نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ پژوهشی

مدیریت ریسک در چارچوب حاکمیت اکوسیستم‌های مبتنی بر اعتماد دیجیتال [۱،۲]

رهی زندی‌فر [۳]

نشریه علمی حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال اول، پیاپی ۱، بهار و تابستان ۱۴۰۴
صص ۵۲ - ۸۰

تاریخ دریافت: ۱۴۰۳/۱۱/۲۹
تاریخ بازنگری: ۱۴۰۴/۰۵/۱۸
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۱

چکیده

در اقتصاد دیجیتال، موفقیت سازمان‌ها وابسته به ایجاد روابط و تعاملات ارزشمند و قابل‌اعتماد است. تدوین الگویی جامع و چابک برای شکل‌دهی و تقویت اعتماد دیجیتال میان ذینفعان، برای شکل‌دهی اکوسیستم‌های دیجیتال تاب‌آور و پایدار ضروری است. هدف پژوهش حاضر، بررسی اکوسیستم اعتماد دیجیتال و ارائه چارچوبی برای حاکمیت اکوسیستمی می‌باشد. در این راستا، ابتدا تمایز میان اعتماد دیجیتال و امنیت دیجیتال تبیین شده و سپس از چارچوب اکوسیستم اعتماد دیجیتال استفاده شده است. این چارچوب شامل شاخص‌ها و کنترل‌هایی است که قابل‌سفارشی‌سازی بر اساس نیازهای هر اکوسیستم بوده و در حاکمیت متمرکز و غیرمتمرکز به کار می‌رود. هرم سلسله‌مراتبی چارچوب شامل شش لایه است: گره‌ها، دامنه‌ها، عوامل اعتماد، روش‌ها، فعالیت‌ها و نتایج. در این مدل، مدیریت ریسک به عنوان یکی از عوامل کلیدی اعتماد در دامنه هدایت و پایش عمل می‌کند. این دامنه، خود به عنوان پل ارتباطی میان بعد سازمانی و فرایندی در نظر گرفته می‌شود. در پژوهش، پس از تبیین سه لایه نخستین هرم، نتایج تحقیقات کاربردی برای لایه‌های چهارم و پنجم، به ترتیب، شامل روش‌ها و فعالیت‌های مدیریت ریسک بر مبنای استاندارد ایزو ۲۷۰۰۵ ارائه شده است.

واژه‌های کلیدی: *اعتماد دیجیتال، اکوسیستم دیجیتال، مدیریت ریسک، حاکمیت اکوسیستمی، هدایت و پایش، چارچوب اکوسیستم اعتماد دیجیتال.*

طبقه‌بندی موضوعی: *M15, G34, D81*

---

[1] https://doi.org/10.22034/JISTA.2025.506948.1017

۲. مقاله منتخب دومین کنگره حسابرسی فناوری اطلاعات و اعتماد دیجیتال

[۳] دانشجوی دکتری مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، دانشگاه تربیت‌مدرس، تهران، ایران. Email: zandifar.rahi@modares.ac.ir

مقدمه

اعتماد، سنگ بنای روابط انسانی و ساختارهای اجتماعی است. اعتماد، به معنای اطمینانی است که یک فرد نسبت به دیگری دارد، مبنی بر اینکه او مطابق با انتظارات عمل کرده و به تعهدات خود پایبند خواهد بود. اعتماد، همکاری را تسهیل می‌کند و عدم قطعیت را کاهش می‌دهد و احساس امنیت ایجاد می‌نماید. اعتماد از طریق ثبات، صداقت و درک متقابل شکل می‌گیرد. ایجاد و حفظ اعتماد دیجیتال[1] شامل جنبه‌های بیشتری نسبت به دنیای سنتی است، زیرا ارتباطات دیجیتال علاوه‌بر انسان‌ها و روابط بین آن‌ها به اجزای دیجیتال اتکا دارند (پاکدل و همکاران، ۱۴۰۲). برای همه اشخاص و ذی‌نفعان، اعتماد دیجیتال، مفهوم یکتایی محسوب نمی‌شود(استرازولو[2]، ۲۰۲۴). اعتماد دیجیتال به معنای اطمینان به اتکاپذیری، یکپارچگی و امنیت سیستم‌های دیجیتال است. عنصر اصلی در اعتماد دیجیتال، تعاملات[3] است. یکی از جنبه‌های حیاتی در صنعت ۴.۰ و ۵.۰، اعتماد دیجیتال است(چاترجی و همکاران[4]، ۲۰۲۳). انقلاب‌های صنعتی به دنبال ایجاد جامعه‌ای دیجیتالی هستند که در آن ماشین‌ها و انسان‌ها، با یکدیگر تعامل کنند. تحلیل کامل مسائل و پیامدهای اعتماد در سطوح مختلف سازمانی، از جمله راهبردها، فرایندها و راه‌حل‌های فنی، به ضروریتی در طراحی سیستم‌های اجتماعی-فنی تبدیل شده است (ریچکووا و همکاران[5]، ۲۰۲۳). مفاهیمی نظیر تجارت الکترونیکی، ارتباطات دیجیتال و دموکراسی دیجیتال، عنایت به موضوع اعتماد را ضروری کرده است(چاترجی و همکاران، ۲۰۲۳).

ظهور فناوری‌های نوین، باعث تحولات بر افکنانه‌ای شده که تغییرات جدی و اساسی در مدل‌های کسب‌وکار را به همراه داشته و ماهیت فرایندی و عملیات کسب‌وکار را تغییر داده و ساختار بازارها، ماهیت تعاملات بین بازیگران مختلف اکوسیستم‌های کسب وکاری را متحول کرده است. در این رویکرد، اعتماد دیجیتال می‌تواند سبب تواناسازی کاربران شود و در برابر، مشتریان با همکاری و ارزش‌آفرینی خود به اعتماد دیجیتال ارزش مضاعفی می‌بخشند. در صورتی که اعتماد دیجیتال نقض شود، می‌تواند عواقب گسترده‌ای به دنبال داشته باشد و اثراتی

[1] Digital Trust
[2] Strazzullo
[3] Collaboration
[4] Chatterjee et al.
[5] Rychkova et al.

دائمی بر جای بگذارد که به‌سختی قابل جبران هستند. عامل اعتماد، جایگاه مهمی در سرمایه اجتماعی و سازوکارهای حکمرانی بین‌شرکتی دارد. اعتماد، عنصری حیاتی برای موفقیت اقتصادی است که می‌تواند چرخ‌های اکوسیستم را روغن‌کاری و توسعه آن را مقیاس‌پذیر کند (آگویار و همکاران[1]، ۲۰۲۳). درک اهمیت قابل‌اعتماد بودن ارتباطات دیجیتال، برای ایجاد روابط سازنده بین ارائه‌دهندگان محصولات، مصرف‌کنندگان و شرکا ضروری است. در روابط بین‌شرکتی، اعتماد به شرکا باعث افزایش تعهدات فیمابین و موجب استحکام همکاری‌های بین‌سازمانی می‌شود (شهزاد و حافیظ[2]، ۲۰۲۲). اعتماد در شبکه‌های بین‌شرکتی می‌تواند به‌عنوان سازوکاری غیرقراردادی تلقی شود (شهزاد و حافیظ، ۲۰۲۲). برای شکل‌دهی اکوسیستم اعتماد دیجیتال[3] نیاز به پیاده‌سازی ضوابط حفاظتی است. تغییرات در صنعت، پایگاه‌های کاربری، فناوری، مدل‌های کسب‌وکاری یا راهبردهای اکوسیستمی سبب می‌شود که ضوابط حفاظتی به‌طور مداوم نظارت و تطبیق داده شوند (آگویار و همکاران، ۲۰۲۳).

این پژوهش، با بررسی تمایز میان اعتماد دیجیتال، امنیت دیجیتال و اعتماد صفر، آغاز شده و جایگاه اعتماد دیجیتال را در اکوسیستم‌های فناورانه مشخص می‌کند. سپس، بوم‌سازگان اعتماد دیجیتال و ارکان آن مورد مطالعه قرار گرفته و چالش‌ها و مخاطرات آن تحلیل می‌شود. در پاسخ به این چالش‌ها، پژوهش حاضر از چارچوب اکوسیستم اعتماد دیجیتال (دی.تی.ئی.اف[4]) به‌عنوان مدلی جامع بهره گرفته است که ابعاد فرایندی، انسانی، سازمانی و فناوری را پوشش می‌دهد(ایساکا[5]، ۲۰۲۴). در این راستا، چارچوبی سلسله مراتبی برای حاکمیت اکوسیستمی مبتنی بر اعتماد دیجیتال مد نظر قرار می‌گیرد که در آن، عوامل کلیدی اعتماد شناسایی می‌شود. اهمیت این پژوهش در آن است که به یکی از حیاتی‌ترین ابعاد اکوسیستم‌های دیجیتال، یعنی مدیریت ریسک در بستر اعتماد دیجیتال می‌پردازد. در بخش روش‌شناسی پژوهش، فرایند استخراج و طراحی روش‌ها و فعالیت‌های مدیریت ریسک بر اساس استاندارد ایزو ۲۷۰۰۵ تشریح می‌شود. در بخش یافته‌های پژوهش نشان داده می‌شود که ادغام چارچوب دی.تی.ئی.اف با استانداردهای بین‌المللی مدیریت ریسک می‌تواند به بهبود تاب‌آوری

[1] Aguiar et al.
[2] Shahzad & Hafeez
[3] Digital Trust Ecosystem (DTE)
[4] Digital Trust Ecosystem Framework (DTEF)
[5] Information Systems Audit and Control Association (ISACA)

سیستم‌ها، افزایش اعتماد ذی‌نفعان و تقویت سازگاری سازمانی منجر شود. در نهایت، با تبیین نقش مکمل چارچوب‌های دی.تی.ئی.اف و کوبیت[1] نسبت به یکدیگر نشان داده می‌شود که ترکیب هم‌زمان این دو می‌تواند یک مدل حاکمیتی یکپارچه برای مدیریت اکوسیستم‌های اعتماد دیجیتال ارائه دهد. انسجام میان مبانی نظری، روش‌شناسی و یافته‌های پژوهش، مسیر روشنی را برای توسعه رویکردهای عملیاتی جهت بهبود اکوسیستم اعتماد دیجیتال ترسیم می‌کند.

