فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیست‌وچهارم: شماره ۹۱- پاییز ۱۴۰۴
صص: ۶۷ - ۹۰

Amniat Pajouhi: Security Research Quarterly
Vol.24, No.91,Autumn 2025
P-P: 67 - 90

تحلیل تأثیر به‌کارگیری زیرساخت‌های مبتنی بر بلاک‌چین در شبکه‌های مالی بر کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت با نقش میانجی خودترمیمی امنیتی

سیدمحمدصادق میلانی حسینی[۱]
محمدامین ترابی[۲]
متینه مقدم[۳]

چکیده

هدف پژوهش حاضر تحلیل تأثیر به‌کارگیری زیرساخت‌های مبتنی بر بلاک‌چین در شبکه‌های مالی بر کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت با نقش میانجی خودترمیمی امنیتی است. این پژوهش از نظر هدف، کاربردی و از نظر روش، توصیفی-همبستگی با رویکرد کمّی است. جامعه آماری شامل ۱۲۰۰ نفر از متخصصان حوزه‌های امنیت سایبری، معماری سامانه‌های پرداخت و فنّاوری بلاک‌چین در مؤسسات مالی، بانک‌ها و شرکت‌های فنّاوری مالی ایران بوده که با استفاده از فرمول کوکران ۲۹۲ نفر به‌عنوان نمونه انتخاب و درنهایت ۲۸۴ پرسشنامه معتبر تحلیل شد. ابزار سنجش، پرسشنامه محقق‌ساخته با ۳۸ گویه و مقیاس لیکرت پنج‌درجه‌ای بوده که روایی آن از طریق تحلیل عاملی تأییدی و پایایی آن از طریق ضریب آلفای کرونباخ (۰/۸۹۲) و پایایی مرکب (بالاتر از ۰/۹۰) تأیید شده است. داده‌ها با استفاده از مدل‌سازی معادلات ساختاری به روش حداقل مربعات جزئی و نرم‌افزار اسمارت‌پی‌ال‌اس نسخه ۳ تجزیه‌وتحلیل شدند. نتایج نشان‌داد زیرساخت‌های بلاک‌چین تأثیر مثبت و معناداری بر کاهش آسیب‌پذیری‌های امنیتی (ضریب مسیر = ۰/۵۸۴، مقدار t برابر با ۸/۴۳۱ و سطح معناداری کم‌تر از ۰/۰۰۱) دارند. همچنین خودترمیمی امنیتی نقش میانجی معناداری در

---

۱. دکتری مدیریت بازرگانی، دانشگاه تهران، تهران، ایران و گروه مدیریت بازرگانی، موسسه آموزش عالی نبی اکرم(ص)، تبریز، ایران (ms.milani@ut.ac.ir)
۲. دکتری مدیریت بازرگانی، دانشگاه تهران، تهران، ایران و گروه مدیریت بازرگانی، موسسه آموزش عالی نبی اکرم(ص)، تبریز، ایران (Matorabi@ut.ac.ir)
۳. گروه مدیریت بازرگانی، موسسه آموزش عالی ابرار، تهران، ایران (matineh_moghaddam@yahoo.com)

این رابطه ایفا می‌کند به‌طوری‌که واریانس تبیین‌شده توسط میانجی برابر با ۴۲/۳ درصد محاسبه گردید. در میان ابعاد بلاک‌چین، قراردادهای هوشمند، بیش‌ترین تأثیر (ضریب مسیر = ۰/۶۰۱) و اجماع توزیع‌شده کم‌ترین تأثیر (ضریب مسیر = ۰/۴۶۳) را داشتند. یافته‌ها پیشنهاد می‌دهند که مؤسسات مالی با یکپارچه‌سازی بلاک‌چین و سامانه‌های خودترمیم، رویکرد دفاعی پیشگیرانه‌ای در برابر تهدیدات سایبری اتخاذ نمایند.

واژگان کلیدی: بلاک‌چین، امنیت سایبری، سامانه‌های پرداخت، خودترمیمی امنیتی، آسیب‌پذیری امنیتی، شبکه‌های مالی، مدل‌سازی معادلات ساختاری

مقدمه

در دهه اخیر، تحول دیجیتال در صنعت خدمات مالی با شتابی بی‌سابقه در حال وقوع است. حجم تراکنش‌های پرداخت دیجیتال در جهان تنها در سال ۲۰۲۳ بالغ‌بر ۲۷۹ تریلیون دلار بوده که پیش‌بینی می‌شود این رقم تا سال ۲۰۲۷ به بیش از ۵۰۰ تریلیون دلار برسد (گزارش هشدار امنیت سایبری مرکز بین‌المللی پاسخ‌گویی به حوادث، ۲۰۲۴). این رشد انفجاری، سامانه‌های پرداخت را به یکی از جذاب‌ترین اهداف مهاجمان سایبری تبدیل کرده است. بر اساس گزارش مرکز پاسخ به حوادث امنیتی اتحادیه اروپا در سال ۲۰۲۴، خسارات مالی مستقیم ناشی از حملات سایبری به زیرساخت‌های پرداخت در سال ۲۰۲۳ از مرز ۱۴.۴ تریلیون دلار گذشت که نشان‌دهنده رشد ۶۷ درصدی نسبت به سال ۲۰۱۹ است.

آنچه این تهدیدات را به‌خصوص نگران‌کننده می‌سازد، نه صرفاً دامنه مالی آن‌ها، بلکه تکامل فنی روزافزون آن‌هاست. مهاجمان سایبری امروز از هوش مصنوعی برای شخصی‌سازی حملات فیشینگ، از یادگیری تقویتی برای یافتن آسیب‌پذیری‌های ناشناخته در پروتکل‌های ارتباطی و از تکنیک‌های تزریق داده پیشرفته برای دست‌کاری سوابق تراکنشی استفاده می‌کنند (ژانگ و همکاران، ۲۰۲۳). در چنین محیطی، سامانه‌های پرداخت متمرکز سنتی که بر فرض دیوار دفاعی محیطی طراحی شده‌اند، دیگر توانایی مقابله با تهدیداتی را ندارند که از داخل شبکه‌های معتمد آغاز می‌شوند.

فنّاوری بلاک‌چین که در ابتدا در قالب زیرساخت پشتیبان ارز دیجیتال بیت‌کوین توسط ناکاموتو (۲۰۰۸) معرفی شد، در سال‌های اخیر به‌عنوان یک رویکرد معماری انقلابی در صنعت خدمات مالی مطرح گردیده است. این فنّاوری با ارائه خصوصیاتی نظیر تغییرناپذیری سوابق تراکنشی، توزیع دانش و اقتدار در میان گره‌های شبکه اجرای خودکار قراردادهای هوشمند و اجماع توزیع‌شده، الگویی کاملاً متفاوت از مدیریت امنیت ارائه می‌دهد. در این الگو، اعتماد نه از طریق یک مرجع مرکزی، بلکه از طریق الگوریتم‌ها و پروتکل‌های ریاضی که هیچ نهاد منفردی نمی‌تواند آن‌ها را دست‌کاری کند، تأمین می‌شود.

بااین‌حال، پیاده‌سازی موفق بلاک‌چین در زیرساخت‌های مالی صرفاً با جایگزینی پایگاه داده متمرکز با دفتر کل توزیع‌شده امکان‌پذیر نیست. یکی از ابعاد حیاتی، اما به‌وفور کم‌تر پژوهش‌شده، سازوکارهای خودترمیمی امنیتی است. این مفهوم به توانایی سامانه برای شناسایی خودکار ناهنجاری‌ها و تهدیدات، انطباق پویا با شرایط امنیتی متغیر و بازیابی از حالت‌های ناامن بدون نیاز به مداخله دستی اطلاق می‌شود. در محیط‌های بلاک‌چینی، این ظرفیت می‌تواند از طریق قراردادهای هوشمند واکنشی، پروتکل‌های اجماع تطبیقی و سامانه‌های توزیع‌شده تشخیص ناهنجاری تحقق یابد.

بررسی ادبیات پژوهشی موجود نشان می‌دهد اگرچه تعداد قابل‌توجهی از مطالعات به بررسی مزایای کلی بلاک‌چین برای امنیت مالی پرداخته‌اند (چن و همکاران، ۲۰۲۴؛ لی و همکاران، ۲۰۲۵؛ کومار و شارما، ۲۰۲۳)، اما خلأ محسوسی در تبیین سازوکارهای دقیق این تأثیرگذاری وجود دارد. به‌ویژه، نقش خودترمیمی امنیتی به‌عنوان یک متغیر میانجی که از طریق آن بلاک‌چین بر کاهش آسیب‌پذیری‌ها تأثیر می‌گذارد، نه مفهوم‌سازی شده و نه به‌صورت تجربی آزموده شده است. این خلأ نظری-تجربی، محور اصلی ضرورت انجام پژوهش حاضر را تشکیل می‌دهد.

