فصلنامه پژوهش های نوین در اقتصاد، حسابداری و بازرگانی
Journal of new researches in economics, accounting and Banking

OPEN ACCESS

تأثیر کامپیوترهای کوانتومی بر زنجیره تأمین بلاکچین

هادی آقایی قلعه چه
صنعتی،موسسه عالی غیر انتفاعی هشت بهشت اصفهان کارشناس ارشد مدیریت
مریم سوری
کارشناسی ارشد مدیریت صنعتی،موسسه نوآوران کوهدشت
فاطمه پورسبحان
کارشناسی ارشدمدیریت دولتی،دانشگاه پیام نوریزد واحد تفت
الهه مهری
کارشناسی ارشد مدیریت فناوری اطلاعات،دانشگاه پیام نور مرکز تهران غرب

چکیده

این مطالعه، تأثیر کامپیوترهای کوانتومی بر بلاکچین‌ها در زمینه زنجیره تأمین را به صورت مفهومی بررسی می‌کند. کامپیوترهای کوانتومی قدرتمند، با سرعت بالا و با استفاده از محاسبات معکوس سریع مشکلات ریاضی که اساس یکی از اصول امنیتی بلاکچین را تشکیل می‌دهد، قادر به شکستن رمزنگاری نامتقارن هستند و همچنین می‌توانند از طریق شتاب دهی ماینینگ، صحت بلاکچین‌های عمومی مانند بیت کوین را مختل کنند. بنابراین، کامپیوترهای کوانتومی می‌توانند تهدیدی برای کاربران زنجیره تأمین بلاکچین باشند. در عین حال، تلاش‌هایی برای ایجاد یک راه‌حل مقاوم در برابر کامپیوترهای کوانتومی در حال انجام است. یکی از راهکارهای این گونه راه‌حل ها، استفاده از ابزارهای کوانتومی است. علاوه بر این، کامپیوترهای کوانتومی قدرتمند هنوز در دست توسعه هستند و هنوز مشخص نیست نتیجه اولیه این توسعه کدام است، راه‌حل یا تهدید. این تضاد دوگانه کامپیوترهای کوانتومی و عدم وجود یک تصویر واضح از زمان ورود راه‌حل و تهدید، منجر به عدم قطعیت می‌شود که ممکن است جذابیت بلاکچین‌ها برای زنجیره‌های تأمین را کاهش دهد.

کلمات کلیدی: زنجیره تامین، محاسبات کوانتومی، کامپیوترهای کوانتومی، بلاکچین.

مقدمه

رشد بلاکچین در زمینه‌های مختلف در سراسر جهان قابل مشاهده است. در حالی که آمریکا و چین رهبران این حوزه هستند، اروپا نیز سعی در بهره‌وری از پتانسیل بلاکچین خود دارد. در یک نظرسنجی در میان کسب‌وکارهای اروپایی، نیمی از پاسخ‌دهندگان معتقد بودند که بلاکچین بر روی مدل کاری کنونی آن‌ها تأثیر خواهد داشت. شرکت‌های بزرگی مانند Maersk دانمارکی ، BASF آلمانی و Bosch از فناوری بلاکچین استفاده می‌کنند. علاوه بر این، مثال‌هایی از سرمایه‌گذاری در بلاکچین در شرکت‌های بزرگ کشورهای دیگری مانند Gazprom روسیه نیز قابل شناسایی هستند. انگلستان، آلمان، فرانسه و استونی، بیشترین تعداد شرکت‌های نوپا بلاکچین را در اتحادیه اروپا دارند. میزان منابع مالی جهانی منتهی به راه حل‌های بلاکچین، رشد پایداری را نشان می‌دهد، از 1.5 میلیارد دلار در سال 2018 تا تخمین 15.9 میلیارد دلار در سال 2024(لیو[1]، 2020). نظرسنجی PwC از 600 مدیر در سال 2018 نشان داد که 84 درصد شرکت‌ها در حال حاضر تا حدودی با بلاکچین همکاری داشته‌اند.

رشد صنعت 4.0 یا همان انقلاب صنعتی چهارم که به عنوان دیجیتالی سازی شناخته می‌شود) به منظور نوآوری در حوزه کسب‌وکار به ارمغان آورده شده است. در این رابطه، بلاکچین یکی از فناوری‌های پایه صنعت 4.0 است که می‌تواند در موفقیت آن نقش مهمی ایفا کند(قباخلو[2]، 2020 و شواب و دیویس،[3] 2018). با این حال، فناوری بلاکچین هنوز در حال تکامل است. بلاکچین هنوز به رشد کامل خود نرسیده است، چراکه جنبه‌های مختلفی مانند مزایا و چالش‌های آن هنوز به طور کامل شرح داده نشده‌اند(ون هوک[4] و همکاران، 2019).

در این رابطه، کامپیوترهای کوانتومی یکی از مسائل اصلی هستند که می‌توانند تأثیر مهمی بر بلاکچین‌ها داشته باشند و ممکن است برای سرمایه‌گذاری‌های مرتبط، پیامدهای جدی داشته باشند. کامپیوترهای کوانتومی به عنوان دستگاه هایی یاد شده‌اند که برای انجام محاسباتی استفاده می‌شوند که در بسیاری از موارد از کامپیوترهای کلاسیک سریعتر عمل می‌کنند. یکی از حوزه‌های استفاده از بلاکچین که می‌تواند تحت تأثیر کامپیوترهای کوانتومی قرار بگیرد، زنجیره تأمین است. بلاکچین فرصت‌های مهمی را برای زنجیره تأمین، مانند شفافیت، غیرقابل تغییری و قابل اعتبارسنجی، فراهم می‌کند(کارامس و لاماس،[5] 2020). یکی از موارد استفاده از بلاکچین در زنجیره تأمین، استفاده Grass Roots از بلاکچین با مزارع تأمین برای ایجاد شفافیت در محتوای منتقل شده است. همچنین، Maersk برای جایگزینی

[1] Liu
[2] Ghobakhloo
[3] Schwab & Davis
[4] Van Hoek
[5] Fernández-Caramès & Fraga-Lamas

محتوای دیجیتال با کاغذهای سخت و دستی و تحقق شفافیتی که امکان نمایش مشترک و همکاری بین شرکای زنجیره تأمین را فراهم می‌کند، از بلاکچین استفاده می‌کند(دیویچنزو،[۶] 2000).

با این حال، ظهور کامپیوترهای کوانتومی قدرتمند می‌تواند بر تمام فرصت‌ها و سرمایه‌گذاری‌های بلاکچین تأثیر بگذارد. کامپیوترهای کوانتومی شمشیر دولبه هستند که می‌توانند به عنوان بخشی از راه حل امنیتی بلاکچین عمل کنند، همچنین از سوی دیگر مشکلاتی را به وجود آورند. این ویژگی‌ها نیاز به تحقیقات بیشتر در مورد جزئیات موضوع دارند تا درک مناسبی با اطمینان بیشتری از آن به دست آید. در حالی که تأثیر کامپیوترهای کوانتومی بر بلاکچین قبلاً بحث شده است، اما در زمینه مرتبط با زنجیره تأمین، تحقیقات بسیار کمی وجود دارد(کوهی زاده و همکاران، 2020).