مبانی نظری

تمایز اعتماد دیجیتال، امنیت دیجیتال و اعتماد صفر

تمرکز اصلی اعتماد دیجیتال، بر اطمینان‌بخشی کاربران و قراردادهای اخلاقی است. همکاری با شرکت‌های دیگر به عنوان یکی از جنبه‌های مهم در چرخه عمر عملیاتی هر شرکت است و منجر به ایجاد معاملات اقتصادی موفق و دستیابی به وضعیت «برد–برد» برای همه مشارکت‌کنندگان می‌شود. اعتماد دیجیتال توسط ارزش‌های سازمانی و تلاش‌های رهبران سازمان هدایت می‌شود. اعتماد به یکباره به دست نمی‌آید، بلکه از طریق رعایت مداوم اصول حکمرانی و عملیاتی قوی ساخته و تقویت می‌شود. عناصر کلیدی اعتماد دیجیتال شامل یکپارچگی داده‌ها و رعایت حریم خصوصی از طریق طراحی، انطباق، حاکمیت، و ارزیابی اعتمادپذیری[2] می‌شود (روی[3]، ۲۰۲۴). کاربست فناوری‌های انقلاب‌های صنعتی اخیر، باعث تسهیل همکاری‌های معتبر در اکوسیستم‌ها می‌شوند. اعتماد دیجیتالی که توسط این فناوری‌ها در طول زنجیره تأمین شرکت ایجاد می‌شود، احتمال نوآوری را افزایش می‌دهد (شهزاد و حافیظ، ۲۰۲۲). استفاده از فناوری‌های دیجیتال از جمله اینترنت اشیاء (اینترنت چیزها[4])، هوش مصنوعی، واقعیت افزوده یا واقعیت مجازی، بلاک‌چین، رباتیک و اتوماسیون نقش بی‌بدیل اعتماد را در عملیات کسب‌وکاری امروزی برجسته می‌کند (استرازولو، ۲۰۲۴).

اعتماد دارای دو جنبه اجتماعی و فنّی است. در رویکرد اجتماعی، اعتماد به اعتمادشونده[5] (متولی) به‌عنوان تابعی از توانایی، خیرخواهی، صداقت اعتمادشونده و تمایل اعتمادکننده به

[1] Control Objectives for Information and Related Technologies (COBIT)
[2] Trustworthiness Assessment
[3] Roy
[4] The Internet of Things (IoT)
[5] Trustee

اعتماد تعریف می‌شود. این عوامل به زمینه و ماهیت تعاملات میان اعتمادکننده و متولی بستگی دارند. در رویکرد فنی اعتماد دیجیتال، بر قابلیت‌های استفاده، وظیفه‌مندی، کمک‌دهی، اتکاپذیری و اعتبارپذیری اطلاعات، سفارشی‌سازی و تطبیق‌پذیری تأکید می‌شود. اعتمادپذیری در این حوزه شامل حفظ حریم خصوصی، امنیت، شفافیت، قابلیت ردیابی و کنترل می‌شود(ریچکووا و همکاران، ۲۰۲۳).

اعتمادپذیری در سیستم‌های اجتماعی-فنّی، معمولاً از منظر مهندسی الزامات (نیازمندی‌ها) بررسی می‌شود. انتظارات اعتمادکننده[1] به اعتمادشونده را می‌توان به‌عنوان الزامات اعتمادپذیری[2] تبیین کرد. این الزامات شامل ویژگی‌های عملیاتی، عملکردی، غیرعملکردی و طراحی است (ریچکووا و همکاران، ۲۰۲۳). به علاوه، این الزامات به‌عنوان طبقه ویژه‌ای از الزامات کیفیتی یا نرم[3] تعریف می‌شوند و اعتماد را با مفاهیم دیگر مانند توانمندی، آسیب‌پذیری و ریسک مرتبط می‌کند. به‌عنوان نمونه، عواملی نظیر فرهنگ شرکت، ارزش‌ها و مدل کسب‌وکار شرکت بر موفقیت پیاده‌سازی هوش مصنوعی در یک اکوسیستم مبتنی بر اعتماد تأثیر دارند (بیکربرون‌بائر[4]، ۲۰۲۱). در کنار اعتماد دیجیتال، امنیت دیجیتال[5] اهمیت پیدا می‌کند. امنیت دیجیتال، به‌عنوان یک عنصر بنیادین، به محافظت از دارایی‌های دیجیتال، سیستم‌ها و داده‌ها در برابر تهدیدات اختصاص دارد. تدابیر امنیت سایبری شامل مدیریت فایروال‌ها، نرم‌افزارهای ضدویروس، سیستم‌های شناسایی و پیشگیری از نفوذ و سایر ابزارهای امنیتی است (مالیک[6]، ۲۰۲۴).

ارتباط و وابستگی متقابل بین مفاهیم اعتماد و امنیت، ماتریس اصلی تحول در اقتصاد دیجیتال را تشکیل می‌دهد. امنیت، به عنوان یکی از ارکان اعتماد دیجیتال محسوب می‌شود (چاترجی و همکاران، ۲۰۲۳). رابطه بین این دو مفهوم به دلیل چندبعدی بودن اعتماد، غیرخطی است. در روسیه، علیرغم وجود سامانه‌های اطلاعاتی مجهز به امنیت، سطح اعتماد عموم مردم به محصولات دیجیتالی پایین است(کولووا[7]، ۲۰۲۰). معماری‌های مبتنی بر اعتماد صفر[8]، توانسته‌اند

[1] Trustor
[2] Trustworthiness Requirements (TwR)
[3] Soft requirements (SR)
[4] Baker-Brunnbauer
[5] Digital Security
[6] Malik
[7] Kulova
[8] Zero-Trust

رابطه بین این دو مفهوم را به صورت درهم‌تنیده‌ای تقویت کنند. اعتماد صفر، بر اصل «به هیچ‌چیز اعتماد نکن، همه‌چیز را تصدیق کن[1]» متمرکز است (روی، ۲۰۲۴). رویکرد این مدل، بر پایه اعتماد نکردن به هیچ کاربر یا دستگاهی شکل گرفته و برای تأمین امنیت، کنترل‌های سختگیرانه اعمال می‌کند (هزم[2]، ۲۰۲۳). اجزای کلیدی مدل اعتماد صفر شامل امنیت مبتنی بر هویت، نظارت مستمر، بخش‌بندی خرد و اجرای پویا و تطبیقی سیاست‌ها می‌شود (روی، ۲۰۲۴). اعتماد دیجیتال برای تقویت تعاملات مثبت، انجام تراکنش‌های روان و حفظ اعتماد کاربران به پلتفرم‌های دیجیتال ضروری است (روی، ۲۰۲۴). چارچوب‌های قانونی مانند جی.دی.پی.آر[3]، هیپا[4] و استانداردهای ایزو به استقرار اعتماد دیجیتال کمک می‌کنند.

بوم‌سازگان اعتماد دیجیتال

مفهوم «بوم‌سازگان» به‌طور فزاینده‌ای در مدیریت داده‌ها، نوآوری و راهبرد کسب‌وکار به کار می‌رود. مترادف‌های دیگر این مفهوم، «زیست‌بوم» یا «اکوسیستم» است. دو ویژگی اصلی اکوسیستم‌های طبیعی که در اغلب رشته‌های علمی و تخصصی بکار گرفته شده‌اند، ارتباط متقابل و رقابت است. برخی از ویژگی‌های اکوسیستم‌های طبیعی نظیر تاب‌آوری، تنوع و سازوکارهای پایداری عمدتاً نادیده گرفته می‌شوند. اکوسیستم اعتماد دیجیتال، به شبکه‌ای از موجودیت‌ها اطلاق می‌شود که برای ایجاد اعتماد و تسهیل تراکنش‌های امن بدون نیاز به واسطه‌های شخص ثالث استفاده می‌کنند. چنین اکوسیستمی از ویژگی‌های اکوسیستم‌های طبیعی برخوردار است و مهمتر از همه، لازم است که از یک سازوکار درونی برای مقابله با بهره‌برداری بیش از حد برخوردار باشد. برای غلبه بر نااطمینانی و توزیع نامتقارن اطلاعات در تعاملات و محیط‌های دیجیتال، اعتماد ضروری است (رینرز[5]، ۲۰۲۲). تا پایان سال ۲۰۲۲، حدود ۵۸ درصد از فروش‌های انجام گرفته در ایالات متحده به‌طور جزئی یا کامل در یک اکوسیستم دیجیتال انجام شده است (بالان[6]، ۲۰۲۳).

[1] Trust nothing, Verify everything
[2] Hazam
[3] General Data Protection Regulation (GDPR)
[4] Health Insurance Portability and Accountability Act (HIPAA)
[5] Reiners
[6] Balan

برای شکل‌دهی مدل‌های حکمرانی جدید در اکوسیستم، از اعتماد استفاده می‌شود. در اکوسیستم دیجیتال، همه چیز حول مولفه کلیدی و محوری اعتماد می‌چرخد(بالان، ۲۰۲۳). اعتماد، یک تواناساز حیاتی در تعاملات کسب‌وکار است که به همکاری مؤثر، استفاده بهینه از منابع، رفتارهای تطبیقی و تلاش جمعی به سمت اهداف مشترک کمک می‌کند (ریچکووا و همکاران، ۲۰۲۳). این نوع از اکوسیستم، یک شبکه همکاری میان کسب‌وکارها، دولت‌ها، افراد و دستگاه‌ها ایجاد می‌کند که دستیابی به اهداف مشترک را از طریق ابزارهای دیجیتال و فناورانه محقق می‌کند. پیامدهای نادیده گرفتن اعتماد دیجیتال می‌تواند اثرات بسیار شدیدی نظیر ناکارآمدی، استثمار و کاهش اطمینان کاربران را به همراه داشته باشد.

اجزای کلیدی اکوسیستم دیجیتال، شامل مشارکت‌کنندگان، پلتفرم‌ها و اهداف مشترک است (بالان، ۲۰۲۳). مشارکت‌کنندگان شامل افراد، شهروندان، مشتریان، کاربران، دولت‌ها و نهادها، شرکت‌ها و کسب‌وکارهای مختلف و حتی دستگاه‌ها می‌شوند. پلتفرم‌های دیجیتالی و اشتراکی، نیز نقش اساسی در شکل‌گیری اکوسیستم‌های دیجیتالی دارند. از جمله اهداف مشترک در چنین اکوسیستم‌هایی می‌تواند به صورت زنجیره تأمین امن، فراهم‌آوری مدارک ضد جعل، مبارزه با کالاهای تقلبی، ساده‌سازی اسناد تجاری، و تأمین هویت‌های دیجیتال امن تجلی یابد.

هدف از ایجاد فرهنگ اعتماد دیجیتال، شکل‌گیری روابطی طولانی‌مدت بر اساس درک و احترام متقابل است. سرمایه‌گذاری در برقراری چنین روابطی، اولویت اول تمام سازمان‌هایی است که می‌خواهند در بازار رقابتی امروز باقی بمانند. تمایل بیشتر کسب‌وکارها به نوآوری باز، نقش اعتماد دیجیتال را ضروری کرده است. برخلاف کسب‌وکارهای ساده، در کسب‌وکارهای اکوسیستمی و شبکه‌ای، اعتماد و شفافیت نمی‌تواند منفرداً محقق شوند. با ایجاد اکوسیستمی که در آن تمام مشارکت‌کنندگان از قوانین و استانداردهای پذیرفته‌شده در زمینه ایمنی، امنیت، حریم خصوصی و اخلاق پیروی می‌کنند، اعتماد دیجیتال می‌تواند به دوران جدیدی از همکاری‌ها و تعاملات منجر شود. بزرگترین مانع برای تحول دیجیتال، فقدان اعتماد مشتری است که می‌تواند به اشکال مختلفی نمایان شود (دیجیتال‌سویتزرلند[1]، ۲۰۲۲).

