهاست که خوشبختانه طی سال‌های اخیر به خوبی انجام می‌شود. با این وجود گروه‌های کلاهبردار، از وضعیت اقتصادی ضعیف مردم سوءاستفاده کرده و با پرداخت مبالغ ناچیز به افرادی که در پلتفرم‌های VASP، احراز هویت نموده و حساب کاربری خود را به آنها اجاره دهند، اقدام به پول‌شویی با حساب این افراد می‌نمایند. این امر به قدری معمول شده که به وفور در شبکه‌های اجتماعی و سایت‌های آگهی مانند دیوار و شیپور، تحت عنوان «کار در منزل» یا مشابه آن، آگهی می‌شود.

۳ جمع‌بندی و نتیجه‌گیری

همان‌طور که ملاحظه شد، بیش از ۳۵ ریسک در دسته‌بندی‌های مختلف در حوزه رمزدارایی‌ها وجود دارد. برای رسیدن به جمع‌بندی و راهکار مناسب جهت تنظیم‌گری و کاهش ریسک‌های مذکور در ایران، در جدول زیر نوع برخورد کشورهای پیشرو با انواع ریسک‌های رمزدارایی‌ها مشخص شده است (به جز دسته ریسک‌های اختصاصی ایران و نیز ریسک‌های ذاتی که اصولاً فقط خود کاربران مسئول کسب دانش جهت کاهش این ریسک‌ها هستند).

[1] Know Your Customer (KYC)

جدول ۱

نهادها و مراکز متولی تنظیم‌گری رمزدارایی‌ها در کشورهای پیشرو

	ریسک‌های کلاهبرداری‌ها و تقلب‌ها	ریسک‌های پرداخت‌های غیرقانونی	ریسک‌های نظام مالی و پولی	ریسک‌های امنیت سایبری	ریسک‌های مرتبط با VASPها
ایالات‌م تحده آمریکا	کمیسیون معاملات آتی کالا (CFTC) و کمیسیون بورس و اوراق بهادار (SEC)	شبکه اجرای جرایم مالی (FinCEN)	FinCEN و دفتر کنترل دارایی‌های خارجی (OFAC)	وزارت امنیت داخلی (DHS) و آژانس امنیت سایبری (CISA)	FinCEN و SEC، نهاد خودتنظیم‌گر: انجمن کالاهای مجازی (VCA)
ژاپن	آژانس خدمات مالی ژاپن (FSA) و نهاد خودتنظیم‌گر: انجمن صرافی ارزهای مجازی ژاپن (JVCEA)	FSA و نهاد خودتنظیم‌گر JVCEA	FSA و نهاد خودتنظیم‌گر JVCEA	آژانس ملی پلیس (NPA) و FSA	نهاد خودتنظیم‌گر JVCEA
انگلستا ن	سازمان رفتار مالی(FCA)	FCA و خزانه‌داری انگلستان	FCA	مرکز ملی امنیت سایبری (NCSC)	FCA
سوئیس	اداره نظارت بر بازار مالی سوئیس (FINMA) و نهاد خودتنظیم‌گر: انجمن استانداردهای خدمات مالی (VQF)	FINMA و نهاد خودتنظیم‌گر VQF	FINMA و نهاد خودتنظیم‌گر VQF	مرکز ملی امنیت سایبری (NCSC)	FINMA و نهاد خودتنظیم‌گر VQF
کره جنوبی	کمیسیون خدمات مالی (FSC) و نهاد خودتنظیم‌گر: انجمن بلاک‌چین کره (KBA)	FSC و مرکز تحلیل مالی	FSC و نهاد خودتنظیم‌گر KBA	آژانس امنیت اینترنت کره (KISA)	FSC و نهاد خودتنظیم‌گر KBA
امارات متحده عربی	سازمان اوراق بهادار و کالاهای امارات (SCA)	مرکز اطلاعات مالی امارات (FIU)	مرکز اطلاعات مالی امارات (FIU)	سازمان تنظیم مقررات ارتباطات و امنیت دیجیتال (TRA)	SCA و نهاد خودتنظیم‌گر: مرکز خدمات مالی دبی (DFSA)