با توجه به کمبود تحقیقات مرتبط و اهمیت موضوع، این مطالعه به بررسی مفهومی تأثیر کامپیوترهای کوانتومی بر امنیت بلاکچین و شناسایی تأثیر آن بر زنجیره تأمین، می‌پردازد. بنابراین، سؤال پژوهش این است که چگونه کامپیوترهای کوانتومی بر زنجیره تأمین مبتنی بر بلاکچین تأثیر می‌گذارند؟

در بخش زیر، روش شناسی این مقاله شرح داده شده است. سپس، بلاکچین و قابلیت های آن برای زنجیره های تأمین مورد بحث قرار گرفته است. پس از آن، هسته امنیتی بلاکچین بررسی شده است. در بخش پنجم، تأثیر کامپیوترهای کوانتومی بر امنیت بلاکچین آشکار می‌شود. به ترتیب، بخش‌های ششم و هفتم، ضمن برجسته کردن پیامدهای مربوط به کوانتوم برای زنجیره‌های تأمین، به دامنه تحقیق مورد بررسی قرار می‌گیرند

روش شناسی

این مقاله از روش نظریه‌پردازی همگن استفاده می‌کند. در این رابطه، جاکولا (2020) می‌گوید: "مقاله نظریه‌پردازی، سعی در دستیابی به یک ادغام مفهومی در چندین نظریه یا جریان ادبیات دارد. اینگونه مقالات با ارائه نگاهی جدید یا بهبود یافته درباره یک مفهوم یا پدیده، با اتصال قطعاتی از پیش تفکیک شده یا ناسازگار، مفاهیم را به شکل نوآورانه به یکدیگر ارتباط می‌دهند. دو مؤلفه‌ی اصلی این روش شامل خلاصه‌سازی و ادغام است (جاکولا،[۷] 2020).

خلاصه‌سازی، به معنای خلاصه کردن و کاهش دانش به یک کلیت قابل مدیریت است (جاکولا، 2020؛ مکینیس، 2011). به همین دلیل، این مقاله توضیحی دقیق از سه مفهوم اصلی و زیرمجموعه‌های مرتبط با هدف پژوهش ارائه می‌دهد. این سه مفهوم اصلی شامل بلاکچین، زنجیره تأمین و کامپیوترهای کوانتوم هستند.

ادغام، ارتباط بینمفاهیم اصلی را برقرار می‌کند که منجر به دستیابی به دیدگاه‌های جدید می‌شود (جاکولا، 2020؛ مکینیس، 2011). به همین منظور، سه مفهوم اصلی این مطالعه با هم ارتباط دارند و کمک می‌کنند تا تأثیر کامپیوترهای

[6] DiVincenzo
[7] Jaakkola

کوانتومی بر زنجیره تأمین مبتنی بر بلاکچین آشکار شود. باتوجه به اینکه مطالعات گذشته این سه مفهوم را به صورت همزمان بررسی نکرده بود، چنین ادغامی درک نوآورانه‌ای را ارائه می‌دهد که می‌تواند برای آینده کاربران زنجیره تأمین برای بلاکچین مهم باشد.

علاوه بر این، استفاده از روش نظریه‌پردازی می‌تواند با مشکلات جمع‌آوری داده‌ها سازگار باشد. در این رابطه، یاداو[8] (2010) می‌گوید که یکی از مزایای قابل توجه مطالعات نظریه‌ای، مرتبط با خصوصیت آزادی در دسترسی به داده است، به عبارت دیگر، این رویکرد با پدیده‌هایی که دسترسی به داده‌های مرتبط با آنها آسان نیست، سازگار است. کامپیوترهای کوانتومی در حال ظهور هستند و هنوز تا رسیدن به بلوغ و کاربردهای عملی گسترده، راه درازی در پیش دارند. به همین دلیل، دسترسی به شواهد تجربی مناسب ممکن است با مشکلاتی همراه باشد که می‌تواند مانع از ارائه نتایج موردنظر این مقاله شود. بنابراین، روش نظریه‌پردازی یک راه حل خوب برای مقابله با محدودیت دسترسی به داده‌های تجربی است.

چیستی بلاکچین

بلاکچین در سال ۲۰۰۸ توسط ساتوشی ناکاموتو[9] به عنوان عنصر اصلی برای پشتیبانی از معاملات ارز دیجیتالی بیت کوین مورد استفاده قرار گرفت(نوینسکی و کوزما،[10] 2017 و ژائو[11] و همکاران، 2016). از آن زمان،، کاربرد بلاکچین به بیت کوین و پشتیبانی از پول دیجیتال، شروع شد و به حوزه های مختلفی مانند بهداشت(کارامس[12] و همکاران، 2019 و جایرمان[13] و همکاران، 2019)، مدیریت زنجیره تامین(رانا[14] و همکاران، 2021 و رجب[15] و همکاران، 2019) ، و رای دهی الکترونیکی(بودیر[16] و همکاران، 2021 و شواب و دیویس، 2018) توسعه یافته است.

اگرچه تعریف واحدی از بلاکچین وجود ندارد، اما تلاش های انجام شده شباهت هایی را به اشتراک می گذارند(ون هوک و همکاران، 2019). بلاکچین به عنوان یک پلتفرم فناوری معرفی شده است که به چندین شرکت کننده اجازه می دهد تا دیتابیس مطمئن و امنی از محتوای دیجیتال (مانند اطلاعات، رکورد و معامله) را ایجاد و به اشتراک بگذارند(بل و لیون،[17] 2019، ون هوک و همکاران، 2019). بلاک چین یک دفتر کل توزیع شده، غیرمتمرکز و اشتراکی است که به صورت زنجیره‌ای از سوابق بنام بلاک ساخته شده است. هر بلاک در این زنجیره، مسئول ذخیره‌سازی نوعی از اطلاعات (مانند سوابق معاملات) است. در واقع می توان بدون اتصال به یک مرکز خاص، مبادلات خود را انجام دهند. بنابراین،

[8] Yadav
[9] Satoshi Nakamoto
[10] Nowiński & Kozma
[11] Zhao
[12] Fernández-Caramés
[13] Jayaraman
[14] Rana
[15] Rejeb
[16] Baudier
[17] Manners-Bell & Lyon

معاملات می‌توانند مستقیماً بین خریدار و فروشنده و با خیال راحت انجام شود(شواب و دیویس، 2018، ون هوک و همکاران، 2019 و بل و لیون،[18] 2019)

به طور ساده تر، بلاکچین یک زنجیره از بلاک ها است که حاوی محتوای ذخیره شده در آن ها است(دولگی[19] و همکاران، 2020، موندال[20] و همکاران، 2019 و شو[21] و همکاران، 2021). هر بلاک شامل یک برچسب زمانی، اطلاعات مربوط به محتوای فعلی بلاک، ارزش هش فعلی بلاک، و ارزش هش بلاک قبلی است(باکار و روسبی،[22] 2018 و یانگ[23] و همکاران، 2018). بلاکچین بر روی چندین نود یا گره کپی می شود که به طور معمول در شبکه های بلاکچین به صورت کامپیوتر هستند و برای تأیید بلوک ها مسئولیت دارند. مسئولیت اصلی یک نود بلاکچینی تایید قانونی بودن هر دسته تراکنش جدید است که با عنوان بلاک شناخته می‌شوند. به‌علاوه، تخصیص یک شناسه معتبر به هر نود در شبکه باعث شناسایی آسان یک نود از سایر نودها می‌شود. یک بلاکچین مبتنی بر گواه اثبات کار[24] مانند بیت کوین[25] یا بلاکچین مونرو[26] دارای ماینرهایی است که وظایف آن‌ها به شرح زیر است:

نودهای کامل[27] باید تمام تراکنش‌های بلاکچین را در دستگاه‌های خود ذخیره کنند. این نودها مسئولیت اعتبارسنجی بلاک‌ها و تراکنش‌ها را بر عهده دارند. و نودهای سبک[28] در این شبکه‌ها ابزارهای ذخیره‌سازی با حجم کم هستند؛ زیرا برای تایید تراکنش‌ها فقط باید هدر بلاک‌ها را تایید کنند(یانگ و همکاران، 2018 و ون هوک و همکاران، 2019)

در بلاکچین وجود مکانیزم های اعتبارسنجی، درجات کنترل و مالکیت متفاوت وجود دارد. این تفاوت ها باعث می شود بلاکچین به دو نوع متفاوت تقسیم شود (Van Hoek et al.، 2019). یک نوع بلاکچین "عمومی" است (مانند بیت کوین و اتریوم) که پلتفرم به طور کامل غیرمتمرکز است و بدون مالک بوده و فرآیند تأیید نیازمند حل یک روش ریاضی پیچیده است که هر کسی قادر به مشاهده تراکنش‌های انجام شده در شبکه این رمز ارز است(ویریاسیتاوات و هونسوپون،[29] 2019).

