طراحی الگوی مفهومی هویت دیجیتال مبتنی بر بلاکچین در کسب‌وکارهای بین‌المللی

حسین رحیمی کلور[*1]

دانشیار، گروه مدیریت بازرگانی، دانشکده علوم اجتماعی، دانشگاه محقق اردبیلی، اردبیل، ایران

مینا پورحسین روشن

دانشجوی دکتری، گروه مدیریت بازرگانی، دانشکده علوم اجتماعی، دانشگاه محقق اردبیلی، اردبیل، ایران

مدیریت اطلاعات

دوره ۱۰، شماره ۲

پاییز و زمستان ۱۴۰۳

چکیده: با توجه به چالش‌های امنیتی و ناکارآمدی در نظام‌های سنتی احراز هویت در تجارت بین‌الملل، این پژوهش با هدف طراحی الگوی مفهومی هویت دیجیتال مبتنی بر بلاکچین در کسب‌وکارهای بین‌المللی انجام شده است. پژوهش حاضر از نوع کیفی است. داده‌ها از طریق مصاحبهٔ نیمه‌ساختاریافته با ۱۲ متخصص در حوزه‌های بلاکچین و تجارت بین‌الملل گردآوری و با استفاده از روش تحلیل مضمون و نرم‌افزار مکس‌کیودا تحلیل شده است. یافته‌ها حاکی از آن است که کاربرد بلاکچین در هویت دیجیتال، می‌تواند از طریق مضامینی همچون «تنظیمگری هوشمند و داده‌محور»، «حاکمیت فردی بر هویت دیجیتال»، «استقلال در مدیریت هویت»، «کارآمدسازی فرایندها و تسهیل صادرات»، «یکپارچگی سامانه‌ها و زیرساخت‌ها» و «اعتمادسازی و شفافیت تجاری» به تحول در فرایندهای هویتی و تعاملات بین‌المللی کمک کند. الگوی مفهومی حاصل، راه‌کاری نوآورانه برای مدیریت غیرمتمرکز و امن هویت دیجیتال ارائه می‌دهد و بستر مناسبی برای سیاست‌گذاری‌های فناورانه، طراحی زیرساخت‌های فرامرزی و توسعهٔ سامانه‌های تجارت الکترونیک فراهم می‌سازد.

کلیدواژه‌ها: هویت دیجیتال، بلاکچین، کسب‌وکارهای بین‌المللی، فناوری.

---

۱. نویسنده مسئول: h_clever@uma.ac.ir

مقدمه

با گسترش فناوری‌های دیجیتال مرزهای جغرافیایی کم‌رنگ‌تر شده و ارتباطات جهانی به‌سرعت در حال گسترش است. در این عصر تحول دیجیتال وابستگی به فناوری برای ارتباطات، تراکنش‌ها و تبادل اطلاعات به‌سرعت رو به افزایش است و جهان کسب‌وکار بیش از هر زمان دیگری، به ابزارهایی برای اعتمادسازی نیاز دارد.

امروزه بیشتر پلتفرم‌های هویتی از ذخیره‌سازی داده‌های متمرکز (مانند ذخیره‌سازی ابری) استفاده می‌کنند. این نوع ذخیره‌سازی با مسائلی ذاتی در زمینهٔ امنیت و حفظ حریم خصوصی، از جمله کنترل، تغییرناپذیری و مدیریت منشأ داده همراه است. اشخاص ثالث غیرمجاز، ممکن است به داده‌ها دسترسی پیدا کنند و آن‌ها را تغییر دهند. هر زمان که مقدار زیادی از داده‌ها در یک مکان مرکزی ذخیره شود، انگیزهٔ بیشتری برای مهاجمان ایجاد می‌شود. از این نظر، ذخیره داده‌های هویتی در این نوع پلتفرم‌های ذخیره‌سازی متمرکز (مانند ذخیره‌سازی ابری و سرورهای مرکزی) به نگرانی جدی در زمینهٔ حفظ حریم خصوصی تبدیل شده است (باندرا، لیانگ، فویتیک، شتی و دی زویسا[1]، ۲۰۲۱). فناوری بلاکچین شکل جدیدی از سازمان‌دهی داده و خدمات است که در سال‌های اخیر ظهور کرده است و با ایجاد یک سیستم جدید تأیید اعتبار داده، انواع داده‌ها را رمزنگاری و مبادله می‌کند (سان و ژانگ[2]، ۲۰۲۰) و روشی موفق برای ایجاد یک سیستم قابل اعتماد و ضد دست‌کاری بین عوامل متقابل است که به شخص سوم قابل اعتماد و متمرکز نیازی ندارد (ژنگ، شی، دای، چن و ونگ[3]، ۲۰۱۸).

این فناوری چهار ویژگی ذاتی دارد که عبارت‌اند از: غیرمتمرکز بودن، قابلیت پیگیری، تغییرناپذیری و خصوصیت‌های ارزی. مزایای عمده‌ای مانند قابلیت اطمینان، اعتماد، امنیت و کارایی را می‌توان بر اساس این ویژگی‌ها تحقق بخشید (گارتنر[4]، ۲۰۲۰). در این رابطه، مدیریت هویت که یکی از جنبه‌های اصلی امنیت سایبری است، هم برای اطمینان از این است که کاربران، همان افرادی هستند که ادعا می‌کنند و هم اینکه از اطلاعات حساس در برابر دسترسی غیرمجاز ضروری حفاظت کند (شاهندشتی و ارشد[5]، ۲۰۲۰). راه‌حل مناسب برای هویت دیجیتال، باید کاربران را قادر سازد تا کنترل کامل بر اطلاعات شخصی خود داشته باشند و فقط اطلاعاتی را که می‌خواهند با هر سرویس به اشتراک بگذارند، به اشتراک بگذارند. فناوری بلاکچین می‌تواند به تحقق یک هویت مستقل کمک کند که کاربر را در کنترل اطلاعات خود قرار می‌دهد (تاکمیا و وانییف[6]، ۲۰۱۸). مدل‌های هویت دیجیتال مبتنی بر بلاکچین به‌عنوان یک راه حل برای چالش‌های امنیتی و حریم خصوصی در کسب‌وکارهای بین‌المللی مطرح شده‌اند. این مدل‌ها که به‌طور فزاینده‌ای در حال توسعه و کاربرد هستند، در مدیریت هویت دیجیتال نقش مهمی دارند. این مسئله، به‌ویژه برای کسب‌وکارهای بین‌المللی اهمیت پیدا می‌کند؛ زیرا آن‌ها نیاز دارند که بتوانند

1. Bandara, Liang, Foytik, Shetty & De Zoysa
2. Sun & Zhang
3. Zheng, Xie, Dai, Chen & Wang
4. Gartner
5. Shahandashti & Arshad
6. Takemiya & Vanieiev

به‌صورت کارآمد با کاربران و مشتریان در کشورهای مختلف ارتباط برقرار کنند. این پژوهش، با ارائهٔ مدلی برای هویت دیجیتال مبتنی بر بلاکچین، در تلاش است به چالش‌های امنیتی و حفظ حریم خصوصی در کسب‌وکارهای بین‌المللی بپردازد. برخلاف تحقیقات قبلی که بیشتر بر جنبه‌های فنی تمرکز داشته‌اند، این مطالعه به نیازهای عملی کسب‌وکارها در تعاملات بین‌المللی توجه دارد و به کاربران امکان کنترل بیشتری بر داده‌های شخصی‌شان می‌دهد. ترکیب اصول امنیت سایبری و مدیریت هویت، رویکرد این پژوهش را به مدلی کاربردی‌تر برای فضای جهانی تبدیل کرده است.

مبانی نظری

فناوری بلاکچین

بلاکچین یک دفترکل توزیع‌شده و غیرقابل‌تغییر است که برای ثبت تراکنش‌ها و ردیابی دارایی‌ها در یک شبکه استفاده می‌شود (آی‌بی‌ام[1]، ۲۰۲۲). مفهوم بلاکچین، نخستین بار در سال ۲۰۰۸ توسط ساتوشی ناکاموتو[2] معرفی شد و به‌عنوان زیرساخت بیت‌کوین، امکان اجماع غیرمتمرکز را بدون نیاز به شخص ثالث فراهم کرد (ناکاموتو، ۲۰۰۸). در واقع، بلاکچین به‌عنوان یک دفترچه ثبت تراکنش‌های الکترونیکی با ویژگی‌های منحصربه‌فرد طراحی شده و به‌منظور ایجاد اسناد ایمن، دقیق، باز و قابل استفاده پدید آمده است. پیاده‌سازی‌های مختلف بلاکچین، بیشتر از سرورها هستند. ظرفیت رمزگذاری و پیاده‌سازی، برخی از منطق تجاری در داخل بلاکچین است؛ اما از آن زمان، فناوری بلاکچین تکامل و توسعه یافته و پیاده‌سازی‌های پیشرفته‌تری نسبت به بیت‌کوین داشته است (السقا، حسین و محمود[3]، ۲۰۱۹). پارامترهای اصلی فناوری بلاکچین شامل بلوک‌ها، گره‌ها، ماینرها و توابع هش هستند. معمولاً هر بلوک شامل داده‌های تراکنش و یک اشاره‌گر هش است که به‌عنوان پیوندی برای بلوک قبلی عمل می‌کند (بلوسی، آیزنهارت و هان[4]، ۲۰۱۹). به این ترتیب، حذف هر بلوک یا وارد کردن یک بلوک جدید در وسط زنجیرهٔ بلاکچین غیرممکن است؛ زیرا در این صورت، تجزیه‌وتحلیل به‌درستی انجام نمی‌شود. سیستم‌هایی که نسخهٔ کامل بلاکچین را ذخیره و اعتبار تراکنش‌ها را تأیید می‌کنند، گره نامیده می‌شوند (ناکاموتو، ۲۰۰۸).