یادداشت. برگرفته از (complyadvantage.com, 2024)

همان‌طور که در جدول ۱ مشخص است، در بسیاری از کشورهای پیشرو، نهادهای مختلفی متولی تنظیم‌گری و تلاش برای کاهش خطرات هر دسته از این ریسک‌ها شده‌اند. در ایالات‌متحده آمریکا و امارات متحده عربی که قطب‌های صنعت بلاکچین و رمزدارایی هستند، نهادهای کاملاً تخصصی مرتبط با موضوع هر ریسک، متولی تنظیم‌گری آن موضوع خاص هستند. در سایر کشورها نیز نهادها و مراکز تخصصیِ مالی مسئول تنظیم‌گری هستند.

در ایران نیز طبق قانون جدید بانک مرکزی، مصوب مجلس شورای اسلامی و مورخ ۷ خرداد ۱۴۰۳، بانک مرکزی ج.ا.ا متولی تنظیم‌گری حوزه «رمزپول» شده است. قانون‌گذار در بند (ض) مادهٔ ۱ قانون جدید بانک مرکزی، «رمزپول» را این‌گونه تعریف کرده است: «رمزپول نوعی پول رقومی (دیجیتال) رمزنگاری شده است که در بستر پایگاه داده اشتراکی به صورت متمرکز (با محوریت بانک مرکزی) یا غیرمتمرکز ایجاد و به صورت غیرمتمرکز مبادله می‌شود». از آنجا که رمزدارایی‌ها به صورت همزمان، هم وجهه دارایی دارند و هم وجهه پولی (به عنوان ابزار پرداخت استفاده می‌شوند)، می‌توان همه انواع رمزدارایی را به عنوان «رمزپول» شناسایی کرد و بدین ترتیب بانک مرکزی ج.ا.ا را به عنوان نهاد تنظیم‌گر آنها در نظر گرفت.

با دقت در گستردگی انواع ریسک‌های شناسایی شده در این مقاله و میزان خطرات آنها و نیز با در نظر گرفتن رویکرد کشورهای پیشرو در تنظیم‌گری رمزدارایی‌ها، می‌توان به این جمع‌بندی رسید که برای پوشش کامل و همه‌جانبه این ریسک‌ها، نمی‌توان تنظیم‌گری کل این حوزه را به یک نهاد خاص سپرد و از آن به بعد، به ازای کشف هر فعالیت

غیرقانونی، آن نهاد را متهم به اهمال و ترک وظایف نمود. مثلاً بخش بسیار مهم و بزرگی از ریسک‌ها مربوط به رمزدارایی‌هایی است که صرفاً با هدف خالی‌فروشی یا کلاهبرداریِ خروج از بازار «Rugpull» منتشر، عرضه و در شبکه‌های اجتماعی و سایر رسانه‌ها تبلیغ می‌شوند. تنظیم‌گری چنین مواردی اساساً در حیطه فعالیت بانک مرکزی نیست، با این وجود در قوه قضاییه به دلیل حجم بالای پرونده‌ها و مبالغ کلان این نوع از کلاهبرداری، بسیار مورد توجه بوده و بانک مرکزی را متولی تنظیم‌گری آن می‌دانند.

دیگر ریسک پراهمیت و کلان که نیاز به تنظیم‌گری ظریف و ماهرانه دارد، به ارائه‌دهندگان خدمات رمزدارایی برمی‌گردد، چرا که بیش از ۱۰ میلیون نفر با سرمایه‌های خود در پلتفرم‌های ارائه‌دهندگان خدمات رمزدارایی فعال هستند. از آن جهت گفته می‌شود نیاز به تنظیم‌گری ظریف و ماهرانه دارد که اگر تنظیم‌گری سخت‌گیرانه، شدید، غیر اصولی و ناهماهنگ با نیازهای مردم و کسب‌وکارها باشد، کاربران سرمایه خود را یا به پلتفرم‌های خارجی منتقل می‌نمایند و یا به بازارهای زیرزمینی و غیرشفاف. از سوی دیگر تنظیم‌گری سهل‌گیرانه می‌تواند ریسک‌ها و مسئولیت‌های حقوقی فراوانی برای بانک مرکزی ج.ا.ا داشته باشد. در اغلب کشورهای پیشرو در تنظیم‌گری رمزدارایی‌ها مطابق جدول ۱، نهادهای متولی درباره ریسک‌های مرتبط با VASPها، از کمک سازمان‌های خودتنظیم‌گر (SRO) استفاده می‌نمایند. در ژاپن این مسئولیت به طور مستقیم بر عهده SRO است.