نوع دوم بلاکچین "مجاز" است که کنترل و مالکیت آن بین کاربران مجاز (که یکدیگر را می شناسند اما لزوماً به یکدیگر اعتماد نمی کنند) به اشتراک گذاشته می شود و در شبکه های تأمین معمول است(ون هوک و همکاران، 2019). در

[18] Manners-Bell & Lyon
[19] Dolgui
[20] Mondal
[21] Xu
[22] Bakar & Rosbi
[23] Ying
[24] PoW
[25] BTC
[26] XMR
[27] Full Node
[28] Lightweight Node
[29] Viriyasitavat & Hoonsopon

این نوع بلاکچین، دسترسی به محتوا بر اساس توافقات کاربران است (ویریاسیتاوات و هونسوپون، 2019) و فرآیند تأیید معمولاً منابع کمتری نیاز دارد و مکانیزم های اجتماعی کارآمدتری دارد(ون هوک و همکاران، 2019).

بلاکچین در زنجیره تأمین

بهره مندی کسب‌وکارها از مزایایی که از بلاکچین ، سطوح مختلفی دارد (ون هوک و همکاران، 2019). با این حال، علیرغم محدودیت‌های موجود، مزایای بسیاری بخاطر ارتباط بلاکچین با زنجیره تأمین وجود دارد(بل و لیون، 2019). به طور کلی، مزایای مشترکی که در ادبیات‌های مختلف شناسایی شده‌اند که شامل تغییرناپذیری محتوا، احراز هویت، شفافیت، قابلیت ردیابی، قراردادهای هوشمند، غیرمتمرکزسازی و کارایی می شود(فرانسیسکو و سوانسون،[۳۰] 2018 و الازاب[۳۱] و همکاران، 2021).

پلتفرم‌های بلاکچین برای شرکت‌کنندگان در زنجیره تأمین یک بلاک قابل تأیید و اصلی ارائه می‌دهند که شفافیت و قابلیت پیگیری فرآیندهای مختلف در میان کاربران زنجیره تأمین را فراهم می‌کند و می‌تواند برای اهداف مختلفی مانند جلوگیری از جعل، ایجاد بینش در موضوعات مختلف (مانند تقاضای مشتری)، تبادل داده‌ها و بازرسی‌ها مورد استفاده قرار گیرد(آگراوال[۳۲] و همکاران، 2021 و ماندولا[۳۳] و همکاران، 2019).

اعتبار سنجی و مالکیت محتوا در سراسر شبکه توزیع می شود تا از کنترل متمرکز جلوگیری شود و غیرمتمرکز سازی را تقویت کند(صابری و همکاران، 2019 و ون هوک و همکاران، 2019). علاوه بر این، بلاکچین هزینه بار سرور پشتیبان را از یک شخص حذف می‌کند و وابستگی به واسطه را کاهش می‌دهد که همین امر منجر به بهبود کارایی می‌شود(چوی[۳۴] و همکاران، 2019 ؛ شارما[۳۵] و همکاران، 2018 و کشتری[۳۶] و همکاران، 2018).

بلاکچین همچنین قراردادهای هوشمندی را فراهم می‌کند که در آن توافقات قراردادی از طریق کدها دیجیتالیزه شده و با شرایط پیش‌تعریف شده، اجرای هماهنگ و خودکاری را ممکن می سازد(دولگوی و همکاران، 2020).

علاوه بر این، تئوری هزینه تراکنش همچنین می تواند برای توسعه بینش در مورد تأثیر بلاک چین بر هزینه های تراکنش مرتبط با روابط زنجیره تامین مورد استفاده قرار گیرد(اهلوالیه[۳۷] و همکاران، 2020 و اشمیت و واگنر،[۳۸] 2019).

[30] Francisco & Swanson
[31] Alazab
[32] Agrawal
[33] Mandolla
[34] Choi
[35] Sharma
[36] Kshetri
[37] Ahluwalia
[38] Schmidt & Wagner

بر اساس این نظریه، دو عامل کلیدی بر هزینه تراکنش تأثیر می‌گذارند: عقلانیت محدود و فرصت‌طلبی(گلور و مالهوترا،[39] 2003). ریندفلیش و هاید[40] (1997) به عقلانیت محدود به عنوان محدودیت توانایی تصمیم گیرندگان برای پردازش اطلاعات با در نظر گرفتن دقیق تمام جوانب و شرایط الزام آور قرارداد اشاره می کنند. در این رابطه، آنها بر کلمه "محدودیت" تاکید می کنند و استدلال می کنند که نباید با "حماقت" بالقوه ای که ممکن است از طرف یک فرد رخ دهد، اشتباه گرفته شود(ریندفلیش و هاید، 1997). یک عامل مهم که بر عقلانیت محدود تأثیر می گذارد درجه عدم اطمینان است. در یک محیط نامطمئن، عقلانیت محدود تاثیرگذارتر است، چراکه بدلیل لزوم توجه به جوانب مختلف، بیشتر احساس می شود. اپورتونیسم یا فرصت طلبی، به رفتارهای غیرصادقانه در روابط مبادله ای می پردازد که مبتنی بر منفعت شخصی است، مانند تقلب، دروغگویی و انحراف عمدی از توافقات. دراین میان رفتارهای فرصت طلبانه نیاز به نظارت و کنترل رفتار را ایجاد می کند که هزینه تراکنش را افزایش می دهد(گلور و مالهوترا، 2003).

در این زمینه، بلاک چین می تواند بر هزینه تراکنش مرتبط با روابط زنجیره تامین تاثیر بگذارد. به عنوان مثال، رویه روشن، از پیش تعریف شده و محتوای غیرقابل تغییر و همچنین قرارداد معتبر هوشمند، رفتارهای فرصت طلبانه را محدود می کند. یک پلت فرم بلاک چین شفاف و قابل اعتماد، عدم اطمینان محیطی را کاهش می دهد و بر عقلانیت محدود تأثیر می گذارد(چانگ، چن و وو،[41] 2019 و تریبل مایر،[42] 2018).