ماینرها، گره‌های کاربری‌ای هستند که یک بلوک جدید در بلاکچین ایجاد می‌کنند. در عمل، آن‌ها تمام تراکنش‌ها را به‌طور هم‌زمان به‌عنوان یک بلوک جمع‌آوری و به بلاکچین اضافه می‌کنند (یاگا، مل، رابی و اسکارفون[5]، ۲۰۱۸). توابع هش، مانند یک اثر انگشت دیجیتال عمل می‌کنند (الجبر، شارما و کومار[6]، ۲۰۱۹). برای اینکه بلوک‌ها به داده‌های تراکنش‌ها در بلاکچین متصل شوند، یک گره باید تابع

1. IBM
2. Nakamoto
3. ALSaqa, Hussein & Mahmood
4. Blossey, Eisenhardt & Hahn
5. Yaga, Mell, Roby & Scarfone
6. Aljabr, Sharma & Kumar

هش یک بلوک را حل کند و شرایط ریاضی خاصی را برآورده کند (پاپاداکیس و کوپاناکی[1]، ۲۰۲۲). بلاکچین‌ها را می‌توان به سه دسته اصلی تقسیم کرد (سازمان تجارت جهانی[2]، ۲۰۱۸):

- بلاکچین‌های عمومی: هر کسی می‌تواند به آن‌ها دسترسی داشته باشد، مشارکت کند و تکمیل تراکنش‌ها را تأیید کند، بدون اینکه به مجوز ثبت‌نام نیاز به داشته باشد. مثال‌هایی از چنین دفاتر کل، ارزهای دیجیتال بیت‌کوین و اتریوم هستند.
- بلاکچین‌های خصوصی: تنها افراد مجاز می‌توانند یک گره را برای تأیید تراکنش‌ها پردازش کنند. آن‌ها همچنین از نظر الگوریتم اجماع تفاوت دارند. تنها گره‌های متعلق به یک سازمان خاص می‌توانند در فرایند اجماع شرکت کنند. یک بلاکچین خصوصی، به‌عنوان یک شبکه مرکزی در نظر گرفته می‌شود؛ زیرا به‌طور کامل تحت کنترل یک سازمان است.
- بلاکچین‌های کنسرسیومی/فدرال: این دسته از بلاکچین‌ها، گسترشی از بلاکچین‌های خصوصی است؛ یعنی گرهی که در قدرت وجود دارد، می‌تواند از ابتدا انتخاب شود و معمولاً دارای شراکت تجاری B2B[3] است. داده‌ها در بلاکچین می‌توانند باز یا خصوصی باشند یا جزئی غیرمتمرکز در نظر گرفته شوند.

هویت دیجیتال

مدیریت هویت دیجیتال، در حال حاضر، یکی از راهبردی‌ترین بحث‌های امنیت سایبری در دنیاست. اعتماد پیش‌نیاز تعاملات و تبادلات در فضای سایبر است و هویت دیجیتال پایهٔ ایجاد اعتماد در فضای سایبر است. طراحی و به‌کارگیری نظام هویت دیجیتال این فرصت را ایجاد می‌کند تا تعاملاتی که در گذشته به‌شکل حضوری و با استفاده از اسناد شناسایی فیزیکی انجام می‌شد، به‌صورت امن و قابل اعتماد و برخط قابل انجام شود. این نظام باید قابل اتکا، امن و گسترش‌پذیر باشد و هیچ‌گونه مخاطره‌ای برای اطلاعات شخصی و حریم خصوصی افراد ایجاد نکند (رسولی، والمحمدی، آزاد و عباس‌پور[4]، ۲۰۲۱). یکی از دلایل اصلی‌ای که افراد به قوانین حریم خصوصی اهمیت می‌دهند، ایجاد بستر برای مدیریت و حفاظت از هویت دیجیتال و ایجاد احساس امنیت برای آن‌ها در فضای سایبر است (پترونیو و چاید[5]، ۲۰۲۰).

سیستم خودمختار هویت[6]

مفهومی است که در آن کاربران بر هویت دیجیتال خود کنترل کامل دارند. به‌گفتهٔ کریستوفر آلن[7] (۲۰۱۶)، این سیستم دارای ده ویژگی اصلی است: وجود مستقل، کنترل بر هویت، دسترسی به داده‌ها، شفافیت سیستم‌ها، ماندگاری هویت، قابلیت حمل اطلاعات، سازگاری با دیگر سیستم‌ها، رضایت کاربر

1. Papadakis & Kopanaki
2. World Trade Organization
3. Business To Business
4. Rasouli, Valmohammadi, Azad & Abbaspour
5. Petronio & Child
6. Sovereign Identity-Self
7. Christopher Allen

برای استفاده از هویت، حداقل‌سازی افشای اطلاعات و حفاظت از حقوق کاربران. این ویژگی‌ها تضمین می‌کنند که کاربران مالک هویت خود هستند و به وابستگی به شخص ثالث نیاز ندارند. به‌کارگیری بلاکچین در این سیستم باعث می‌شود که برخی از این ویژگی‌ها به‌طور ذاتی تحقق یابند؛ از جمله شفافیت که از طریق سازوکار اجماع و ماندگاری داده‌ها و به‌واسطه ساختار غیرقابل‌حذف بلاکچین تأمین می‌شود. علاوه‌براین، سیستم خودمختار هویت به کاربران این امکان را می‌دهد تا اطلاعات خود را مدیریت کنندو تنها با رضایت خود آن را به اشتراک بگذارند. این ویژگی‌ها باعث می‌شود که کاربران هم مالک و هم مدیر اطلاعات هویتی خود باشند، در حالی که سیستم‌های فعلی، مانند زیرساخت‌های کلید عمومی (PKI)[1]، به‌دلیل وابستگی به سرورهای متمرکز، اعتماد کاربران را جلب نکرده‌اند (استوکیکنک و پاولز[2]، ۲۰۱۸). یکی از مشکلات اساسی در سیستم‌های فعلی هویت دیجیتال، وابستگی به نهادهای مرکزی است که علاوه‌بر آسیب‌پذیری در برابر حمله‌ها، اعتماد کاربران را کاهش می‌دهد. برای مثال، زیرساخت‌های کلید عمومی، به‌دلیل مدل متمرکز خود، توانایی برقراری اعتماد بین کاربران و نهادها را ندارند.

از مزایای سیستم خودمختار هویت، می‌توان به کاهش خطرهای افشای اطلاعات، مالکیت کامل کاربران بر هویت دیجیتال و حذف واسطه‌های متمرکز اشاره کرد. همچنین، استفاده از بلاکچین در این سیستم، شفافیت و ماندگاری اطلاعات را تضمین می‌کند؛ زیرا سازوکار اجماع آن، از تغییرات غیرمجاز جلوگیری می‌کند و امکان ثبت دائمی اطلاعات را فراهم می‌آورد. با این حال، چالش‌هایی نیز وجود دارد، از جمله پیچیدگی در پیاده‌سازی، نیاز به زیرساخت‌های پیشرفته و تضمین صحت ادعاهای کاربران که این موارد، به توسعهٔ سازوکارهای اثبات‌پذیری مانند اثبات بدون افشا[3] نیازمند است (استرن و ریدل[4]، ۲۰۲۱). در ادامه، تعدادی از مدل‌های هویت دیجیتال مبتنی بر بلاکچین که در کسب‌وکارهای بین‌المللی کاربرد دارد، معرفی شده است:

مدل تأیید هویت مشتری (KYC)[5]

این مدل به‌عنوان یک فرایند ضروری در صنعت مالی شناخته می‌شود که هدف آن، شناسایی و تأیید هویت مشتریان برای جلوگیری از فعالیت‌های غیرقانونی مانند پول‌شویی است. حنان، شهریار، فردوس و ماروپ[6] (۲۰۲۳)، در پژوهشی به این نکته اشاره می‌کنند که استفاده از این فناوری، می‌تواند هزینه‌های انطباق را کاهش دهد و امنیت بیشتری را فراهم کند. همچنین، مرور سیستماتیک ادبیات موجود در این زمینه نشان می‌دهد که چالش‌هایی همچون عدم استانداردسازی جهانی و نگرانی‌های حریم خصوصی باید حل شوند (شلات، سدلمیر، فولنر و اورباخ[7]، ۲۰۲۲). تحقیقات نشان داده‌اند که سیستم‌های KYC

1. Poblic Key Infrastructure
2. Stokkink & Pouwelse
3. Knowledge Proofs-Zero
4. Ostern & Riedel
5. Know Your Customer
6. Hannan, Shahriar, Ferdous & Maarop
7. Schlatt, Sedlmeir, Feulner & Urbach

دیجیتال می‌توانند با استفاده از هویت خودمختار مبتنی بر بلاکچین، کارایی و راحتی بیشتری را برای کاربران فراهم کنند (سیاحرین، حفیظه، ماروپ و مسلینان[1]، ۲۰۲۴).