[1] Digitalswitzerland

علاوه بر اعتماد، مفاهیم بی‌اعتمادی[1] و قدرت نیز در جهت‌دهی چنین اکوسیستم‌هایی موثر هستند. لازم است مفهوم بی‌اعتمادی در ادبیات موضوعی به‌عنوان مفهومی مستقل و زیرمجموعه‌ای از اعتماد در نظر گرفته شود (رینرز، ۲۰۲۲). حاکمیت پلتفرمی ممکن است باعث عدم تعادل و توازن قدرت بین بازیگران اکوسیستم شود. نامتوازن بودن قدرت بین ارائه‌دهنده پلتفرم و کاربران، می‌تواند علت تضعیف اعتماد باشد (رینرز، ۲۰۲۲). یکی از اهداف نوین در اکوسیستم اعتماد دیجیتال، حذف نیاز به تشکیلات متمرکز و واسطه‌های مرکزی است. این موضوع باعث می‌شود تراکنش‌ها سریع‌تر، ارزان‌تر، شفاف‌تر و امن‌تر شوند.

اکوسیستم‌های اعتماد دیجیتال در صنایع مختلفی کاربرد دارند. به‌عنوان نمونه، یک سیستم زنجیره تأمین می‌تواند از توسعه بلاکچین برای ردیابی کالاها و پرداخت‌ها در زنجیره ارزش استفاده کند. استفاده از این روش، اعتماد میان موجودیت‌هایی را امکان‌پذیر می‌سازد که ممکن است حتی یکدیگر را نشناسند یا به هم اعتماد نداشته باشند. اکوسیستم اعتماد دیجیتال، می‌تواند همانند پل محافظت‌شده‌ای، اطلاعات رمزنگاری‌شده را انتقال دهد. فناوری بلاکچین با ماهیتی غیرمتمرکز، غیرقابل تغییر و شفاف می‌تواند چنین اکوسیستمی را متحول کند. ویژگی‌های امنیتی ذاتی زنجیره بلوکی، از جمله رمزنگاری[2]، دفترهای توزیع‌شده[3] و قراردادهای هوشمند[4]، زنجیره‌ای از اعتماد را فراهم می‌کنند. این تغییر پارادایم، تحولات اساسی در صنایعی همچون بهداشت و درمان، زنجیره تأمین، مالی و غیره ایجاد کرده است. بیت‌کوین به‌عنوان نمونه‌ای از بکارگیری بلاکچین نشان می‌دهد که بدون نیاز به یک عنصر مرکزی، چگونه تراکنش‌های تجاری به صورت غیرمتمرکز انجام می‌شود (کایا[5]، ۲۰۲۵). در دوره بیماری کووید ۱۹، برخی از کشورها توانستند اکوسیستم اعتماد دیجیتالی را ایجاد کنند که احراز هویت گواهی‌های دریافت واکسن نزد شهروندان را ممکن می‌ساخت. به عنوان نمونه دیگر، بر اساس تصمیمات راهبردی شورای فدرالی در اواخر سال ۲۰۲۱ در سوییس، اکوسیستمی مبتنی بر هویت الکترونیکی[6] ایجاد شد که بر اساس زیرساخت‌های دولتی و مطابق با اصول هویت خودمختار[7]

[1] Distrust
[2] Cryptography
[3] Distributed Ledgers
[4] Smart Contracts
[5] Kaya
[6] e-ID
[7] Self-Sovereign Identity (SSI)

و تمرکز بر حفاظت از داده‌ها، رعایت حریم خصوصی، کمینه‌سازی داده‌ها و ذخیره‌سازی غیرمتمرکز عمل می‌کرد. در این سیستم، هویت الکترونیکی به عنوان اصلی‌ترین اعتبار قابل تأیید[1] به کیف پول دیجیتال متصل می‌شد (دیجیتال‌سویتزرلند، ۲۰۲۲). سیستم‌های اعتماد داده خودمختار[2] نمونه دیگری است که با استفاده از محیط اوپن دی.اس.یو[3] برای مقابله با مسائل مربوط به حفظ حریم خصوصی و محرمانگی طراحی و آزمایش شده‌اند. فناوری اوپن دی.اس.یو برای مدیریت تبادل داده‌های حساس به حریم خصوصی در پلتفرم‌های باز شهر هوشمند بکار گرفته شده است. این فناوری، به ایجاد محیط‌هایی امن‌تر و شفاف‌تر برای مدیریت و تبادل داده‌های دیجیتال کمک کرده است (بالان، ۲۰۲۳). در پلتفرم‌های متمرکز دیجیتالی معمولاً سود و ارزش قابل توجهی برای نهاد کنترل‌گر مرکزی حاصل می‌شود که می‌تواند به کنترل‌گری بازارهای جهانی و انحصارطلبی منجر شود (کایا، ۲۰۲۵). برای کاهش این مشکلات، اکوسیستم‌های غیرمتمرکزی شکل گرفت که قدرت تصمیم‌گیری را به‌طور عادلانه‌تری بین ذی‌نفعان توزیع می‌کند.

اکوسیستم‌های دیجیتالی با بکارگیری فناوری‌های نوین می‌توانند حاکمیت غیرمتمرکز را ممکن سازند. در اکوسیستم‌های سنتی، شرکت‌ها به صورت سلسله‌مراتبی توسط هیئت مدیره و سهامداران کنترل می‌شوند. اما در اکوسیستم‌های همتا به همتا، حاکمیت به روش جدیدی از مذاکره بین مشارکت‌کنندگان تبدیل می‌شود. در حاکمیت غیرمتمرکز، نهادها خود قوانین را تعیین و درباره آن‌ها تصمیم‌گیری می‌کنند. این نوع از حاکمیت می‌تواند به توزیع قدرت و تصمیم‌گیری عادلانه‌تر و پایدارتری کمک کند (کایا، ۲۰۲۵). حاکمیت اکوسیستمی[4] می‌تواند بر پایه حاکمیت غیرمتمرکز مستقر شود و اعتماد را مقیاس‌پذیر سازد. حکمرانی اکوسیستمی، می‌تواند به صورت فراملی در چارچوب توافقات دوجانبه یا چندجانبه و حتی بین‌المللی شکل گیرد.

به منظور اجرای مناسب حکمرانی اکوسیستمی لازم است پیوند میان سطوح محلی و جهانی اکوسیستم، مدیریت و تسهیل مشارکت و تعامل بین ذینفعان، تعادل بین همکاری و رقابت از

[1] Verifiable Credential (VC)
[2] Self-Sovereign Data Trust Systems
[3] Data-Sharing Unit (DSU)
[4] Ecosystem Governance

طریق ایجاد ساختارهای انگیزشی و ترویج فرهنگ گزارش‌دهی شفاف، تشویق شوند (هرزوگ و همکاران[1]، ۲۰۲۴). از جمله اهداف این نوع از حاکمیت، توزیع مسئولیت‌های اخلاقی و ترسیم چشم‌انداز اخلاقی مشترک، ایجاد ساختارهای حکمرانی مبتنی بر پلتفرم، برقراری تعادل میان تلاش‌های نهادی با رویکرد غیرمتمرکز است. لازم است به تعریف ارزش‌ها، مسئولیت‌های اجتماعی و فنی و دیگر جنبه‌های پلتفرمی برای حمایت فرعی، عملیاتی و راهبردی از نوآوری‌های مسئولانه پرداخته شود و بر اهمیت اجتناب از دخالت و اختلال در روابط اعتمادمحور تأکید شود (هرزوگ و همکاران، ۲۰۲۴). در این راستا، چارچوب‌های متعددی برای ایجاد حکمرانی اکوسیستمی ایجاد شده است. طبق آینده‌پژوهی انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی(ایساکا)، بیش از نیمی از سازمان‌ها معتقدند که داشتن یک چارچوب اعتماد دیجیتال برای سازمان بسیار مهم است. طبق تحقیقات این موسسه، مزایای اعتماد دیجیتال منجر به بهبود شهرت مثبت در حدود ۷۱ درصد، داشتن داده‌های قابل اطمینان‌تر برای تصمیم‌گیری نزدیک به ۶۰ درصد و کاهش نقض حریم خصوصی در حدود ۶۰ درصد، رویدادهای امنیت سایبری در حدود ۵۹ درصد، و افزایش وفاداری مشتریان نزدیک به ۵۶ درصد شده است (ایساکا، ۲۰۲۴). به‌عنوان نمونه، چارچوب دی.تی.ئی.اف، توسط همین انجمن منتشر شده است که سازمان‌ها را با بهترین روش‌ها و راهنمایی‌های لازم برای یکپارچه‌سازی اعتماد دیجیتال تجهیز می‌کند. این چارچوب می‌تواند راهبردهای محصول و ابتکارات را با رویکردی متمرکز بر اعتماد شکل دهد و رقابت‌پذیری و شهرت را بهبود بخشد. این چارچوب توانسته با بهره‌گیری امن از فناوری، افزایش همکاری، کاهش زمان واکنش به رویدادهای غیرمنتظره، تمرکز بر مدیریت برند و بهبود عملکرد مالی، بستری مبتنی بر اعتماد در اختیار سازمان‌ها قرار دهد(ایساکا، ۲۰۲۴). این چارچوب در مدیریت پورتفولیوی منابع به سازمان‌ها کمک می‌کند تا اعتمادپذیری و شهرت خود را بهبود دهند و به اجزای کلیدی اعتماد دیجیتال یعنی صحت، امنیت، حریم خصوصی، تاب‌آوری، کیفیت، اطمینان و اعتماد رسیدگی کنند.

چارچوب اکوسیستم اعتماد دیجیتال (دی.تی.ئی.اف) نقشه‌راه جامعی برای سازمان‌ها فراهم می‌آورد تا روابط و فرایندهای تسهیلگرانه‌ای برای کسب‌وکار تعیین کنند. با بکارگیری چنین چارچوبی، موانع تعاملاتی کاهش یافته و وفاداری مشارکت‌کنندگان تقویت می‌شود و می‌توان

[1] Herzog et al.

انتظار داشت که ارزش مشترکی در اکوسیستم خلق شود. این چارچوب به گونه‌ای طراحی شده است که با طیف وسیعی از چارچوب‌ها نظیر کوبیت، آی.تی.آی.ال[1]، جی.دی.پی.آر، و استانداردهای مختلف ایزو و ان.آی.اس.تی (نیست)[2] سازگار باشد(توماس و همکاران[3]، ۲۰۲۴). یافته‌های بیکربرون‌بائر چارچوب دیگری برای پیاده‌سازی هوش مصنوعی قابل اعتماد (تی.ای.آی.آی[4]) ارائه می‌کند که اصول اخلاقی، ارزش‌های شرکت، مدل‌های کسب‌وکار و جنبه‌های عمومی مانند اهداف توسعه پایدار و اعلامیه جهانی حقوق بشر را در نظر می‌گیرد (بیکربرون‌بائر، ۲۰۲۱).