جمع‌بندی آخر آن‌که به نظر می‌رسد نهاد تنظیم‌گر باید هر چه سریع‌تر برای حساس‌ترین ریسک حال حاضر فضای رمزدارایی‌ها در ایران یعنی رصد شدن آدرس کیف‌پول ارائه‌دهندگان خدمات رمزدارایی و ریسک قفل شدن دارایی‌های کاربران آنها وجود دارد، به فکر راه‌حلی مناسب باشد، به خصوص آن‌که به دلیل ملاحظات سیاسی، در صورت ورود مستقیم خود بانک مرکزی ج.ا.ا به تنظیم‌گری این حوزه، امکان افزایش ریسک وجود دارد.

۴ پیشنهادهای کاربردی

تجربیات جهانی نشان داده است که تمرکز بر ایجاد چارچوب‌های قانونیِ شفاف و جامع و نظارت دقیق بر فعالیت‌های مرتبط با رمزدارایی‌ها می‌تواند اثرگذاری مطلوبی در کاهش ریسک‌های رمزدارایی‌ها داشته باشد.

برای کسب بهترین نتیجه پیشنهاد می‌گردد که نهاد قانون‌گذار تمام ریسک و مسئولیت را متوجه بانک مرکزی نکند و درباره هر ریسک، مراکز و نهادهای تخصصیِ مرتبط را درگیر نماید. در این صورت علاوه بر حمایت از مصرف‌کننده و حفظ یکپارچگی بازار، ریسک‌های بیشتری پوشش داده می‌شود و اکوسیستم پویا و نوآور در چارچوب استانداردهای مالی جهانی ایجاد خواهد شد.

همچنین پیشنهاد می‌شود در شرایط فعلی بانک مرکزی ج.ا.ا به عنوان تنها نهادی که قانون‌گذار وی را متولی تنظیم‌گری بازار رمزدارایی‌ها نموده است، همکاری و گفتگوهای نزدیکی با سایر مراکز و نهادهای دولتی، قضایی و انتظامی در زمینه تنظیم‌گری رمزدارایی‌ها داشته باشد.

با توجه به اینکه در اغلب کشورهای پیشرو در تنظیم‌گری رمزدارایی‌ها، بانک‌های مرکزی هیچ کدام از ایشان به صورت مستقیم وارد تنظیم‌گری رمزدارایی‌ها نشده‌اند و نیز با عنایت به محدودیت‌های سیاسی بانک مرکزی ج.ا.ا و در نظر گرفتن این مهم که رمزدارایی‌ها، استفاده بین‌المللی دارند و توسط نهادهای بین‌المللی نیز نظارت می‌شوند،

پیشنهاد می‌شود فرایند تنظیم‌گری و نظارت توسط سازمان‌های تخصصیِ زیرمجموعه بانک مرکزی ج.ا.ا و با استفاده از کمک نهادهای خودتنظیم‌گر انجام پذیرد.

آخرین پیشنهاد که اهمیت آن کمتر از موارد قبل نیست، سرمایه‌گذاری نهاد تنظیم‌گر روی استارتاپ‌های رگ‌تک در حوزه رمزدارایی‌ها و نیز استفاده همزمان از ظرفیت فناوری‌های رگ‌تک بین‌المللی برای رصد و پایش تراکنش‌های پرخطر است.