مدل هویت چند عاملی[2]

به‌عنوان راه‌حلی برای چالش‌های مختلف مطرح‌شده در نظر گرفته می‌شود. MFA یک طرح احراز هویت چندلایه‌ای است که ریسک‌های مربوط به احراز هویت تک‌عاملی (SFA)[3]، مانند دسترسی غیرمجاز به دستگاه‌های مورد اعتماد و تغییر در ساختار داده را کاهش می‌دهد. چارچوب‌های MFA باید شامل سه عامل اساسی احراز هویت باشند: چیزی که می‌دانید (مانند رمز عبور)، چیزی که دارید (مانند یک دستگاه) و چیزی که هستید (مانند اطلاعات بیومتریک) (ولاسکوئز[4]، ۲۰۲۱). توسعهٔ یک چارچوب MFA حداقل به دو روش احراز هویت نیاز دارد که مالکیت، دانش و یگانگی را تأمین کند. در چارچوب MFA، رمز عبور کاربری و بیومتریک، دو روش رایج احراز هویت است که با روش‌های اضافی دیگر ترکیب می‌شود (فاروق و همکاران[5]، ۲۰۲۲).

مدل اعتبارنامه‌های قابل‌تأیید[6]

این گواهی‌ها از رویکردی غیرمتمرکز برای احراز هویت استفاده می‌کنند و از تکنیک‌های رمزنگاری برای تصدیق و تأیید بهره می‌برند. این گواهی‌ها می‌توانند توسط کاربران ذخیره، مدیریت و ارائه شوند و امکان مدیریت هویت خودمختار را فراهم می‌کنند. گواهی‌های قابل‌تأیید از امضاهای دیجیتال استفاده می‌کنند و می‌توان آن‌ها را با استفاده از یک رجیستری مانند دفتر کل توزیع‌شده (بلاکچین) یا یک پایگاه دادهٔ متمرکز تأیید کرد. این گواهی‌ها امکان مجوزدهی مبتنی بر ویژگی را فراهم می‌کنند؛ به‌طوری که کاربران می‌توانند هنگام درخواست دسترسی به داده‌های علمی، تنها ویژگی‌های خاصی را به‌صورت انتخابی افشا کنند. جنبه‌های عملکردی گواهی‌های قابل‌تأیید به راه‌حل رجیستری انتخاب‌شده وابسته است و پیچیدگی ادغام نیز ممکن است بر همین اساس متغیر باشد (فاروق، ساها و باسنی[7]، ۲۰۲۳).

پیشینه پژوهش

آئین و نوری (۱۴۰۳)، طی پژوهشی نشان دادند که بلاکچین با فراهم‌سازی بستر شفاف، امن و بدون واسطه، از طریق ویژگی‌هایی چون قراردادهای هوشمند، غیرمتمرکز بودن و ثبت تغییرناپذیر اطلاعات، می‌تواند به کاهش هزینه‌ها، افزایش کارایی، بهبود مدیریت ریسک و تسریع فرایندهای مالی در زنجیرهٔ

1. Syahreen, Hafizah, Maarop & Maslinan
2. Multi-Factor Authentication model
3. Single Factor Authentication
4. Velásquez
5. Faruk et al
6. Verifiable credentials model
7. Faruk, Saha & Basney

تأمین منجر شود. این یافته‌ها بیانگر آن است که رویکردهای SCF مبتنی بر بلاکچین، نسبت به روش‌های سنتی، در ایجاد اعتماد میان طرف‌های زنجیره و ارتقای عملکرد از قابلیت بیشتری برخوردارند.

قربان‌پور قارقشلاقی، زینالی و پورکریم (۱۴۰۳)، در پژوهش خود، ابعاد و الزامات انتشار صکوک هوشمند مبتنی بر فناوری بلاکچین را در بازار سرمایهٔ ایران بررسی کردند. نتایج نشان داد که صکوک هوشمند می‌تواند با کاهش هزینه‌های انتشار، افزایش شفافیت و تسریع فرایند تسویه، کارایی بازار سرمایه را به‌طور چشمگیری بهبود بخشد. همچنین، الزامات متعددی در زمینه‌های فناورانه، حقوقی، مدیریتی و ساختاری برای پیاده‌سازی موفق این ابزار شناسایی شد؛ از جمله ایجاد زیرساخت‌های بلاکچینی، بهره‌گیری از قراردادهای هوشمند، تضمین امنیت داده‌ها و تدوین قوانین حمایتی. در مجموع، نتایج این مطالعه بیانگر آن است که استفاده از صکوک هوشمند، نه‌تنها می‌تواند به ارتقای سطح اعتماد و جذب سرمایه‌گذاران داخلی و بین‌المللی منجر شود، بلکه زمینه‌ساز تحول در شیوه‌های تأمین مالی اسلامی در ایران خواهد بود.

شاه‌ویسی و طارمی (۱۴۰۰) تأکید می‌کنند که بلاکچین با حذف واسطه‌ها و افزایش شفافیت، تأثیر چشمگیری بر بازارهای مالی و پولی دارد. همچنین، دژدانی، شاهین پنجه، ابراهیمی و فاضل دربندی (۱۴۰۳) به تأثیر بلاکچین بر مدل‌های کسب‌وکار و ایجاد شفافیت در فرایندهای بازاریابی اشاره می‌کنند. با توجه به افزایش تعداد دستگاه‌ها و کاربران، معماری‌ها و پروتکل‌های فعلی، قادر به پاسخ‌گویی کامل به نیازهای امنیتی، از جمله احراز هویت و مدیریت دسترسی، نیستند. در این رابطه سلامی و حسینی (۱۴۰۲)، به بررسی چالش‌های امنیتی ارتباطات در سیستم‌های هواشناسی مبتنی بر اینترنت اشیا پرداختند و یک طرح احراز هویت ایمن مبتنی بر بلاکچین را برای این سیستم‌ها پیشنهاد کردند. طرح پیشنهادی شامل احراز هویت متقابل، سیاست‌های دسترسی و تولید توکن است که امنیت ارتباط بین تجهیزات هواشناسی را تضمین می‌کند. نتایج ارزیابی امنیتی، به‌صورت رسمی و غیررسمی، نشان می‌دهد که این طرح در برابر حمله‌های فعال و غیرفعال مقاوم است.

یافته‌های پژوهش قلی‌زاده، اسماعیلی، ابراهیم‌پور و مرادی (۱۴۰۲)، نشان می‌دهد که پیاده‌سازی فناوری بلاکچین در سازمان تأمین اجتماعی با چالش‌های متعددی نظیر انطباق منابع انسانی، محدودیت منابع مالی، نقش کنشگران برون‌سازمانی و نیاز به فرهنگ‌سازی همراه است. این فناوری با ویژگی‌هایی همچون جعل‌ناپذیری، شفافیت، تغییرناپذیری اطلاعات و تمرکززدایی، می‌تواند فرایندهایی مانند احراز هویت مشتریان را تسهیل کند و موجب کاهش ریسک تقلب، افزایش اعتمادپذیری، سرعت در ارائه خدمات و بوروکراسی‌زدایی شود. با وجود مزایای مهم، سازمان با چالش‌هایی نظیر هزینه‌های استقرار، اصلاح زمان‌بر اطلاعات و آموزش کاربران روبه‌رو است. به‌منظور غلبه بر این چالش‌ها، تقویت زیرساخت‌ها، مدیریت بهینهٔ منابع و بهره‌گیری از قراردادهای هوشمند برای جایگزینی سیستم‌های فعلی توصیه می‌شود. در نهایت، موفقیت در پیاده‌سازی نیازمند توجه ویژه به ابعاد مدیریتی، فنی و فرهنگی سازمان است.

آبی‌زاده، فتحی و مینویی (۱۴۰۱)، به بررسی چالش‌های کنترل دسترسی در شبکه بلاکچین پرداخته و روشی نوین مبتنی بر یادگیری ماشین پیشنهاد می‌دهد. فرایند تأیید دستی تراکنش‌ها در بلاکچین، به‌دلیل زمان‌بر بودن و غیرکاربرپسند بودن، از پذیرش کامل این فناوری جلوگیری می‌کند. روش ارائه‌شده ترکیبی از الگوریتم‌های خوشه‌بندی و دسته‌بندی است که با برچسب‌گذاری داده‌ها و آموزش مدل یادگیری ماشین، تراکنش‌های سالم را با دقت ۹۸ درصد از تراکنش‌های مشکوک تفکیک می‌کند. این روش امضای خودکار تراکنش‌ها و شناسایی ناهنجاری‌ها را ممکن می‌سازد و با بهبود امنیت، از تقلب و کلاه‌برداری جلوگیری می‌کند. همچنین، سیستم تشخیص ناهنجاری ارائه‌شده، داده‌های مربوط به امنیت کاربران را به‌صورت محلی ذخیره و اجرا می‌کند و قابلیت استفاده در برنامه‌های غیرمتمرکز و تبادلات منظم را دارد. این رویکرد کاربردهای گسترده‌ای در بهبود فرایندهای اینترنت اشیا و جلوگیری از فعالیت‌های مخرب در کیف‌پول‌های بلاکچینی ارائه می‌دهد.