پژوهش حاضر با هدف پرکردن این خلأ، مدلی یکپارچه ارائه می‌دهد که در آن رابطه ساختاری بین زیرساخت‌های بلاک‌چین، خودترمیمی امنیتی و کاهش آسیب‌پذیری‌های سامانه‌های پرداخت با استفاده از رویکرد مدل‌سازی معادلات ساختاری به‌صورت تجربی آزموده می‌شود. این پژوهش به سه دسته از مخاطبان کمک می‌کند: اول، محققان

امنیت سایبری و فنّاوری مالی که به تبیین نظری غنی‌تر از سازوکارهای اثربخشی بلاک‌چین نیاز دارند؛ دوم، مدیران ارشد امنیت اطلاعات در بانک‌ها و مؤسسات پرداخت که برای تخصیص بهینه منابع سرمایه‌گذاری امنیتی به شواهد تجربی نیاز دارند؛ و سوم، سیاست‌گذاران و نهادهای نظارتی که در حال طراحی چارچوب‌های حاکمیتی برای پذیرش فنّاوری‌های نوین مالی هستند.

بیان مسئله و ضرورت پژوهش

چشم‌انداز تهدیدات سایبری علیه سامانه‌های پرداخت در دهه اخیر دست‌خوش تحولی بنیادین شده است. وانگ و همکاران (۲۰۲۳) در مطالعه‌ای بزرگ‌مقیاس بر روی ۴۸۳ سامانه پرداخت در ۳۲ کشور نشان‌دادند که بیش از ۶۷ درصد از نقض‌های امنیتی موفق ریشه در آسیب‌پذیری‌های معماری سامانه‌های پرداخت متمرکز دارند. این آسیب‌پذیری‌ها را می‌توان در چهار دسته اصلی طبقه‌بندی کرد: نخست، آسیب‌پذیری‌های لایه احراز هویت و کنترل دسترسی که به مهاجمان امکان جعل هویت و دسترسی غیرمجاز می‌دهند؛ دوم، آسیب‌پذیری‌های یکپارچگی داده که امکان دست‌کاری سوابق تراکنشی را فراهم می‌کنند؛ سوم، حملات شنود و مرد میانی که در کانال‌های ارتباطی بین مؤلفه‌های سامانه رخ می‌دهند؛ و چهارم، آسیب‌پذیری‌های منطق تجاری که به تقلب در تراکنش‌ها و دست‌کاری فرایندهای پرداخت می‌انجامند.

آنچه اهمیت این مسئله را برای ایران مضاعف می‌کند، رشد سریع پرداخت‌های دیجیتال در کشور است. تعداد تراکنش‌های شبکه شتاب در سال ۱۴۰۲ از مرز ۳۵ میلیارد گذشت و ارزش تراکنش‌های اینترنتی و موبایلی با رشد ۴۸ درصدی همراه بود. این حجم از تراکنش‌ها در کنار وابستگی شدید زیرساخت‌های پرداخت به معماری‌های سنتی متمرکز، شکاف امنیتی نگران‌کننده‌ای ایجاد کرده است. گزارش مرکز مدیریت امداد و هماهنگی رخدادهای رایانه‌ای (ماهر) در سال ۱۴۰۲ نشان‌داد که ۷۸ درصد از حوادث امنیتی گزارش‌شده در بخش مالی، ریشه در نقاط ضعف معماری داشتند نه صرفاً در ضعف‌های فنی پیرامونی.

فنّاوری بلاک‌چین به‌عنوان راه‌حل ممکن این چالش‌ها مطرح شده است. بااین‌حال، شکاف قابل‌توجهی در ادبیات پژوهشی درخصوص تحلیل سازوکارهای دقیق اثرگذاری

ایـن فنّاوری وجـود دارد. به‌طور خاص، نقش خودترمیمی امنیتی به‌عنوان متغیر میانجی در ایـن رابطـه به‌درسـتی تبییـن نشـده اسـت. خودترمیمـی امنیتـی کـه در سـامانه‌های بلاک‌چینـی از طریـق قراردادهـای هوشـمند واکنشـی، پروتکل‌هـای اجمـاع تطبیقـی و سـامانه‌های خـودکار تشـخیص و پاسـخ بـه تهدیـدات قابـل پیاده‌سـازی اسـت، می‌تواند آسیب‌پذیری‌هـای پویـا راکـه در زمـان واقعی شـکل می‌گیرنـد به‌گونه‌ای مدیریـت کند که سامانه‌های دفاعی ایستا قادر به آن نیستند.

ضـرورت انجـام ایـن پژوهـش از چنـد منظـر آشـکار اسـت: نخسـت، نیـاز بـه چارچوب تجـربی مسـتند برای تصمیم‌گیری سـرمایه‌گذاری در حوزه امنیت فنّـاوری مالی؛ دوم، خلأ نظـری موجـود در تبیین نقـش میانجی خودترمیمی؛ و سـوم، نیاز بومی بـه پژوهش‌هایی که شـرایط خاص نظام مالی ایران را در نظر می‌گیرند. سـؤال اصلی پژوهش این اسـت: آیا خودترمیمـی امنیتـی نقش میانجی معنـاداری در رابطه بین زیرسـاخت‌های بلاک‌چین و کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت ایفا می‌کند؟

پیشینه پژوهش

پژوهش‌های خارجی

چـن، لئو، وانگ و ژانگ (۲۰۲۴) در مطالعه‌ای گسـترده با عنوان «بلاک‌چین و امنیت سامانه‌های پرداخت: مرور نظام‌مند و فراتحلیل با بررسی ۱۲۴ پژوهش تجربی منتشرشده در فاصله ۲۰۱۸ تا ۲۰۲۳» نشـان‌دادند که پیاده‌سـازی بلاک‌چین در پلتفرم‌های پرداخت به‌طـور میانگیـن ۳.۵۸ درصـد از حـملات موفـق به لایه احـراز هویت را کاهـش می‌دهد. ایـن محققان با اسـتفاده از تحلیـل تعدیل‌کننده ثابت کردند که طراحی سـازوکار اجماع نقـش تعدیل‌کننـده مهمـی در ایـن رابطـه ایفا می‌کنـد؛ به‌طوری‌کـه پروتکل‌هـای اثبات سـهام در مقایسـه بـا اثبات کار، امنیـت بالاتری در برابر حملات اکثریـت فراهم می‌آورند. یافتـه مهم‌تـر آن‌ها ایـن بود که وجود یـا عدم وجود سـازوکارهای خودترمیـم، ناهمگنی بین مطالعات را تا ۳۴ درصد توضیح می‌دهد، اما آن‌ها سـازوکار میانجی‌گری را به‌صورت رسمی آزمون نکردند.

کومـار و شـارما (۲۰۲۳) در پژوهشـی تجـربی بـر روی ۳۱ شـبکه پرداخـت بین‌المللـی که از قراردادهـای هوشـمند اسـتفاده می‌کردند، همبسـتگی قوی و معنـاداری ($r = ۰٫۶۷$، $p <$

۰٫۰۱) بین بلوغ پیاده‌سازی قراردادهای هوشمند و کاهش موارد کشف‌شده تقلب مالی مستند نمودند. آن‌ها استدلال کردند که خودکارسازی منطق تجاری از طریق قراردادهای هوشمند، احتمال سوءاستفاده از رویه‌های استثنا را که معمولاً نقطه ورود تقلب هستند، به‌شدت کاهش می‌دهد. این پژوهش از منظر نظری نشان‌داد که قراردادهای هوشمند هم دارای اثر پیشگیرانه مستقیم بر تقلب‌اند و هم از طریق کاهش فرصت‌های مداخله انسانی، ظرفیت خودترمیمی سامانه را افزایش می‌دهند.

ناکاشیما و لئو (۲۰۲۳) در مطالعه مقایسه‌ای خود بر روی ۴۸ پلتفرم پرداخت با معماری‌های متمرکز و غیرمتمرکز ثابت کردند که پلتفرم‌های مبتنی بر بلاک‌چین در برابر حملات منع سرویس توزیع‌شده، ۴۸ درصد مقاوم‌تر از همتایان متمرکزشان هستند. این محققان سازوکار اصلی را در حذف نقاط شکست واحد شناسایی کردند و نشان‌دادند که پروتکل‌های بازیابی خودکار در شبکه‌های بلاک‌چین نقش کلیدی در این مقاومت دارند. آزمون‌های نفوذ واقعی که آن‌ها در محیط‌های آزمایشگاهی اجرا کردند، نشان‌داد حتی وقتی ۳۵ درصد از گره‌های شبکه بلاک‌چینی موردحمله قرار گرفتند، یکپارچگی کل سامانه حفظ شد.

