Defense Policy

Explaining the Legal Function of Blockchain Technology in Defense Policy

Alireza Rezaei [1]| Mehdi Eskandari Khoshguo [2]

1. Corresponding Author: Associate Professor of International Relations, Islamic Azad University, Hamadan Branch, Hamadan, Iran. Email: ir.alirezarezaei@gmail.com
2. PhD student in Public International Law, Faculty of Humanities, Islamic Azad University, Hamedan Branch, Hamedan, Iran.

Volume info

Vol. 34
Series: 132
Autumn 2025
P.P: 33-56

Article Type

Research Paper

Article History

Received:
2025-01-02
Revised:
2025-06-03
Accepted:
2025-06-16
Published:
2026-01-05

ISSN – E-ISSN

ISSN: 2008-6121
E-ISSN: 2645-5218

Abstract

Blockchain technology, as a fundamental innovation in the digital world, is a new and efficient tool for managing data and information. The effects of blockchain in various fields, including financial, social, and political, are significant. Especially in the defense field, given the complexities and challenges of cybersecurity, blockchain as a tool can be effective in strengthening and securing information security and strengthening defense infrastructure. With the advancement of technology and the emergence of new cyber threats, the need for strong legal and regulatory frameworks in defense policies is increasingly felt. Challenges related to privacy, data transparency, and legal conflicts between national and international laws are among the main obstacles to the use of blockchain in defense policy. Such an issue creates the need to carefully examine and analyze the legal functions of blockchain technology in this area. The main objective of this study is to examine the legal functions of blockchain technology in defense policies and analyze its impact on improving cybersecurity and information management in defense institutions. The present study, which is expressed in an analytical-descriptive manner, has attempted to answer the question of how blockchain technology can help strengthen defense policies in the field of cybersecurity and information management and what challenges and opportunities exist in this field? The findings of this study show that blockchain technology, with its unique features, has the ability to increase transparency and accountability in information management, strengthen data security, and improve the supply chain management of military and defense equipment.

Keywords: Blockchain technology, defense policy, legal functions, international law, cybersecurity.

Cite this Article: Rezaei, A., & Eskandari Khoshguo, M. (2025). Explaining the Legal Function of Blockchain Technology in Defense Policy. Scientific Journal of Defense Policy, 34(132), 33-56.
doi : 10.47176/dpj.2025.1799

Publisher: Imam Hossein University.

تبیین کارکرد حقوقی فناوری در سیاست دفاعی

علیرضا رضایی[۱] | مهدی اسکندری خوشگو[۲]

۱. نویسنده مسئول: دانشیار روابط بین الملل، دانشگاه آزاد اسلامی واحد همدان، همدان، ایران.

Email: ir.alirezarezaei@gmail.com

۲. دانشجوی دکتری حقوق بین الملل عمومی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد همدان، همدان، ایران.

چکیده

فناوری بلاکچین به‌عنوان یک نوآوری اساسی در دنیای دیجیتال، ابزاری جدید و کارآمد برای مدیریت داده‌ها و اطلاعات به حساب می‌آید. تأثیرات بلاکچین در زمینه‌های مختلف از جمله مالی، اجتماعی و سیاسی چشم‌گیر است. به‌ویژه در عرصه‌های دفاعی، با توجه به پیچیدگی‌ها و چالش‌های امنیت سایبری، بلاکچین به‌عنوان ابزاری می‌تواند به تقویت و تأمین امنیت اطلاعات و تقویت زیرساخت‌های دفاعی موثر باشد. با پیشرفت فناوری و ظهور تهدیدات جدید سایبری، نیاز به چهارچوب‌های قانونی و حقوقی قوی در سیاست‌های دفاعی بیش از پیش احساس می‌شود. چالش‌های مربوط به حریم خصوصی، شفافیت داده‌ها، و تضادهای قانونی بین قوانین ملی و بین‌المللی، از جمله موانع اصلی در بهره‌برداری از بلاکچین در سیاست دفاعی هستند. چنین مسأله ای نیاز به بررسی و تحلیل دقیق کارکردهای حقوقی فناوری بلاکچین در این حوزه را به وجود می‌آورد. هدف اصلی پژوهش حاضر، بررسی کارکردهای حقوقی فناوری بلاکچین در سیاست‌های دفاعی و تحلیل تأثیر آن بر بهبود امنیت سایبری و مدیریت اطلاعات در نهادهای دفاعی می‌باشد. پژوهش حاضر که به شیوه تحلیلی ـ توصیفی بیان شده، تلاش نموده است تا به این پرسش، پاسخ دهد که فناوری در حوزه سیاست دفاعی دارای چه کارکردها و چالش هایی می باشد؟ یافته‌های پژوهش نشان می‌دهد که فناوری بلاکچین با ویژگی‌های منحصر به فرد خود، قابلیت افزایش شفافیت و مسئولیت‌پذیری در مدیریت اطلاعات، تقویت امنیت داده‌ها و بهبود مدیریت زنجیره تأمین تجهیزات نظامی و دفاعی را دارد.

کلیدواژه‌ها: فناوری بلاکچین، سیاست دفاعی، کارکردهای حقوقی، حقوق بین الملل، امنیت سایبری.

استناد: رضایی، علیرضا، و اسکندری خوشگو ، مهدی. (۱۴۰۴). تبیین کارکرد حقوقی فناوری در سیاست دفاعی. فصلنامه سیاست دفاعی، ۳۴(۱۳۲)، ۳۳- ۵۶. doi : 10.47176/dpj.2025.1799

ناشر: دانشگاه جام امام حسین(ع).