بلاک چین می تواند مشکلات اعتماد در زنجیره تامین را کاهش دهد. نظریه عامل اصل[43] به روابط بین دو فرد یا دو گروه که به عنوان نماینده (عامل) و مجری (اصل) عمل می‌کنند، می پردازد. در این رابطه، نماینده (عامل) مسئول انجام وظایفی است که به وی سپرده شده و مجری (اصل) نظارت بر اجرای صحیح این وظایف را بر عهده دارد. در این نظریه، معمولاً ارتباط بین نماینده و مجری به صورت قراردادی است و نماینده به عنوان عامل در حال انجام وظایفی است که به وی سپرده شده و در عوض مجری به عنوان اصل، به نماینده پاداش می‌دهد. در اینجا ممکن است وجود تفاوت‌هایی در هدف و مصالح نماینده و مجری باشد که می‌تواند به مشکلاتی منجر شود. به عنوان مثال، نماینده ممکن است برای رسیدن به مصالح شخصی خود، در انجام وظایف بهینه عمل نکند یا اطلاعات مهمی را پنهان کند. در نتیجه، مجری ممکن است با مشکلاتی مواجه شود که با نقض قرارداد و قوانین مربوطه به وجود آمده است. از این رو، نظریه عامل-اصل برای بررسی وضعیت‌هایی استفاده می‌شود که ممکن است در آن‌ها تفاوت‌هایی بین مصالح نماینده و مجری باشد و تلاش

[39] Grover & Malhotra
[40] Rindfleisch and Heide
[41] Chang, Chen, and Wu
[42] Treiblmaier
[43] The principle-agent theory

می‌کند تا راه‌کارهایی برای کاهش این تفاوت‌ها و رفع مشکلات پیش‌آمده ارائه کند (براون و گاستون،[44] 2003؛ استاینل[45] و همکاران، 2014).

در زمینه زنجیره تامین، رابطه خریدار و تامین کننده نمونه خوبی از رابطه بین نماینده (عامل) و مجری (اصل) است. بر اساس قرارداد، تامین کننده (نماینده) موظف است وظایف خاصی را انجام دهد که این امر آن تامین کننده را با دانش نسبتاً بیشتری در مورد جزئیات (و پیرامون) کار در مقایسه با خریدار مجهز می کند (استاینل و همکاران، 2014؛ تریبل مایر، 2018).

با توجه به این عدم تقارن اطلاعاتی، خریدار (اصلی) باید مکانیسم‌های اعتماد متحمل هزینه و کنترل را ایجاد کند تا از واگرایی تامین‌کننده جلوگیری کند (جنسن و مکلینگ،[46] 1976؛ استاینل و همکاران، 2014؛ تریبلمایر، 2018). در این راستا، شفافیت بلاک چین و دسترسی به محتوای قابل اعتماد، عدم تقارن اطلاعاتی در روابط تجاری بین مدیر و نماینده را کاهش می دهد. از این رو، مکانیسم های اعتماد و کنترل هزینه کمتری خواهند داشت(چانگ، چن و وو، 2019؛ تریبلمایر، 2018).

یکی از ویژگی های مهم بلاک چین امنیت است که نقش بسزایی در تحقق منافع دارد (چالمرز[47] و همکاران، 2019؛ کارامس و لاماس، 2020؛ کومار[48] و همکاران، 2020؛ صابری و همکاران، 2019). نکته اینجاست که فقدان امنیت در نهایت هسته اصلی مزایای بلاک چین را به چالش می کشد. به عنوان مثال، بدون ابزارهای امنیتی بلاک چین، ممکن است دستکاری محتوای بلاک چین، جعل هویت کاربران، مختل کردن مکانیسم اعتماد و تحریف قراردادهای هوشمند امکان پذیر شود.

بلاکچین همچنین می‌تواند در بهبود امنیت زنجیره تأمین نقش داشته باشد. با استفاده از الگوریتم‌های رمزنگاری و امضای دیجیتالی، بلاکچین می‌تواند اطمینان حاصل کند که اطلاعات در زنجیره تأمین بدون تغییر وارد شده‌اند و هیچ کس غیرمجازی به آنها دسترسی ندارد. همچنین، با استفاده از بلاکچین، می‌توان اطمینان حاصل کرد که هیچ کس نمی‌تواند از اطلاعات شخصی و حریم خصوصی دیگران سوءاستفاده کند(ون هوک و همکاران، 2019).

در کل، بلاکچین می‌تواند به عنوان یک ابزار موثر در بهبود کارایی، شفافیت، امنیت، قابلیت پیگیری و هماهنگی در زنجیره تأمین استفاده شود. با این حال، برای استفاده بهینه از بلاکچین در زنجیره تأمین، نیاز به همکاری و هماهنگی

[44] Braun & Guston
[45] Steinle
[46] Jensen & Meckling
[47] Chalmers
[48] Kumar

بین شرکت‌ها، استانداردسازی و شناسایی موضوعاتی مانند حریم خصوصی و امنیت داده‌ها وجود دارد(کشتری، 2018؛ ون هوک و همکاران، 2019).

امنیت بلاک چین

امنیت بلاک چین عمدتاً به دو مفهوم رمزنگاری اصلی بستگی دارد: رمزنگاری کلید عمومی/نامتقارن و عملکرد هش (فرناندز و لاماس، 2020؛ ماندولا و همکاران، 2019؛ رجب و همکاران، 2019).

رمزنگاری نامتقارن

رمزنگاری نامتقارن از کلیدهای عمومی و خصوصی برای احراز هویت مبادلات محتوا بین کاربران درگیر استفاده می کند و از آنچه به عنوان "امضای دیجیتال" شناخته می شود، استفاده می کند (فرناندز-کارامس و فراگا-لاماس، 2020؛ نیرانجانامورتی[۴۹] و همکاران، 2019). همانطور که از نام ها پیداست، یک کلید خصوصی همیشه خصوصی نگه داشته می شود و کلیدهای عمومی برای دیگران در دسترس هستند(ژائو و همکاران، 2018).

در بلاک چین، امضای دیجیتال معمولی شامل هش کردن محتوا (از طریق تابع هش) توسط کاربر است که منجر به خروجی هش با اندازه ثابت می شود. خروجی هش توسط یک کلید خصوصی رمزگذاری می‌شود که امضای دیجیتال را ایجاد می‌کند، و سپس امضا توسط دیگران با استفاده از کلید عمومی همان کاربر تأیید می‌شود(ژنگ[۵۰] و همکاران، 2018). با توجه به رابطه ریاضی ایمن بین جفت کلید عمومی و خصوصی، وقتی کسی امضا را توسط یک کلید عمومی تأیید می‌کند، تضمین می‌کند که تنها کاربری که کلید خصوصی را دارد امضا را ایجاد کرده(کارامس و لاماس، 2020)، از این رو، احراز هویت برقرار می شود. رمزنگاری نامتقارن نیز برای کیف پول بلاک چین ضروری است. کیف پول حاوی یک کلید عمومی است که آدرس عمومی کیف پول را از طریق تابع هش ارائه می کند (آدرس عمومی برای ارسال/دریافت محتوای دیجیتال استفاده می شود) و یک کلید خصوصی که برای دسترسی به کیف پول، مدیریت و امضا استفاده می شود (دیکشیت و سینگ،[۵۱] 2017؛ دوایر،[۵۲] 2015؛ کارامس و لاماس، 2020).

عملکرد هش

[49] Niranjanamurthy
[50] Zheng
[51] Dikshit & Singh
[52] Dwyer,

به عبارت ساده، تابع هش محتوای اندازه‌های دلخواه را به یک خروجی/مقدار هش با اندازه ثابت تبدیل می‌کند و نقشه‌برداری می‌کند که (تقریباً همیشه) برای ورودی محتوای اصلی منحصربه‌فرد است (دی پیرو،[۵۳] 2017؛ التاییب[۵۴] و همکاران، 2020). به عبارت دیگر، یک مقدار هش با اندازه ثابت، بدون تبانی یا بدون توطئه(به این معنا که هیچ دو یا چند شخص نمی‌توانند با هم توطئه کنند تا تراکنش‌ها را تغییر دهند یا به طور ناعادلانه ارز دیجیتال را به دست آورند) است، به این معنی که هیچ دو ورودی محتوایی نباید خروجی هش یکسانی داشته باشند. کوچکترین تغییر در ورودی محتوا، مانند اضافه کردن یک کاراکتر، منجر به خروجی هش کاملاً متفاوتی می‌شود (وانگ[۵۵] و همکاران، 2019). تابع هش همچنین مقاوم در برابر تصویر اولیه و قطعی است (لی و لی،[۵۶] 2017). اولی به ویژگی‌ای اشاره دارد که از طریق آن معکوس کردن تابع هش دشوار می‌شود، و دومی تضمین می‌کند که ورودی یکسان محتوای همیشه به همان خروجی هش منجر می‌شود. تابع هش، با توجه به ویژگی های ذکر شده، نقش مهمی در امنیت بلاک چین ایفا می کند.