مخاطرات و چالش‌های بوم‌سازگان اعتماد دیجیتال

رشد فناوری باعث ظهور نوآوری‌های برافکنی شده است که مفهوم زنجیره ارزش را به یک اکوسیستم دیجیتال تبدیل می‌کند. هر شرکت نوعی می‌تواند از منابع دیگر شرکت‌ها، به‌عنوان بخشی از زنجیره ارزش خود استفاده کنند بدون اینکه لزوماً مالک آن‌ها باشند. بنابراین، به دلیل حضور عوامل خارجی که نمی‌توان به‌طور مستقیم آن‌ها راکنترل کرد، مخاطرات بیشتری محتمل می‌شود(فیرداوس و توبینگ[5]، ۲۰۲۲). شناسایی و تحلیل مسائل اعتماد بین مشارکت‌کنندگان در اکوسیستم‌های کسب‌وکار دیجیتال[6] یک وظیفه حیاتی است که تأثیر بزرگی بر پایداری و تاب‌آوری آن‌ها دارد. این وظیفه نیاز به روش‌های عملی و مدل‌سازی مناسب سازمانی دارد (ریچکووا و همکاران، ۲۰۲۳). ۸۶ درصد از اکوسیستم‌های موفق، سازوکارهای اعتماد را به‌طور فعال در نظام‌ها و رویه‌های خود تعبیه کرده‌اند(آگویار و همکاران، ۲۰۲۳). در دنیای دیجیتال، ریسک‌های متعددی وجود دارد. ریسک‌های امنیت سایبری می‌توانند باعث از دست رفتن داده‌ها، اختلال در خدمات و از دست رفتن اعتماد مشتریان شوند. عدم مدیریت ریسک‌های مرتبط با حریم خصوصی (شامل دسترسی غیرمجاز به داده‌های حساس یا جمع‌آوری و استفاده از اطلاعات شخصی بدون رضایت) موجب افشای اطلاعات شخصی و حساس می‌شوند.

[1] Information Technology Infrastructure Library (ITIL)
[2] National Institute of Standards and Technology (NIST)
[3] Thomas et al.
[4] Trustworthy Artificial Intelligence Implementation (TAII)
[5] Firdaus & Tobing
[6] Digital Business Ecosystem (DBE)

ریسک‌های شهرت مانند پوشش منفی در شبکه‌های اجتماعی می‌توانند به شهرت شرکت آسیب برسانند و منجر به از دست رفتن اعتماد مشتریان و کاهش فروش شوند (چاترجی و همکاران، ۲۰۲۳). به‌عنوان نمونه، علی‌رغم بهبودها و بهینه‌سازی‌های کسب‌وکاری که هوش مصنوعی با خود به همراه آورده است، در بسیاری از موارد، می‌تواند ریسک را افزایش دهد. این احتمال وجود دارد که بازیگران مخرب از هوش مصنوعی برای اهداف شرورانه استفاده کنند.

ضوابط حفاظتی برای حفاظت از طرفین در تراکنش‌ها یا تعاملات اکوسیستمی و کاهش آثار منفی آن در نظر گرفته می‌شوند. تعداد کم آن‌ها می‌تواند رشد اکوسیستم را محدود کند. اعتماد کم به این ضوابط، ریسک رفتارها و نتایج نامطلوب از جمله اصطکاک بین مشارکت‌کنندگان اکوسیستم را افزایش می‌دهد. تعداد زیاد این ضوابط می‌تواند زمان و هزینه را افزایش دهد. بیش از حد بودن این ضوابط می‌تواند تعاملاتی را محدود نماید که محرک نوآوری و خلاقیت بوده و موجب رشد طبیعی اعتماد بین مشارکت‌کنندگان می‌شود(آگویار و همکاران، ۲۰۲۳). در بوم‌سازگان بانکداری دیجیتال به عنوان یکی از اکوسیستم‌های دیجیتال، بانک‌ها ریسک تأثیرات اخلاقی ناشی از بکارگیری سیستم‌های مبتنی بر هوش مصنوعی را شناسایی و ارزیابی می‌کنند و آسیب‌های احتمالی بکارگیری چنین سیستم‌هایی و مشتریان آسیب‌پذیر را در نظر می‌گیرند(بیکربرون‌بائر، ۲۰۲۱). در صورت عدم رسیدگی مناسب به مسائل مرتبط با اعتماد میان بازیگران اکوسیستم کسب‌وکار دیجیتال، ممکن است عملکرد و تاب‌آوری آن به خطر بیفتد (ریچکووا و همکاران، ۲۰۲۳). رهبران اکوسیستم‌ها، باید به‌طور فعال تأثیر واقعی اعتماد را هم به‌طور فردی و هم به‌طور جمعی در مدیریت رفتارهای مطلوب ارزیابی کنند. رهبر اکوسیستم، نمی‌تواند بدون توجه به طرح‌ریزی سازوکارهای اعتماد آن را ایجاد کند و صرفاً امیدوار باشد که اعتماد به‌طور خودجوش بین اشخاص ناآشنا با یکدیگر ایجاد شود (آگویار و همکاران، ۲۰۲۳). فقدان اعتماد مشتری می‌تواند به دلیل ترس کاربران از ریسک‌های بالقوه فناوری جدید یا تمایل به کم‌ارزش جلوه دادن مزایای بلندمدت ناشی شود. در نتیجه، در کوتاه‌مدت هزینه‌ها و ریسک‌ها از مزایا فراتر می‌روند و تمایلی برای استفاده از فناوری باقی نمی‌ماند(دیجیتال‌سویتزرلند، ۲۰۲۲). ترفند رهبران هماهنگ‌ساز، برقراری تعادل مناسب بین کنترل و خودمختاری است. چنین رهبرانی، برای دستیابی به ترکیبی بهینه از سازوکارهای

محافظتی متأثر از هدف اصلی اکوسیستم، عدم تقارن قدرت[1] بین فروشنده و خریدار، سطح مهارت یا پیچیدگی مشارکت‌کنندگان، ماهیت کالاها یا خدمات قابل تبادل، میزان و شدت ریسک‌های احتمالی، هزینه نتایج منفی، رقابت، تغییرات مداوم در ضوابط بر اساس تغییرات بازار، تغییرات فناوری و تغییرات مدل کسب‌وکار تلاش می‌کنند. اکوسیستم‌های خلاقانه یا برخوردار از تراکنش‌های با ریسک پایین‌تر به ضوابط کمتری نیاز دارند(آگویار و همکاران، ۲۰۲۳). ضوابط حفاظتی ممکن است شامل سازوکارهای سخت‌افزاری، نرم‌افزاری و انسانی باشند. برای نمونه، می‌توان به سازوکارهای امانت‌گذاری در بلاکچین، ابزارهای تأیید هویت (مانند کلمات عبور، بیومتریک و احراز هویت چندعاملی)، کنترل‌های داده، ابزارهای اعتبار دیجیتال (شامل امتیازات، نظرات و جوایز) و اعمال محدودیت‌ها (مانند سیاست‌ها، تحریم‌ها و قراردادها) اشاره کرد. ضوابط حفاظتی در بسیاری از مراحل سفر کاربر یا مشتری بکار گرفته می‌شوند. حفظ اعتماد دیجیتال از طریق مدیریت موثر ریسک تقلب، امری حیاتی است (چاترجی و همکاران، ۲۰۲۳).

یکی از چالش‌های دیگر شکل‌گیری اکوسیستم‌های اعتماد دیجیتال، تمایل طبیعی به تمرکزگرایی است. بیشتر بازیگران اکوسیستمی، از فرهنگ، تجربه و عادت حکمرانی متمرکز و سنتی برخوردار هستند. علاوه بر این، تعارض فرهنگی و قانونی در سیاست‌های داخلی سازمان‌های تشکیل‌دهنده، می‌تواند پذیرش اکوسیستم اعتماد دیجیتال را دشوارتر کند (بالان، ۲۰۲۳). در برابر، فرصت‌های جدید زیادی نیز وجود دارد. بخش پزشکی و دارویی با نیازهای سختگیرانه حریم خصوصی و محرمانگی مواجه است. یکی از اکوسیستم‌های برجسته و نوظهور اعتماد دیجیتال، فارمالدجر[2] است که پلتفرمی مبتنی بر بلاکچین برای حکمرانی مشترک و کاربردهای متعدد در صنعت داروسازی ایجاد می‌کند(بالان، ۲۰۲۳). شرکای کنسرسیوم فارمالدجر، چارچوبی را پیشنهاد کرده‌اند که هدف آن جلوگیری از نگرانی‌های مربوط به محرمانگی بین کاربران بالقوه است. این گروه برای مدیریت برگه‌های الکترونیکی، مقابله با جعل دارو، مدیریت زنجیره تأمین، ردیابی محصولات نهایی و مدیریت کارآزمایی‌های بالینی تصمیم به پذیرش زیرساخت فناوری اوپن دی.اس.یو گرفت.

[1] Power asymmetry
[2] PharmaLedger

پیشینه تحقیق

به فراخور موضوعات، پیشینه تحقیق در مبانی نظری اشاره شده است. بااین‌وجود، به برخی از سایر تحقیقات پژوهشگران که به موضوع اعتماد دیجیتال و اکوسیستم اعتماد دیجیتال پرداخته‌اند، در جدول ۱ اشاره می‌شود.