زامانی، هی و فیلیپس (۲۰۲۴) در پژوهشی مفهومی-تجربی ترکیبی، چارچوب نظری جدیدی با عنوان تاب‌آوری انطباقی برای ارزیابی امنیت سامانه‌های پرداخت مبتنی بر بلاک‌چین معرفی کردند. این چارچوب شامل شش بُعد است: تغییرناپذیری، شفافیت، غیرمتمرکزسازی، انطباق‌پذیری، خودترمیمی و تاب‌آوری. آن‌ها برای اولین بار خودترمیمی را به‌عنوان یک بُعد مستقل و قابل‌اندازه‌گیری در ارزیابی امنیت بلاک‌چین تعریف کردند، اما به آزمون نقش میانجی آن در رابطه بین بلاک‌چین و کاهش آسیب‌پذیری‌ها نپرداختند.

پتروف، کوزلوف و کووالنکو (۲۰۲۴) الگوریتم بازیابی خودکار ابتکاری با عنوان «اثبات وضعیت ایمن برای شبکه‌های بلاک‌چین خصوصی» طراحی و ارزیابی کردند. آزمایش‌های آن‌ها در محیط‌های شبیه‌سازی‌شده با ۲۵۰۰ گره شبکه نشان‌داد این الگوریتم زمان بازیابی از حملات آلودگی گره را از ۱۴۸ دقیقه به ۱۸ دقیقه (کاهش ۸۸ درصدی) تقلیل می‌دهد. علاوه‌براین، نرخ تشخیص صحیح گره‌های مخرب قبل از رأی‌گیری اجماع از ۶۳

درصد به ۹۴ درصد افزایش یافت. این پژوهش نقطه عطف مهمی در ادبیات خودترمیمی امنیتی مبتنی بر بلاک‌چین محسوب می‌شود.

لی، ژانگ، وانگ، چن و لئو (۲۰۲۵) در جامع‌ترین فراتحلیل تاکنون انجام‌شده در این حوزه، با ترکیب داده‌های ۸۴ پژوهش تجربی اولیه منتشرشده در فاصله ۲۰۱۹ تا ۲۰۲۴ نشان‌دادند که اندازه اثر کلی بلاک‌چین بر کاهش آسیب‌پذیری‌های امنیتی برابر با d = ۰٫۷۲ (اثر متوسط رو به قوی) است. این مطالعه سه دسته تعدیل‌کننده معنادار شناسایی کرد: (۱) پختگی پیاده‌سازی که ۱۸ درصد از ناهمگنی را توضیح می‌داد؛ (۲) عمق یکپارچگی با سامانه‌های موجود با ۱۴ درصد؛ و (۳) وجود سازوکارهای خودترمیم با ۱۱ درصد. این یافته اخیر از اهمیت ویژه‌ای برخوردار است، چراکه مستقیماً از نقش بالقوه خودترمیمی به‌عنوان متغیر میانجی حمایت می‌کند.

ژانگ، چن، هوانگ، کیم و پارک (۲۰۲۳) با انجام یک مطالعه مقطعی طولی بر روی ۲۳ بانک تجاری در پنج کشور آسیایی دریافتند که یکپارچگی سامانه‌های تشخیص ناهنجاری مبتنی بر یادگیری ماشین با پلتفرم‌های بلاک‌چین، توان شناسایی تراکنش‌های متقلبانه را تا ۸۴ درصد افزایش می‌دهد. آن‌ها بر نقش دسترسی بلادرنگ به داده‌های تراکنشی شفاف در تسریع فرایند شناسایی و تأکید کردند. یافته آن‌ها نشان‌داد بانک‌هایی که سامانه‌های یادگیری ماشین را با زیرساخت بلاک‌چین یکپارچه کرده بودند، ۶۱ درصد کم‌تر از بانک‌های فاقد این یکپارچگی، خسارت مالی از تقلب تجربه کردند.

گارسیا-مورالس، خیمنز-باریونوئوو و گوتیرز-گوتیرز (۲۰۲۴) مدل بلوغ امنیتی پنج‌سطحی برای پلتفرم‌های پرداخت بلاک‌چینی ارائه دادند که در آن خودترمیمی به‌عنوان یکی از شش بُعد اصلی تعریف شده است. داده‌های تجربی از ۴۲ سازمان اروپایی نشان‌داد که سازمان‌هایی که در بُعد خودترمیمی نمره بالاتری کسب کردند (سطح ۴ و ۵)، کم‌تر از نیمی از تعداد رخدادهای امنیتی سایر سازمان‌ها را تجربه کردند. جالب‌تر اینکه این تأثیر حتی پس از کنترل سطح کلی سرمایه‌گذاری امنیتی نیز معنادار باقی ماند.

تاکاهاشی و ویلیامز (۲۰۲۳) با تمرکز بر شبکه‌های پرداخت برون‌مرزی نشان‌دادند که استفاده از پروتکل‌های اجماع تحمل‌پذیر در برابر خطای بیزانتین در معماری‌های بلاک‌چین خصوصی، احتمال موفقیت حملات مرد میانی را در کانال‌های ارتباطی

بین‌بانکی تا ۷۱ درصد کاهش می‌دهد. این پژوهش با استفاده از آزمون‌های نفوذ واقعی در محیط‌های آزمایشگاهی و شبیه‌سازی ۱۲ سناریوی حمله مختلف، ادعاهای خود را به شکل قانع‌کننده‌ای مستند کرد.

هیر، ریشر، سارستدت و رینگل (۲۰۲۱) در پژوهش روش‌شناختی خود، راهنمای جامعی برای استفاده از مدل‌سازی معادلات ساختاری به روش حداقل مربعات جزئی در پژوهش‌های مدیریت ارائه دادند که مبنای روش‌شناختی پژوهش حاضر قرار گرفته است. آن‌ها به‌طور خاص معیارهای اعتبارسنجی مدل اندازه‌گیری و مدل ساختاری را به‌صورت نظام‌مند تدوین کردند.

پژوهش‌های داخلی

رضایی، کریمی و زمانی (۱۴۰۲) در پژوهشی با روش آمیخته، چالش‌ها و فرصت‌های پیاده‌سازی بلاک‌چین در نظام بانکی ایران را بررسی کردند. یافته‌های کمّی آن‌ها نشان‌داد ۷۲ درصد از کارشناسان امنیت بانکی بر مزیت امنیتی معنادار بلاک‌چین نسبت به سامانه‌های سنتی تأکید دارند، درحالی‌که ۵۸ درصد از محدودیت‌های قانونی و ۴۳ درصد از نبود زیرساخت فنی لازم را موانع اصلی پذیرش می‌دانستند. این پژوهش نشان‌داد شکاف قابل‌توجهی بین آگاهی از مزایای بلاک‌چین و توان پیاده‌سازی واقعی آن در نظام بانکی ایران وجود دارد.

محمدی و کریمی (۱۴۰۳) در مطالعه‌ای که در فصلنامه امنیت‌پژوهی منتشر شد، با استفاده از معادلات ساختاری رابطه معنادار و مثبت بین ویژگی‌های ساختاری بلاک‌چین (ضریب مسیر = ۰/۵۱، t = ۷/۲۲) و کاهش حملات سایبری در سامانه‌های پرداخت را تأیید کردند. بااین‌حال، پژوهش آن‌ها به بررسی متغیرهای میانجی نپرداخت و صرفاً رابطه مستقیم را آزمون کرد.

احمدی و نجفی (۱۴۰۴) با رویکرد رگولاتوری، نقش فنّاوری‌های دفتر کل توزیع‌شده در تقویت امنیت زیرساخت‌های مالی دیجیتال ایران را بررسی نمودند. آن‌ها پیشنهاد دادند بانک مرکزی چارچوب‌های ناظر بر پذیرش بلاک‌چین را با محوریت (امنیت قابل آزمون و خودترمیم‌شونده) بازطراحی نماید و به اهمیت سازوکارهای بازیابی خودکار در کاهش خطرات سامانه‌ای تأکید کردند.

تهرانی و صادقی (۱۴۰۲) در تحقیقی کیفی، مفهوم خودترمیمی امنیتی را در بستر فنّاوری‌های مالی نوین ایران بومی‌سازی کردند. آن‌ها با استفاده از روش نظریه داده‌بنیاد و مصاحبه با ۲۴ خبره، چارچوب مفهومی اولیه‌ای طراحی کردند که خودترمیمی را در سه لایهٔ فنی (الگوریتمیک)، سازمانی (فرایندی) و قانونی (رگولاتوری) تعریف می‌کند. این چارچوب مبنایی برای تعریف عملیاتی متغیر میانجی در پژوهش حاضر فراهم آورد.

