



ارزیابی امنیتی، قضایی و تحریم پیش نویس «ضوابط کارگزاران رمزپول»

خلاصه مدیریتی

پیش نویس فعلی، هم زمان در سه جبهه تحریم/ریسک های فرااختیاری، امنیت سایبری/عملیاتی و دادرسی/صلاحیت قضایی کاستی های بنیادین دارد:

- ریسک فریز/فلگ دارایی ها و **second-order sanctions** نادیده گرفته شده و هیچ سازوکار جبران (compensation) یا «قوه قاهره تحریمی» پیش بینی نشده است.
 - معماری تمرکز نگرنداری دارایی (Custody) نقاط تکین شکست (Single Points of Failure) ایجاد می کند و ریسک های «نفوذ درونی/زنجیره تأمین» را بالا می برد.
 - اختیارات شبه قضایی برای بانک (تعطیل/حذف دارایی/مجازات اداری) بدون دادرسی منصفانه، موجی از دعاوی و تعارض صلاحیت می سازد.
- نتیجه محتمل: افزایش شدید هزینه های اجتماعی/حقوقی، بی اعتمادی سیستمی، و انباشت پرونده ها در پلیس فتا و دادستانی. و مراجع جهانی

1) تحلیل تحریم و ریسک های فرااختیاری (Sanctions/OFAC Risk)

اشکالات کلیدی

- انتقال ریسک به کاربر و کارگزار: با وجود الزام به نهاد امین و تمرکز نگرنداری، پیش نویس هیچ تعهد جبرانی در صورت فریز برونزا (تحریم، blacklisting شرکت های خارجی، رهگیری vendor) مقرر نکرده است.
- عدم توجه به **Force Majeure** تحریمی: نه در متن مجوز، نه در رابطه امین-کارگزار-کاربر.
- **Delist** بدون معیار شفاف: حذف ناگهانی دارایی ها می تواند به عنوان «پذیرش ضمنی فشار تحریمی» تلقی شود و به اثر سرریز (spillover) روی سایر دارایی ها منجر گردد.
- وابستگی به کانال های بانکی داخلی: ریسک هم بستگی (correlated risk) در رخداد های تحریمی، امکان «قفل نقدینگی» را بالا می برد.

تبعات مستقیم

- فریز/فلگ ناگهانی دارایی کاربران و صف های برداشت؛
- دود شدن پوشش ریسک (هج) به دلیل حذف دارایی/تعطیل نماد؛
- مسئولیت ناپذیری نهادی: همه بار زیان بر دوش کاربر/کسب و کار.

iranblockchain.org

همراه: ۰۹۳۶۶۶۸۲۴۸۸

تلفکس: ۰۲۱ - ۹۱۳۰۰۰۷۷

نشانی: تهران، بزرگراه امیر

سرلشکر حسین لشگری،

پلاک ۳۱، ساختمان کارخانه نوآوری

کد پستی: ۱۳۹۱۹۵۵۴۱۶

info@iranblockchain.org

@iranblockchaincommunity

@iran_blockchain



توصیه‌های اصلاحی

۱. چارچوب **Delist** شفاف با حق اعتراض و «دوره تنفس» برای خروج منظم کاربر از دارایی‌های در معرض تحریم تنها پس از نظر کارشناسی بخش خصوصی متخصص و کارگروه علمی بخش خصوصی.
۲. تعیین **SLA** برداشت بحرانی و مسیرهای جایگزین تسویه در سناریو تحریم.
۳. ایجاد عدم تمرکز و واگذاری نگاه داری دارایی‌ها در هر صرافی به صورت مجزا با پروتکل‌های نگاه داری و سایبری

(2) ارزیابی امنیتی (Cyber/Operational Security)

اشکالات کلیدی

- تمرکز اجباری نگاه داری (مواد ۴۲-۴۵) → ایجاد «Honeypot» داده و دارایی؛ جذاب‌ترین هدف برای مهاجم بیرونی/داخلی.
- ابهام نقش‌ها بین امین/کارگزار (م ۴۵) → خلأ پاسخ‌گویی در رخداد امنیتی.
- عدم الزام به استانداردهای امنیتی مرجع (ISO 27001/ SOC2/ رمزنگاری HSM/ MPC Wallets/ Segregation سرد-گرم)

سناریوهای خطر

- نفوذ داخلی (Insider) در امین/کارگزار؛
- **Compromise** زنجیره تأمین (کتابخانه، کیف پول، امضای دیجیتال)؛
- باج‌افزار/حمله مهندسی اجتماعی به تیم‌های عملیاتی؛
- هم‌زمانی رخداد امنیتی با موج برداشت (Bank-run کریپتویی)

توصیه‌های اصلاحی

۱. الزام معماری تفکیک شده **Custody** (MPC یا HSM با **Threshold Signatures**) **Cold/Warm Segregation**، و **Two-person rule** برای عملیات کلیدی.
۲. گواهی‌نامه‌های امنیتی اجباری (ISO 27001/ SOC2) و **Red-Team** سالانه با گزارش به ناظر.
۳. جزءنگاری **SLA** امنیتی: زمان شناسایی، مهار، بازیابی، و گزارش‌دهی حادثه. (MTTD/MTTR)
۴. **Bounded Responsibility** تفکیک شفاف مسئولیت امنیتی امین و کارگزار در متن آیین‌نامه و قرارداد.