در پژوهشی که توسط محمدی و قنبری در سال ۱۳۹۹ انجام شد، یک مدل احراز هویت امن و توزیع‌شده برای شبکهٔ سلامت الکترونیک ارائه شد که با ترکیب زیرساخت کلید عمومی و فناوری بلاکچین طراحی شده بود. این مدل برای حل چالش‌هایی نظیر حفظ محرمانگی، یکپارچگی داده‌ها و جلوگیری از نقطه یگانه شکست ارائه شده و در نسخه‌نویسی الکترونیکی به‌عنوان یک مصداق عملی مورد بررسی قرار گرفته است. نتایج نشان می‌دهد که این مدل می‌تواند احراز هویت دوطرفه، مقیاس‌پذیر و توزیع‌شده را فراهم کند و نیازمندی‌های امنیتی شبکه‌های سلامت الکترونیک را پوشش دهد. مدل پیشنهادی علاوه‌بر امنیت زیاد، از نظیربه‌نظیر بودن و عدم وابستگی به سرور مرکزی بهره می‌برد و قادر است با خدمات متنوع حوزهٔ سلامت الکترونیک منطبق شود؛ با این حال، برای بهبود سرعت اجرا می‌توان از الگوریتم‌های رمزگذاری متفاوت استفاده کرد. همچنین امکان پیاده‌سازی این مدل در بلاکچین‌های عمومی و خصوصی و مقایسه نتایج وجود دارد. با توسعهٔ خدمات سلامت الکترونیک و افزایش نیاز به امنیت و کارایی در تبادلات، این مدل می‌تواند در بهبود فرایندهای احراز هویت نقش مهمی ایفا کند و با به‌روزرسانی‌های آینده، کارایی خود را ارتقا بخشد.

آیبو و اوجو[1] (۲۰۲۵)، به بررسی نقش فناوری بلاکچین در ایجاد و تقویت هویت دیجیتال پرداختند. یافته‌های آن‌ها نشان می‌دهد که فناوری بلاکچین با ویژگی‌هایی چون غیرمتمرکز بودن، شفافیت، امنیت زیاد و کنترل کاربر بر داده‌ها، می‌تواند مشکلات سنتی هویت دیجیتال مانند جعل هویت، تمرکز اطلاعات در دست نهادهای مرکزی و نبود حریم خصوصی را کاهش دهد. مقاله تأکید می‌کند که مدل‌های مبتنی بر «هویت خودمختار»[2] با بهره‌گیری از بلاکچین، می‌توانند تحولی در مدیریت هویت افراد و سازمان‌ها ایجاد کنند؛ به‌طوری‌که افراد بتوانند بدون وابستگی به دولت یا شرکت ثالث، هویت خود را اثبات و کنترل کنند.

1. Ayebo & Ojo
2. Self-Sovereign Identity

خاوند[1] (۲۰۲۵) با استفاده از مطالعهٔ نگاشت نظام‌مند، به بررسی وضعیت موجود پژوهش‌ها در خصوص هویت دیجیتال مبتنی بر فناوری بلاکچین در محیط شهرهای هوشمند پرداخته است. یافته‌ها نشان می‌دهند که بلاکچین، به‌دلیل ویژگی‌هایی چون امنیت، تمامیت داده و حذف واسطه‌ها، بستری مناسب برای پیاده‌سازی سیستم‌های هویت دیجیتال فراهم می‌کند. این فناوری امکان احراز هویت امن، سریع و تغییرناپذیر را فراهم می‌کند و می‌تواند در بخش‌هایی چون خدمات بانکی، رأی‌گیری الکترونیکی، سیستم سلامت، حمل‌ونقل و عملیات دولت الکترونیک به‌کار رود.

پاراته، ردی، آگاروال و سوریادورا[2] (۲۰۲۳)، در مقاله‌ای به بررسی تکامل و اهمیت سازوکارهای احراز هویت دیجیتال پرداختند، به‌ویژه در زمینهٔ فرایندهای KYC که در تضمین امنیت و یکپارچگی تراکنش‌های مالی در عصر دیجیتال نقش حیاتی دارند. این مقاله، مزایای فناوری‌های احراز هویت دیجیتال شامل امنیت پیشرفته، کارایی و تجربهٔ بهتر مشتری را مورد تأکید قرار می‌دهد و در عین حال، به چالش‌هایی مانند نگرانی‌های امنیتی، مسائل مربوط به قابلیت همکاری و محیط‌های نظارتی در حال تغییر می‌پردازد. ادغام تکنولوژی‌هایی مانند بلاکچین، یادگیری ماشین و سیستم‌های ارتباطی پیشرفته، این پتانسیل را دارد که چشم‌انداز تأیید هویت دیجیتال در بانکداری را بازتعریف کند. علاوه‌براین، پژوهش بر اهمیت اعتماد، شفافیت و کاربرپسندی در سیستم‌های احراز هویت دیجیتال تأکید می‌کند. نتیجه‌گیری مقاله، آیندهٔ امیدوارکننده احراز هویت دیجیتال در بانکداری را بازتاب می‌دهد و بر لزوم نوآوری و انطباق مداوم برای مواجهه با چالش‌های جدید تأکید می‌کند.

جگاناتان[3] (۲۰۲۱)، در پژوهشی ضمن بیان این نکته که هویت دیجیتال خودمختار، دیدگاهی جایگزین برای حفاظت از اطلاعات کاربران نهایی در فضای سایبری بسیار آسیب‌پذیر است، بیان می‌کند که این مفهوم در مراحل اولیهٔ توسعه قرار دارد و توسط چندین سازمان پیشرو در سراسر جهان پشتیبانی می‌شود. کاربران باید کنترل مستقیم اطلاعات خود را به‌دست آورند و ملزم نباشند که شرایط و ضوابط ارائه‌دهندگان خدمات را رعایت کنند تا حریم خصوصی و امنیت داده‌هایشان تضمین شود. با اتخاذ این اصل، به‌عنوان یکی از اصول راهنمای هویت دیجیتال خودمختار، این مفهوم تلاش می‌کند که مشکلات مربوط به سرقت هویت و کلاه‌برداری را حل کند و خطرهای نقض داده‌ها را کاهش دهد. با پذیرش این رویکرد، همهٔ بخش‌های صنعتی از آن بهره‌مند خواهند شد، هزینه‌های مربوط به مدیریت هویت دیجیتال و دسترسی کاهش خواهد یافت و رضایت کاربران نهایی بهبود می‌یابد.

ماهولا، تان و کرامپووتس[4] (۲۰۲۱)، بیان می‌کنند که اگرچه SSI[5] ک تغییر پارادایم امیدوارکننده برای مدیریت هویت است، پیش‌بینی زمان و نحوهٔ پذیرش آن به‌دلیل چالش‌های موجود همچنان دشوار است. اتحادیهٔ اروپا، می‌تواند به‌عنوان شتاب‌دهنده در صحنهٔ بین‌المللی و محرک اعضای خود برای حرکت

1. Khaund
2. Parate, Reddi, Agarwal & Suryadevara
3. Jeganathan
4. Mahula, Tan & Crompvoets
5. Self-sovereign Identity Implementation

به‌سمت SSI عمل کند. در این زمینه، پیشرفت‌های مرتبط با EBSI[1] و ESSIF[2] می‌تواند به همگرایی SSI و فناوری بلاکچین کمک کند؛ با این حال، در این مرحله، به‌ویژه با توجه به تنوع زیرساختی، سیاسی و سازمانی میان کشورهای عضو اتحادی، اروپا، پیش‌بینی عملکرد SSI در سراسر اروپا دشوار است. در این مقاله، یک چارچوب تحلیلی برای ارزیابی سازگاری بلاکچین با بخش عمومی ایجاد شده است. این مطالعه نشان می‌دهد که این دو نوآوری، به‌ویژه در سطح مفهومی، اشتراکات زیادی دارند، مانند حذف واسطه‌ها، تراکنش‌های شفاف و زیرساخت‌های غیرمتمرکز. این پژوهش بر ضرورت تمرکز بر مدل‌های تجاری و فنی SSI و شناسایی بهترین فناوری‌های مکمل برای آن تأکید می‌کند.