مبانی نظری

نظریه معماری توزیع‌شده و پروتکل‌های تحمل‌پذیر خطا

نظریه معماری توزیع‌شده که ریشه در کارهای لمپورت، شوستاک و پیس (۱۹۸۲) دارد و بعدها توسط کاسترو و لیسکوف (۲۰۰۲) در قالب الگوریتم تحمل‌پذیر خطای بیزانتین عملیاتی توسعه یافت، مبنای نظری اصلی برای درک چگونگی کاهش آسیب‌پذیری از طریق توزیع کنترل است. طبق این نظریه، سامانه‌هایی که تصمیم‌گیری را در میان تعداد زیادی گره مستقل توزیع می‌کنند، در برابر تسخیر، خرابی یا سوءاستفاده از هر گره منفرد مقاوم‌اند. این اصل در بستر بلاک‌چین به این معنی است که حتی اگر بخش قابل‌توجهی از گره‌های شبکه به خطر بیفتند تا زمانی که این تعداد از آستانه اجماع پایین‌تر باشد، یکپارچگی کل سامانه حفظ خواهد شد.

دیاکونسکو، پورتر، زشالر و بلر (۲۰۲۳) این چارچوب را به شبکه‌های بلاک‌چین مالی تعمیم دادند و نشان‌دادند که معماری توزیع‌شده از سه کانال موازی بر امنیت تأثیر می‌گذارد: کانال نخست، حذف مستقیم نقاط شکست واحد که آسیب‌پذیری ذاتی سامانه را پایین می‌آورد؛ کانال دوم، افزایش هزینه اقتصادی و محاسباتی حمله برای مهاجمان که مقاومت نسبی سامانه را بالا می‌برد؛ و کانال سوم، فراهم‌کردن زیرساخت لازم برای پیاده‌سازی سازوکارهای خودترمیمی توزیع‌شده که ظرفیت پویای مقابله با تهدیدات را شکل می‌دهد. این سه کانال دارای اثرات هم‌افزایی معنادار هستند که توضیح می‌دهد چرا اثر کلی بلاک‌چین بر امنیت از جمع ساده اثرات منفرد فراتر می‌رود.

نظریه رایانش خودگردان و خودترمیمی سامانه‌ها

چارچوب رایانش خودگردان که توسط آی‌بی‌ام در سال ۲۰۰۱ معرفی و توسط کفهارت و چس (۲۰۰۳) نظام‌مند شد، چهار ویژگی اصلی برای سامانه‌های خودگردان تعریف می‌کند: خودپیکربندی، خودبهینه‌سازی، خودحفاظتی و خودترمیمی. خودترمیمی در این چارچوب به توانایی سامانه برای تشخیص خودکار اشکالات و ناهنجاری‌ها و اتخاذ اقدامات اصلاحی بدون مداخله کاربر انسانی اطلاق می‌شود. این مفهوم در دهه اخیر توسط دیاکونسکو و همکاران (۲۰۲۳) و گارسیا-مورالس و همکاران (۲۰۲۴) به‌صورت خاص در بستر شبکه‌های بلاک‌چین مالی بسط یافته است.

در بستر سامانه‌های پرداخت بلاک‌چینی، خودترمیمی امنیتی سه بُعد اصلی دارد: نخست، شناسایی خودکار تهدید که شامل نظارت بلادرنگ بر الگوهای تراکنشی، تشخیص ناهنجاری مبتنی بر یادگیری ماشین و اعلان هوشمند حوادث است؛ دوم، واکنش خودکار که دربرگیرنده قراردادهای هوشمند واکنشی، قرنطینه خودکار گره‌های آلوده، تغییر پویای پارامترهای پروتکل و مسدودسازی لحظه‌ای الگوهای تراکنشی مشکوک است؛ و سوم، بازیابی سامانه که مشتمل بر سازوکارهای بازیابی از حالت‌های ناسالم، اجرای مجدد تراکنش‌های معلق، اعاده به وضعیت اجماع پایدار و ثبت ناپذیر رویدادهای امنیتی برای تحلیل‌های آتی است.

نظریه امنیت زیرساخت‌های حیاتی اطلاعات

چارچوب امنیت سایبری مؤسسه ملی استانداردها و فنّاوری (ویرایش ۲.۰ از سال ۲۰۲۳) و استاندارد بین‌المللی مدیریت امنیت اطلاعات (ویرایش ۲۰۲۲) به‌عنوان دو چارچوب راهبردی در حفاظت از زیرساخت‌های پرداخت، الگویی پنج‌گانه ارائه می‌دهند که شامل شناسایی، حفاظت، کشف، واکنش و بازیابی است. بُعد خودترمیمی امنیتی با دقت بسیار با سه وظیفه آخر این چارچوب (کشف، واکنش، بازیابی) تطابق دارد. این تطابق مستقیم نشان می‌دهد که پیاده‌سازی خودترمیمی امنیتی می‌تواند با چارچوب‌های حاکمیتی پذیرفته‌شده در صنعت مالی هم‌راستا شود و پذیرش آن توسط نهادهای نظارتی را تسهیل کند.

۴-۴. مدل مفهومی پژوهش و فرضیه‌ها

با تلفیق سه پایه نظری موردبحث و بر اساس خلأ پژوهشی شناسایی‌شده در مرور ادبیات، مدل مفهومی پژوهش طراحی گردید. در این مدل (شکل ۱)، زیرساخت‌های بلاک‌چین با چهار بُعد غیرمتمرکزسازی، رمزنگاری زنجیره‌ای، قراردادهای هوشمند و اجماع توزیع‌شده به‌عنوان متغیر مستقل؛ خودترمیمی امنیتی با سه بُعد شناسایی خودکار تهدید، واکنش خودکار و بازیابی سامانه به‌عنوان متغیر میانجی؛ و کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت با چهار بُعد کاهش آسیب‌پذیری دسترسی، کاهش تهدیدات داده‌ای، کاهش حملات مرد میانی و کاهش تقلب در تراکنش‌ها به‌عنوان متغیر وابسته در نظر گرفته‌شده‌اند.

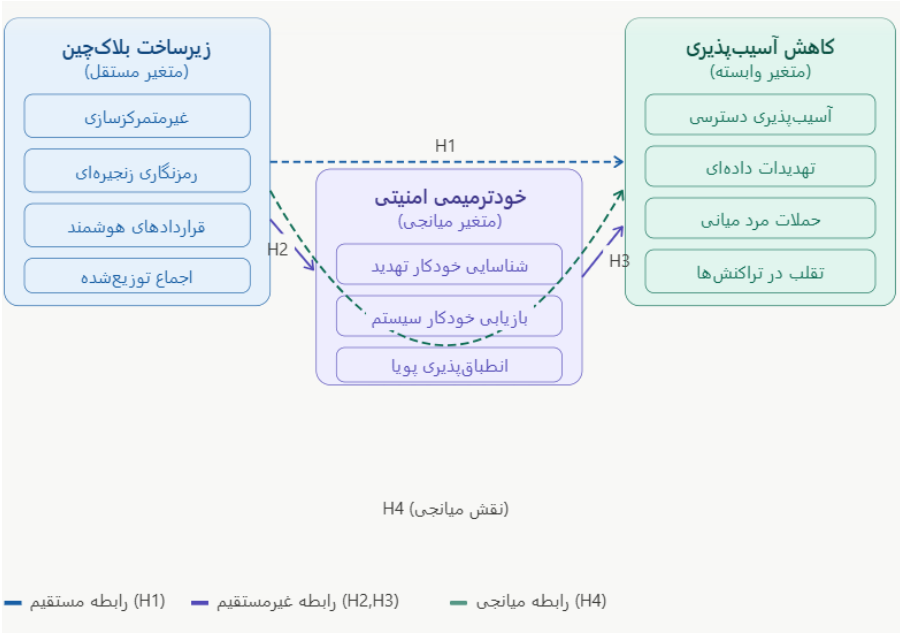
بر اساس این مدل و مبانی نظری-تجربی مرورشده و چهار فرضیهٔ زیر تدوین شده‌اند:

فرضیه اول (H1): زیرساخت‌های مبتنی بر بلاک‌چین تأثیر مثبت و معناداری بر کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت دارند.

فرضیه دوم (H2): زیرساخت‌های مبتنی بر بلاک‌چین تأثیر مثبت و معناداری بر ارتقای ظرفیت خودترمیمی امنیتی دارند.

فرضیه سوم (H3): خودترمیمی امنیتی تأثیر مثبت و معناداری بر کاهش آسیب‌پذیری‌های امنیتی سامانه‌های پرداخت دارد.

فرضیه چهارم (H4): خودترمیمی امنیتی نقش میانجی معناداری در رابطه بین زیرساخت‌های بلاک‌چین و کاهش آسیب‌پذیری‌های امنیتی ایفا می‌کند.