جدول ۱. پیشینه تحقیق

داخلی	یافته‌های با اهمیت
(خاشعی ورنامخواستی و همکاران، ۱۴۰۳)	بانک‌ها برای پایدارسازی کسب‌وکار خود، نیازمند راه‌اندازی پلتفرم‌های دیجیتالی و ایجاد اکوسیستم‌های قوی در پیرامون آن‌ها دارند که توانایی تکامل و سازگاری با چالش‌های ناشی از افزایش ناکارآمدی‌های داخلی و مواجهه با فضای فعالیت آشفته و نامطمئن را داشته باشند. طبق یافته‌های این پژوهش، عناصر اکوسیستم پلتفرم بانکداری دیجیتال شامل بازیگران اکوسیستم، معماری پلتفرم و حاکمیت پلتفرم است.
(خورسندی شامیر، ۱۴۰۳)	طبق یافته‌های این پژوهش بر مبنای بررسی نقش میانجی‌گری اعتماد در شعب بانک آینده در مشهد، خدمات بانکداری الکترونیک تأثیر مثبت و معناداری بر وفاداری مشتریان و اعتماد آن‌ها دارد.
(زارع پور نصیرآبادی و قمری پور، ۱۴۰۳)	شکل‌دهی اکوسیستم‌های بانکداری همراه، نقش مؤثری در جلب‌اعتماد و رضایت مشتریان در ارائه خدمات مناسب به آن‌ها دارد. ضمناً رابطه مثبت و معنی‌داری بین مولفه‌های زیبایی‌شناختی، کیفیت سیستم، کیفیت خدمات، کیفیت اطلاعات، ویژگی‌های وظیفه، تضمین ساختاری و اجتماعی بودن با اعتماد و رضایت در اکوسیستم‌های بانکداری همراه وجود دارد.
(پاکدل و همکاران، ۱۴۰۲)	عوامل اجتماعی، فرهنگی و فنی متعددی بر اعتماد دیجیتال تأثیرگذارند. این عوامل شامل افزایش سطح اعتماد و فرهنگ عمومی، توجه به چارچوب‌ها و نیازهای خدمات دیجیتال، توسعه زیرساخت‌ها، پشتیبانی و الزامات، تغییر و تحولات بین‌المللی، بهبود و رشد شرایط داخلی و بین‌المللی و افزایش اعتماد عمومی و سرمایه اجتماعی می‌شود.
(جوان امانی و اکبری، ۱۴۰۱)	بعد اعتماد و اعتبار، به عنوان مهمترین بعد کیفیت خدمات در شعب بانک مسکن تلقی می‌گردد. شایستگی و توانایی کارکنان بانک در ایجاد حس اطمینان و اعتماد در نزد مشتریان دارای اهمیت است.
خارجی	**نکات با اهمیت**
(عبدلسلام و همکاران[1]، ۲۰۲۴)	اعتماد به عنوان یک مکانیسم حاکمیتی جایگزین، به جای نهادهای رسمی ناکارآمد عمل می‌کند. اعتماد می تواند به طور قابل‌توجهی ریسک کلی و غیرمعمول بانک‌ها را کاهش می‌دهد. در کشورهایی با حفاظت ضعیف‌تر سرمایه‌گذاران، حقوق قانونی کمتر، نارضایتی

[1] Abdelsalam et al.

	بیشتر از سیاست‌های اقتصادی دولت و ناآرامی سیاسی بیشتر قرار دارند، آثار کاهش‌دهنده ریسک حاصل از اعتماد اجتماعی برجسته‌تر است.
(یوسف و همکاران[1]، ۲۰۲۴)	محققین در این پژوهش، چارچوبی برای اعتماد دیجیتال ارائه می‌کنند که می‌تواند به کاهش چالش‌های امنیت سایبری کمک کند و محیطی امن برای اقتصاد دیجیتال فراهم نماید. چارچوب پیشنهادی شامل سه بخش اصلی است: (۱) فناوری‌های نوین به عنوان ستون‌های اصلی مدیریت اعتماد در محیط‌های غیرمتمرکز شناخته می‌شوند. (۲) حاکمیت اینترنتی اطمینان از امنیت و حفظ اعتماد را تضمین می‌کند. (۳) مدل‌های جدید کسب‌وکار دیجیتال که برنامه‌ریزی و پاسخگویی به حملات سایبری و افزایش اعتماد کاربران را شامل می‌شود.
(چانگ[2]، ۲۰۲۴)	نتایج بررسی مصرف‌کنندگان خدمات بانکداری دیجیتال در تایوان نشان می‌دهد که کیفیت اطلاعات، کیفیت سیستم و کیفیت خدمات تأثیر مثبتی بر رضایت کاربر دارند. اعتماد نقش محوری در شکل‌گیری رضایت‌مندی از بانکداری دیجیتال دارد و دومین عامل مهم پس از کیفیت سیستم و خدمات است. امنیت و حریم خصوصی نیز عوامل اساسی در ایجاد اعتماد در بانک‌های دیجیتال هستند.
(گوپتا و شوکلا[3]، ۲۰۲۴)	چارچوب قانونی و نظارتی قوی، تدابیر امنیتی مؤثر، و شیوه‌های پویای اعتمادبخش در تقویت اعتماد مصرف‌کنندگان به بانکداری دیجیتال مهم هستند. وجود استانداردهای تطابق، سیاست‌های حفاظت از مصرف‌کننده، شفافیت و سازوکارهای اجرای قوانین به طور قابل توجهی اعتماد مصرف‌کنندگان به بانکداری دیجیتال را افزایش می‌دهد. علاوه بر این، تدابیر امنیتی فناورانه، مدیریت ریسک مؤثر، و تجربه کاربری خوب از جمله عوامل مهمی هستند که به تقویت اعتماد کاربران کمک می‌کنند.
(بیکربرون‌بائر، ۲۰۲۱)	در خصوص جهت‌گیری و پیاده‌سازی اخلاق هوش مصنوعی درون سازمان، چارچوب تی.ای.آی. از مدیران حمایت می‌کند. این چارچوب، رویکردی جامع برای شناسایی روابط سیستماتیک اخلاقی برای اکوسیستم شرکت اتخاذ می‌کند. اصول چارچوب مذکور شامل ارزش‌های شرکتی، مدل‌های کسب‌وکاری، منافع و خیر عمومی (مانند اهداف توسعه پایدار و متناسب با اعلامیه جهانی حقوق بشر)، تعامل با ذینفعان، ارزیابی ریسک و تاثیرات اجتماعی، و روش‌های مناسب فنی (مانند معماری‌های قابل اعتماد، در نظر گرفتن قوانین و اصول اخلاقی در طراحی) و روش‌های غیرفنی (مانند مقررات، استانداردها، آموزش و آگاهی‌رسانی) می‌شود.

[1] Yusof et al.
[2] Chang
[3] Gupta & Shukla

روش‌شناسی پژوهش

ارائه الگو

تحقیق حاضر، از لحاظ هدف پژوهش، از نوع تحقیقات کاربردی است. در این تحقیق، به بررسی و توسعه دانش کاربردی در زمینه اکوسیستم اعتماد دیجیتال با رویکرد پدیدارشناسی تمرکز شده است. این روش، به دنبال درک تجارب و برداشت‌های مختلف افراد در مواجهه با یک پدیده خاص است. در این تحقیق، داده‌های حاصل از بررسی منابع آنلاین، مقالات و مصاحبه‌های غیرمستقیم از طریق تحلیل محتوای ویدئوها و مقایسه تجربه خبرگان با چارچوب‌های اعتماد دیجیتال به منظور استخراج الگوهای کلیدی در اکوسیستم‌های دیجیتال مورد تحلیل قرار گرفته‌اند. این روش به پژوهشگر اجازه می‌دهد تا نه‌تنها به یک چارچوب نظری جامع دست یابد، بلکه ارتباط بین واقعیت‌های عملی و مفاهیم آکادمیک را نیز به شکلی دقیق‌تر توصیف کند. با این شیوه، یافته‌های پژوهش، نه‌تنها از پشتوانه تجربی قوی‌تری برخوردار خواهند شد، بلکه امکان تعمیم آن‌ها در محیط‌های مختلف دیجیتال نیز فراهم می‌شود. مسیر انتخاب چارچوب دی.تی.ئی.اف به‌عنوان مدل اصلی حاکمیت اکوسیستم‌های اعتماد دیجیتال از طریق یک فرایند پدیدارشناسانه حاصل شد. این پژوهش، به دنبال ارائه راهکاری برای مسئله بررسی چگونگی مدیریت ریسک در اکوسیستم‌های دیجیتال مبتنی بر اعتماد تمرکز دارد و می‌تواند مسبب تضمین امنیت سایبری، بهبود شفافیت، انطباق با مقررات و تقویت اعتماد میان ذی‌نفعان شود. در اولین گام، برای ایده‌یابی مفهوم نوظهور اکوسیستم‌های اعتماد دیجیتال، ادبیات موضوعی کاربردی و به‌روز، و مصاحبه غیرمستقیم تجارب متخصصان بین المللی در پلتفرم‌ها و شبکه‌های اجتماعی مرور شد. تحلیل داده‌های به‌دست‌آمده از فضای آنلاین، از جمله نظرات کاربران در شبکه‌های اجتماعی حرفه‌ای و پلتفرم‌های ویدئویی، به درک جامع‌تری از چالش‌ها و فرصت‌های موجود کمک کرد. یکی از اقدامات، جستجوی کلیدواژه «اکوسیستم اعتماد دیجیتال» در پلتفرم یوتیوب به عنوان فضای به‌اشتراک‌گذاری بیان تجارب تخصصی توسط متخصصان ذیربط بود؛ خروجی نتایج اولیه از این جستجو، ۲۵۹ ویدئو بود. فرض بر این شد که در الگوریتم‌های موتورهای جستجو، مرتبط‌ترین نتایج در اولویت نمایش قرار می‌گیرند. بنابراین، در ۱۰۰ نتیجه برتر از جستجوی نامبرده، ۶۷ درصد مرتبط با اکوسیستم اعتماد دیجیتال، ۲۷درصد مرتبط با اعتماد دیجیتال بود و مابقی نامرتبط بودند. ۲۸ درصد از نتایج مرتبط با

اکوسیستم اعتماد دیجیتال، مترادف با چارچوب دی.تی.ئی.اف بودند که در روش پدیدارشناسی حائز اهمیت می‌شد. سایر موارد، به چارچوب‌های فارمالدجر، هایپرلدجر و چارچوب‌های زنجیره بلوکی اختصاصی مرتبط می‌شد که با توجه به کاربرد اختصاصی آنها در صنایع خاص، قابلیت تعمیم به کلیه صنایع را به همراه نداشت. بررسی تجربیات متخصصان، سازمان‌ها، و پژوهشگران مختلف در فضای دیجیتال، نشان داد که چارچوب دی.تی.ئی.اف نه‌تنها تمام مؤلفه‌های حیاتی اکوسیستم‌های دیجیتال را در برمی‌گیرد، بلکه به‌عنوان الگوی تطبیق‌پذیر و منعطف، امکان مدیریت اعتماد و مخاطرات در سطوح مختلف را چارچوب‌دهی می‌کند. در مرحله بعد، انتخاب الگوی استاندارد برای مدیریت ریسک در لایه چهارم هرم دی.تی.ئی.اف بر مبنای روش پدیدارشناسی انجام شد. با تحلیل تجربیات و مطالعات موردی مرتبط، مشخص شد که چند چارچوب مختلف برای مدیریت ریسک وجود دارند که هر یک در موقعیت‌های خاص کاربرد دارند. محتواهای ویدئویی و مقالاتی که به بررسی عملی پیاده‌سازی استانداردهای مدیریت ریسک پرداخته‌اند، نشان دادند که استاندارد ایزو ۲۷۰۰۵ به دلیل انطباق بالا با ساختارهای امنیت اطلاعات و اعتماد دیجیتال، پرکاربردترین مدل در این حوزه محسوب می‌شود. این استاندارد از یک رویکرد سیستماتیک برای شناسایی، تحلیل، و برطرف‌سازی مخاطرات پیروی می‌کند که در اکوسیستم‌های دیجیتال به‌خوبی قابل اجراست (ایزو ۲۷۰۰۵[1]، ۲۰۲۲).