روش‌شناسی پژوهش

این پژوهش به‌روش کیفی و با استراتژی تحلیل مضمون انجام شده است و هدف آن شناسایی ابعاد کلیدی فناوری بلاکچین و ارائه الگویی مفهومی است که بتواند نحوهٔ تأثیرگذاری بلاکچین بر بهبود تعاملات، امنیت و کارایی در حوزه‌های بین‌المللی را تبیین کند. تحلیل مضمون فرایندی برای تحلیل داده‌های متنی است و داده‌های پراکنده و متنوع را به داده‌های غنی و تفصیلی تبدیل می‌کند (خنیفر و مسلمی، ۱۳۹۷). در این تحقیق، از نمونه‌گیری هدفمند برای اتخاذ نمونه استفاده شد و نمونه‌گیری تا اشباع نظری ادامه یافت. مصاحبه از بین ۱۲ نفر از کسانی انجام شد که در زمینهٔ بلاکچین و کسب‌وکارهای بین‌المللی تخصص داشتند. این افراد شامل اساتید دانشگاه، پژوهشگران، مشاوران کسب‌وکار و مدیر تحقیق و توسعه بودند. این افراد به‌دلیل داشتن تخصص و تجربه در زمینه‌های مختلف بلاکچین و تحولات دیجیتال در سطح بین‌المللی انتخاب شدند. در گام نخست، از ۷ سؤال باز در پروتکل مصاحبه استفاده شد و در طول فرایند مصاحبه نیز سؤال‌های جدیدی مطرح شد. متن سؤال‌ها به شرح زیر است:

۱. چه عواملی مانع شکل‌گیری یک سیستم احراز هویت دیجیتال مؤثر در کسب‌وکارهای فراملی می‌شوند؟
۲. چه ویژگی‌هایی را برای یک سیستم احراز هویت امن و قابل اعتماد در تعاملات بین‌المللی ضروری می‌دانید؟
۳. از نگاه شما، چطور می‌توان اعتبار و اصالت اسناد و اطلاعات کاربران را در فضای دیجیتال حفظ و اثبات کرد؟
۴. تجربهٔ شما در مواجهه با چالش‌های مربوط به شفافیت و اعتماد در فرایندهای دیجیتال چه بوده و چه راه‌کارهایی مؤثر بوده‌اند؟
۵. در چه شرایطی حاضرید به یک زیرساخت دیجیتال برای مدیریت اطلاعات حساس خود اعتماد کنید؟

1. European Blockchain Services Infrastructure
2. European Self-Sovereign Identity Framework

۶. به نظر شما، چه سازوکارهایی می‌توانند تعامل میان سامانه‌های مختلف در کشورهای گوناگون را در حوزهٔ احراز هویت تسهیل کنند؟
۷. اگر امکان طراحی یک سیستم نوین احراز هویت را داشتید، چه اصول یا قابلیت‌هایی را در اولویت قرار می‌دادید و چرا؟

بعد از انجام مصاحبه بلافاصله محتوای آن مکتوب و تحلیل آن‌ها آغاز شد. نتایج مصاحبه‌ها با روش تحلیل مضمون تحلیل شد. بعد از مرور مکرر متن مصاحبه‌ها، داده‌ها در قالب جملات و پاراگراف‌های مرتبط با متن اصلی شکسته شد. سپس کدهای مناسب هر واحد معنایی نوشته و کدها بر اساس تشابه معنایی طبقه‌بندی شد. در ابتدا تعداد ۳۲۴ کد اولیه استخراج شد؛ سپس با مرور و ادغام کدهای هم‌معنا و حذف موارد تکراری یا فاقد ارتباط مفهومی، ۲۱۰ کد نهایی تأیید شد. این کدها در مرحلهٔ بعد، به ۵۶ مضمون پایه دسته‌بندی شدند. در ادامه با ترکیب مفاهیم مشابه و تحلیل روابط میان آن‌ها، ۱۶ مضمون سازمان‌دهنده استخراج شد. در نهایت، ۶ مضمون فراگیر به‌عنوان برداشت کل‌نگرانه از یافته‌ها ارائه شد. از نرم‌افزار مکس کیودا[1] نسخهٔ ۲۰۲۰ برای واکاوی نتایج پژوهش استفاده شد. برای ارزیابی و اعتبارسنجی کیفیت تحقیق از فرایند ارزیابی به وسیلهٔ بازخورد از پاسخ‌دهندگان استفاده شد. تمامی اظهارنظرهای پاسخ‌دهندگان بررسی و در فرایند تحلیل پژوهش از آن استفاده شد. همچنین سه نفر از مصاحبه‌شوندگان که از استادان دانشگاه بودند و تجربهٔ زیادی در انجام تحقیقات کیفی و کار با نرم‌افزار مکس کیودا داشتند، فرایند کدگذاری را بازبینی کردند و نظرهای آن‌ها اِعمال شد.

یافته‌های پژوهش

در پژوهش حاضر، از نظرهای ۱۲مصاحبه‌شونده استفاده شده که اطلاعات افراد مصاحبه‌شونده در جدول ۱ آمده است.

داده‌های گردآوری شده نشان می‌دهد که مصاحبه‌شوندگان از نظر سمت شغلی، سطح تحصیلات، سابقهٔ کاری و سن تنوع چشمگیری داشتند. گروه نمونه شامل اعضای هیئت علمی دانشگاه، پژوهشگران، مشاوران کسب‌وکار، مدیران تحقیق و توسعه و دانشجویان دکتری بود که هر یک سابقه‌ای بین ۴ تا ۱۱ سال در حوزه‌های مرتبط با بلاکچین و تجارت بین‌الملل داشت. این تنوع باعث افزایش عمق و جامعیت داده‌ها شده است. از نظر تحصیلات، اکثر مشارکت‌کنندگان دارای مدرک دکتری یا کارشناسی‌ارشد بودند که نشان‌دهندهٔ تخصص زیاد در موضوعات مرتبط است. همچنین، ردهٔ سنی افراد بین ۳۸ تا ۵۶ سال بوده است که ترکیبی از تجربهٔ میدانی و بینش تحلیلی را در اختیار پژوهش قرار داده است. استفاده از نمونه‌گیری هدفمند نظری و انتخاب مشارکت‌کنندگانی با تجارب حرفه‌ای متفاوت، به افزایش قابلیت اعتماد و غنای داده‌های کیفی کمک کرده است.

1. MAXQDA

جدول ۱. ویژگی‌های جمعیت شناختی مصاحبه شوندگان

کد	سمت شغلی	سن	تحصیلات	سابقه کاری مرتبط (سال)
P۱	اساتید دانشگاه	۵۱	دکتری	۱۱
P۲		۴۸	دکتری	۹
P۳		۵۶	دکتری	۱۰
P۴		۴۶	دکتری	۸
P۵		۴۲	دکتری	۵
P۶		۴۶	دکتری	۷
P۷	پژوهشگر	۳۸	کارشناسی ارشد	۴
P۸		۴۴	کارشناسی ارشد	۵
P۹		۴۷	کارشناسی ارشد	۵
P۱۰	مشاور کسب‌وکار	۴۳	دانشجوی دکتری	۶
P۱۱		۴۰	کارشناسی ارشد	۵
P۱۲	مدیر تحقیق و توسعه	۴۵	کارشناسی ارشد	۸

فرایند تحلیل داده‌ها از طریق کدگذاری مضمون انجام شد. ابتدا تمامی مصاحبه‌ها به‌طور کامل ضبط و سپس به متن مکتوب تبدیل شدند. در مرحلهٔ بعد، این متن‌ها کدگذاری شدند و کدهای اولیه از آن‌ها استخراج شد. این کدها سپس دسته‌بندی و تجزیه وتحلیل شدند و شش مضمون اصلی به‌دست آمد.

جدول ۲. مقوله‌های زیربنایی مدل‌سازی هویت دیجیتال مبانی بر بلاکچین در کسب‌وکارهای بین‌المللی

مضامین پایه	مضامین سازمان‌دهنده	مضامین فراگیر
استفاده از هویت دیجیتال در صدور گواهی مبدأ کالا	سیاست‌گذاری مبتنی بر هویت	تنظیمگری هوشمند و داده‌محور
ثبت مالکیت برندها بر بستر بلاکچین با شناسهٔ دیجیتال		
اعطای مجوز دسترسی به بازارها بر اساس پروفایل دیجیتال		
تقویت سامانه‌های گزارشگری تخلف با احراز هویت مطمئن	کنترل ریسک و تقلب	
توسعهٔ الگوریتم‌های تطبیق هویتی برای مقابله با هویت‌های جعلی		
کنترل نقل‌وانتقال مالکیت در تجارت جهانی با پروفایل هویتی	هماهنگی مقرراتی	یکپارچگی سامانه‌ها و زیرساخت‌ها
اتصال پروفایل دیجیتال شرکت‌ها به مجوزهای صادراتی		
صدور گواهی‌های اعتباری قابل‌ردیابی مبتنی بر هویت دیجیتال	استانداردسازی داده‌های هویتی	
طراحی شناسهٔ یکتای تجاری برای کسب‌وکارهای بین‌المللی		
یکپارچه‌سازی اطلاعات احراز هویت در سامانه‌های لجستیکی		
استانداردسازی پروتکل‌های هویت دیجیتال بین کشورها		
یکپارچه‌سازی داده‌های هویتی با سامانه‌های گمرکی	همکاری سامانه‌های بین‌المللی	
ادغام سامانه‌های احراز هویت در پلتفرم‌های تجارت الکترونیک		