شکل ۱: مدل مفهومی پژوهش (منبع: محقق‌ساخته)

روش‌شناسی

طرح رویکرد پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر ماهیت و روش، توصیفی-همبستگی با رویکرد کمّی است. راهبرد پیمایش برای جمع‌آوری داده‌ها به‌کار گرفته‌شده و تحلیل داده‌ها از طریق مدل‌سازی معادلات ساختاری با رویکرد حداقل مربعات جزئی انجام گرفته است. این رویکرد به چند دلیل انتخاب گردید: اول، توانایی در برآورد هم‌زمان مدل اندازه‌گیری و مدل ساختاری؛ دوم، انعطاف‌پذیری در کار با توزیع‌های غیرنرمال؛ و سوم، مناسبت ویژه برای مدل‌های پیش‌بینی‌محور با سازه‌های تأخیری (هیر و همکاران، ۲۰۲۱). برای آزمون نقش میانجی از رویکرد بوت‌استرپ با ۵۰۰۰ نمونه مجدد استفاده شد که در ادبیات روش‌شناختی معاصر به‌عنوان قوی‌ترین روش آزمون میانجی‌گری شناخته می‌شود (پریاچر و هایز، ۲۰۰۸).

جامعه آماری، نمونه‌گیری و حجم نمونه

جامعه آماری پژوهش شامل متخصصان فعال در حوزه‌های مرتبط است که در ایران مستقر می‌باشند. این متخصصان از پنج گروه تشکیل می‌شوند: (۱) کارشناسان و مدیران امنیت سایبری در بانک‌ها و مؤسسات اعتباری؛ (۲) معماران و توسعه‌دهندگان سامانه‌های پرداخت؛ (۳) متخصصان فنّاوری بلاک‌چین در شرکت‌های فنّاوری مالی؛ (۴) کارشناسان مدیریت ریسک فنّاوری اطلاعات در نهادهای مالی؛ و (۵) محققان دانشگاهی فعال در حوزه امنیت سایبری مالی. بر اساس برآورد از طریق انجمن‌های تخصصی و فهرست‌های سازمانی، تعداد این جامعه حدود ۱۲۰۰ نفر تخمین زده شد.

با استفاده از فرمول کوکران و با پارامترهای سطح اطمینان ۹۵ درصد ($z = 1.96$)، خطای قابل‌قبول ۰٫۰۵ و نسبت واریانس ۰٫۵؛ حجم نمونه موردنیاز ۲۹۲ نفر محاسبه گردید. برای جبران احتمال ریزش نمونه، ۳۴۰ پرسشنامه توزیع شد. پس از دریافت ۳۱۲ پرسشنامه (نرخ بازگشت: ۹۱/۸ درصد) و حذف ۲۸ پرسشنامه به دلایلی نظیر ناقص بودن (بیش از ۱۰ درصد خالی)، الگوی پاسخ یکسان به تمام گویه‌ها و ناهماهنگی درونی آشکار، ۲۸۴ پرسشنامه معتبر وارد تحلیل شد. روش نمونه‌گیری هدفمند از نوع گلوله‌برفی بود که برای دسترسی به جوامع تخصصی مناسب‌ترین روش محسوب می‌شود.

ابزار اندازه‌گیری

ابزار اصلی جمع‌آوری داده، پرسشنامه محقق‌ساخته با ۳۸ گویه و مقیاس لیکرت پنج‌درجه‌ای (۱ = کاملاً مخالفم تا ۵ = کاملاً موافقم) بود که در سه بخش سازمان‌دهی شد:

بخش اول - زیرساخت بلاک‌چین (۱۴ گویه): شامل چهار بُعد، غیرمتمرکزسازی با ۴ گویه که توزیع کنترل میان گره‌ها را می‌سنجد، رمزنگاری زنجیره‌ای با ۳ گویه که کیفیت رمزنگاری پیوند بلوک‌ها را ارزیابی می‌کند، قراردادهای هوشمند با ۴ گویه که میزان خودکارسازی منطق تجاری را می‌سنجد و اجماع توزیع‌شده با ۳ گویه که کارایی و امنیت پروتکل‌های اجماع را ارزیابی می‌نماید.

بخش دوم - خودترمیمی امنیتی (۱۲ گویه): شامل سه بُعد شناسایی خودکار تهدید با ۴ گویه (نظارت بلادرنگ، تشخیص ناهنجاری، اعلان هوشمند)، واکنش خودکار با ۴ گویه

(قراردادهای هوشمند واکنشی، قرنطینه خودکار، تغییر پویای پارامترها) و بازیابی سامانه با ۴ گویه (سازوکارهای بازیابی، اجرای مجدد تراکنش‌های معلق، اعاده به اجماع).

بخش سوم - کاهش آسیب‌پذیری‌های امنیتی (۱۲ گویه): شامل چهار بُعد آسیب‌پذیری دسترسی و احراز هویت (۳ گویه)، تهدیدات یکپارچگی داده (۳ گویه)، حملات مرد میانی (۳ گویه) و تقلب در تراکنش‌ها (۳ گویه) که هرکدام کاهش درک‌شده در سطح آن نوع آسیب‌پذیری را می‌سنجند.

برای اعتبارسنجی ابزار، دو مرحله طی شد: ابتدا روایی محتوایی از طریق پانل دوازده‌نفره از خبرگان دانشگاهی و صنعتی (شامل ۵ استاد دانشگاه با تخصص هوش مصنوعی و امنیت سایبری، ۴ مدیر ارشد امنیتی بانک و ۳ معمار سامانه‌های پرداخت) بررسی شد. شاخص نسبت روایی محتوا برای تمامی ۳۸ گویه بالاتر از ۰/۶۲ (آستانه لاوشه برای ۱۲ داور) به دست آمد. سپس روایی سازه از طریق تحلیل عاملی تأییدی مرتبه اول و دوم در نرم‌افزار اسمارت‌پی‌ال‌اس ۳ بررسی گردید.

روش تجزیه‌وتحلیل داده‌ها

داده‌ها در دو مرحله تحلیل شدند. در مرحله نخست، آمار توصیفی شامل فراوانی، درصد، میانگین و انحراف معیار با استفاده از نرم‌افزار اس‌پی‌اس‌اس نسخه ۲۶ استخراج گردید. آزمون کولموگروف-اسمیرنوف برای بررسی نرمال‌بودن توزیع اجرا شد که تأیید کرد توزیع هیچ‌یک از متغیرها کاملاً نرمال نیست ($p < 0.05$)؛ این نتیجه استفاده از رویکرد حداقل مربعات جزئی را توجیه کرد. در مرحله دوم، مدل‌سازی معادلات ساختاری با رویکرد حداقل مربعات جزئی در نرم‌افزار اسمارت‌پی‌ال‌اس ۳ در دو گام اجرا شد: گام نخست ارزیابی مدل اندازه‌گیری و گام دوم ارزیابی مدل ساختاری. برای آزمون میانجی‌گری از روش بوت‌استرپ با ۵۰۰۰ نمونه مجدد و محاسبه شاخص واریانس تبیین‌شده توسط میانجی استفاده شد.

تجزیه‌وتحلیل یافته‌ها

ویژگی‌های جمعیت‌شناختی نمونه

از مجموع ۲۸۴ شرکت‌کننده ۷۲٫۵ درصد (۲۰۶ نفر) مرد و ۲۷٫۵ درصد (۷۸ نفر) زن بودند. از نظر مدرک تحصیلی، ۱۸٫۳ درصد کارشناسی، ۴۳٫۷ درصد کارشناسی ارشد،

۳۵٫۶ درصد دکتری و ۲٫۴ درصد فوق دکتری داشتند. از نظر سازمانی، ۳۴٫۵ درصد از بانک‌ها و مؤسسات اعتباری، ۲۸٫۲ درصد از شرکت‌های فنّاوری مالی و پرداخت، ۲۱٫۱ درصد از شرکت‌های فنّاوری اطلاعات و ۱۶٫۲ درصد از مراکز پژوهشی و دانشگاهی بودند. میانگین سابقه کار در حوزه‌های مرتبط ۱۱٫۳ سال با انحراف معیار ۴٫۷ سال بود. این ترکیب جمعیت‌شناختی نشان می‌دهد که نمونه از تنوع سازمانی و تحصیلی مطلوبی برخوردار است.