تابع هش، بلاک چین را تغییرناپذیر و ضد دستکاری می کند. هر بلوک حاوی هش خود و هش بلوک قبلی است که باعث می شود بلوک ها به یکدیگر متصل شوند (باکار و روسبی، 2018؛ فرناندز-کارامس و فراگا-لاماس، 2020؛ یانگ و همکاران، 2018).

اگر محتوای بلوک بعداً تغییر کند، هش آن نیز تغییر می‌کند که دیگر با هش بلوک مشابه در بلوک بعدی مطابقت ندارد و آن را نامعتبر می‌کند (رجب و همکاران، 2019؛ وونگ و همکاران، 2019). تابع هش همچنین برای تولید آدرس، کاهش اندازه آدرس عمومی، و هش محتوا در طول فرآیند امضا استفاده می‌شود (کارامس و لاماس، 2020؛ رایکوار و همکاران، 2019؛ وانگ و همکاران، 2019).

الگوریتم‌های امنیتی و تابع یکطرفه

این دو مفهوم اصلی رمزنگاری بر پایه "تابع یکطرفه" بنا شده‌اند. تابع یکطرفه به تابعی گفته می‌شود که در آن محاسبات ریاضی در یک جهت ممکن و آسان هستند، اما در جهت معکوس، محاسبات به صورت محاسباتی غیرممکن و پیچیده هستند(دی لئون[۵۷] و همکاران، 2017).

در رمزنگاری نامتقارن، کلیدهای عمومی و خصوصی به عنوان توابع یکطرفه عمل می‌کنند، به این معنی که از یک کلید خصوصی، رسیدن به کلید عمومی آسان است، اما جهت معکوس به صورت محاسباتی پیچیده و غیرقابل ممکن است

[53] Di Pierro
[54] Eltayieb
[55] Wong
[56] Lee & Lee
[57] De Leon

(کنکایورو پاتریک،[58] 2011). در بلاکچین‌ها، دو الگوریتم رمزنگاری کلید عمومی رایج، که برای امنیت و تولید جفت کلید استفاده می‌شوند، دو الگوریتم رایج برای رمزنگاری با کلید عمومی عبارتند از رمزنگاری منحنی بیضی(ECC) و (RSA)[59] که برای امنیت و تولید جفت کلید، بر اساس مسائل ریاضی که تابع یک طرفه تولید می کنند، استفاده می شوند(چندل[60] و همکاران، 2019؛ داسگوپتا[61] و همکاران، 2019؛ گرکوچیو[62] و همکاران، 2020).

سطح امنیت ECC و RSA بر اساس "بیت‌های امنیتی" تعیین می‌شود (چندل و همکاران، 2019؛ لنسترا[63]، 2002). به دلیل ماهیت متفاوت RSA و ECC، تعداد مورد نیاز بیت‌ها برای ارائه قدرت امنیتی یکسان بین آن‌ها متفاوت است (چندل و همکاران، 2019). به عنوان مثال، یک کلید 256ECC بیتی معادل یک کلید 3072RSA بیتی است. هرکدام از آن‌ها به تعداد بیشتری از بیت‌ها در کلاس خود نیاز دارند تا امنیت قوی‌تری را ارائه دهند (مانند 256ECC بیتی که امنیت قوی‌تری از 224ECC بیتی ارائه می‌دهد بارکر و دانگ (2016) مقایسه دقیقی از نقاط قوت هر الگوریتم ارائه می دهند.

متداول ترین تابع هش در یک بلاک چین، الگوریتم هش امن است(SHA) که برای تولید خروجی هش با اندازه ثابت از ورودی محتوا استفاده می‌شود (داسگوپتا[64] و همکاران، 2019؛ گرکوچیو و همکاران، 2020). SHA خانواده ای از توابع هش رمزنگاری است که در ابتدا توسط آژانس امنیت ملی NSAو استاندارد پردازش اطلاعات فدرال در ایالات متحده (آجائو[65] و همکاران، 2019) توسعه داده شد. نسخه اولیه SHAیعنی -SHAدر نهایت کرک شد. بنابراین، دیگر نمی تواند امنیت مورد نیاز را ارائه دهد (داسگوپتا و همکاران، 2019؛ زو و همکاران، 2019). در عوض، نسخه‌های دوم و سوم برای رفع شکاف‌های امنیتی معرفی شده‌اند، و در زمان نگارش، نسخه دوم، -256SHA، یک الگوریتم رایج در هش کردن بلاک‌چین است و هش 256 بیتی ثابت را تولید می‌کند (داسگوپتا و همکاران، 2019). هش و الگوریتم آن نیز به عنوان یک تابع یک طرفه رفتار می کنند (شیتال و ونکاتش،[66] 2018 و ورما و گارگ،[67] 2017).

[58] Kenekayoro Patrick
[59] Rivest-Shamir-Adleman
[60] Chandel
[61] Dasgupta
[62] Grecuccio
[63] Lenstra
[64] Dasgupta
[65] Ajao
[66] Sheetal & Venkatesh
[67] Verma & Garg

OPEN ACCESS

عوامل تهدید امنیت بلاک چین و راه حل آن

در اوایل دهه 80، ریچارد فاینمن آنچه را که محاسبات کوانتومی نامیده می‌شود، پایه‌گذاری کرد (فاینمن،[۶۸] 1982؛ نگوین و کیم،[۶۹] 2019).

محاسبات مدرن (یعنی کلاسیک) بر اساس یکی از دو موقعیت 0 و 1 عمل می کند که به اصطلاح "بیت" اطلاعات را تشکیل می دهد، در حالی که محاسبات کوانتومی از "کیوبیت ها" استفاده می کند که شامل 0 و 1 و همچنین تمام حالت های بین آن می شود(موستئانو و فاسیا،[۷۰] 2021).

رمزنگاری نامتقارن بلاک چین از الگوریتم‌هایی استفاده می‌کند که مبتنی بر مسائل ریاضی هستند که توابع یک طرفه تولید می‌کنند و محاسبات معکوس را برای رایانه‌های کلاسیک بسیار طولانی می‌کنند(کیکتنکو[۷۱] و همکاران، 2018 و گئورگیو[۷۲] و همکاران، 2017). با این حال، با استفاده از الگوریتم Shor، رایانه‌های کوانتومی قدرتمند می‌توانند این محاسبات معکوس را انجام دهند و مسائل ریاضی را به صورت نجومی سریع‌تر حل کنند(کارامس و لاماس، 2020؛ گئورگیو و همکاران، 2017؛ کیکتنکو و همکاران، 2018). تفاوت در محاسبات می تواند از دهه ها یا قرن ها (یا حتی هزاره) توسط رایانه های کلاسیک به ثانیه ها، دقیقه ها یا ساعت ها با استفاده از رایانه های کوانتومی برسد. این بدان معناست که شکستن هسته رمزنگاری نامتقارن بلاک چین‌های معاصر دیگر غیرممکن خواهد بود. به عنوان مثال، از طریق رایانه های کلاسیک، برای نفوذ به سیستم های رمزنگاری با 112 بیت امنیتی (چن و همکاران، 2016) طی 30 تا 40 سال، به یک میلیارد دلار نیاز است، در حالی که 160ECC بیتی را می توان با 1000 کیوبیت و 1024 بیت RSA (RSA) با حدود 20 بیت کوانتومی و 30 بیتی شکست داد.