مقدمه

در دنیای امروز، فناوری به‌عنوان یکی از ارکان اصلی توسعه اجتماعی، اقتصادی و سیاسی مطرح است و تأثیرات آن به تمامی ابعاد زندگی بشر نفوذ کرده است. یکی از بارزترین و تحول‌آفرین‌ترین این فناوری‌ها، بلاکچین است که به‌عنوان یک زیرساخت غیرقابل تغییر و ایمن برای تبادل اطلاعات، به‌ویژه در زمینه‌های مالی و قراردادی شناخته می‌شود. بلاکچین با ویژگی‌های منحصر به فرد خود نظیر عدم تمرکز، شفافیت و تضمین امنیت، موجب ایجاد تحولاتی اساسی در عرصه‌های مختلف صنعت و دولت‌ها شده‌است. چنین فناوری به‌خصوص در حوزه‌های حساس و حیاتی نظیر سیاست دفاعی و امنیت ملی، اهمیت فزاینده‌ای پیدا کرده و به‌عنوان ابزاری مؤثر در تقویت امنیت سایبری، مدیریت بحران‌ها و تسهیل ارتباطات استراتژیک به‌کار می‌رود. با توسعه روزافزون تهدیدات سایبری، کشورها به‌دنبال یافتن راه‌حل‌های مدرن برای حفظ امنیت ملی خود هستند. چنین تهدیداتی شامل هک‌های سایبری، سرقت اطلاعات، نفوذ به سیستم‌های حیاتی و تلاش برای تخریب زیرساخت‌ها می‌باشد. از این‌رو، ضرورت طراحی و پیاده‌سازی سیستم‌هایی که قادر به حفظ اطلاعات و ارتقاء شفافیت در حوزه‌های نظامی و امنیتی باشند، بیش از پیش احساس می‌شود. بلاکچین قادر است با ارائه راه‌حل‌هایی برای جلوگیری از نقایص موجود در سیستم‌های سنتی، به افزایش امنیت و کارایی در عملیات نظامی و دفاعی یاری رساند. در محیطی که اطلاعات با سرعت بالا مبادله می‌شوند و هرگونه نقص در امنیت ممکن است به نتایج وخیم و ناخواسته منجر شود، بررسی مزایا و معایب بلاکچین در سیاست‌های دفاعی و همچنین تحلیل چالش‌های حقوقی مرتبط با آن، از اهمیت بسزایی برخوردار است. بلاکچین نه‌تنها قادر است باعث افزایش مسئولیت‌پذیری و شفافیت در فرآیندها شود، بلکه قابلیت‌هایی نظیر ایجاد سوابق نامعتبری و تأمین اطلاعات واقعی را نیز در نوشتن قراردادهای هوشمند ارائه می‌دهد (Huumo & Etc, 2016). با این حال، دغدغه‌هایی از جمله تضادهای قانونی، حریم خصوصی و نحوه تطابق فناوری بلاکچین با سیاست‌های ملی و بین‌المللی نیز وجود دارد که نیاز به تحلیل دقیق و رویکردی نظام‌مند دارد. به عنوان شواهد میدانی، گزارش های پروژه های DARPA, NATO BLOCKCHAIN PILOT مورد بررسی قرار خواهد گرفت. الف) DARPA (آژانس پروژه‌های پیشرفته تحقیقاتی دفاعی ایالات متحده): DARPA در حال تحقیق بر روی قابلیت

استفاده از بلاک‌چین برای ایجاد سیستم‌های اطلاعاتی مقاوم و غیرقابل نفوذ است. پروژه مذکور، بر ایجاد پلتفرم‌های اطلاعاتی تمرکز دارد که قادرند به تغییرات محیطی و تهدیدات سایبری پاسخ داده و در عین حال امنیت داده‌ها را حفظ نمایند. یکی از فعالیت‌های DARPA استفاده از فناوری بلاک‌چین برای مدیریت زنجیره تأمین است. بلاکچین، به شفافیت و تتبع بهتر محصولات نظامی کمک و مانع از ورود تجهیزات تقلبی به زنجیره تأمین می گردد. DARPA همچنین در حال بررسی چگونگی استفاده از بلاک‌چین، برای ذخیره و مدیریت داده‌های زیاد است و به تجزیه و تحلیل داده‌های اطلاعاتی بیشتر و بهبود عملکرد تحلیل‌گران یاری می رساند. DARPA تلاش دارد تا با همکاری با دانشگاه‌ها و مؤسسات تحقیقاتی از فناوری‌های نوین بهره‌برداری نموده و از پژوهش‌های بین‌المللی حمایت نماید تا راه‌حل‌های مناسبی برای چالش‌های جدید پیدا کند. ب) آزمایش‌های بلاکچین ناتو NATO BLOCKCHAIN PILOT: ناتو بر این باور است که بلاک‌چین می‌تواند به بهبود امنیت و قابلیت همکاری اطلاعاتی میان کشورهای عضو کمک نماید. هدف این است که پروتکل‌های جدیدی برای انتقال داده‌ها و مدیریت اطلاعات طراحی شود که شفافیت و امنیت را افزایش دهد. ناتو به بررسی استفاده از بلاک‌چین در زمینه امنیت سایبری پرداخته است تا به امنیت اطلاعات نظامی یاری رساند. بلاکچین، به جلوگیری از دسترسی غیرمجاز به داده‌ها و جلوگیری از نفوذ سیستم‌های اطلاعاتی کمک می نماید. ناتو برخی آزمایش‌های عملی با همکاری کشورهای عضو انجام داده است تا تأثیر بلاک‌چین بر روی عملیات مشترک و امنیت اطلاعاتی فضایی را بررسی کند. آزمایش‌های مذکور، شامل سیستم‌های ارتباطی نهفته، پلتفرم‌های اطلاعاتی مشترک و پروتکل‌های جدید هستند. تحلیل هزینه فایده (Cost-Benefit Analysis یا CBA) ابزاری قوی برای ارزیابی مزایا و معایب سرمایه‌گذاری در فناوری‌های جدید است. در زمینه فناوری بلاکچین، این تحلیل، به‌ویژه در حوزه‌های حساس مانند دفاعی که امنیت و کارایی بسیار حائز ضروری است، کاربردی باشد. پیاده‌سازی ساختاری ایمن که دربردارنده سرورها، نرم‌افزارها و تجهیزات جانبی باشد، ممکن است هزینه‌ای بین ۱ تا ۵ میلیون دلار داشته باشد. برای استفاده از بلاکچین، کارکنان نیاز به آموزش دارند. هزینه چنین اقدامی، در حدود ۱۰۰ هزار دلار است. با استفاده از بلاکچین، پیش‌بینی می‌شود که موارد نقض امنیت اطلاعات به اندازه ۷۰٪ کاهش یابد. چنین کاهشی، به صرفه‌جویی در هزینه‌های ناشی از نقض