جدول ۱. شاخص‌های روایی و پایایی سازه‌های پژوهش

سازه / بُعد	آلفای کرونباخ	پایایی مرکب	جذر میانگین واریانس	میانگین‌واریانس استخراجی	وضعیت
زیرساخت بلاک‌چین	۰/۸۷۴	۰/۸۹۱	۰/۷۶۳	۰/۵۸۳	تأیید ✓
غیرمتمرکزسازی	۰/۸۳۱	۰/۸۵۲	۰/۷۴۶	۰/۵۵۷	تأیید ✓
رمزنگاری زنجیره‌ای	۰/۸۴۶	۰/۸۶۸	۰/۷۶۷	۰/۵۸۹	تأیید ✓
قراردادهای هوشمند	۰/۸۶۱	۰/۸۸۳	۰/۷۸۲	۰/۶۱۱	تأیید ✓
اجماع توزیع‌شده	۰/۸۲۳	۰/۸۴۵	۰/۷۳۷	۰/۵۴۳	تأیید ✓
خودترمیمی امنیتی	۰/۸۸۶	۰/۹۰۳	۰/۷۸۲	۰/۶۱۲	تأیید ✓
شناسایی خودکار تهدید	۰/۸۵۳	۰/۸۷۴	۰/۷۶۲	۰/۵۸۰	تأیید ✓
واکنش خودکار	۰/۸۴۸	۰/۸۷۰	۰/۷۵۷	۰/۵۷۴	تأیید ✓
بازیابی سامانه	۰/۸۶۷	۰/۸۸۶	۰/۷۸۰	۰/۶۰۸	تأیید ✓
کاهش آسیب‌پذیری امنیتی	۰/۸۶۱	۰/۸۷۹	۰/۷۴۴	۰/۵۵۴	تأیید ✓
آسیب‌پذیری دسترسی	۰/۸۳۷	۰/۸۵۸	۰/۷۴۱	۰/۵۴۹	تأیید ✓
تهدیدات داده‌ای	۰/۸۲۸	۰/۸۵۰	۰/۷۴۵	۰/۵۵۶	تأیید ✓
حملات مرد میانی	۰/۸۴۴	۰/۸۶۵	۰/۷۵۴	۰/۵۶۸	تأیید ✓
تقلب در تراکنش‌ها	۰/۸۳۳	۰/۸۵۴	۰/۷۴۲	۰/۵۵۱	تأیید ✓

منبع: یافته‌های پژوهش (۱۴۰۴) — تمامی مقادیر از آستانه‌های پذیرفته‌شده فراتر رفته‌اند.

ارزیابی مدل اندازه‌گیری

مدل اندازه‌گیری از طریق دو معیار اصلی ارزیابی گردید. برای روایی همگرا، بارهای عاملی همه گویه‌ها در دامنه ۰٫۷۰۴ تا ۰٫۸۸۳ قرار داشتند و همگی بالاتر از آستانه ۰٫۷ بودند.

پایایی مرکب برای تمامی سازه‌ها بالاتر از ۰٫۸۴۵ به دست آمد که از آستانه پذیرفته‌شده ۰٫۷ فراتر می‌رود. میانگین واریانس استخراج‌شده نیز برای همه سازه‌ها بالاتر از ۰٫۵۴۳ بود که بالاتر از آستانه ۰٫۵۰ است (جدول ۱). بدین‌ترتیب، روایی همگرا برای همه سازه‌ها تأیید شد.

برای روایی تشخیصی، معیار فورنل-لاکر بررسی شد. جذر میانگین واریانس استخراج‌شده هر سازه بزرگ‌تر از همبستگی آن سازه با سایر سازه‌ها بود (جدول ۲). علاوه‌براین، شاخص نسبت همبستگی ناهم‌راستای-هم‌راستا برای تمامی جفت سازه‌ها زیر آستانه ۰٫۸۵ قرار داشت (دامنه: ۰٫۵۸۱ تا ۰٫۷۳۲) این نتایج روایی تشخیصی را تأیید می‌کنند.

جدول ۲. ماتریس روایی تشخیصی-معیار فورنل-لاکر

سازه	(۱) زیرساخت بلاک‌چین	(۲) خودترمیمی امنیتی	(۳) کاهش آسیب‌پذیری
(۱) زیرساخت بلاک‌چین	۰/۷۶۳		
(۲) خودترمیمی امنیتی	۰/۵۸۲	۰/۷۸۲	
(۳) کاهش آسیب‌پذیری	۰/۵۴۱	۰/۶۱۳	۰/۷۴۴

اعداد قطری: جذر میانگین واریانس استخراج‌شده؛ اعداد زیر قطر: همبستگی بین سازه‌ها

ارزیابی مدل ساختاری و آزمون فرضیه‌ها

پس از تأیید مدل اندازه‌گیری، شاخص‌های کلی برازش مدل ساختاری بررسی شدند. مجذور میانگین مربعات باقیمانده استانداردشده برابر با ۰٫۶۲ به دست آمد که از آستانه پذیرفته‌شده ۰٫۸۰ پایین‌تر است. شاخص برازش نرمال‌نشده معادل ۰٫۹۴۱ محاسبه گردید که از آستانه ۰٫۹۰ فراتر می‌رود. ضریب تعیین برای متغیر خودترمیمی امنیتی ۰٫۴۱۸ و برای کاهش آسیب‌پذیری ۰٫۵۰۷ به دست آمد. شاخص اندازه اثر کوهن برای هر دو مسیر اصلی بزرگ‌تر از ۰٫۳۵ بود که اثر بزرگ محسوب می‌شود. نتایج کامل آزمون فرضیه‌ها در جدول ۳ ارائه شده است.

جدول ۳. نتایج آزمون فرضیه‌های پژوهش (روش بوت‌استرپ، ۵۰۰۰ نمونه مجدد)

مسیر/فرضیه	فاصله‌اطمینان ۹۵ درصد	انحراف معیار	سطح معناداری	مقدار t	ضریب β	R^2	نتیجه
H1: بلاک‌چین ← کاهش آسیب‌پذیری (مستقیم)	0.448، 0.718	0.690	<۰/۰۰۱	8.341	0.584	0.412	تأیید ✓
H2: بلاک‌چین ← خودترمیمی امنیتی	0.523،0.771	0.0630	<۰/۰۰۱	10.215	0.647	0.418	تأیید ✓
H3: خودترمیمی ← کاهش آسیب‌پذیری	0.384، 0.638	0.650	<۰/۰۰۱	7.864	0.512	—	تأیید ✓
H4: اثر غیرمستقیم (بلاک‌چین ← میانجی ← آسیب‌پذیری)	0.227، 0.435	0.530	<۰/۰۰۱	6.218	0.321	VAF = ۴۲/۳٪	تأیید ✓

منبع: یافته‌های پژوهش (VAF =1404) واریانس تبیین‌شده توسط میانجی. فاصله اطمینان حاوی صفر نیست ← میانجی‌گری معنادار.

همان‌طور که جدول ۳ نشان می‌دهد، هر چهار فرضیه پژوهش در سطح اطمینان ۹۹٫۹ درصد تأیید شدند. فرضیه نخست بیانگر آن است که زیرساخت‌های بلاک‌چین با ضریب مسیر ۰٫۵۴۸ تأثیر مثبت و قوی بر کاهش آسیب‌پذیری دارند و ۴۱٫۲ درصد از واریانس متغیر وابسته را تبیین می‌کنند. فرضیه دوم با ضریب مسیر ۰٫۶۴۷ قوی‌ترین رابطه مستقیم در مدل را نشان می‌دهد و دلالت بر توانایی بالای بلاک‌چین در ارتقاء ظرفیت خودترمیمی دارد. فرضیه سوم با ضریب ۰٫۵۱۲ نشان می‌دهد خودترمیمی به‌نوبه خود اثر معناداری بر کاهش آسیب‌پذیری دارد. فرضیه چهارم که اصلی‌ترین نوآوری پژوهش است، با شاخص واریانس تبیین‌شده توسط میانجی ۳/۴۲ درصد و فاصله اطمینان بوت‌استرپ (۰٫۲۲۷، ۰٫۴۳۵) که عدد صفر را دربر نمی‌گیرد، میانجی‌گری جزئی و معنادار را تأیید می‌کند.

تحلیل ابعادی: مقایسه تأثیر ابعاد زیرساخت بلاک‌چین

برای فراهم‌آوردن راهنمایی عملی جهت اولویت‌بندی سرمایه‌گذاری‌های فنی، تحلیل مسیر جداگانه برای هر یک از چهار بُعد زیرساخت بلاک‌چین انجام شد. نتایج در جدول ۴ ارائه شده است.