فهرست منابع

اسماعیلی، ا. (۱۴۰۲). چطور سایت‌های کلاهبرداری استخراج ابری را شناسایی کنیم، میهن بلاکچین، https://mihanblockchain.com/how-trust-cloud-mining-websites

ایزک‌شیریان، ک. (۱۴۰۳). رأی پرونده «کینگ مانی» صادر شد. میهن بلاکچین، https://mihanblockchain.com/verdict-in-the-king-money-case-was-issued

حاتمی، ن. (۱۴۰۳). با پلتفرم‌های ایرانی که سرویس اعتباردهی رمزارز دارند، آشنا شوید، رسانه رمزارز، https://ramzarzmedia.com/8zcc

راه پرداخت (۱۴۰۳). درباره ماجرای حمله سایبری به بانک‌های ایران چه می‌دانیم؟ نگاهی به گزارش پولیتیکو اروپا، راه پرداخت، https://way2pay.ir/377035

علی‌پور، م. (۱۴۰۳). «خانه رمزارز ایران» پلمب شد، زومیت، https://www.zoomit.ir/tech-iran/423889-sealing-illegal-digital-currency-center-in-iran/

علی‌یاری، م. (۱۴۰۲). هشدار انجمن بلاکچین ایران: پروژه «کربلا کوین» کلاهبرداری است، ارز دیجیتال، https://arzdigital.com/blog/karbala-coin-fraud

مناجاتی‌پور، س. (۱۴۰۲). فراز و نشیب پرونده صرافی کریپتولند، تجارت نیوز، https://tejaratnews.com/fa/tiny/news-899580

Congressional Research Service. (2023). Introduction to Cryptocurrency. Publisher: Congressional Research Service (CRS). https://sgp.fas.org/crs/misc/IF12405.pdf

Antonovici, A. (2024). How Crypto Tokenization Works in 2024. Publisher: TastyCrypto. https://www.tastycrypto.com/blog/crypto-tokenization-explained/

CompaniesMarketCap. (2024). Top Assets by Market Cap. Publisher: CompaniesMarketCap. https://companiesmarketcap.com/assets-by-market-cap/

TRM Labs. (2023). Illicit Crypto Ecosystem Report, A Comprehensive Guide to Illicit Finance Risks in Crypto. Publisher: TRM Labs. https://www.trmlabs.com/report

Chainalysis. (2024). Money Laundering and Cryptocurrency, Trends and new techniques for detection and investigation. Publisher: Chainalysis. https://www.chainalysis.com/blog/money-laundering-cryptocurrency/

Casino, F. (2019). Blockchain Mutability: Challenges and Proposed Solutions. Publisher: IEEE. https://ieeexplore.ieee.org/document/8883080

Weichbroth, P. (2023). Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. Publisher: MDPI. https://www.mdpi.com/1424-8220/23/6/3155

Scharfman, J. (2023). The Cryptocurrency and Digital Asset Fraud Casebook. Publisher: Palgrave Macmillan.

Akolkar, B. (2024). Ethereum Price Declines as Chinese Govt Offloads 7,000 ETH Seized from PlusToken Scam. Publisher: CoinGape. https://coingape.com/ethereum-price-drops-as-chinese-govt-sells-7000-eth-seized-from-plustoken-scam/

TRM Labs. (2022). On the Trail of the Squid Game Scammers. Publisher: TRM Labs. https://www.trmlabs.com/post/on-the-trail-of-the-squid-game-scammers

Kaaru, S. (2023). SafeMoon charged in $5.7 billion 'crypto' scam. Publisher: CoinGeek. https://coingeek.com/safemoon-charged-in-5-7-billion-crypto-scam

Alnasaa, M. (2022). Crypto, Corruption, and Capital Controls: CrossCountry Correlations. Publisher: International Monetary Fund (IMF).