در مورد تابع هش، رایانه‌های کوانتومی با استفاده از الگوریتم‌های گروور، فقط می‌توانند با یک عامل درجه دوم، حمله brute force را سرعت بخشند (کارامس و لاماس، 2020؛ گئورگیو و همکاران، 2017). از این رو، معمولاً پیشنهاد می‌شود که اندازه خروجی هش را افزایش دهید (چن و همکاران، 2016؛ کارامس و لاماس، 2020). با این وجود، الگوریتم گروور را می توان برای استخراج سریع در بلاک چین های عمومی مانند بیت کوین مورد استفاده قرار داد، که بازآفرینی سریع کل بلاک چین را امکان پذیر می کند و می تواند یکپارچگی آن را نقض کند(کارامس و لاماس، 2020؛ گئورگیو و همکاران، 2017). در حالی که این تهدیدها اهمیت خاصی دارند، خطرات امنیتی کوانتومی مرتبط دیگری نیز ممکن است وجود داشته باشند که به طور بالقوه هنوز به طور کامل کشف نشده اند(گئورگیو و همکاران، 2017). خوشبختانه رایانه‌های کوانتومی قدرتمند هنوز در حال توسعه هستند و در حال حاضر قوی‌ترین رایانه‌های موجود دارای

[68] Feynman
[69] Nguyen & Kim
[70] Mosteanu & Faccia
[71] Kiktenko
[72] Gheorghiu

64 کیلوبیت است که توسط هانیول ادعا شده است (شانکلند[۷۳]، 2020). تخمین‌های مختلفی در مورد اینکه چه زمانی رایانه‌های کوانتومی به اندازه کافی قوی خواهند بود تا امنیت بلاک چین معاصر را تهدید کنند، وجود دارد (استیونز، 2020). در حالی که برخی تخمین می‌زنند که ظهور رایانه‌های کوانتومی به اندازه کافی قدرتمند ممکن است ظرف چند سال اتفاق بیفتد، برخی دیگر پیش‌بینی می‌کنند که ورود آنها در آینده اتفاق بیفتد، مانند سال 2026 یا 2031 (چن و همکاران، 2016؛ گئورگیو و همکاران، 2017؛ موسکا، 2018، استیونز، 2018).

دو راه حل بالقوه برای ایجاد مقاومت کوانتومی وجود دارد: یکی به «رمزنگاری پس کوانتومی» اشاره دارد که از مسائل ریاضی، به غیر از موارد معمولی(که در برابر حملات کوانتومی ایمن تلقی می شوند) استفاده می کند. یکی دیگر «رمزنگاری کوانتومی» است که از ویژگی‌های مکانیک کوانتومی برای تأمین امنیت استفاده می‌کند(موسکا،[۷۴] 2018؛ کیکتنکو و همکاران، 2018). با این حال، رمزنگاری پس کوانتومی می تواند با عوارض فنی و ناکارآمدی همراه باشد (کمپبل، 2019؛ گئورگیو و همکاران، 2017؛ کیکتنکو و همکاران، 2018). همچنین، رمزنگاری کوانتومی نیازمند محاسبات کوانتومی و ابزارهای ارتباطی است که برای استفاده عملی در آینده نزدیک به راحتی در دسترس نخواهد بود (گئورگیو وهمکاران، 2017). علاوه بر این، توسعه رمزنگاری مقاوم در برابر کوانتومی و تبدیل مربوطه به زمان و تلاش قابل توجهی نیاز دارد(کمپبل[۷۵]، 2019؛ چن و همکاران، 2016) که ممکن است به معنای عدم آمادگی اکنون باشد که کامپیوترهای کوانتومی به اندازه کافی قدرتمند در دسترس نیستند. در این رابطه چن و همکاران. (2016) خواستار اقدام فوری در مورد این موضوع شدند.

پیامدها و تبعات برای زنجیره تأمین

تهدید رایانه‌های کوانتومی برای بلاک‌چین‌های معمولی به این معنی است که امنیت اطلاعات (محتوای دیجیتال) دیگر در چارچوب زنجیره تأمین تضمین نخواهد شد. این می تواند هر گونه عملکرد بلاک چین را که ریشه در کلیدهای خصوصی دارد، به خطر بیاندازد. کلیدهای خصوصی که قرار بود مخفی نگه داشته شوند، از طریق کلیدهای عمومی مربوطه به راحتی قابل دستیابی خواهند بود زیرا مسائل ریاضی به طور موثر قابل برگشت می شوند، در نتیجه، مهاجم می تواند جایگزین کاربر زنجیره تامین شود، اقداماتی که می‌خواهد (مانند دسترسی به اطلاعات حساس یا وارد کردن داده های نادرست به زنجیره بلوکچین) و بدون اینکه کسی بتواند آن را شناسایی کند، محتوا را امضا کند(گئورگیو و همکاران، 2017). از آنجایی که هویت افراد دیگر به طور ایمن قابل تأیید نخواهد بود، می‌توان بلوک‌های نادرست و دستورالعمل‌های مخرب ایجاد کرد که می‌تواند بر قراردادهای هوشمند تأثیر بگذارد و ردیابی و شفافیت زنجیره تأمین را

[73] Shankland
[74] Mosca
[75] Campbell

تضعیف کند. علاوه بر این، یکپارچگی بلاک چین‌های عمومی مانند بیت‌کوین می‌تواند از طریق حملات مبتنی بر کوانتوم در برابر استخراج سریع آسیب‌پذیر شود (کارامس و لاماس، 2020؛ گئورگیو و همکاران، 2017)، که می‌تواند کاربران ارزهای دیجیتال مربوطه را در چشم‌انداز زنجیره تامین تهدید کند. از دیدگاه تئوری عامل اصلی و هزینه مبادله، محیط زنجیره تأمین قابل اعتماد که توسط زنجیره بلاکچین فراهم شده است، به شدت مختل می‌شود، امکان رفتارهای فرصت‌طلبانه فراهم خواهد شد و عدم قطعیت افزایش خواهد یافت. افراد درگیر نگرانی‌های امنیتی جدید خواهند شد و عقلانیت محدود تحت تأثیر قرار خواهد گرفت. علاوه بر این، نیاز به واسطه‌گران دوباره وجود خواهد داشت، زیرا عناصر همکاری در امنیت زنجیره بلاکچین به خطر می‌افتند، و هزینه‌های جدیدی به آن اضافه خواهد شد. به طور کلی، تهدید رایانه‌های کوانتومی، کاربرد آینده بلاک‌چین‌ها را برای زنجیره‌های تأمین نامشخص می‌سازد. این عدم قطعیت می‌تواند به طور جدی تصویر ایده آل زنجیره‌های تامین را به چالش بکشد، تاجایی که فرآیندها به شدت به زنجیره‌های بلوکی متکی هستند، و باعث جایگزینی با دوباره بررسی سرمایه‌گذاری در زنجیره بلاکچین منجر شود.