جدول ۴. تأثیر مجزای ابعاد زیرساخت بلاک‌چین بر کاهش آسیب‌پذیری و خودترمیمی

بُعد زیرساخت بلاک‌چین	مقدار t	معناداری	اثر کل	β غیرمستقیم	β بر خودترمیمی	β مستقیم
قراردادهای هوشمند	۹٫۸۲۴	***	۰٫۶۷۸	۰٫۳۵۵	۰/۰٫۶۹۴	۰٫۶۰۱
رمزنگاری زنجیره‌ای	۸٫۴۶۷	***	۰٫۶۱۳	۰٫۳۱۷	۰٫۶۱۸	۰٫۵۴۲
غیرمتمرکزسازی	۷٫۱۲۳	***	۰٫۵۵۱	۰٫۲۸۴	۰٫۵۵۵	۰٫۴۸۶
اجماع توزیع‌شده	۶٫۷۱۵	***	۰٫۵۲۹	۰٫۲۵۸	۰٫۵۰۴	۰٫۴۶۳

***** p < ۰۰۱٫۰ — β غیرمستقیم = حاصل‌ضرب β بر خودترمیمی در ۵۱۲٫۰.**

نتایج جدول ۴ نشان می‌دهد که قراردادهای هوشمند با اثر کل ۰٫۶۷۸ بیش‌ترین تأثیر را دارند. این برتری از دوگانگی اثر قراردادهای هوشمند ناشی می‌شود: آن‌ها از یک‌سو مستقیماً آسیب‌پذیری‌های منطق تجاری را با خودکارسازی و استانداردسازی فرایندها کاهش می‌دهند و ازسوی‌دیگر با فراهم‌کردن زیرساخت کدپایهٔ خودکار، بالاترین پتانسیل را برای پیاده‌سازی سازوکارهای واکنش خودکار به تهدیدات دارند. اجماع توزیع‌شده کم‌ترین اثر کل (۰٫۵۲۹) را داشت که احتمالاً به بلوغ نسبتاً کم‌تر این مؤلفه در پیاده‌سازی‌های فعلی ایران مرتبط است.

تحلیل ابعادی: کدام آسیب‌پذیری‌ها بیشتر کاهش می‌یابند؟

جدول ۵ نتایج مقایسه سطح آسیب‌پذیری در سازمان‌های با و بدون پیاده‌سازی بلاک‌چین را نشان می‌دهد. این تحلیل بر اساس تقسیم نمونه به دو گروه (بر اساس پرسش فیلتر اول پرسشنامه که سطح پیاده‌سازی بلاک‌چین را سنجید) انجام گرفت.

جدول ۵. مقایسه میانگین آسیب‌پذیری‌ها در سازمان‌های با پیاده‌سازی پایین و بالای بلاک‌چین

نوع آسیب‌پذیری	ضریب مسیر β	اندازه اثر (d)	درصد کاهش	میانگین پیاده‌سازی بالا	میانگین پیاده‌سازی پایین
حملات مرد میانی	۰/۶۳۴	۱٫۱۸	٪۶۰٫۶۰	۱٫۵۴	۳٫۹۱
تقلب در تراکنش‌ها	۰/۵۷۸	۱٫۰۹	٪۵۸٫۵	۱٫۶۱	۳٫۸۸
تهدیدات یکپارچگی داده	۰/۵۵۲	۱٫۰۳	٪۵۵٫۳	۱٫۶۸	۳٫۷۶
آسیب‌پذیری دسترسی	۰/۴۹۵	۰٫۹۱	٪۰٫۵۰	۱٫۹۲	۳٫۸۴

منبع: یافته‌های پژوهش (۱۴۰۴) تمامی تفاوت‌ها در سطح p < ۰۰۱٫۰ معنادار هستند.

نتایج جدول ۵ نشان می‌دهد که بزرگ‌ترین کاهش در حملات مرد میانی (۶۰٫۶ درصد) مشاهده می‌شود. این یافته با مبانی نظری کاملاً منطبق است: رمزنگاری نقطه‌به‌نقطه بلاک‌چین، امضای دیجیتال و احراز هویت غیرمتمرکز، دقیقاً سازوکارهای موردنیاز برای استراق سمع و جعل هویت در حملات مرد میانی را از بین می‌برند. این یافته با نتایج تاکاهاشی و ویلیامز (۲۰۲۳) که کاهش ۷۱ درصدی را در شبکه‌های پرداخت برون‌مرزی گزارش کردند، هم‌راستاست. کم‌ترین کاهش در آسیب‌پذیری‌های دسترسی (۰٫۵۰) درصد به این دلیل است که این دسته از آسیب‌پذیری‌ها عمدتاً به عوامل انسانی و سیاست‌های مدیریت هویت مرتبط‌اند که بلاک‌چین تأثیر کم‌تری بر آن‌ها دارد.

تحلیل نقش تعدیل‌کننده نوع معماری بلاک‌چین

در تحلیل تکمیلی، نقش تعدیل‌کننده نوع معماری بلاک‌چین (عمومی، خصوصی، کنسرسیومی) بررسی شد. نتایج آزمون اثر تعامل نشان‌داد که نوع معماری تعدیل‌کننده معناداری در رابطه بین بلاک‌چین و خودترمیمی امنیتی است (ضریب اثر تعامل = ۰٫۲۲۳، t = ۳/۸۷، p < ۰/۰۰۱). در این زمینه، سازمان‌هایی که از معماری کنسرسیوم استفاده می‌کنند، رابطه قوی‌تری بین بلاک‌چین و خودترمیمی تجربه می‌کنند. این یافته احتمالاً به‌دلیل توازن بهتر بین شفافیت برای شناسایی ناهنجاری و کنترل کافی برای پیاده‌سازی واکنش‌های خودکار در معماری کنسرسیوم است. این نتیجه با یافته‌های گارسیا-مورالس و همکاران (۲۰۲۴) که سازمان‌های کنسرسیومی را در بُعد خودترمیمی برتر از دیگران یافتند، سازگار است.

نتیجه پژوهش و پیشنهادها

تفسیر یافته‌ها و نظریه‌پردازی

یافته اصلی پژوهش حاضر، تأیید چهارگانه فرضیه‌هاست که جمعاً یک تصویر یکپارچه و غنی از چگونگی عملکرد بلاک‌چین برای تقویت امنیت سامانه‌های پرداخت ارائه می‌دهد. مهم‌ترین نوآوری، کشف نقش میانجی جزئی خودترمیمی امنیتی با شاخص واریانس تبیین‌شده توسط میانجی ۳/۴۲ درصد است. این یافته دلالت مهمی دارد: بلاک‌چین نه از یک مسیر، بلکه از دو مسیر موازی و مکمل بر امنیت تأثیر می‌گذارد. مسیر نخست مستقیم است: بلاک‌چین از طریق ویژگی‌های ذاتی معماری‌اش

(غیرمتمرکزسازی، تغییرناپذیری، رمزنگاری) نقاط ضعف ساختاری سامانه‌های پرداخت را برطرف می‌کند. مسیر دوم غیرمستقیم است: بلاک‌چین با ایجاد زیرساخت مناسب، ظرفیت خودترمیمی سامانه را ارتقاء می‌دهد و از این طریق توانایی سامانه برای مقابله پویا با تهدیدات جدید را افزایش می‌دهد.

این دوگانگی مسیر توضیح می‌دهد چرا در فراتحلیل لی و همکاران (۲۰۲۵)، وجود سازوکارهای خودترمیم ۱۱ درصد از ناهمگنی بین مطالعات را توضیح داد: مطالعاتی که سامانه‌های خودترمیم قوی داشتند، نتایج امنیتی بسیار بهتری گزارش کردند چون هر دو مسیر اثرگذاری فعال بودند. همچنین، این دوگانگی توضیح می‌دهد چرا پتروف و همکاران (۲۰۲۴) توانستند با بهبود صرف سازوکارهای خودترمیمی (بدون تغییر در معماری اصلی بلاک‌چین)، بهبود قابل‌توجه امنیتی را به دست آورند.

برتری قراردادهای هوشمند در میان ابعاد بلاک‌چین با اثر کل ۰٫۶۷۸ با نتایج کومار و شارما (۲۰۲۳) کاملاً سازگار است. تبیین نظری این برتری در چارچوب رایانش خودگردان کفهارت و چس (۲۰۰۳) قابل‌ارائه است: قراردادهای هوشمند اصل عدم نیاز به مداخله انسانی را در بالاترین سطح پیاده می‌کنند. آن‌ها نه‌تنها واکنش خودکار به تهدیدات را ممکن می‌سازند، بلکه با ازبین‌بردن نقاط تصمیم‌گیری انسانی (که معمولاً ضعیف‌ترین حلقه در زنجیره امنیتی هستند)، آسیب‌پذیری منطق تجاری را در ریشه می‌زنند.

پیشنهادهای کاربردی

پیشنهاد نخست: راهبرد پیاده‌سازی اولویت‌بندی‌شده. یافته‌های این پژوهش به‌وضوح نشان می‌دهد که قراردادهای هوشمند باید در اولویت اول سرمایه‌گذاری قرار گیرند. پیشنهاد می‌شود مؤسسات مالی در مرحله اول پیاده‌سازی، تمرکز خود را بر بازنویسی فرایندهای پرداخت کلیدی (تسویه، تطبیق و مدیریت استثنا) در قالب قراردادهای هوشمند قرار دهند.