مضامین پایه	مضامین سازمان‌دهنده	مضامین فراگیر
کنترل کلید خصوصی توسط فرد	مالکیت و کنترل هویت	حاکمیت فردی بر هویت دیجیتال
اختیار حذف اطلاعات هویتی		
امکان بازیابی دسترسی از سوی صاحب هویت		
قابلیت تنظیم دسترسی به داده‌ها		
امکان رمزنگاری اطلاعات حساس	حریم خصوصی مبتنی بر رضایت	
انتخاب سطح افشای اطلاعات		
امکان ناشناس‌بودن در پلتفرم‌ها		
ارائه انتخابی اطلاعات هویتی	افشای کنترل‌شده اطلاعات	
امکان افشای حداقلی اطلاعات		
اثبات هویت بدون افشای کامل		
کنترل کاربر بر زمان افشا		
خودتأییدی هویت از طریق بلاکچین	تمرکززدایی ساختاری	استقلال در مدیریت هویت
نبود مرجع متمرکز		
اعتبارسنجی توزیع‌شده در شبکه		
ثبت هویت بدون مراجعه به مرجع دولتی		
عدم نیاز به مجوز نهادی		
ایجاد هویت خودسازمان‌ده		
کنترل کاربر بر فرایند احراز هویت		
توانایی اصلاح و به‌روزرسانی اطلاعات	خود تعریفگری هویتی	
امکان انتخاب اطلاعات هویتی		
رصد اصالت گواهی‌ها و مدارک با ثبت دیجیتال هویت صادرکننده	مدیریت اسناد دیجیتال	کارامدسازی فرایندها و تسهیل صادرات
توسعه امضای هوشمند قراردادها بر پایه احراز هویت دیجیتال		
کاهش جعل اسناد تجاری از طریق امضای دیجیتال مبتنی بر هویت		
افزایش شفافیت سوابق عملکرد تجار با ردیابی دیجیتال	ارزیابی اعتبار شرکت‌ها	
استفاده از بلاکچین برای اعتبارسنجی سوابق هویتی شرکت‌ها		
احراز هویت دیجیتال صادرکنندگان در سامانه‌های تجارت بین‌الملل	افزایش شفافیت تبادلات	اعتمادسازی و شفافیت تجاری
اعتبارسنجی تجار با تحلیل رفتار تراکنشی مبتنی بر هویت		
توسعه شناسه‌های دیجیتال قابل‌اعتماد برای بازیگران زنجیرهٔ تأمین		

مضامین پایه	مضامین سازمان‌دهنده	مضامین فراگیر
احراز هویت دیجیتال شرکت‌های حمل‌ونقل بین‌المللی		
کنترل تطبیق صادرات با مجوزها از طریق احراز هویت دیجیتال		
طراحی زیرساخت احراز هویت قابل‌اعتماد فرامرزی		
بهبود امنیت سایبری معاملات بین‌المللی با تأیید هویت دیجیتال		
ایجاد گذرنامه تجاری دیجیتال برای فعالان اقتصادی		
هش‌گذاری اطلاعات هویتی	امنیت رمزگذاری شده	
جلوگیری از دست‌کاری داده‌ها		
رمزنگاری غیرقابل شکستن		
امنیت چندلایه برای داده‌های هویتی		
ثبت دائمی تراکنش‌های هویتی	پایداری داده‌های هویتی	
قابلیت ردیابی تغییرات		
مستندسازی غیرقابل حذف		
داده‌های تغییرناپذیر		
قابلیت اثبات مالکیت بدون افشا	تأییدپذیری بدون افشا	
تأیید صحت داده از سوی اشخاص ثالث		

شش مضمون اصلی در زمینه تأثیر بلاکچین بر کسب‌وکارهای بین‌المللی شناسایی شده که در ادامه تشریح می‌شود.

۱. تنظیمگری هوشمند و داده‌محور

این یافته ناظر بر ظرفیت بلاکچین در تسهیل سیاست‌گذاری‌های هوشمند، صدور گواهی‌های مبتنی بر شناسه دیجیتال و نظارت بی‌واسطه در فرایندهای تجارت جهانی است. داده‌های هویتی رمزنگاری‌شده و تغییرناپذیر، مرجع موثقی برای تصمیم‌گیری تنظیمگران فراهم می‌آورد. مصاحبه‌شوندهٔ (P۳) بیان می‌کند: «وقتی گواهی مبدأ کالا با شناسه بلاکچینی صادر بشه، خود گمرک دیگه نیاز به بررسی‌های وقت‌گیر نداره.» برخلاف مدل e-KYC که تمرکز آن بر تأیید مشتری در خدمات مالی است (حنان و همکاران، ۲۰۲۳)، این مدل از بلاکچین برای خلق یک چارچوب تنظیمگری چندسطحی استفاده می‌کند. مدل‌های SSI نیز فاقد قابلیت تطبیق با الزامات قانونی تجارت بین‌المللی هستند (ماهولا و همکاران، ۲۰۲۱).

۲. یکپارچگی سامانه‌ها و زیرساخت‌ها

یافته‌ها نشان دادند که بلاکچین می‌تواند نقش زیربنایی در همگرایی زیرساخت‌های گمرکی، سامانه‌های احراز هویت و پلتفرم‌های تجارت جهانی ایفا کند. این یکپارچگی مستلزم استانداردسازی پروتکل‌های

هویت دیجیتال است. طبق گفتهٔ مصاحبه‌شونده (P۷): «پروفایل دیجیتال شرکت باید به‌طور خودکار با سامانه صادرات همگام بشه، نه اینکه دوباره مدارک بخواد.» مدل‌های DID و VC به لحاظ فنی قابلیت تعامل‌پذیری دارند (آلن، ۲۰۱۶)؛ اما اغلب به لایهٔ زیرساختی محدود می‌مانند. مدل پژوهش حاضر، نوعی پیوند فنی ـ عملیاتی میان سامانه‌ها برقرار کرده است.

۳. حاکمیت فردی بر هویت دیجیتال

این مضمون تأکید می‌کند که کاربران باید امکان کنترل سطح افشای اطلاعات، رمزنگاری اطلاعات حساس و حذف یا بازیابی هویت خود را داشته باشند. این ویژگی، نه‌تنها به افزایش امنیت منجر می‌شود، بلکه حقوق داده‌ای کاربران را تضمین می‌کند. بنابر نظر مصاحبه‌شونده (P۶): «وقتی من می‌تونم انتخاب کنم که چه اطلاعاتی فاش بشه، احساس مالکیت واقعی دارم.»

در مدل‌های SSI این اصل محوری است (آلن، ۲۰۱۶)؛ ولی در عمل، هنوز بسیاری از چارچوب‌ها به زیرساخت‌های شخص ثالث وابسته‌اند. مدل این پژوهش با تکیه بر قابلیت‌های رمزنگاری و ذخیره‌سازی توزیع‌شده، این حاکمیت را از سطح تئوری به اجرا نزدیک می‌کند.

۴. استقلال در مدیریت هویت

هویت خودسازمان‌ده بر پایهٔ بلاکچین، با حذف مرجع صدور متمرکز و امکان ثبت، تأیید و به‌روزرسانی هویت در شبکهٔ توزیع‌شده، ساختاری نوین و قابل‌اعتماد برای فعالیت بین‌المللی ایجاد می‌کند. مصاحبه‌شوندهٔ (P۹) بیان کرد: «هویتی که وابسته به دولت یا بانک خاص نباشه، برای تجارت بین‌المللی کاربردی‌تره.» DIDها از این ویژگی برخوردارند؛ اما در عمل، همچنان به یک ارائه‌دهندهٔ رجیستری نیاز دارند. مدل حاضر بر نبود مرجع مرکزی و قابلیت خودتأییدی، تأکید داشته است.

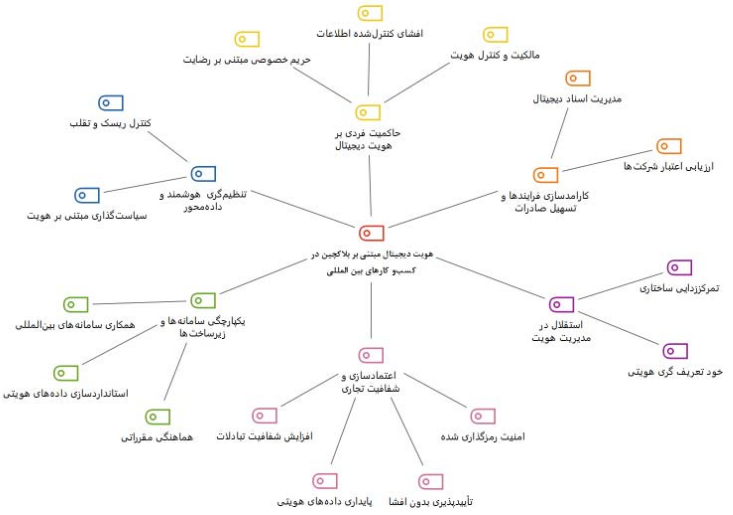
۵. کارآمدسازی فرایندها و تسهیل صادرات

بلاکچین با ثبت دیجیتال امضاها، اصالت گواهی‌ها و قراردادهای هوشمند، روندهای صادراتی را تسهیل می‌کند و احتمال جعل را به حداقل می‌رساند. با توجه به نظر یکی از مصاحبه‌شونده‌ها (P۱۰): «گواهی‌ای که مهر فیزیکی بخواد یعنی عقب‌ماندگی. با بلاکچین، امضای دیجیتال خودش حرف می‌زنه.» در مدل‌های e-KYC، این روند محدود به تأیید هویت است (شلات و همکاران، ۲۰۲۱). در حالی‌که مدل پژوهش حاضر، ثبت سوابق، تطبیق با مجوزها و یکپارچه‌سازی با لجستیک را نیز شامل می‌شود.