امنیت موارد طراحی‌شده و داده‌های حساس (مانند هزینه‌های خسارت یا تحقیق و توسعه) کمک شایانی می نماید که برآورد می‌شود تا ۲ میلیون دلار در سال باشد. یک سیستم بلاکچین به سبب غیرقابل تغییر بودن داده‌ها، اعتماد را بیشتر نموده و تبادلات داده را ایمن‌تر می‌کند. برنامه‌نویسی و تست قراردادهای هوشمند که به صورت خودکار عمل می‌کنند، هزینه‌ای حدود ۲۰۰ هزار دلار را در بر می گیرد. به دلیل نیاز به هماهنگی با سیستم‌های فعلی، هزینه‌هایی بالغ بر ۵۰۰ هزار دلار رخ خواهد داد. بلاکچین، زمان‌های تأمین کالاها را تا ۳۰٪ کاهش می دهد. به عنوان مثال، چرخه تأمین از دو هفته به یک هفته کاهش می یابد که به معنای صرفه‌جویی سالانه حدود ۱ میلیون دلار در هزینه‌های تأمین است. با پیاده‌سازی بلاکچین، شفافیت در زنجیره تأمین افزایش یافته و به حداقل رساندن موارد کلاهبرداری و کاهش خسارت‌ها به صرفه‌جویی تا ۲ میلیون دلار در سال می انجامد. هزینه‌های مربوط به تولید و نگهداری یک پایگاه داده مناسب، به ۳۰۰ هزار دلار می رسد. بلاکچین نیاز به تأییدات دستی را کاهش می‌دهد که این موضوع سبب کاهش زمان و هزینه‌های اداری می گردد. زمان ممکن است از ۳ ساعت به ۱,۵ ساعت برسد که این نیز به معنای افزایش کارایی و کاهش هزینه‌های عملیاتی است. برای ایجاد یک شبکه همکاری میان سازمان‌ها، هزینه‌های راه‌اندازی ممکن است حدود ۲۵۰ هزار دلار باشد. بلاکچین، کارایی پروژه‌های مشترک را ۲۰٪ افزایش دهد. بدین معنا که کاهش هزینه‌های ارتباطی و هماهنگی است که به حدود ۲۵۰ هزار دلار در سال می رسد (Cohen, 2017: 556).. فناوری بلاکچین و سیستم‌های کلید عمومی (PKI) هر دو ابزارهایی هستند که برای تأمین امنیت تراکنش‌ها و اطلاعات در فضای دیجیتال به کار می‌روند، اما هر یک از آن‌ها ویژگی‌ها و قابلیت‌های خاص خود را دارند. مزایای ویژه بلاکچین نسبت به سیستم‌های PKI و سایر سیستم‌های مرتبط به ویژه از نظر تأخیر و مقیاس‌پذیری عبارت اند از: الف) عدم نیاز به اعتماد به نهاد مرکزی: یکی از مزایای اصلی بلاکچین عدم نیاز به یک نهاد مرکزی برای تأیید و اعتبارسنجی تراکنش‌ها است. بدین معنا که بلاکچین، بین شرکای غیرقابل اعتماد همکاری ایجاد می کند و نیاز به اعتماد به یک مرکز خاص را از بین می برد. در سیستم‌های IPK، کاربران باید به یک CA (Certificate Authority) اعتماد کنند. اگر این CA مورد حمله قرار گیرد یا به هر دلیلی از اعتبار ساقط شود، امنیت کل سیستم زیر سوال می‌رود. ب) مقیاس‌پذیری معاملات: با استفاده از تکنیک‌هایی مانند شاردینگ

(Sharding) و Layer 2 solutions (مانند Lightning Network در بیت‌کوین یا زنجیره‌های جانبی)، فناوری بلاکچین قادر است تا مقیاس‌پذیری بالاتری را ارائه دهد. تکنیک‌های مذکور، به پردازش همزمان تعداد زیادی از تراکنش‌ها کمک نموده و تأخیر را کاهش می دهند. در سیستم‌های PKI، با افزایش تعداد کاربران و نیاز به صدور گواهینامه‌های دیجیتال، تأخیر می‌تواند به‌طور قابل توجهی افزایش یابد، زیرا هر بار که کاربری نیاز به گواهینامه جدید دارد، نیاز به درخواست و تأیید از CA وجود دارد که زمان‌بر است. پ) شفافیت و ثبت دائمی: اطلاعات روی بلاکچین به‌طور دائمی ثبت می‌شود و به راحتی قابل‌بررسی و پیگیری است. ویژگی مذکور، باعث می‌شود که تمام تراکنش‌ها شفاف و غیرقابل تغییر باشند و کاربران به راحتی بتوانند به تاریخچه تراکنش‌ها دسترسی پیدا نمایند. در سیستم‌های IPK، تاریخچه و اعتبار گواهینامه‌ها معمولاً در پایگاه داده‌های متمرکز ذخیره می‌شود و ممکن است نیاز به زمان داشته باشد تا اعتبار یک گواهی‌نامه بررسی گردد. ت) کاهش هزینه‌های نگهداری: پس از پیاده‌سازی، هزینه‌های نگهداری بلاکچین می تواند کمتر از PKI باشد. اداره یک سیستم PKI به تجهیزات و منابع بیشتری برای مدیریت گواهی‌نامه‌ها و سرورهای CA نیاز دارد که می‌تواند مانند کارآمدی بلاکچین باشد. ث) حفظ حریم خصوصی و امنیت: با استفاده از تکنولوژی‌های رمزنگاری پیشرفته، بلاکچین، به حفظ حریم خصوصی کاربران یاری رسانده و در عین حال امنیت اطلاعات را تضمین می کند. همچنین با استفاده از ماهیت توزیع‌شده خود، از حملات DDoS و سایر حملات سایبری مصون است. در سیستم‌های PKI، امنیت به مرکزیت CA بستگی دارد. اگر CA هدف حمله قرار گیرد، ممکن است داده‌ها و اطلاعات کاربران در خطر قرار گیرد. ج) کاهش تأخیر در مدیریت اعتبار: در بلاکچین، هر کاربر، به‌طور خودکار و بدون نیاز به انتظار برای تأییدات، اعتبار معامله‌اش را تأسیس می کند. مسئله موردنظر، تأخیر را به حداقل می‌رساند. در سیستم‌های PKI، تأیید اعتبار معمولاً دربردارنده مراحل گوناگونی است که زمان‌بر بوده و موجب تأخیر در انجام کارها می گردد. فناوری بلاکچین به دلیل ویژگی‌های ذاتی خود از جمله عدم تمرکز، مقیاس‌پذیری بالاتر، شفافیت و حفظ حریم خصوصی، نسبت به سیستم‌های PKI و سایر سیستم‌های مشابه advantages مزیت بسیاری دارد. اما لازم به ذکر است که بلاکچین نیز چالش‌هایی دارد و برای همه کاربردها مناسب نیست و در برخی موارد ممکن است سیستم‌های PKI گزینه بهتری باشد. انتخاب بهترین گزینه

بستگی به نیازهای خاص امنیتی، مقیاس و ساختار مورد نظر در هر سازمان دارد. پژوهش حاضر با هدف تبیین کارکردهای حقوقی فناوری بلاکچین در سیاست دفاعی طراحی شده و در جست‌وجوی درک عمق نقش فناوری بلاکچین در بهبود عملکرد نظامی و امنیتی کشورهاست (Young, 2017: 9). پژوهش حاضر که به شیوه تحلیلی ـ توصیفی بیان شده، تلاش نموده است تا به این پرسش، پاسخ دهد که فناوری بلاکچین در سیاست دفاعی دارای چه کارکردها و چالش هایی می باشد؟ فرض اصلی این تحقیق بر آن است که بلاکچین می‌تواند با افزایش شفافیت، مسئولیت‌پذیری و امنیت اطلاعات، به‌عنوان ابزاری مؤثر در تقویت سیاست‌های دفاعی عمل کند. پژوهش حاضر بر این فرض است که فناوری بلاکچین قادر می باشد، به‌عنوان ابزاری کارآمد در استحکام اجزای گوناگون سیاست دفاعی عمل نموده و با ارائه راه‌حل‌هایی جدید، به کشورهای مختلف یاری رساند تا در عصر دیجیتال، امنیت و کارایی را در اولویت قرار دهند. با به‌کارگیری فناوری بلاکچین، کشورها قادر خواهند بود تا ضمن بهره‌مندی از مزایای بلاکچین، به چالش‌ها و تهدیدات موجود واکنش مناسبی نشان دهند و به بهبود زیرساخت‌های دفاعی خود بپردازند.