الگوی سه بُعدی معرفی شده در چارچوب دی.تی.ئی.اف دارای چهار عنصر اصلی (۱) افراد؛ (۲) فرایند؛ (۳) فناوری و (۴) سازمان است که به صورت سه بُعدی به یکدیگر وابسته هستند (ایساکا، ۲۰۲۴). این چارچوب به بررسی دامنه‌ها (حوزه‌ها) می‌پردازد تا عوامل اعتماد، روش‌ها، فعالیت‌ها و نتایج را به‌عنوان بخشی از سفر اعتماد دیجیتال سازمان‌ها شناسایی کند. این چارچوب با در نظر گرفتن کلیه ذی‌نفعان، اطمینان حاصل می‌کند که همه تعاملات و تراکنش‌های دیجیتالی مشروع، مورد اعتماد و منطبق بر اصول یکپارچگی، امنیت، حریم خصوصی، تاب‌آوری، کیفیت، قابلیت اطمینان و اعتمادپذیری هستند. چارچوب دی.تی.ئی.اف شامل شاخص‌ها و کنترل‌هایی است که می‌توان آن‌ها را بر اساس نیازهای یک سازمان سفارشی‌سازی کرد. این چارچوب، رویکرد نوآورانه‌ای برای ایجاد اعتماد دیجیتال و تحول

[1] ISO/IEC 27005

سازمانی ارائه می‌دهد که برای هر موضوع جدیدی از جمله فناوری هوش مصنوعی قابل استفاده است. دی.تی.ئی.اف شامل روش‌های دقیق، فعالیت‌ها، خروجی‌ها، کنترل‌ها، شاخص‌های کلیدی عملکرد[1] و شاخص‌های کلیدی ریسک[2] است(ایساکا، ۲۰۲۴). اعتماد دیجیتال صرفاً مربوط به اطلاعات و فناوری دیجیتال نیست. اعتماد دیجیتال، بر کل کسب‌وکار تأثیر می‌گذارد؛ بنابراین، شرکت‌های برخوردار، مزیت رقابتی قابل‌توجهی کسب می‌کنند.

این چارچوب، صرفاً نسخه‌برداری یا محدود شده نیست، بلکه شامل رویه‌ها، فعالیت‌ها، نتایج، کنترل‌ها، و شاخص‌های تفصیلی است. علاوه بر این، دی.تی.ئی.اف با بسیاری از چارچوب‌های موجود در بازار مانند ایزو ۲۷۰۰۱ یا چارچوب امنیت سایبری ان.آی.اس.تی سازگار است (ایساکا، ۲۰۲۴). این چارچوب، با ایجاد بدنه دانشی به سازمان‌ها کمک می‌کند تا در برابر تغییرات پویا در قوانین، مقررات، فناوری، نیازهای کسب‌وکاری مدرن و عوامل داخلی و خارجی واکنش مناسبی نشان دهند.

مطابق شکل ۱، هرم دی.تی.ئی.اف از شش لایه تشکیل می‌شود. در این سلسله مراتب هرمی، گره‌ها در اولین لایه قرار می‌گیرند و شامل عناصر سنتی فناوری اطلاعات شامل افراد، فرایند، فناوری و سازمان می‌شوند. در لایه دوم، دامنه‌ها قرار می‌گیرند. شش دامنه شامل (۱) فرهنگ، (۲) نوپدیدی[3]، (۳) عوامل انسانی، (۴) هدایت و پایش[4]، (۵) معماری و (۶) تواناسازی و پشتیبانی در این چارچوب معرفی می‌شود. در لایه سوم، عوامل اعتماد قرار می‌گیرند که عناصر اساسی برای هر دامنه را تبیین می‌کنند. به‌رغم اینکه طبق این چارچوب، امکان سفارشی‌سازی و متناسب‌سازی وجود دارد، الگویی پیشفرض برای سطوح اول، دوم و سوم توسط این انجمن ارائه شده است، اما برای سطوح بعدی هرم، الگویی مشخص نشده و لذا نیازمند خلق یا متناسب‌سازی است. در لایه چهارم، روش‌ها قرار می‌گیرند که عوامل اعتماد را توضیح و تشریح می‌دهند. در لایه پنجم، فعالیت‌های عملی برای اجرای روش‌ها تعریف می‌شوند. نهایتاً در لایه ششم به عنوان آخرین لایه، نتایج حاصل از انجام فعالیت‌ها توصیف می‌شوند (ایساکا، ۲۰۲۴).

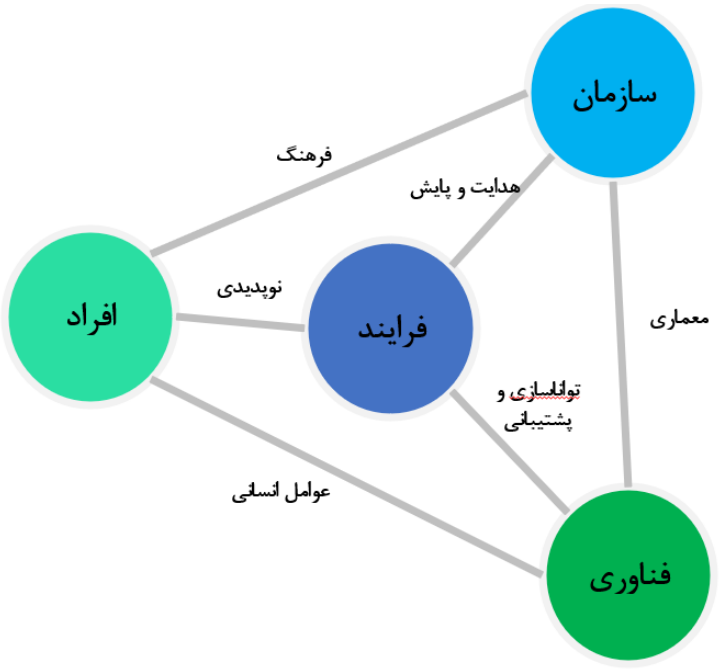
[1] Key Performance Indicator (KPI)
[2] Key Risk Indicator (KRI)
[3] Emergence
[4] Direct and Monitor

شکل ۱. هرم دی.تی.ئی.اف (برگرفته از ایساکا، ۲۰۲۴)

طبق شکل ۲، چهار گره اصلی از لایه اول از طریق شش دامنه در لایه دوم به یکدیگر متصل می‌شوند (ایساکا، ۲۰۲۴):

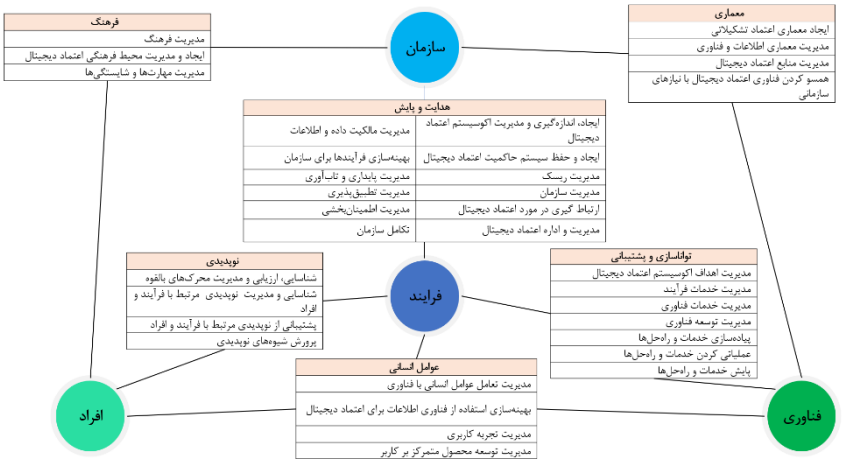
- فرهنگ: اتصال بین سازمان و افراد
- نوپدیدی: اتصال بین افراد و فرایند
- عوامل انسانی: اتصال بین افراد و فناوری
- هدایت و پایش: اتصال بین سازمان و فرایند
- معماری: اتصال بین سازمان و فناوری
- تواناسازی و پشتیبانی: اتصال بین فناوری و فرایند

هر دامنه در دی.تی.ئی.اف می‌تواند بر یک یا چند گره اصلی تأثیر بگذارد. دامنه‌ها نقش حیاتی در مدیریت ارتباطات متقابل و پیچیدگی‌های سازمانی ایفا می‌کنند و در مواجهه با تغییرات مقرراتی، ظهور فناوری‌های جدید، تهدیدات نوظهور و اصلاحات رویه‌ای، سازمان را قادر به انطباق و واکنش سریع‌تر می‌سازند.



شکل ۲. مدل دی.تی.ئی.اف (برگرفته از ایساکا، ۲۰۲۴)

مدل سه بُعدی گره و دامنه، با افزوده شدن عوامل اعتماد تفصیل می‌یابند. هر دامنه شامل مجموعه‌ای از عوامل ساختاری و سازنده است که پایه‌های اعتماد دیجیتال را شکل می‌دهند. شکل ۳ به مولفه‌های اعتماد دیجیتال تا سطح سوم از هرم دی.تی.ئی.اف می‌پردازد (ایساکا، ۲۰۲۴). لایه‌های بعدی هرم، می‌تواند بر حسب نیازهای اکوسیستمی و سازمانی متناسب‌سازی شوند. لذا امکان الگوگیری در سطح روش‌ها و فعالیت‌ها به‌عنوان لایه‌های بعدی وجود ندارد. بنابراین، لازم است برای تبیین لایه‌های بعدی، از رویکردی تجربی و ابتکارآمیز استفاده شود. با توجه به گستردگی دامنه اجرایی در لایه سوم که مشتمل بر ۳۴ عامل اعتماد است، در این پژوهش صرفاً به «مدیریت ریسک» پرداخته شده است.



شکل ۳. مولفه‌های دی.تی.ئی.اف (برگرفته از ایساکا، ۲۰۲۴)

یکی از الگوهای مناسب برای مدیریت ریسک، مدل مطرح شده در ایزو ۲۷۰۰۵ (۲۰۲۲) است. در این الگو فرایند اصلی مدیریت ریسک شامل استقرار زمینه، بررسی ریسک[1] و برطرف‌سازی ریسک[2] است. دو مولفه دیگر شامل (۱) ارتباطات و مشورت‌گیری و (۲) پایش و مرور نیز به صورت مشترک بر فرایند مدیریت ریسک تأثیر می‌گذارند. در این الگو، بررسی ریسک شامل شناسایی ریسک، تحلیل ریسک و ارزیابی قضاوتی ریسک[3] می‌شود.[4] با در نظر گرفتن اکوسیستم به‌عنوان زمینه موضوعی، می‌توان روش‌های مرتبط با عوامل اعتماد را بر مبنای استاندارد ایزو ۲۷۰۰۵ استخراج کرد (ایزو ۲۷۰۰۵، ۲۰۲۲).