دوگانگی بین تهدیدات کوانتومی و رمزنگاری مقاوم در برابر کوانتومی مانع از پیش‌بینی دقیق نقش آینده رایانه‌های کوانتومی در بلاک چین می‌شود. در حالی که تخمین‌های خاصی نشان می‌دهند که تهدید کوانتومی واقعی است و می‌تواند محسوس تر از راه‌حل باشد، دیدگاه‌های خوش‌بینانه‌تری نیز وجود دارد (کمپبل، 2019؛ چن و همکاران، 2016؛ گئورگیو و همکاران، 2017؛ موسکا، 2018؛ استیونز، 2020).با این وجود، ایجاد استراتژی‌های تجاری مرتبط برای بلاک چین ممکن است به سطح بالاتری از اطمینان نیاز داشته باشد، زیرا ریسک‌ها بسیار زیاد است. با وجود عدم قطعیت، تعهد قابل توجه و همکاری چند جانبه بین مجریان مختلف مانند دولت‌ها، توسعه‌دهندگان نرم‌افزار و استاندارد، دانشگاه‌ها، متخصصان بلاک چین، کارشناسان رمزنگاری و کسب‌وکارها برای تسریع در توسعه و اجرای گسترده یک راه‌حل کوانتومی مستدل مورد نیاز است(گئورگیو وهمکاران، 2017).

بحث و نتیجه گیری

این مطالعه با هدف ارائه یکی از اولین قدم‌ها در خصوص تأثیر آینده کامپیوترهای کوانتومی بر زنجیره تأمین مبتنی بر بلاکچین انجام شده است. با مطالعه دقیق منابع مشخص گردید تأثیر کوانتومی بر زنجیره‌های بلوکی قبلاً در زمینه زنجیره تأمین مورد بحث قرار نگرفته است، در حالی که سرمایه‌گذاری بزرگ جهانی در این فناوری می‌تواند در آینده به‌زودی در معرض تهدید جدی قرار گیرد. با توجه به تازگی موضوع و عدم توجه کافی علمی، بدیهی است که محققان آینده می‌توانند به این موضوع متمرکز شوند. روش‌های پژوهشی آینده می‌توانند تحقیقات تجربی را در خصوص آگاهی کسب‌وکارها از تأثیر کوانتومی و مشارکت‌های ممکنی که می‌توانند در مقابله با تهدید ارائه دهند، به انجام برسانند. همچنین، مطالعات می‌توانند بر آمادگی کسب‌وکارها، در سطوح فردی و زنجیره تامین، برای پذیرش رمزنگاری مقاوم در برابر کوانتومی تمرکز کنند، که به آن تأکید شده است (موسکا، 2018).علاوه بر این، از آنجایی که تأثیر رایانه‌های

کوانتومی بر زنجیره‌های تأمین مبتنی بر بلاک چین از مرز مدیریت زنجیره تأمین فراتر می‌رود، تحقیقات آینده ممکن است نیاز به ترکیب دانش از رشته‌های مختلف برای ایجاد بینش جامعی داشته باشد که به حوزه موضوعی کمک می‌کند.

منابع و مآخذ

1. Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. Computers & Industrial Engineering, 154, 107130. doi:10.1016/j.cie.2021.107130
2. Ahluwalia, S., Mahto, R. V., & Guerrero, M. (2020). Blockchain technology and startup financing: A transaction cost economics perspective. Technological Forecasting and Social Change, 151, 119854.
3. Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019). Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. J—Multidisciplinary Scientific Journal, 2(3), 300-325.
4. Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2021). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. Cluster Computing, 24(1), 83–101. doi:10.1007/s10586-020-03200-4
5. Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., Spirito, L. (2019). Blockchain now and tomorrow: Assessing multidimensional impacts of distributed ledger technologies (EUR 29813 EN). Publications Office of the European Union. 10.2760/901029
6. Bakar, N. A., & Rosbi, S. (2018). Robust framework diagnostics of blockchain for bitcoin transaction system: A technical analysis from Islamic financial technology (i-FinTech) perspective. International Journal of Business and Management, 2(3), 22–29. doi:10.26666/rmp.ijbm.2018.2.4
7. Barker, E., & Dang, Q. (2016). Nist special publication 800-57 part 1, revision 4. NIST, Tech. Rep, 16.
8. Baudier, P., Kondrateva, G., Ammi, C., & Seulliet, E. (2021). Peace engineering: The contribution of blockchain systems to the e-voting process. Technological Forecasting and Social Change, 162, 120397.
9. Braun, D., & Guston, D. H. (2003). Principal-agent theory and research policy: An introduction. Science & Public Policy, 30(5), 302–308. doi:10.3152/147154303781780290
10. Campbell, R. Sr. (2019). Evaluation of post-quantum distributed ledger cryptography. The Journal of The British
11. Blockchain Association, 2(1), 7679. doi:10.31585/jbba-2-1-(4)2019

12. Chalmers, D., Matthews, R., & Hyslop, A. (2019). Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry. Journal of Business Research, 125, 577–591. doi:10.1016/j.jbusres.2019.09.002
13. Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T. Y. (2019). A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. In Future of Information and Communication Conference (pp.988-1003). Springer.
14. Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. Technological Forecasting and Social Change, 144, 1–11. doi:10.1016/j.techfore.2019.03.015
15. Chang, S. E., Chen, Y. C., & Wu, T. C. (2019). Exploring blockchain technology in international trade. Industrial Management & Data Systems, 119(8), 1712–1733.
16. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12). US Department of Commerce, National Institute of Standards and Technology. doi:10.6028/NIST.IR.8105
17. Choi, T. M., Wen, X., Sun, X., & Chung, S. H. (2019). The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. Transportation Research Part E, Logistics and Transportation Review, 127, 178–191. doi:10.1016/j.tre.2019.05.007
18. Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3(1), 1–17.
19. Davies, S., & Likens, S. (2018). Blockchain is here. What's your next move? PWC. https://www.pwc.com/gx/ en/issues/blockchain/blockchain-in-business.html
20. De Leon, D. C., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: Properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship.
21. Di Pierro, M. (2017). What is the blockchain? Computing in Science & Engineering, 19(5), 92–95. doi:10.1109/ MCSE.2017.3421554
22. Dikshit, P., & Singh, K. (2017). Efficient weighted threshold ECDSA for securing bitcoin wallet. In 2017 ISEA Asia Security and Privacy (ISEASP) (pp. 1-9). IEEE. doi:10.1109/ISEASP.2017.7976994
23. DiVincenzo, D. P. (2000). The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics, 48(9-11), 771–783.
24. Djemame, S., & Batouche, M. C. (2016). Quantum Genetic Computing and Cellular Automata for Solving Edge
25. Detection. The First International Conference on Computer Science's Complex Systems and their Applications (ICCSA).
26. Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). Blockchain-oriented dynamic modeling of smart contract design and execution in the supply chain. International Journal of Production Research, 58(7), 2184–2199. doi:10.1080/00207543.2019.1627439
27. Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability, 17, 81–91. doi:10.1016/j.jfs.2014.11.006
28. Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2020). A blockchain-based attribute-based encryption scheme to secure data sharing in the cloud. Journal of Systems Architecture, 102, 101653. doi:10.1016/j.sysarc.2019.101653
29. Fernández-Caramès, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access: Practical Innovations, Open Solutions, 8, 21091–21116. doi:10.1109/ACCESS.2020.2968985