فناوری بلاکچین

بلاکچین، فناوری جدید و انقلابی است که در سیستم‌های مدیریتی دنیا استفاده می‌شود و در واقع یک نوع خاص از پایگاه داده است که اطلاعات در آن ذخیره می‌شود. بلاکچین می تواند خصوص و محرمانه باشد و بدون نیاز به بیت کوین ی هر رمزارز دیگری مورد استفاده قرار گیرد (شیرانی و طلاکش، ۱۳۹۹: ۱۷۷). دیکشنری انگلیسی آکسفورد یک چنین تعریف وسیعی از بلاکچین ارائه می دهد: یک دفتر کل دیجیتال که در آن تراکنش های انجام شده در بین کوین یا یک رمزارز دیگر از لحاظ تاریخی و به طور عمومی ثبت می شوند. این تعریف نیز مرز ظریف بین فناوری بلاکچین و رمزارزها را به هم میریزد (اسماعیلی عطاآبادی و فتحی زاده، الف، ۱۳۹۸: ۲). هنوز هیچ ارتباط مستقیمی بین بلاکچین و جهان فیزیکی وجود ندارد، هرچند تلاش هایی برای اتصال دنیای دیجیتال و فیزیکی از طریق بلاکچین و از طریق مفهوم اینترنت اشیا وجود دارد (اسماعیلی عطاآبادی و فتحی زاده، ب، ۱۳۹۸: ۳). فناوری بلاکچین با سایر پایگاه‌های داده متفاوت است، چون برای اضافه‌کردن یک دادهٔ جدید به بلاکچین، قواعدی وجود دارد و همچنین

پس از اضافه‌شدن داده به بلاکچین و ذخیرهٔ آن، امکان حذف و ویرایش ندارد. داده‌ها در شبکهٔ بلاکچین در ساختاری متشکل از بلوک‌ها وارد پایگاه داده می‌شوند، هر بلوک در ادامهٔ بلوک قبلی ساخته می‌شود و شامل اطلاعاتی است که آن را به بلوک قبلی متصل می‌کند (صادقی و همکاران، ۱۴۰۲: ۳۶). با توجه به اینکه بلوک‌ها به وسیلهٔ اطلاعاتی به هم وصل هستند، یک زنجیره تشکیل می‌دهند که در آن بلوک‌ها به ترتیب ساخت در کنار هم قرار می‌گیرند. به اولین بلوک شبکه که قبل از آن بلوک دیگری وجود ندارد، بلوک پیدایش گفته می‌شود. با توجه به اینکه هر بلوک حاوی یک هَش خود و هَش بلوک قبلی است، زنجیرهٔ بلوک‌ها از امنیت و ارتباط محکمی برخوردارند. هَش یک تابع رمزنگاری است که از داده‌ها، یک عدد ثابت به نام هَش تولید می‌کند. حتی تغییر کوچک در داده‌ها، تغییر زیادی در هَش ایجاد می‌نماید. فناوری بلاکچین و دفترهای توزیع‌شده به‌شدت مورد توجه قرار گرفته و پروژه‌های متعددی را در صنایع مختلف راه‌اندازی کرده است. (Nofer et al., 2020, p. 6). اولین استفاده گسترده و عمومی از فناوری بلاکچین، در رمزارز بیت کوین رخ داد (حدادی و مظفری، ۱۴۰۱: ۱۳۲). بلاکچین از شبکهٔ پخش متقابل استفاده می‌کند که به هر شخص (نود) در شبکه امکان دسترسی به کل زنجیرهٔ بلوک‌ها و اطلاعات داخل آن را می‌دهد. برخی از بلاکچین‌ها از الگوریتم معدن برای ایجاد بلوک‌ها و تأیید معاملات استفاده می‌کنند. بلاکچین توزیع‌شده است، به این معنا که اطلاعات در تمام شبکه‌ی بلاکچین موجود است. هر نود (رایانهٔ شخصی یا سرور) که به شبکه متصل است، دارای یک کپی از زنجیرهٔ بلوک‌ها است. به دلیل استفاده از هش‌ها و زنجیرهٔ بلوک‌ها، بلاکچین امنیت بالایی ارائه می‌دهد. هرگونه تغییر در یک بلوک، نیاز به تغییر در تمام بلوک‌های بعدی دارد که این امر، تقلب را دشوار می‌کند. تمام تراکنش‌ها در بلاکچین قابل مشاهده هستند. فناوری بلاکچین به‌عنوان راه‌حلی برای دستیابی به توسعهٔ پایدار از طریق راهکارهای مختلف، ازجمله تجارت اعتبار کربن، سیستم‌های انرژی و مدیریت زنجیرهٔ تأمین، مطرح شده است. قراردادهای هوشمند تعریف نشده است؛ مثلاً شاید بتوان گفت نتیجهٔ برنامه‌های رایانه‌ای که به‌صورت توزیع‌شده و تحت سامانهٔ بلاکچین اجرا می‌شوند، قابل دستکاری و اعتراض نیست و نمی‌توان مفاد آن‌ها را به طرق گوناگون تفسیر کرد. البته فناوری بلاکچین و قراردادهای هوشمند، نقایصی هم دارند. با توجه به توزیع‌شده‌بودن فناوری بلاکچین و نیاز به تأیید چند عضو برای ثبت هر تراکنش (برخلاف

سامانه‌های مرکزی که یک عضو تأیید می‌کند)، سرعت انجام تغییرات و تراکنش‌ها و ثبت اطلاعات پایین است. اعضای مشارکت‌کننده در یک بلاکچین (رایانه¬ها) با اطلاعات داخل بلاکچین کار می‌کنند. بنابراین برای اجرای قراردادهایی که بر اساس اتفاقات دنیای فیزیکی طراحی شده‌اند، نیاز دارند این اطلاعات به بلاکچین منتقل شود. انتقال این اطلاعات باید توسط گروهی از اعضا انجام شود تا صحت آن زیر سؤال نرود و امکان تبانی نیز وجود نداشته باشد. برای اجرای قراردادها نیاز است که سازوکارهایی طراحی شود که اولاً انگیزه (معمولاً انگیزهٔ مالی) برای انتقال درست اطلاعات به بلاکچین وجود داشته باشد. همچنین اجرای قراردادها بتواند اثرات مالی داشته باشد. در واقع به نوعی نظام پاداش و جریمه نیاز است که برای شرکت‌های فضایی قابل‌توجه باشد. (Bhutta et al., 2021, p. 8).