Cohen, L. (2023). U.S. charges FTX's Bankman-Fried with paying $40 mln Chinese bribe. Publisher: Reuters. https://www.reuters.com/legal/ftxs-bankman-fried-charged-with-bribery-conspiracy-new-indictment-2023-03-28/

Sengupta, B. (2022). Iran executes 4 people accused of working with Israeli intelligence agencies. Publisher: RepublicWorld. https://www.republicworld.com/world-news/iran-executes-4-people-accused-of-working-with-israeli-intelligence-agencies-articleshow

Hu, M. (2019). Capital Flight: Evidence from the Bitcoin Blockchain. Publisher: Asia-Pacific Research Exchange. https://www.arx.cfa/~/media/480585B00971442D8E7ADD6FE94495F1.ashx

Johnson, M. (2023). What a Devalued Naira Means for the Nigerian Economy. Publisher: International Banker. https://internationalbanker.com/brokerage/what-a-devalued-naira-means-for-the-nigerian-economy/

Iacurci, G. (2021). Cryptocurrency poses a significant risk of tax evasion. Publisher: CNBC. https://www.cnbc.com/2021/05/31/cryptocurrency-poses-a-significant-risk-of-tax-evasion.html

CoinTelegraph. (2020). Reports on Crypto-Exchange Hacks. Publisher: CoinTelegraph. https://cointelegraph.com/magazine/crypto-exchange-hacks/

Kolakowski, M. (2022). Crypto Worth Over $320 Million Taken in Wormhole Hack. Publisher: Investopedia. https://www.investopedia.com/crypto-theft-of-usd320-million-wormhole-hack-5218062

Tidy, J. (2022). Ronin Network: What a $600m hack says about the state of crypto. Publisher: BBC. https://www.bbc.com/news/technology-60933174

U.S. Attorney's Office. (2022). Florida Man Sentenced To 18 Months for Theft of Over $20 Million In SIM Swap Scheme. Publisher: U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/florida-man-sentenced-18-months-theft-over-20-million-sim-swap-scheme

Okoth, C, J. (2024). U.S. sanctions lead to Iranians' frozen crypto assets in CEXs amid escalating global tensions. Publisher: Cryptopolitan. https://www.cryptopolitan.com/iranians-frozen-crypto-assets-in-cexs/

OSC. (2020). QuadrigaCX, Ontario Coat of Arms. Publisher: Ontario Securities Commission. https://www.osc.ca/quadrigacxreport

Statista. (2024). Number of cryptocurrencies worldwide from 2013 to September 2024. Publisher: Statista. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Roush, T. (2023). Celsius Network Ends Bankruptcy Case—Will Pay Back Customers Through New Company. Publisher: Forbes.

ComplyAdvantage. (2024). Cryptocurrency regulations around the world. Publisher: ComplyAdvantage. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

The Identification of Various Risks Associated with Cryptocurrencies in Iran and Solutions for Their Proper Regulation

Sadegh Saberi[1]

Abstract

This article examines and identifies various risks associated with crypto assets at both national and global levels. Crypto assets, which include cryptocurrencies and non-fungible tokens (NFTs), have emerged as one of the latest financial technologies in the past decade, presenting new opportunities and threats for investors, governments, and users. Given the high global market value of these assets and the rapid development of related technologies, significant risks such as fraud and scams, illegal payments, financial and monetary system risks, cybersecurity risks, and risks related to crypto-asset service providers (VASPs) are evident in this domain.

Another section of the article addresses the regulatory challenges of crypto assets at both the international and Iranian levels. While different countries have adopted various approaches to address these challenges, Iran, due to its specific economic and political conditions, faces unique risks. These risks include the possibility of tracking the wallet addresses of Iranian crypto service providers, market disruption, and the use of rented accounts.

Finally, by considering the type of regulation in leading countries, the article offers solutions to address the aforementioned risks. Key recommendations include specializing regulations for each category of risks, collaborating and consulting with other governmental, judicial, and law enforcement agencies, and utilizing the capabilities of self-regulation organization (SRO). These measures could help reduce negative impacts and increase the benefits of opportunities in the crypto asset field.

[1] The Former Director of Kuknos Blockchain Academy, Crypto-Assets Instructor and Consultant at The Tehran Chamber of Commerce. sadeghsaberi@gmail.com

Keywords: Cryptocurrency Regulation, Risks of Cryptocurrencies, Fraud, Money Laundering, Cryptocurrency Service Providers, Self-Regulation Organization

JEL Classification: K22, K24, G28, L86, O33