۶. اعتمادسازی و شفافیت تجاری

ایجاد شناسه‌های دیجیتال قابل ردیابی برای بازیگران زنجیره تأمین، اعتبارسنجی عملکرد تجاری و تعاملات بدون واسطه، بستری شفاف و قابل اعتماد در تجارت بین‌المللی ایجاد می‌کند. مصاحبه‌شونده‌ای بیان کرد (P۱): «شفافیت یعنی بتونی مسیر یک کالا یا بازیگر تجاری رو از ابتدا تا انتها ببینی.» DID و VC قابلیت ثبت سوابق دارند؛ اما در عمل، فاقد پیوند با شبکه‌های حمل‌ونقل و گمرکی هستند. مدل پژوهش با پیوند مستقیم هویت دیجیتال به فرایندهای زنجیره تأمین، این شکاف را پوشش می‌دهد.

الگوی حاصل از تحلیل مضامین، در قالب شکل ۱ نشان داده شده است.



شکل ۱. الگوی مفهومی پژوهش

بحث و نتیجه‌گیری

نتایج این پژوهش نشان می‌دهد که فناوری بلاکچین با ارائه ساختار غیرمتمرکز، شفاف و مقاوم در برابر دست‌کاری، قابلیت‌های نوینی را برای بازطراحی نظام هویت دیجیتال در عرصهٔ تجارت بین‌المللی فراهم می‌کند، مشخص شد که تنظیمگری هوشمند بر پایهٔ داده‌های هویتی می‌تواند سیاست‌گذاری مبتنی بر پروفایل دیجیتال را ممکن سازد؛ حاکمیت فردی بر هویت، از طریق مالکیت کلید خصوصی و کنترل افشای اطلاعات، کاربران را از وابستگی به نهادهای مرکزی رها می‌سازد؛ استقلال در مدیریت هویت و ساختار خودتأییدکننده، اعتماد بین‌المللی را تقویت می‌کند؛ و کارآمدسازی فرایندها از طریق امضای هوشمند و ثبت اسناد بر بستر بلاکچین، جعل و تأخیر را به حداقل می‌رساند. همچنین اتصال زیرساخت‌های لجستیکی، گمرکی و سامانه‌های بین‌المللی با هویت دیجیتال، موجب تسریع صادرات و افزایش شفافیت و اعتبارسنجی در زنجیرهٔ تأمین می‌شود. الگوی نهایی پژوهش، چارچوبی استراتژیک برای توسعهٔ زیرساخت‌های فرامرزی هویت دیجیتال با رویکرد فناوری‌محور ارائه می‌دهد.

همچنین نتایج نشان می‌دهد که مفهوم هویت دیجیتال مبتنی بر بلاکچین، در بستر کسب‌وکارهای بین‌المللی، واجد ابعاد پیچیده و چندلایه‌ای است که صرفاً از مسیر تحلیل‌های فناورانه قابل تبیین نیست. مضامین فراگیر شناسایی‌شده نمایانگر این واقعیت‌اند که مقولهٔ هویت دیجیتال در زمینه‌های بین‌المللی، نه‌تنها با زیرساخت‌های فنی و داده‌ای گره خورده است، بلکه به‌طور مستقیم با ابعاد حقوقی، نهادی و عملیاتی نیز درگیر است. در مقایسه با پژوهش‌های پیشین، یافته‌های این مطالعه در بسیاری از موارد با

مفروضات و دستاوردهای نظری موجود در ادبیات تطبیق دارد. برای نمونه، مفهوم «حاکمیت فردی بر هویت دیجیتال» که در مدل‌های self-sovereign identity مورد تأکید قرار گرفته (آلن، ۲۰۱۶)، در این مطالعه نیز به‌عنوان یک محور اساسی درک شده است و مصاحبه‌شوندگان بر لزوم استقلال کاربران در مدیریت داده‌های شخصی خود تأکید داشتند. همچنین، یافته‌های مربوط به امنیت داده و تأییدپذیری بدون افشا، با مطالعاتی نظیر (ژنگ و همکاران، ۲۰۱۸؛ شاهندشتی و ارشد، ۲۰۲۰) هم‌سو است که بلاکچین را به‌عنوان بستری برای حفظ یکپارچگی و اعتبار اطلاعات هویتی معرفی کرده‌اند. این پژوهش نشان می‌دهد که هویت دیجیتال در بستر بین‌المللی، نیازمند الگویی است که بتواند به شکل یکپارچه، با فرایندهای گمرکی، تجارت برون‌مرزی، و زنجیرهٔ تأمین ارتباط برقرار کند. به بیان دیگر، پژوهش حاضر از منظر کاربردی، افق وسیع‌تری را در نظر گرفته و ابعاد نهادی ـ سازمانی هویت دیجیتال را پررنگ‌تر دیده است. همچنین، در حالی‌که اغلب پژوهش‌های پیشین بر سطوح کاربرمحور تمرکز داشته‌اند، این تحقیق نشان داد که برای پیاده‌سازی مؤثر هویت دیجیتال در کسب‌وکارهای بین‌المللی، نیاز به ساختاری فراتر از کنترل فردی بر داده‌ها وجود دارد؛ ساختاری که قادر باشد تنظیمگری چندسطحی، هماهنگی بین سازمانی، و امکان تعامل‌پذیری میان سامانه‌ها را فراهم آورد. این امر، اگرچه با برخی مطالعات نهادی مانند (ماهولا و همکاران، ۲۰۲۱) هم‌پوشانی دارد؛ اما در این پژوهش با نگاهی جزئی‌تر و مبتنی بر داده‌های میدانی تبیین شده است.

با توجه به یافته‌های پژوهش، توصیه می‌شود که سیاست‌گذاران و نهادهای ذی‌ربط در سطح ملی و بین‌المللی، به ایجاد بسترهای حقوقی و فناورانه برای پیاده‌سازی هویت دیجیتال مبتنی بر بلاکچین توجه ویژه‌ای داشته باشند. این امر مستلزم تدوین مقرراتی است که ضمن حفظ حریم خصوصی کاربران، امکان تعامل‌پذیری میان سامانه‌های مختلف را نیز فراهم سازد. ایجاد زیرساخت‌های منسجم برای ذخیره، تبادل و تأیید هویت دیجیتال، به‌ویژه در حوزه صادرات، لجستیک، گمرک و تجارت الکترونیک، از اولویت‌های کلیدی محسوب می‌شود. همچنین، پیشنهاد می‌شود که برنامه‌هایی برای آموزش و توانمندسازی کسب‌وکارها در زمینه کاربرد بلاکچین و مزایای آن در احراز هویت و شفافیت داده‌ها طراحی و اجرا شود.

از سوی دیگر، توسعه و بهره‌گیری از فناوری‌های نوین مانند امضای دیجیتال، الگوریتم‌های اعتبارسنجی و روش‌های رمزنگاری پیشرفته باید مورد حمایت قرار گیرد تا بتوان سطح امنیت اطلاعات هویتی را ارتقا داد. کسب‌وکارها نیز می‌توانند با تعریف شناسه‌های دیجیتال اختصاصی و استفاده از فناوری‌های غیرمتمرکز، شفافیت عملکرد خود را افزایش داده و در بازارهای بین‌المللی مزیت رقابتی به‌دست آورند. در نهایت، پیشنهاد می‌شود که نهادهای تخصصی، طرح‌های پایلوت برای یکپارچه‌سازی هویت دیجیتال در زنجیرهٔ تأمین، گمرک و پلتفرم‌های تجاری راه‌اندازی کنند تا اثربخشی عملی این رویکردها در میدان واقعی مورد سنجش قرار گیرد و زمینه‌ساز تعمیم آن‌ها در سطح گسترده‌تر شود.

فهرست منابع

آبی‌زاده، علی؛ فتحی، زاداله و مینویی، مهرزاد (۱۴۰۱). کنترل دسترسی در قراردادهای هوشمند مالی با استفاده از مدیریت هویت دیجیتالی و یادگیری ماشین برای تسهیل تبادلات اینترنت اشیا. *دانش مالی تحلیل اوراق بهادار (مطالعات مالی)*، ۱۴(۵۳)، ۱۱۱-۱۲۲.

آئین، سهیل و نوری، مهدی (۱۴۰۳). ارائه مدل مفهومی و عوامل مؤثر بر پیاده‌سازی تأمین مالی زنجیره تأمین مبتنی بر بلاکچین در اقتصاد ایران. *فصلنامه پژوهش‌های پولی ـ بانکی*، ۱۷(۶۲)، ۵۶۵-۵۹۵.