مبانی نظری و حقوق بلاکچین

اصول حقوقی بلاکچین

فناوری بلاکچین نه تنها یک ساختار نوآورانه برای ذخیره و انتقال داده‌ها است، بلکه به شکل‌گیری ساختاری جدید در دنیای حقوق و قوانین نیز منجر شده است. بررسی مفاهیم کلیدی حقوقی مرتبط با بلاکچین دیدگاه عمیق‌تری در زمینه تعامل فناوری بلاکچین با سیاست‌ها و قوانین فراهم می‌آورد. الف) مالکیت اطلاعات و داده‌ها: یکی از مسائل اساسی حقوقی در عصر دیجیتال، مالکیت اطلاعات و داده‌هاست. با ظهور بلاکچین، مفهوم مالکیت پیچیده‌تر شده و چالش‌های جدیدی در زمینه حقوقی ایجاد کرده است. در بلاکچین عمومی، داده‌ها به صورت توزیع‌شده میان کاربران مختلف ذخیره می‌شود، بنابراین، شناسایی مالکیت و حقوق مالکیتی که معمولاً به صورت متمرکز تعریف می‌شود، به مشکل برمی‌خورد. از منظر حقوقی، هر داده‌ای که در بلاکچین ذخیره می‌شود، می‌تواند شامل اطلاعات شخصی، تراکنش‌های مالی، یا حتی داده‌های مربوط به قراردادهای هوشمند باشد. موضوعاتی مانند حقوق انتشار، اجازه استفاده از اطلاعات و قوانین مربوط به کپی‌رایت، نیاز به بازنگری و تعریف مجدد دارند. برای مثال، آیا می‌توان فردی را که داده‌هایش در بلاکچین ذخیره شده است، به عنوان مالک اطلاعات شناسایی کرد یا خیر؟ آیا داده‌های دودویی به معنای قابل دسترسی بودن برای عموم به معنای فقدان مالکیت شخصی‌اش

است؟ چنین سوالاتی نیازمند رویکردهای نوینی در سیستم‌های حقوقی کنونی است. ب) قراردادهای هوشمند و اعتبار قانونی آن‌ها: قراردادهای هوشمند به‌عنوان الگوریتم‌هایی خودکار و غیرمتمرکز، معادله جدیدی را در دنیای حقوق ارائه می‌دهند. قراردادها به‌طور مستقل از انسان‌ها عمل کرده و می‌توانند در بستر بلاکچین به انعقاد قراردادها پرداخته و اجرای آن‌ها را تضمین کنند. یکی از چالش‌های حقوقی اساسی در این زمینه اعتبار قانونی این قراردادهاست. آیا یک قرارداد هوشمند به‌طور قانونی قابل قبول است؟ آیا اگر یک طرف قرارداد ادعا کند که قرارداد به درستی اجرا نشده یا تفاسیر متفاوتی از آن داشته باشد، قادر است به دادگاه مراجعه کند؟ سؤالات مذکور مستلزم بحث در مورد اصل تفکیک مسئولیت‌ها، قدرت اثبات و اعتبار حقوقی در محیط بلاکچین است (Muhati, et al., 2022: 107). علاوه بر این، نیاز به قوانین جدید و تدوین قواعد خاص برای نحوه برخورد با مشکلات ناشی از قراردادهای هوشمند در دادگاه‌ها وجود دارد. یاری‌دهی به این موضوع می‌تواند به شفاف‌سازی بیشتر حقوق و مسئولیت‌های طرفین در قراردادهای هوشمند یاری رساند و موجب ایجاد اعتماد به نفس در استفاده از فناوری بلاکچین در حوزه‌های مختلف شود. پ) حریم خصوصی و حفاظت از داده‌ها: حفاظت از حریم خصوصی یکی از حساس‌ترین مسائل در دنیای دیجیتال است. با توجه به اینکه بلاکچین به صورت ذاتی شفاف و قابل مشاهده است، حفاظت از اطلاعات شخصی در چنین محیط چالش بزرگی به شمار می‌آید. داده‌هایی که در بلاکچین ثبت می‌شوند به صورت دائمی و غیرقابل تغییر باقی می‌مانند، که این موضوع می‌تواند به نقض حریم خصوصی افراد منجر شود. علاوه بر مسائل اخلاقی و اجتماعی مربوط به حفظ حریم خصوصی، متغیرهای حقوقی نیز در این زمینه به وجود می‌آید. قوانین مانند GDPR در اروپا، مقررات خاصی را برای حفاظت از داده‌های شخصی ایجاد کرده‌اند، اما آیا این قوانین برای بلاکچین قابل اجرا هستند؟ سوال این است که چگونه می‌توان شفافیت بلاکچین را با نیاز به حفاظت از اطلاعات شخصی هماهنگ کرد. برای مثال، آیا امکان حذف داده‌ها از بلاکچین وجود دارد؟ آیا باید حق «فراموش شدن» را در بیس بلاکچین تعریف کرد؟

رابطه بلاکچین با حقوق بین‌الملل

فناوری زنجیره بلوک، یک فناوری نهادی است که می تواند کارکرد های نظام حقوقی برای عملکرد مطلوب نظام اقتصادی را در قالب الگوریتم ها و کدها ایفا کند (نصیری اقدم، ۱۳۹۹: ۶۱۰). بلاکچین بستری است که از قابلیت تبادل و ذخیره سازی داده پیام های الکترونیکی در محیطی نامتمرکز برخوردار است (آقایی طوق و ناصر، ۱۳۹۸: ۹). بلاکچین یک پدیده جهانی و فراملی است که تأثیرات عمیقی بر نیمه‌های مختلف حقوق بین‌الملل می‌گذارد. بنابراین، فهم تعامل فناوری بلاکچین با احکام و قواعد حقوق بین‌المللی ضروری است. بلاکچین به عنوان یک فناوری غیرمتمرکز، به حاکمیت ملی به چالش می‌کشد. اصول حاکمیت ملی که به معنای کنترل یک کشور بر سرزمین و مردم خود است، با ظهور بلاکچین و ماهیت بین‌المللی آن دچار تزلزل می‌شود. بخصوص در مواردی که بلاکچین در زمینه‌های تجاری و مالی استفاده می‌شود، ایجاد قوانین و مقررات ملی جدید ضروری به نظر می‌رسد .(Akter, et al., 2022: 32) چنین مسئله ای ممکن است کشمکش‌هایی را میان کشورها ایجاد کند، به‌خصوص زمانی که قوانین یک کشور با قوانین کشور دیگر هم‌خوانی نداشته باشد. به‌عنوان مثال، اگر یک تراکنش مالی در بلاکچین که شامل پول‌های مجازی است در کشوری صورت گیرد که این عمل قانونی نیست، وضعیت مذکور به مشکل حقوقی و مالی بزرگی تبدیل خواهد شد. لذا ایجاد سازوکارهای بین‌المللی هماهنگ برای مواجهه با چنین چالش‌هایی از اهمیت بالایی برخوردار است (Marwala & Xing, 2018: 45). عدم وجود چارچوب‌های حقوقی مشترک برای بلاکچین در سطح جهانی، مشکلاتی را در روابط تجاری، سرمایه‌گذاری و تبادل اطلاعات ایجاد می‌کند. همچنین، وجود اختلافات میان نظام‌های حقوقی مختلف می‌تواند بر عدم قطعیت در سرمایه‌گذاری‌های بین‌المللی اثر بگذارد. به طور مثال، اگر کشوری از دیگر کشورها قوانینی بگیرد که با استفاده از بلاکچین تضاد دارد، این امر می‌تواند به تنش‌های اقتصادی و سیاسی بینجامد. همچنین نبود یک مرجع مشخص برای حل و فصل اختلافات مرتبط با بلاکچین قادر است چالش دیگری باشد. در صورتی که طرف ثالثی ادعایی را از طریق بلاکچین مطرح کند، شناسایی مرجع قانونی تصمیم‌گیری در این موارد با مشکلات مواجه است. بنابراین، تجدید نظر در قوانین بین‌المللی و ایجاد چارچوب‌های حقوقی جدید برای پاسخ به این چالش‌ها ضروری است. تحلیل