یافته‌های پژوهش

ارائه نتایج پژوهش

در ابتدا، از میان ۳۴ عامل اعتماد که در لایه سوم از چارچوب دی.تی.ئی.اف قرار می‌گیرند، «مدیریت ریسک» در نظر گرفته شد. این عامل اعتماد، در دامنه «هدایت و پایش» قرار می‌گیرد

[1] Risk assessment
[2] Risk treatment
[3] Risk evaluation
[4] Evaluation به نتیجه‌گیری و تصمیم‌گیری قضاوتی درباره یک پروژه یا فرایند اشاره دارد. Assessment بیشتر به ارزیابی و تجزیه و تحلیل دقیق داده‌ها یا شرایط خاص می‌پردازد. Evaluation را می‌توان بخش انتهایی Assessment در نظر گرفت.

و متعاقباً دامنه «هدایت و پایش» یال اتصالی بین ابعاد «سازمان» و «فرایند» از لایه اول است. برای تعریف روش‌ها و فعالیت‌های مرتبط با «مدیریت ریسک» از تلفیق الگوی دی.تی.ئی.اف و استاندارد ایزو ۲۷۰۰۵ استفاده شد. هدف مورد انتظار، ایجاد روش‌ها و فعالیت‌هایی برای عامل اعتماد «مدیریت ریسک» است.

جهت تصدیق روش‌ها و فعالیت‌های استخراج شده، از مصداق بکارگیری هوش مصنوعی برای بانکداری دیجیتال به عنوان یکی از اکوسیستم‌های درون‌کشوری استفاده شد و روش‌ها و فعالیت‌ها بر این کاربرد بومی‌سازی شده است. چارچوب ارائه شده برای اکوسیستم مبتنی بر اعتماد دیجیتال در سطح روش‌ها و فعالیت‌ها، به صورت جامع در جدول ۲ قابل مشاهده است.

جدول ۲. لایه ۴ و ۵ بر مبنای چارچوب دی.تی.ئی.اف

کد روش	عنوان روش	کد فعالیت	عنوان فعالیت
DM.03.01	هدایت و پایش بر مدیریت ریسک	DM.03.01.1	شناسایی نقش‌ها و مسئولیت‌ها برای مدیریت ریسک
		DM.03.01.2	مرور برنامه‌های شناسایی، تحلیل و ارزیابی و برطرف‌سازی ریسک‌های اکوسیستم دیجیتال
		DM.03.01.3	بررسی اثربخشی سیستم مدیریت ریسک
		DM.03.01.4	بررسی کارایی سیستم مدیریت ریسک
		DM.03.01.5	پایش مستمر برای شناسایی ریسک‌های ناشی از تغییرات قوانین و مقررات
		DM.03.01.6	پایش مستمر برای شناسایی ریسک‌های ناشی از تغییرات محیطی
DM.03.02	شناسایی ریسک‌های اکوسیستم دیجیتال	DM.03.02.1	شناسایی سرچشمه ریسک، رویدادها، و علل آن
		DM.03.02.2	شناسایی صاحبان ریسک و مسئولیت‌های مرتبط
		DM.03.02.3	شناسایی کنترل‌های ریسک فعلی و محیط کنترلی
		DM.03.02.4	شناسایی پیامدهای بالقوه ریسک و نحوه مدیریت آن
		DM.03.02.5	تعیین معیارهایی برای طبقه‌بندی ریسک ها
		DM.03.02.6	ادغام ریسک اکوسیستم دیجیتال در مدیریت کلان ریسک سازمانی (ERM)

کد روش	عنوان روش	کد فعالیت	عنوان فعالیت
DM.03.03	تحلیل و ارزیابی ریسک‌ها	DM.03.03.1	برآورد ریسک
		DM.03.03.2	تعیین سطح ریسک‌پذیری و میزان تحمل ریسک
		DM.03.03.3	اولویت دهی و مقایسه بین ریسک‌ها بر اساس معیارهای ریسک
		DM.03.03.4	مقایسه نتایج تحلیل ریسک با معیارهای ریسک
DM.03.04	برطرف‌سازی ریسک‌ها	DM.03.04.1	تصمیم به اجتناب از ریسک با عدم شروع
		DM.03.04.2	حذف سرچشمه‌های ریسک
		DM.03.04.3	تغییر احتمالات ریسک
		DM.03.04.4	تغییر پیامدهای ریسک
		DM.03.04.5	به اشتراک‌گذاری ریسک با سایر طرف‌ها در اکوسیستم دیجیتال
		DM.03.04.6	تصمیم‌گیری برای کاهش، حذف، پیشگیری، یا پذیرش ریسک

قالب کدگذاری مورد استفاده برای «روش‌ها» و «فعالیت‌ها»، به ترتیب، شامل سه و چهار بخش است. با توجه به قرارگیری عامل اعتماد «مدیریت ریسک» در دامنه «هدایت و پایش»، برای بخش اول کد از دو حرفی اختصاری معادل عنوان انگلیسی این دامنه استفاده شد. بخش دوم کد، نمایان‌گر جایگاه «مدیریت ریسک» در بین کلیه مولفه‌های اعتماد مرتبط با این دامنه است که به صورت عددی تعریف می‌شود. بخش سوم کد، مرتبط با روش‌های مورد استفاده است که به صورت اعداد ترتیبی اتخاذ می‌شود. در الگوی پیشنهادی، چهار روش بر مبنای اکتشاف و الگوگیری از الگوی مدیریت ریسک مرتبط در استاندارد ایزو ۲۷۰۰۵ استخراج گردید که در جدول ۲ قابل مشاهده است. در کد مرتبط با فعالیت‌های تعریف شده برای هر یک از روش‌ها از بخش چهارمی در قالب اعداد ترتیبی استفاده شد. به‌عنوان مثال، کد DM.03.02.4، مرتبط با فعالیت چهارم با عنوان «شناسایی پیامدهای بالقوه ریسک و نحوه مدیریت آن» است که به روش دوم با عنوان «شناسایی ریسک‌های اکوسیستم دیجیتال» مرتبط می‌شود.

نقش مکمل چارچوب‌های دی.تی.ئی.اف و کوبیت

انجمن ایساکا، انجمن حرفه‌ای بین‌المللی متمرکز بر حاکمیت فناوری اطلاعات است. این انجمن، چارچوب استانداردی برای مدیریت و حاکمیت فناوری اطلاعات، حسابرسی و کنترل اطلاعات و فناوری‌های مرتبط و طراحی سیستم فناوری اطلاعات تحت عنوان کوبیت منتشر کرده است. چارچوب مذکور بر کسب‌وکار سازمان متمرکز بوده و مجموعه‌ای از فرایندهای کلی و عمومی برای مدیریت فناوری اطلاعات تعریف می‌کند. هرکدام از این فرایندها با ورودی‌ها و خروجی‌های فرایندی، فعالیت‌های کلیدی فرایند، اهداف و مقاصد فرایند، سنجه‌های اندازه‌گیری کارایی فرایند و مدل بلوغ اولیه از فرایند همراه می‌باشند. این چارچوب با استانداردها و مدل‌های کوزو، آی.تی.آی.ال، بی‌اس.ال[1]، ایزو ۲۷۰۰۰، سی.ام.ام.آی[2]، توگاف[3] و پی‌ام‌باک[4] هماهنگ است. این استاندارد، از بررسی وابستگی به تولیدکنندگان، فناوری‌ها و پلتفرم‌های خاص مستقل باقی می‌ماند. آخرین نسخه این استاندارد، کوبیت ۲۰۱۹ است که در آن اصول چارچوب حکمرانی[5] نسبت به نسخه قبلی (کوبیت ۵) اضافه شده است. اصل اول به شناسایی سازگاری حداکثری و خودکارسازی چارچوب حکمرانی معطوف است که مشتمل بر مدل مفهومی، اجزای کلیدی و روابط فیمابین آنها است. اصل دوم مبنی بر گشودگی و انعطاف‌پذیری است؛ به این معنا که چارچوب باید اجازه افزودن محتوای جدید و پرداختن به مسائل نوظهور را بدهد و در عین حال یکپارچگی و سازگاری را حفظ کند. اصل سوم تأکید می‌کند که این مدل باید با استانداردها، چارچوب‌ها و مقررات اصلی هماهنگ باشد. بنابراین، به اتکای متناسب‌سازی با نیازهای شرکت، الزامات صنعت و زمینه‌های عملیاتی، این نسخه کوبیت، از انعطاف‌پذیری و سفارشی‌سازی قوی‌تری برخوردار است. این چارچوب، پشتیبانی مجموعه ابزارهایی را بر عهده دارد که به مدیران اجازه می‌دهد تا بین شکاف کنترل نیازها، مشکلات فناورانه و ریسک‌های اقتصادی پلی بزنند (توماس و همکاران، ۲۰۲۴).

چارچوب دی.تی.ئی.اف از «مدل کسب‌وکار برای امنیت اینترنت[6]» که ایساکا در سال ۲۰۱۰ منتشر کرده بود، توسعه یافته است. این چارچوب به درک سطح بالایی از نحوه اجرا،

[1] Business Information Services Library (BiSL)
[2] Capability Maturity Model Integration (CMMI)
[3] The Open Group Architecture Framework (TOGAF)
[4] Project Management Body of Knowledge (PMBOK)
[5] Governance framework principles
[6] the Business Model for Internet Security

نگهداری و نظارت بر اعتماد دیجیتال در میان ذی‌نفعان سازمان کمک می‌کند. این چارچوب، عوامل انسانی، فرهنگی و ارتباطات را مورد توجه قرار می‌دهد که بخش‌های مختلف یک سازمان را به هم متصل می‌کنند. دی.تی.ئی.اف به کاربران خود این امکان را می‌دهد که دریابند چه اقداماتی باید توسط خود آنها، شرکا و ارائه‌دهندگان شخص ثالث انجام شود تا اعتماد مشتریان ایجاد و حفظ شود. این چارچوب به سازمان‌ها کمک می‌کند که به‌جای تمرکز مستقیم بر جنبه‌های فنی، به سؤالات راهبردی و کسب‌وکاری فکر کنند (توماس و همکاران، ۲۰۲۴). چارچوب دی.تی.ئی.اف جایگزین کوبیت نیست. کوبیت چارچوبی ارزشمند برای حاکمیت سازمانی فناوری اطلاعات است. در برابر، چارچوب دی.تی.ئی.اف چارچوب گسترده‌تری برای اعتماد دیجیتال ارائه می‌دهد. هر دو چارچوب می‌توانند همزمان مورد استفاده قرار گیرند تا نیازهای مختلف سازمانی را برآورده کنند(ایساکا، ۲۰۲۴). برخی از عناصر کوبیت در دی.تی.ئی.اف، به‌ویژه در حوزه‌های هدایت و پایش، وجود دارد. با توجه به رشد بی‌سابقه داده‌ها و فرایندهای کسب‌وکارهای فناورانه، حاکمیت سازمانی پیچیده‌تر از همیشه شده است. با استفاده همزمان از این دو چارچوب، سازمان‌ها می‌توانند نسبت به رقبا، ایمن‌تر، مقاوم‌تر و قابل‌اعتمادتر شوند.