پیشنهاد دوم: یکپارچه‌سازی لازمه موفقیت. با توجه به نقش میانجی معنادار خودترمیمی (واریانس تبیین‌شده توسط میانجی = ۴۲٫۳ درصد)، پیاده‌سازی بلاک‌چین بدون سامانه‌های هوشمند شناسایی و واکنش به تهدیدات، تنها ۵۷٫۷ درصد از بهره‌وری امنیتی ممکن را فراهم می‌آورد. توصیه می‌شود به‌موازات پیاده‌سازی بلاک‌چین،

سامانه‌های تشخیص ناهنجاری مبتنی بر یادگیری ماشین و قراردادهای هوشمند واکنشی برای خودکارسازی پاسخ به تهدیدات نیز مستقر شوند.

پیشنهاد سوم: اولویت‌بخشی به رمزنگاری کانال‌های ارتباطی. نظر به اینکه حملات مرد میانی بیش‌ترین کاهش را تجربه کردند (۶۰٫۶ درصد)، پیاده‌سازی لایه‌های رمزنگاری زنجیره‌ای در کانال‌های بین‌بانکی و بین کیف پول‌های دیجیتال، سریع‌ترین بازگشت سرمایه امنیتی را به همراه خواهد داشت.

پیشنهاد چهارم: سرمایه‌گذاری مکمل در مدیریت هویت دیجیتال. با توجه به اینکه آسیب‌پذیری‌های دسترسی کم‌ترین کاهش را نشان‌دادند (۰٫۵۰ درصد)، توصیه می‌شود پیاده‌سازی بلاک‌چین با راه‌حل‌های هویت غیرمتمرکز و احراز هویت چندعاملی ترکیب شود.

پیشنهاد پنجم: ترجیح معماری کنسرسیوم برای صنعت بانکی ایران. نتایج تحلیل تعدیل‌کننده نشان‌داد که معماری کنسرسیوم در تقویت خودترمیمی امنیتی مؤثرتر عمل می‌کند. این معماری به‌دلیل حفظ سطحی از کنترل نهادی (که برای تمکین رگولاتوری ضروری است) در عین برخورداری از مزایای توزیع‌شده، بهترین تناسب را با محیط نظارتی ایران دارد.

پیشنهاد ششم: برای سیاست‌گذاران، توصیه می‌شود که بانک مرکزی و سازمان‌های نظارتی چارچوب‌هایی طراحی کنند که قابلیت خودترمیمی مستند را به‌عنوان یکی از معیارهای اصلی صدور مجوز پلتفرم‌های پرداخت دیجیتال در نظر بگیرند. این رویکرد با یافته احمدی و نجفی (۱۴۰۴) که بر امنیت قابل آزمون تأکید داشتند، همسو است.

محدودیت‌های پژوهش و پیشنهادهای آتی

پژوهش حاضر با محدودیت‌هایی روبروست که باید در تفسیر نتایج در نظر گرفته شوند: نخست، اتکا به داده‌های خودگزارشی که احتمال سوگیری مطلوبیت اجتماعی را به همراه دارد؛ دوم، طرح مقطعی که امکان استنتاج علّی قوی را محدود می‌کند؛ سوم، محدودبودن نمونه به متخصصان ایرانی که تعمیم‌پذیری بین‌المللی را محدود می‌سازد؛ و چهارم، ناهمگنی سطح پیاده‌سازی واقعی بلاک‌چین در سازمان‌های مختلف نمونه که می‌توانست از طریق پرسش‌های عینی‌تر بهتر کنترل شود.

برای پژوهش‌های آتی پیشنهادهای زیر ارائه می‌گردد: (۱) مطالعه طولی برای تحلیل تغییرات آسیب‌پذیری در طول فرایند پیاده‌سازی بلاک‌چین؛ (۲) پژوهش مقایسه‌ای بین‌المللی برای بررسی اثر تعدیل‌کنندگی محیط رگولاتوری؛ (۳) استفاده از روش‌های تجربی شامل شبیه‌سازی حملات واقعی و اندازه‌گیری عینی شاخص‌های امنیتی؛ و (۴) بررسی نقش هوش مصنوعی تولیدی در تقویت خودترمیمی امنیتی شبکه‌های بلاک‌چین.

منابع و مراجع

الف) منابع فارسی

- احمدی، علیرضا و نجفی، سعید. (۱۴۰۴). نقش فنّاوری‌های دفتر کل توزیع‌شده در تقویت امنیت زیرساخت‌های مالی دیجیتال ایران: رویکرد رگولاتوری. فصلنامه امنیت‌پژوهی، ۲۳ (۹۲)، ۴۵-۷۲.
- تهرانی، محمدرضا و صادقی، حمید. (۱۴۰۲). بومی‌سازی مفهوم خودترمیمی امنیتی در بستر فنّاوری‌های مالی نوین ایران: مطالعه کیفی. فصلنامه مطالعات مدیریت فنّاوری اطلاعات، ۱۱ (۴۴)، ۸۷-۱۱۴.
- رضایی، محمد؛ کریمی، علی و زمانی، فاطمه. (۱۴۰۲). ارزیابی پیاده‌سازی بلاک‌چین در نظام بانکی ایران: چالش‌ها، فرصت‌ها و موانع سازمانی. فصلنامه پژوهش‌های مدیریت، ۱۵ (۵۸)، ۱۲۳-۱۵۸.
- محمدی، حسن و کریمی، رضا. (۱۴۰۳). تأثیر ویژگی‌های ساختاری بلاک‌چین بر کاهش حملات سایبری در سامانه‌های پرداخت ایران: آزمون مدل معادلات ساختاری. فصلنامه امنیت‌پژوهی، ۲۲ (۸۸)، ۳۱-۵۸.

ب) منابع انگلیسی

- Castro, M., & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems, 20(4), 398–461. https://doi.org/10.1145/571637.571640
- Chen, X., Liu, Y., Wang, Z., & Zhang, H. (2024). Blockchain and payment system security: A systematic review and meta-analysis. IEEE Transactions on Information Forensics and Security, 19(2), 1124–1141. https://doi.org/10.1109/TIFS.2024.3412561
- Diaconescu, A., Porter, B., Zschaler, S., & Blair, G. (2023). Architectures for autonomic computing and self-healing systems: A systematic review. ACM Computing Surveys, 55(8), 1–38. https://doi.org/10.1145/3571847
- Garcia-Morales, V., Jimenez-Barrionuevo, M., & Gutierrez-Gutierrez, L. (2024). A five-level security maturity model for blockchain payment platforms: Empirical evidence from 42 European organizations. Computers & Security, 140, 103712. https://doi.org/10.1016/j.cose.2024.103712
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2021). When to use and how to report results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
- Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, 36(1), 41–50. https://doi.org/10.1109/MC.2003.1160055
- Kumar, A., & Sharma, R. (2023). Smart contract-based payment fraud reduction: Empirical evidence from international payment networks. Journal of Financial Crime, 30(5), 1581–1599. https://doi.org/10.1108/JFC-09-2022-0218
- Li, M., Zhang, K., Wang, H., Chen, J., & Liu, T. (2025). Blockchain adoption and cybersecurity in financial services: A meta-analysis of 84 empirical studies (2019–2024). Computers & Security, 138, 103631. https://doi.org/10.1016/j.cose.2025.103631

- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
- Nakashima, T., & Liu, C. (2023). Decentralized vs. centralized payment platforms: A comparative security analysis against DDoS and MITM attacks. Computers & Security, 131, 103298. https://doi.org/10.1016/j.cose.2023.103298
- NIST. (2023). Cybersecurity framework version 2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
- Petrov, I., Kozlov, A., & Kovalenko, M. (2024). Self-healing algorithms for private blockchain security: Design and experimental evaluation. Future Generation Computer Systems, 152, 45–58. https://doi.org/10.1016/j.future.2024.01.023
- Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40(3), 879–891. https://doi.org/10.3758/BRM.40.3.879
- Takahashi, K., & Williams, S. (2023). Byzantine fault-tolerant consensus for cross-border payment security: Empirical reduction of man-in-the-middle vulnerabilities. Journal of Network and Computer Applications, 219, 103726. https://doi.org/10.1016/j.jnca.2023.103726
- Wang, J., Chen, R., Li, X., & Zhou, M. (2023). Centralized architecture vulnerabilities in digital payment systems: A large-scale empirical study. IEEE Access, 11, 52314–52328. https://doi.org/10.1109/ACCESS.2023.3278562
- Zamani, E., He, Y., & Phillips, M. (2024). Adaptive resilience: A theoretical framework for blockchain-based payment systems security assessment. International Journal of Information Management, 75, 102715. https://doi.org/10.1016/j.ijinfomgt.2024.102715
- Zhang, W., Chen, L., Huang, Y., Kim, J., & Park, S. (2023). Machine learning-integrated blockchain anomaly detection: Cross-bank evidence from five Asian countries. Expert Systems with Applications, 224, 120056. https://doi.org/10.1016/j.eswa.2023.120056