عمیق حقوق مالکیت، اعتبار قراردادهای هوشمند، و مسائل حریم خصوصی به روشن‌شدن زمینه‌های مختلف فناوری بلاکچین کمک می‌کند. در سطح بین‌المللی، تعامل بلاکچین با حاکمیت ملی و ضعف‌های موجود در قوانین بین‌المللی، ضرورت تدوین چارچوب‌های جدید و عمومی را اجتناب‌ناپذیر می‌سازد. به‌طور کلی، توجه به این جوانب می‌تواند در پیشبرد سیاست‌های دفاعی و امنیتی نقش مؤثری ایفا کند و با افزایش شفافیت و اعتماد عمومی، زمینه‌های حل بحران‌های حقوقی و بین‌المللی بهبود بخشد (Charles, et al., 2023: 41).

سیاست دفاعی و امنیت سایبری

امنیت ملی و دفاعی یک کشور یکی از مهم‌ترین اولویت‌های هر دولتی به شمار می‌آید. تهدیدات امنیتی می‌توانند از طریق حملات سایبری، تروریسم، و سایر فعالیت‌های غیرقانونی بر دولت‌ها تأثیر بگذارند. با پیشرفت فناوری، چنین تهدیدهایی نیز شکل جدیدی به خود گرفته‌اند. به همین دلیل، اتخاذ سیاست‌های مؤثر امنیتی و دفاعی برای حفاظت از اطلاعات و زیرساخت‌ها حائز اهمیت است. در دنیای امروزی، مخاطرات سایبری به شدت گسترش یافته است. حملات هکرها، نقض‌های داده‌ای و حتی حملات زیربنایی می‌توانند تبعات سنگینی بر مؤسسات دولتی و نظامی داشته باشند. اطلاعات حساس و استراتژیک نیازمند حفاظت بیشتری هستند و هر نوع آسیب به این اطلاعات ممکن است به امنیت ملی لطمه بزند. بلاکچین به عنوان یک فناوری نوین، می‌تواند به حل این چالش‌ها یاری نماید و امنیت بیشتری ایجاد نماید. فناوری‌های نوین مانند بلاکچین، اینترنت اشیا، و هوش مصنوعی می‌توانند به سیاست‌های دفاعی کمک کنند. بلاکچین به دلیل عدم تمرکز و شفافیتی که در انتقال اطلاعات دارد، قادر است به عنوان ابزاری مؤثر در بهبود امنیت اطلاعات، تجزیه و تحلیل داده‌ها، و ایجاد قراردادهای هوشمند در زمینه‌های نظامی مورد بهره‌برداری قرار گیرد. سیاست دفاعی به‌عنوان مجموعه‌ای از راهبردها، برنامه‌ها و اقداماتی که کشورها برای حفاظت از منافع ملی و تأمین امنیت خود اتخاذ می‌کنند، تعریف می‌گردد. چنین سیاست‌هایی شامل ابعاد مختلفی هستند که هر یک نقش خاصی در توانمندسازی کشورها ایفا می‌کنند. در سطح ملی، سیاست دفاعی شامل بررسی تهدیدات، برنامه‌ریزی‌های نظامی، و توسعه ظرفیت‌های امنیتی می‌گردد (Sivarethinamohan, et al., 2022: 195). به‌طور کلی، ابعاد

سیاست دفاعی را می‌توان به چهار دسته اصلی تقسیم کرد: ۱. بُعد نظامی: شامل توانمندی‌های نظامی و تجهیزات دفاعی است که کشورها به‌منظور آمادگی برای جنگ و دفاع در برابر تهدیدات ایجاد می‌کنند. در این حوزه، سیاست‌های مرتبط با خرید سلاح، آموزش نیروهای نظامی و استراتژی‌های دفاعی از اهمیت بالایی برخوردارند. ۲. بُعد اقتصادی: سیاست‌های دفاعی نیاز به تأمین مالی و اقتصادی دارد. کشورها باید منابع مالی کافی برای تحقیق و توسعه در حوزه‌های نظامی، فناوری و امنیت سایبری تأمین کنند، همچنین تطابق با مولفه‌های اقتصادی جهانی. ۳. بُعد اجتماعی: امنیت اجتماعی به معنای امنیت روانی و اجتماعی مردم است. هنگام تدوین سیاست‌های دفاعی، توجه به نظر و رضایت عمومی و نیز ارتباط میان دولت و مردم از اهمیت ویژه‌ای برخوردار است. ۴. بعد فناوری: فناوری به‌عنوان پیشران اصلی تغییر در سیاست‌های دفاعی تلقی می‌شود. قدرت‌های نوظهور در بخش فناوری قادر است تأثیر عمیقی بر استراتژی‌ها و تاکتیک‌های نظامی بگذارد، به‌ویژه با ظهور فناوری‌های نوینی مانند هوش مصنوعی، بلاکچین و اینترنت اشیاء. فناوری به‌عنوان یک عامل کلیدی در تحولات نظامی و امنیتی، توانسته است به ارتقاء کارایی در نبرد و عملیات دفاعی ختم شود. به‌ویژه، فناوری اطلاعات و ارتباطات (ICT)، در امنیت سایبری و قابلیت‌های نظامی نقش بسزایی ایفا می‌کند. به‌عنوان مثال، پیشرفت در زمینه تحلیل داده‌ها و هوش مصنوعی به نیروهای نظامی این امکان را می‌دهد که تصمیمات استراتژیک سریع‌تر و مؤثرتری اتخاذ نمایند. فناوری بلاکچین نیز به‌عنوان یک نوآوری در سال‌های اخیر، نقش‌های مهمی در تقویت سیاست‌های دفاعی ایفا کرده است. چنین فناوری قادر است به بهبود شفافیت، امنیت داده‌ها، و مدیریت زنجیره تأمین تجهیزات نظامی یاری رساند. با استفاده از بلاکچین، احتمال هک و دستکاری اطلاعات به حداقل می‌رسد و شفافیت در عملیات نظامی افزایش می‌یابد. با افزایش وابستگی کشورها به فناوری در سیاست‌های دفاعی، آسیب‌پذیری‌ها نیز رشد پیدا کرده است. برخی از آسیب‌پذیری‌های رایج عبارتند از: ۱. نقص‌های امنیتی در نرم‌افزارها: بسیاری از نرم‌افزارهای نظامی به‌دلیل عدم به‌روزرسانی یا مشکلات کدنویسی مستعد آسیب‌پذیری هستند. نرم‌افزارها اگر مورد حمله قرار بگیرند می‌توانند به تخریب داده‌های حیاتی منجر شوند (Dyevre & MC Namara, 2018: 52). 2. حملات سایبری هدفمند: گروه‌های سایبری به‌ویژه آن هایی که از دولت‌ها پشتیبانی می‌کنند، به‌طور مداوم و به‌صورت هدفمند به زیرساخت‌های نظامی و