۳) ارزیابی قضایی/دادرسی و صلاحیتها

اشکالات کلیدی

- اختیارات شبه قضایی بانک (م ۵۷) بدون مرجع بی طرف → تعارض با اصول دادرسی منصفانه و احتمال ابطال در دیوان عدالت.
- Delist بدون فرآیند اعتراض (م ۴۷) → تضییع حقوق مالکیت و افزایش دعاوی.
- تناقض بار مسئولیت (م ۲۸ vs م ۳۳) → ابهام در تقصیر/تضمین و غیرممکن شدن جبران منصفانه.
- تداخل مقررات (اینماد/بانکی/بازار سرمایه) → بروز دعاوی صلاحیتی و افزایش ارجاعات.

پیامدهای قضایی

- انفجار پرونده‌ها در پلیس فتا و دادسراها (دعاوی کثیر از سمت کاربران/کارگزاران)
- دستورات موقت قضایی برای توقف/Delist تعلیق‌های اداری؛
- رویه‌های متعارض در محاکم و بی‌ثباتی حقوقی.

توصیه‌های اصلاحی

۱. تشکیل کمیته شبه قضایی مستقل (قوه قضائیه + مرکز ملی + نماینده تشکل‌ها)؛ لازم‌الاجرا بودن آرای آن پیش از هر اقدام اداری شدید.
۲. تدوین فرآیند اعتراض چند مرحله‌ای (Administrative Review → Independent Panel → Judicial Review)
۳. اصل تناسب و قطعیت حقوقی: هر محدودیت باید معیار، زمان، و امکان تجدیدنظر داشته باشد.
۴. پیش‌نویس قراردادهای تیپ امین-کارگزار-کاربر با بندهای مسئولیت/جبران.

۴) جدول تداخل نهادی و پیامدها (امنیتی-قضایی-تحریمی)

نهاد/مرجع	دغدغه اصلی	تداخل با پیش‌نویس	پیامد برای کاربر	پیامد برای کسب‌وکار	ریسک نهادی/حاکمیتی
-----------	------------	-------------------	------------------	---------------------	--------------------

iranblockchain.org

همراه: ۰۹۳۶۶۶۸۲۴۸۸

تلفکس: ۰۲۱ - ۹۱۳۰۰۰۷۷

نشانی: تهران، بزرگراه امیر

سرلشکر حسین لشگری،

پلاک ۳۱، ساختمان کارخانه نوآوری

کد پستی: ۱۳۹۱۹۵۵۴۱۶

info@iranblockchain.org

@iranblockchaincommunity

@iran_blockchain



وزارت اطلاعات (واجب)	سوءاستفاده مجرمانه، تأمین مالی غیرقانونی	تمرکز Custody بدون استاندارد؛ Delist مبهم	فریز/فلگ، ناگهانی، سردرگمی حقوقی	توقف سرویس، فرار کاربر	افزایش پرونده‌های امنیتی مبتنی بر ظن/ابهام
پلیس فتا	کلاهبرداری/فیشینگ/نفوذ	ابهام نقش امین/کارگزار؛ نبود SLA گزارش حادثه	تأخیر در رسیدگی و استرداد	سیل شکایات، مسئولیت نامشخص	انفجار ورودی پرونده‌ها، اطلاع رسیدگی
سازمان اطلاعات سپاه/امنیت اقتصادی	جرائم سازمان یافته/تلاطم بازار	سقف‌ها/Delist/های ناگهانی؛ مهاجرت نقدینگی	افزایش بازار غیررسمی	دور زدن مقررات، فعالیت زیرزمینی	دشواری پایش واقعی بازار
مرکز ملی فضای مجازی	حکمرانی داده/نوآوری	منع نوآوری	محرومیت از خدمات نو	تعطیلی مدل‌های کسب و کار	کاهش سرمایه اجتماعی تنظیم‌گری
قوه قضائیه/دادستانی کل	دادرسی منصفانه	اختیارات شبه قضایی بانک، فقدان اعتراض	بلا تکلیفی حقوقی	نااطمینانی مقرراتی	احکام متعارض، ابطال مقررات
مرکز اطلاعات مالی (FIU)	AML/CFT کارآمد	سقف‌های مطلق به جای RBA	فشار بر کاربر سالم	هزینه تطبیق بالا، بی‌اثر بر مجرم حرفه‌ای	کاهش اثربخشی مبارزه با پولشویی
شورای رقابت	ضدانحصار	امین محدود/بانک محور، سرمایه نجومی	انتخاب محدود، هزینه بالاتر	تمرکز بازار، سد ورود	ساخت انحصار ساختاری
بانک مرکزی	کنترل ریسک سیستمی	جمع مجزوده‌ی مجازات بدون مسئولیت	فقدان مرجع پاسخ‌گو	تغییر اقلیم ریسک به مقرراتی	مسئولیت‌گریزی نهادی (پرریسک برای کشور)

۵) جمع‌بندی انتقادی

۱. **تحریم/فریز:** پیش‌نویس، «تمرکز» را الزام می‌کند اما مسئولیت «خسارت ناشی از تمرکز» را نمی‌پذیرد؛ این طراحی، ریسک سیستماتیک می‌آفریند.
۲. **امنیت:** معماری و الزامات فعلی، استانداردهای مرجع امنیتی را الزام نکرده و پاسخ‌گویی را مبهم گذاشته است؛ وقوع رخداد گسترده محتمل است.
۳. **قضایی:** اعطای اختیارات سنگین بدون دادرسی منصفانه و مسیر اعتراض، در تعارض با اصول حقوق عمومی است و موج دعاوی قطعی خواهد بود.