30. Fernández-Caramés, T. M., Froiz-Míguez, I., Blanco-Novoa, O., & Fraga-Lamas, P. (2019). Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. Sensors (Basel), 19(15), 3319.
31. Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7).
32. Firdaus, A., Ab Razak, M. F., Feizollah, A., Hashem, I. A. T., Hazim, M., & Anuar, N. B. (2019). The rise of "blockchain": Bibliometric analysis of blockchain study. Scientometrics, 120(3), 1289–1331.
33. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2. doi:10.3390/logistics2010002
34. Gheorghiu, V., Gorbunov, S., Mosca, M., & Munson, B. (2017). Quantum-proofing the blockchain. Blockchain Research Institute: University of Waterloo.
35. Ghobakhloo, M. (2018). The future of manufacturing industry: A strategic roadmap toward industry 4.0. Journal of Manufacturing Technology Management, 29(6), 910–936. doi:10.1108/JMTM-02-2018-0057
36. Grecuccio, J., Giusto, E., Fiori, F., & Rebaudengo, M. (2020). Combining blockchain and IoT: Food-chain traceability and beyond. Energies, 13(15), 3820. doi:10.3390/en13153820
37. Grover, V., & Malhotra, M. K. (2003). Transaction cost framework in operations and supply chain management research: Theory and measurement. Journal of Operations Management, 21(4), 457–473.
38. Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In Digitalization in supply chain management and logistics: Smart and digital solutions for an industry 4.0 environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23 (pp. 3-18). Berlin: Epubli GmbH.
39. Jaakkola, E. (2020). Designing conceptual articles: Four approaches. AMS Review, 1-9.
40. Jayaraman, R., Salah, K., & King, N. (2019). Improving opportunities in healthcare supply chain processes via the internet of things and blockchain technology. International Journal of Healthcare Information Systems and Informatics, 14(2), 49–65. doi:10.4018/IJHISI.2019040104
41. Kenekayoro Patrick, T. (2011). One way functions and public key cryptography. African Journal of Mathematics and Computer Science Research, 4(6), 213–216.
42. Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, I., & Fedorov, A. K. (2018). Quantum-secured blockchain. Quantum Science and Technology, 3(3), 035004. doi:10.1088/2058-9565/aabc6b
43. Kouhizadeh, M., Zhu, Q., & Sarkis, J. (2020). Blockchain and the circular economy: Potential tensions and critical reflections from practice. Production Planning and Control, 31(11-12), 950–966.
44. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. doi:10.1016/j.ijinfomgt.2017.12.005
45. Kumar, V., Ramachandran, D., & Kumar, B. (2020). Influence of new-age technologies on marketing: A research agenda. Journal of Business Research, 125, 864–877. doi:10.1016/j.jbusres.2020.01.007
46. Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an internet of things environment. The Journal of Supercomputing, 73(3), 1152–1167.
47. Lenstra, A. K. (2002). Citibank, NA and technische universiteit eindhoven. Coding Theory And Cryptology, 1, 175. doi:10.1142/9789812388841_0005
48. Liu, S. (2020, May 13). Blockchain - Statistics & Facts. Statista. https://www.statista.com/topics/5122/blockch

49. Mandolla, C., Petruzzelli, A. M., Percoco, G., & Urbinati, A. (2019). Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. Computers in Industry, 109, 134–152. doi:10.1016/j.compind.2019.04.011
50. Manners-Bell, J., & Lyon, K. (2019). The logistics and supply chain innovation handbook: Disruptive technologies and new business models. Kogan Page Publishers.
51. Mondal, S., Wijewardena, K. P., Karuppuswami, S., Kriti, N., Kumar, D., & Chahal, P. (2019). Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet of Things Journal, 6(3), 5803–5813. doi:10.1109/JIOT.2019.2907658
52. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security and Privacy, 16(5), 38–41. doi:10.1109/MSP.2018.3761723
53. Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. Journal of Open Innovation, 7(1), 19. doi:10.3390/joitmc7010019
54. Nguyen, D. M., & Kim, S. (2019). Multi-bits transfer based on the quantum three-stage protocol with quantum error correction codes. International Journal of Theoretical Physics, 58(6), 2043–2053.
55. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. Cluster Computing, 22(6), 14743–14757. doi:10.1007/s10586-018-2387-5
56. Nowiński, W., & Kozma, M. (2017). How can blockchain technology disrupt the existing business models? Entrepreneurial Business and Economics Review, 5(3), 173–188. doi:10.15678/EBER.2017.050309
57. Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. IEEE Access: Practical Innovations, Open Solutions, 7, 148550–148575.
58. Rana, R. L., Tricase, C., & De Cesare, L. (2021). Blockchain technology for a sustainable agri-food supply chain. British Food Journal. Advance online publication. doi:10.1108/BFJ-09-2020-0832
59. Raz, R. (1999). Exponential separation of quantum and classical communication complexity. In Proceedings of the thirty-first annual ACM symposium on Theory of Computing (pp. 358-367). doi:10.1145/301250.301343
60. Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. Future Internet, 11(7), 161. doi:10.3390/fi11070161
61. Rindfleisch, A., & Heide, J. B. (1997). Transaction cost analysis: Past, present, and future applications. Journal of Marketing, 61(4), 30–54. doi:10.1177/002224299706100403
62. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135.
63. Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. Journal of Purchasing and Supply Management, 25(4), 100552. doi:10.1016/j.pursup.2019.100552
64. Schwab, K., & Davis, N. (2018). Shaping the future of the fourth industrial revolution. Currency.
65. Shankland, S. (2020, June 18). Honeywell says it's got the fastest quantum computer on the planet For now.
66. Sharma, P. K., Kumar, N., & Park, J. H. (2018). Blockchain-based distributed framework for automotive industry in a smart city. IEEE Transactions on Industrial Informatics.
67. Sheetal, M., & Venkatesh, K. A. (2018). Necessary requirements for blockchain technology and its applications. International Journal of Computer Science and Information Technologies.
68. Steinle, C., Schiele, H., & Ernst, T. (2014). Information asymmetries as antecedents of opportunism in buyersupplier relationships: Testing principal-agent theory. Journal of Business-To-Business Marketing, 21(2), 123–140.

69. Stevens, R. (2020, May 12). Quantum computers could crack Bitcoin by 2022: Quantum computers could one day be used to crack the encryption of cryptocurrencies like Bitcoin. And that day could come sooner than anticipated. Decrypt.
70. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management, 23(6), 545–559. doi:10.1108/SCM-01-2018-0029
71. Van Hoek, R., Fugate, B., Davletshin, M., & Waller, M. A. (2019). Integrating blockchain into supply chain management: A toolkit for practical implementation. Kogan Page.
72. Verma, A. K., & Garg, A. (2017). Blockchain: An analysis on next-generation internet. International Journal of Advanced Research in Computer Science, 8(8), 429–432. doi:10.26483/ijarcs.v8i8.4769
73. Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration, 13, 32–39. doi:10.1016/j.jii.2018.07.004
74. Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. Journal of Network and Computer Applications, 127, 43–58. doi:10.1016/j.jnca.2018.11.003
75. Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. Nature Communications, 10(1), 1–8.
76. Xu, P., Lee, J., Barth, J. R., & Richey, R. G. (2021). Blockchain as supply chain technology: Considering transparency and security. International Journal of Physical Distribution & Logistics Management, 51(3), 305–324. doi:10.1108/IJPDLM-08-2019-0234
77. Xue, X., Wang, C., Liu, W., Lv, H., Wang, M., & Zeng, X. (2019). A RISC-V processor with area-efficient memristor-based in-memory computing for hash algorithm in blockchain applications. Micromachines, 10(8), 541. doi:10.3390/mi10080541 PMID:31426443
78. Yadav, M. S. (2010). The decline of conceptual articles and implications for knowledge development. Journal of Marketing, 74(1), 1–19. doi:10.1509/jmkg.74.1.1
79. Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. International Journal of Information Management, 39, 1–4. doi:10.1016/j.ijinfomgt.2017.10.004
80. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267–278.
81. Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2(1), 1–7. doi:10.1186/s40854-016-0049-2
82. 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. doi:10.1504/IJWGS.2018.095647