امنیتی کشورها حمله می‌کنند. گروه‌ها معمولاً تخصص بالایی دارند و می‌توانند به‌راحتی نقاط ضعف سیستم‌ها را شناسایی کنند. ۳. ضعف در آموزش پرسنل: عدم آموزش کافی پرسنل نظامی در زمینه امنیت سایبری و روش‌های حفاظت از داده‌ها می‌تواند به سهل‌انگاری و ایجاد نقاط ضعف در سیستم‌ها منجر شود. ۴. تکنیک‌های فیشینگ و مهندسی اجتماعی: چنین روش‌هایی به‌عنوان یکی از معمول‌ترین راه‌های نفوذ به سیستم‌های امنیتی به حساب می‌آیند. با استفاده از تکنیک‌های فیشینگ، هکرها، به اطلاعات حساس و دسترسی به سیستم‌ها دست می یابند. تاریخ معاصر به وضوح نشان‌دهنده این است که نقض‌های امنیتی به تبعات جدی برای کشورها و سازمان‌ها منجر شده‌اند. چندین نمونه از این نقض‌ها عبارتند از: ۱. حمله به زیرساخت‌های انرژی ایالات متحده در سال ۲۰۱۵: هکرها موفق شدند به سیستم‌های الکتریکی ایالات متحده نفوذ کنند و این موضوع به اختلال در تأمین برق در برخی مناطق منجر شد. چنین نقض امنیتی نه تنها تبعات اقتصادی داشت بلکه به بحرانی اجتماعی تبدیل شده و تأثیر منفی بر اعتماد عمومی به سیستم‌های امنیتی داشت. ۲. حمله به شرکت سونی در سال ۲۰۱۴: هکرها اطلاعات حساس و خصوصی شرکت سونی را فاش کردند که منجر به افشای اسناد محرمانه و اختلال جدی در روند کاری این شرکت شد. حادثه مذکور، توجهات جهانی را به چالش‌های امنیت سایبری و آسیب‌پذیری‌های موجود جلب کرد. ۳. حمله سایبری به ناتو: روحیه بسیاری از کشورها در برابر چالش‌های امنیتی به‌خاطر حملات سایبری به ناتو کاهش یافت و مسئله اعتماد به نفس و کارایی نیروهای نظامی در برابر تهدیدات سایبری به‌طور جدی مورد بحث قرار گرفت. تبعات این نوع حملات، نه‌تنها محدود به اختلالات اقتصادی و اجتماعی‌ست، بلکه می‌تواند به تغییر سیاست‌های داخلی و بین‌المللی نیز منجر شود. به عنوان مثال، حملات سایبری قادر است بر روی تصمیمات استراتژیک یک کشور در زمینه‌های نظامی و امنیتی تأثیر بگذارد و موجب افزایش هزینه‌های امنیتی گردد (Yaga et al., 2018: 67).

کارکردهای فناوری بلاکچین در سیاست دفاعی

بلاکچین با ارایه راه‌حل‌های نوین و مؤثر، می‌تواند بهبودهای چشمگیری در امنیت، شفافیت و کارایی در عرصه دفاعی به ارمغان آورد. در این بخش، به بررسی کارکردهای سه‌گانه بلاکچین در سیاست دفاعی پرداخته خواهد شد: افزایش شفافیت و مسئولیت‌پذیری، تقویت امنیت اطلاعات

و داده‌ها، و بهبود مدیریت زنجیره تأمین. شفافیت یکی از ارکان اساسی در مدیریت مؤثر و بهینه سیاست‌های دفاعی است. بلاکچین با قابلیت ثبت دائمی و غیرقابل تغییر اطلاعات، قادر است در ایجاد سیستم‌های شفاف و قابل پیگیری نقش بسزایی ایفا کند. هر تغییر یا افزوده‌ای به داده‌ها در بلاکچین به‌طور دقیق ثبت می‌شود و امکان ردیابی تاریخچه تمامی تعاملات و تراکنش‌ها وجود دارد. چنین ویژگی موجب کاهش فساد، تقلب و سوء استفاده‌های احتمالی در سیستم‌های دفاعی می‌شود (Muheidat & Tawalbeh, 2021: 26). به‌عنوان مثال، در پیاده‌سازی قراردادهای هوشمند در زنجیره تأمین نظامی، تمامی مراحل تأمین، توزیع و نگهداری تجهیزات می‌توانند در بلاکچین ثبت شوند. این امر به مدیران نظامی این امکان را می‌دهد که به‌طور لحظه‌ای از وضعیت و مکان تجهیزات آگاهی داشته باشند و در راستای مدیریت منابع خود بهتر عمل نمایند. یکی از اثرات مثبت شفافیت در سیاست‌های دفاعی، افزایش اعتماد عمومی به نهادهای نظامی و دولتی است. وقتی که مردم می‌دانند که تمامی داده‌ها در یک سیستم شفاف ثبت می‌شوند، احتمال از دست رفتن اعتبار نهادها کاهش می‌یابد. اعتماد نه تنها به نهادهای داخلی مرتبط می‌شود بلکه می‌تواند بر روابط بین‌الملل نیز تأثیر بگذارد. شفافیت در اطلاعات قادر است در مذاکرات بین‌المللی، مخصوصاً در زمینه‌های امنیتی و دفاعی، به تسهیل روابط میان کشورها یاری رساند. کشورهای مختلف که از نظام‌های بلاکچینی استفاده می‌کنند، می‌توانند به هم اعتماد بیشتری داشته باشند و به توافقات بین‌المللی در زمینه امنیت و دفاع پایبندتر باشند (Daley, 2020: 44). فناوری بلاکچین به‌واسطه معماری امن خود، می‌تواند در حفاظت از اطلاعات حساس و بحرانی نظامی مؤثر باشد. با ترکیب رمزنگاری پیشرفته و توزیع داده‌ها در سراسر شبکه، بلاکچین نه تنها آسیب‌پذیری‌های معمول در سیستم‌های متمرکز را کاهش می‌دهد، بلکه داده‌ها را در برابر حملات سایبری مقاوم‌تر می‌سازد. به‌عنوان نمونه، با استفاده از بلاکچین، سازمان‌های نظامی، اطلاعات محموله‌ها و تجهیزات خود را به‌صورت رمزگذاری‌شده و در یک دفتر کل مشترک ذخیره می کنند. چنین روشی نه تنها دسترسی غیرمجاز به داده‌ها را دشوارتر می‌کند بلکه به تأیید اصالت اطلاعات نیز کمک می‌کند. یکی از بزرگ‌ترین چالش‌های سیاست‌های دفاعی، جلوگیری از جعل و تقلب اطلاعات است. بلاکچین با ویژگی عدم‌تغییر داده‌ها قادر است نقشی حیاتی در کاهش این مشکلات ایفا کند. به‌عنوان مثال، استفاده از بلاکچین برای ثبت و تأیید توزیع و