خنیفر، حسین و مسلمی، ناهید (۱۳۹۷). *اصول و مبانی روش‌های پژوهش کیفی*. انتشارات نگاه دانش.

سلامی، یاشار و حسینی، سیدرضا (۱۴۰۲). طرح احراز هویت ایمن مبتنی بر بلاکچین در سیستم‌های هواشناسی. *نیوار*، ۴۷(۱۲۰-۱۲۱)، ۱۸۱-۱۹۷.

دژدانی، مهسا؛ شاهین پنجه، ریحانه، ابراهیمی، ریحانه و فاضل دربندی، پریا (۱۴۰۳). بلاکچین و تأثیر آن بر دنیای کسب‌وکارها. *نهمین همایش ملی تحقیقات میان‌رشته‌ای در مدیریت و علوم انسانی*.

شاه‌ویسی، فرهاد و طارمی، شهرام (۱۴۰۰). تأثیر فناوری بلاکچین بر تجارت داخلی و بین‌الملل، *همایش ملی چالش و راه‌کارهای مالی تجارت بین‌المللی با رویکرد حمایت از تولید ملی*، تهران.

قربانپور قارقشلاقی، مهدی؛ زینالی، مهدی و پورکریم، یعقوب (۱۴۰۳). بررسی ابعاد و مزایای انتشار صکوک هوشمند با استفاده از فناوری بلاکچین در بازار سرمایه ایران. *پژوهش‌های راهبردی بودجه و مالیه*، ۵(۴)، ۱۲۱-۱۵۱.

قلی‌زاده، محمدحسن؛ اسماعیلی، محبوبه؛ ابراهیم‌پور، مصطفی و مرادی، محمود (۱۴۰۲). فراکافت راهبردی استفاده از فناوری بلاکچین جهت تسهیل فرایند تأیید هویت مشتریان سازمان تأمین اجتماعی با رویکرد نظریه کنشگر- شبکه. *علوم و فنون مدیریت اطلاعات*، ۹(۱)، ۲۷۹-۳۱۰.

محمدی، شهریار و قنبری، نازنین (۱۳۹۹). ارائه مدلی برای احراز هویت توزیع شده در یک شبکه سلامت الکترونیک با استفاده از بلاکچین. *مجله انفورماتیک سلامت و زیست پزشکی*، ۷ (۴)، ۴۱۳- ۴۲۴.

Aljabr, A. A., Sharma, A. & Kumar, K. (2019). Mining process in cryptocurrency using blockchain technology: Bitcoin as a case study. Journal of Computational and Theoretical Nanoscience, 16(10), 4293-4298. 10.1166/jctn.2019.8515

Allen, C. (2016). *The path to self-sovereign identity. Blockchain Commons*. Retrieved from https://www.blockchaincommons.com/musings/SSI-5-Years-On/

ALSaqa, Z. H., Hussein, A. I. & Mahmood, S. M. (2019). The impact of blockchain on accounting information systems. *Journal of Information Technology Management*, *11*(3), 62-80.

Ayebo, I. S. & Ojo, O. (2025). *Digital Identity and Blockchain: Regulatory Challenges and Opportunities*.

Bandara, E., Liang, X., Foytik, P., Shetty, S. & De Zoysa, K. (2021, July). A blockchain and self-sovereign identity empowered digital identity platform. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). IEEE.

Blossey, G., Eisenhardt, J. & Hahn, G. (2019). Blockchain Technology in Supply Chain Management: An Application Perspective. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2013.

Faruk, M. J., Saha, B. & Basney, J. (2023). A comparative analysis between scitokens, verifiable credentials, and smart contracts: Novel approaches for authentication and secure access to scientific data. In *Practice and Experience in Advanced Research Computing 2023: Computing for the Common Good* (pp. 302-305).

Faruk, M. J. H., Subramanian, S., Shahriar, H., Valero, M., Li, X. & Tasnim, M. (2022, May). Software engineering process and methodology in blockchain-oriented software development: A systematic study. In *2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA)* (pp. 120-127). IEEE. https://doi.org/10.1109/SERA54885.2022.9806817

Gartner. (2020). *Top 10 strategic technology trends for 2020.* Retrieved from https://www.gartner.com

Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Chowdhury, M. J. M. & Rahman, M. S. (2023). A systematic literature review of blockchain-based e-KYC systems. *Computing*, *105*(10), 2089-2118. https://doi.org/10.1007/s00607-023-01176-8

IBM. (2022). *What is blockchain?* Retrieved from https://www.ibm.com/topics/what-is-blockchain

Jeganathan, S. (2021). Self-sovereign digital identity leveraging blockchain networks Opportunities and challenges. *ISSA Journal*, 10–19.

Khaund, B. (2025). Decentralized Identity Using Blockchain: Enhancing Security and Privacy in Digital Identity Management. *Journal of Computer Science and Technology Studies*, 7(6), 858-866

Mahula, S., Tan, E. & Crompvoets, J. (2021, June). With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. In *Proceedings of the 22nd Annual International Conference on Digital Government Research* (pp. 495-504). https://doi.org/10.1145/3463677.3463705

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Ostern, N. K. & Riedel, J. (2021). Know-your-customer (KYC) requirements for initial coin offerings. *Business & Information Systems Engineering*, *63*(5), 551-567. https://doi.org/10.1007/s12599-020-00677-6

Papadakis, M. N. & Kopanaki, E. (2022). Innovative maritime operations management using blockchain technology & standardization. *Journal of ICT Standardization*, *10*(4), 469-507.

Petronio, S. & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current opinion in psychology*, *31*, 76-82.

Parate, S., Reddi, L. T., Agarwal, S. & Suryadevara, M. (2023). Analyzing the impact of open data ecosystems and standardized interfaces on product development and innovation. *International Journal of Advanced Research in Science, Communication and Technology*, *3*(1), 476-485.

Rasouli, H., Valmohammadi, C., Azad, N. & Abbaspour Esfeden, G. (2021). Presenting digital identity management framework in cyberspace: Mixed-method approach. *National Security*, *11*(40), 121-154.

Schlatt, V., Sedlmeir, J., Feulner, S. & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, *59*(7), 103553. arXiv. https://doi.org/10.48550/arXiv.2112.01237

Shahandashti, S. F. & Arshad, J. (2020). A survey on blockchain-based identity management and decentralized privacy for personal data. *IEEE Access*, 8, 219134-219156. https://doi.org/10.1109/ACCESS.2020.3039753

Stokkink, Q. & Pouwelse, J. (2018, July). Deployment of a blockchain-based self-sovereign identity. *In 2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 1336-1342). IEEE.

Sun, M. & Zhang, J. (2020). Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Computer Communications*, 149, 332-342. doi:https://doi.org/10.1016/j.comcom.2019.10.031

Syahreen, M., Hafizah, N., Maarop, N. & Maslinan, M. (2024). Systematic Review on Multi-Factor Authentication Framework. *International Journal of Advanced Computer Science & Applications*, *15*(5).

Takemiya, M. & Vanieiev, B. (2018, July). Sora identity: Secure, digital identity on the blockchain. In *2018 ieee 42nd annual computer software and applications conference (compsac)* (Vol. 2, pp. 582-587). IEEE.

Velásquez, I. (2021). Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication. *Clei Electronic Journal*, *24*(1), 9-1.

World Trade Organization (2018). *Can Blockchain revolutionize international trade?* https://www.wto.org/english/res_e/publications_e/blockchainrev18_e.htm?utm_source=chatgpt.com

Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

Zheng, Z., Xie, S., Dai, H. N., Chen, X. & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

Designing a Conceptual Model of Blockchain-Based Digital Identityin International Businesses

Hossein Rahimi Kolour [*1]
Associate Prof., Department of Business Management, Faculty of Social Science, University of Mohaqheqh Ardabili, Ardabili, Iran

Mina Purhossein Roshan
Ph.D. Candidate, Department of Business Management, Faculty of Social Science, University of Mohaqheqh Ardabili, Ardabil, Iran

Abstract

Given the security challenges and inefficiencies inherent in traditional identity verification systems within international trade, this study aims to design a conceptual model for blockchain-based digital identity in international business. This qualitative research collected data through semi-structured interviews with 12 experts in the fields of blockchain and international commerce. The data were analyzed using thematic analysis with the aid of MAXQDA software. The findings suggest that the application of blockchain in digital identity can contribute to transforming identity processes and international interactions through themes such as “data-driven and smart regulation,” “self-sovereign identity governance,” “autonomous identity management,” “process optimization and export facilitation,” “integration of systems and infrastructures,” and “trust-building and commercial transparency.”The resulting conceptual model offers an innovative solution for decentralized and secure digital identity management. Furthermore, it provides a robust foundation for technological policymaking, cross-border infrastructure design, and the development of e-commerce systems, ultimately contributing to the modernization and reliability of identity practices in the global business environment.

Keywords: Digital identity, Blockchain, International business, Innovation.

1. Corresponding Author: h_clever@uma.ac.ir