با توجه به ماهیت اکوسیستمی دی.تی.ئی.اف، باید توجه داشت که این الگو، یک چارچوب مستقل نیست و باید در کنار سیستم حاکمیتی موجود سازمان به کار گرفته شود. برای جلوگیری از بار اضافی ناشی از استفاده از چند چارچوب، می‌توان دی.تی.ئی.اف را به عنوان میان‌افزاری در نظر گرفت که به ایجاد و تسهیل ارتباط میان این چارچوب‌ها کمک می‌کند (توماس و همکاران، ۲۰۲۴). دی.تی.ئی.اف به عنوان چارچوبی جامع علاوه بر حاکمیت (حاصل شده از طریق کوبیت)، به ریسک‌های شهرتی و اخلاقی در اکوسیستم دیجیتال می‌پردازد. دی.تی.ئی.اف شامل موضوعاتی فراتر از فناوری اطلاعات است و می‌تواند شهرت برند، فرایندهای استخدامی و آموزش کارکنان، و مدیریت تأمین‌کنندگان را شامل شود.

بحث و نتیجه گیری

در اقتصاد دیجیتال، موفقیت سازمان‌ها به توانایی آن‌ها در ایجاد روابط و تعاملات قابل‌اعتماد بستگی دارد. اعتماد دیجیتال، یکی از ارکان اصلی در اکوسیستم‌های دیجیتال پایدار و تاب‌آور

به شمار می‌رود. این تحقیق نشان داد که در اکوسیستم‌های دیجیتال، مدیریت اعتماد دیجیتال به‌عنوان فرایندی پویا و مداوم ضروری است. اعتماد دیجیتال و امنیت دیجیتال دو مفهوم مرتبط، متفاوت و مکمل یکدیگر هستند. این پژوهش به اهمیت نقش اعتماد دیجیتال در شکل‌گیری اکوسیستم‌های دیجیتال از طریق استفاده از فناوری‌های نوین و حاکمیت اکوسیستمی تأکید کرده است. پژوهش حاضر، چالش‌ها و ریسک‌های مرتبط با مدیریت اعتماد دیجیتال را شناسایی کرده و راهکارهایی برای مقابله با تهدیدات نوظهور ارائه می‌دهد. این راهکارها شامل ارتقاء شفافیت، ایجاد چارچوب‌های حاکمیتی کارآمد و استفاده از مدل‌های امنیتی مبتنی بر استانداردهای بین‌المللی است. در این پژوهش، مدیریت ریسک به عنوان یکی از عوامل اعتماد هدفگیری شد و بر اساس نتایج تحقیقات کاربردی در این پژوهش، روش‌ها و فعالیت‌های مرتبط با مدیریت ریسک در اکوسیستم اعتماد دیجیتال، بر مبنای استاندارد ایزو ۲۷۰۰۵ پیشنهاد شد. به علاوه، پژوهش حاضر با بررسی نقش مکمل چارچوب‌های دی.تی.ئی.اف و کوبیت نشان داد که چگونه این دو چارچوب می‌توانند در کنار یکدیگر به ایجاد مدلی جامع برای مدیریت ریسک در اکوسیستم‌های دیجیتال کمک کنند.

از جمله پیشنهادهایی که می‌تواند در پژوهش‌های آتی مد نظر قرار گیرد، بررسی و استخراج روش‌ها و اقدامات مرتبط با دیگر عوامل اعتماد از دی.تی.ئی.اف و یکپارچه‌سازی یافته‌ها با روش‌ها و اقدامات پیشنهاد شده برای مدیریت ریسک است. بازخوردگیری عملیاتی از نتایج حاصل از انجام فعالیت‌ها و رعایت روش‌ها، می‌تواند به شکل‌دهی الگویی با ظرافت بیشتر کمک کند. با توجه مقیاس‌پذیر بودن چارچوب دی.تی.ئی.اف می‌توان از آن در تنظیم روش‌ها و فعالیت‌های مورد نیاز در صنایع مختلف استفاده کرد و عملکرد و اثربخشی آن را مورد مقایسه قرار داد.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

منابع

پاکدل، محمدرضا، حقیقت منفرد، جلال و علیقلی، منصوره. (۱۴۰۲)، ارایه مدل بومی عوامل موثر بر شکل دهی اعتماد دیجیتال (با بهره‌گیری از رویکرد و نظریه داده بنیاد)، *فصلنامه مدیریت توسعه و تحول*، ۱۶ (۵۶).

جوان امانی، ودود و اکبری، حمید. (۱۴۰۱) بررسی تاثیر کیفیت خدمات بانکداری بر رضایت مندی مشتریان با استفاده از مدل سروکوال (مورد مطالعه: بانک مسکن شعب تهران). *نشریه اقتصاد و بانکداری اسلامی*، ۱۱ (۴۰): ۶۴-۴۳.

خاشعی ورنامخواستی، وحید، ابراهیمی، مهدی، خلیل‌نژاد، شهرام و مطهری‌نژاد، فاطمه. (۱۴۰۳). مکانیزم‌های مولد تکامل اکوسیستم بانکداری دیجیتال. *مطالعات مدیریت کسب و کار هوشمند*، ۱۲ (۴۸): ۸۱-۳۳.

خورسندی شامیر، حمید. (۱۴۰۳). خدمات بانکداری الکترونیک و وفاداری مشتریان: تحلیل نقش میانجی‌گری اعتماد در شعب بانک آینده مشهد. *مجله کاوش‌های نوین در علوم محاسباتی و مدیریت رفتاری*، ۲ (۱): ۲۳- ۴۱.

زارع پور نصیرآبادی، ابراهیم و قمری پور، ندا. (۱۴۰۳). بررسی رابطه بین مؤلفه‌های مؤثر بر اعتماد و رضایت مشتریان در اکوسیستم‌های بانکداری همراه. *فصلنامه پژوهش‌های مدیریت در ایران*، ۲۸ (۱): ۱۵۴-۱۳۱.

References

Abdelsalam, O; Chantziaras, A; Joseph N. L; & Tsileponis, N. (2024). Trust matters: A global perspective on the influence of trust on bank market risk. *Journal of International Financial Markets, Institutions and Money*, *92*, 101959.

Aguiar, M; Kiderman, J; Shekar, H. C; & Schilke, O. (2023). Safeguarding trust in a digital ecosystem. *Journal of Business Strategy*, (ahead-of-print).

Baker-Brunnbauer, J. (2021). TAII framework for trustworthy AI systems. ROBONOMICS*: The Journal of the Automated Economy*, *2*, 17.

Balan, A; Tan, A. G; Kourtit, K; & Nijkamp, P. (2023). Data-Driven Intelligent Platforms—Design of Self-Sovereign Data Trust Systems. *Land*, *12*(6), 1224.

Chang, W. (2024). The Impact of Trust on Digital Banking Services. *Americas Conference on Information Systems (AMCIS) 2024, Proceedings*. 1.

Chatterjee, J; Damle M; & Aslekar, A. (2023). Digital Trust in Industry 4.0 & 5.0: Impact of Frauds. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 922-928). IEEE.

Digitalswitzerland. (2022). Building a Swiss Digital Trust Ecosystem, Discussion Input.

Firdaus, F; & Tobing, A. N. (2022). The Digital Ecosystem Risk in Digital Banking: a Case Study. *Risk Governance & Control: Financial Markets & Institutions*, *12*(4).

Gupta, V; & Shukla, S. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. *Interdisciplinary Studies in Society, Law, and Politics*, *3*(2), 18-24.

Hazam, G. (2023). Extending Zero Trust to the End User Ecosystem, *ISACA Journal*, Issues 2023, vol. 1.

Herzog, C; Blank, S; & Stahl, B. C. (2024). Towards trustworthy medical AI ecosystems–a proposal for supporting responsible innovation practices in AI-based medical innovation. *AI & SOCIETY*, 1-21.

ISACA. (2024). Using the Digital Trust Ecosystem Framework to Achieve Trustworthy AI. White Paper.

ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection: Guidance on managing information security risks, Publication date : 2022-10.

Javan Amani, V; & Akbari, H. (2022). The Effect of Quality of Banking Services on Customer Satisfaction using SERVQUAL Model (Case study: Maskan Bank Branches in Tehran). *Journal of Islamic Economicis & Banking*, 11 (40). (In Persian)

Kaya, F. (2025). Decentralized Governance Design: A Model-Based Approach. *PhD-Thesis - Research and graduation internal*, Vrije Universiteit Amsterdam.

Khashei Varnamkhasti, V; Ebrahimi, M; Khalil Nezhad, Sh; & Motahari Nezhad, F. (2024). Generative Mechanisms of Digital Banking Ecosystem Evolution, *Journal of Business Intelligence Management Studies*, 12(48), 33-81. (In Persian)

Khorsandi Shamir, H. (2024). Electronic banking services and customer loyalty: An analysis of the mediating role of trust in the branches of Ayandeh bank in Mashhad. *Novel Explorations in Computational Science and Behavioral Management*, 2(1), 23-41. (In Persian)

Kulova, M. R. (2020). Trust and Security in the Digital Economy. *In International Session on Factors of Regional Extensive Development* (FRED 2019) (pp. 271-274). Atlantis Press.

Malik , P. K. (2024). The Role of Digital Trust in Enhancing Cyber Security Resilience. *Transforming Industry using Digital Twin Technology* (pp. 59-67). Cham: Springer Nature Switzerland.

Pakdel, M; Haghighat Monfared, J; & Aligholi, M. (2024). Presenting a native model of factors affecting the formation of digital trust using a data-based approach and theory, *Development and Transformation Management Journal* , No. 56 (Spring 1403). (In Persian)

Reiners, S. (2022, June). Trust and its Extensions in Digital Platform Ecosystems: Key Concepts and Issues for Future Research. In *2022 IEEE 24th Conference on Business Informatics (CBI)* (Vol. 2, pp. 1-8). IEEE.

Roy, S. (2024). Understanding Zero-Trust vs. Digital Trust: Demystifying Cybersecurity Paradigms, *IDM Technologies*.

Rychkova, I; Zdravkovic, J; & Stirna, J. (2023). Implications of trust in digital business ecosystem design: A systematic analysis of roles. *PoEM Companion*.

Shahzad, K; & Shahid, H. (2022). Digital trust in business ecosystem collaboration: Leveraging digital technologies to develop a framework. *Trust,*

Digital Business and Technology: Issues and Challenges, 242- 254. Routledge Studies in Trust Research. New York: Routledge.

Strazzullo, S. (2024). Fostering digital trust in manufacturing companies: Exploring the impact of industry 4.0 technologies. *Journal of Innovation & Knowledge*, 9(4), 100621.

Thomas, M; Witte, G; & Von Roessing, R. (2024). Digital Trust Ecosystem Framework a Valuable Complement to COBIT, Other Frameworks.

Yusof, A. M; Zaini, M. K; Khairuddin, I. E; & Uzir, N. A. (2024). Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy, *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, 15(4), 15A4B, 1-12.

Zarepour Nasirabadi, E; & Ghamaripoor N. (2024). Investigating the relationship between the components affecting customer trust and satisfaction in mobile banking ecosystems. *Management Research in Iran*, 28(1), 131-154. (In Persian)