مصرف تجهیزات نظامی، به طرز قابل توجهی ریسک جعل را کاهش می‌دهد، زیرا هکرها و عوامل مخرب به آسانی نمی‌توانند به داده‌های ثبت‌شده دسترسی پیدا و در آن تغییر ایجاد کنند. چنین رویکردی ممکن است به کاهش هزینه‌های مربوط به بررسی و تأیید اطلاعات نیز یاری رساند. با توجه به اینکه اطلاعات ثبت شده در بلاکچین قابل تغییر نیستند، نیاز به بررسی‌های دوره‌ای برای تأیید صحت اطلاعات کاهش می‌یابد و می‌توان از منابع به‌دست‌آمده به‌طور مؤثرتری استفاده کرد. زنجیره تأمین تجهیزات نظامی به‌طور معمول شامل مراحل پیچیده‌ای از تولید تا توزیع و نگهداری است. در این فرآیند، اطمینان از اصالت و کیفیت تجهیزات با توجه به میزان سرمایه‌گذاری کلان، ضروری است (Eckel, 2019: 26). بلاکچین قادر است به‌عنوان یک راهکار نوآورانه در این زمینه عمل نموده و با فراهم کردن یک سیستم قابل اطمینان برای پیگیری وضعیت هر یک از اقلام، شفافیت و کارایی را بهبود بخشد. بهره‌برداری از طریق رمزنگاری داده‌ها، سیستم‌های هوشمند برای تأیید اصالت تجهیزات، و ردیابی فرآیند تأمین‌کنندگان و توزیع‌کنندگان محقق می‌شود. به‌طور مثال، بلاکچین می‌تواند به سازمان‌های دفاعی این امکان را بدهد که در صورت بروز هرگونه مشکل، بلافاصله منبع آن را شناسایی کنند و به طور مؤثرتری اقدام نمایند. در سطح بین‌المللی، نمونه‌های موفقی از استفاده از بلاکچین در زنجیره تأمین تجهیزات نظامی وجود دارد. به‌عنوان مثال، ارتش ایالات متحده در پروژه‌هایی به کارگیری بلاکچین برای مدیریت زنجیره تأمین تجهیزات پزشکی و نظامی پرداخته است. چنین پروژه‌هایی نشان‌دهنده این هستند که چگونه بلاکچین قادر است به بهبود پیگیری، کاهش هزینه‌ها و افزایش کارایی در زنجیره تأمین نظامی منجر شود. علاوه بر ارتش ایالات متحده، کشورهای دیگر از جمله چین و کره جنوبی نیز در حال آزمایش و پیاده‌سازی راه‌حل‌های بلاکچینی برای مدیریت زنجیره تأمین تجهیزات نظامی خود هستند. اقدامات مذکور به‌طور مستمر در حال گسترش است و با به‌کارگیری موفقیت‌آمیز بلاکچین، انتظار می‌رود که بسیاری از کشورهای دیگر نیز در آینده‌ای نزدیک از فناوری بلاکچین بهره‌برداری کنند (Hamilton, 2018:54)

مشکلات فناوری بلاکچین در حوزه های دفاعی بر مبنای طبقه بندی

یکی از مزایای اصلی بلاکچین امنیت بالای آن است، اما این بدان معنی نیست که مشکلات امنیتی وجود ندارد. در حالی که خود بلاکچین، به دلیل ساختار توزیع‌شده‌اش ایمن است، اما زیرساخت‌ها و نرم‌افزارهای مرتبط با آن، هدف حملات سایبری قرار می گیرند. هکرها، به نقاط ضعف در نرم‌افزارهای موجود دسترسی پیدا کرده و از آن‌ها برای ورود به شبکه‌های بلاکچینی استفاده می نمایند. قراردادهای هوشمند، که برنامه‌های خوداجرا در بلاکچین هستند، مستعد خطاهای برنامه‌نویسی می باشند. یک خطای کوچک در کد به نتیجه‌های ناخواسته و تهدیدات امنیتی منجر می گردد که از بین بردن منابع یا داده‌ها را می‌تواند در پی داشته باشد. در مناطق دفاعی، نیاز به سرعت و کارایی عملیاتی بسیار بالا است. بلاکچین‌های عمومی مانند بیت‌کوین زمان بیشتری برای پردازش هر تراکنش نیاز دارند، که این مسئله در موقعیت‌های حساس زمان واقعی ناکافی می باشد. در زمان‌هایی که تعداد تراکنش‌ها بسیار بالا می‌رود، هزینه هر تراکنش می‌تواند به چالشی تبدیل شود. هزینه‌ها ممکن است باعث عدم استقبال از انحصار در بخش دفاعی شوند. قوانین و مقررات حاکم بر فناوری بلاکچین وضعیت قابل‌توجهی در هر کشوری دارند. هنوز بسیاری از کشورها قوانین واضح و دقیقی برای مدیریت و نظارت بر استفاده از بلاکچین ندارند. در حوزه دفاعی، دقت و صحت داده‌ها از اهمیت بالایی برخوردار است (Hebblethwaite, 2017: 19). ذخیره‌سازی اطلاعات در بلاکچین به معنای اطمینان از صحت آن‌ها است. وجود نقص در اطلاعات، تبعات جدی برای امنیت ملی دارد. پیاده‌سازی موفقیت‌آمیز بلاکچین نیازمند همکاری نزدیک بین چندین سازمان و نهاد مختلف است. نهادهای نظامی و غیرنظامی معمولاً سیستم‌ها و پروتکل‌های متفاوتی دارند. ناهمگونی در این زمینه، مانع از یکپارچگی و کارایی فناوری بلاکچین می شود. بسیاری از سازمان‌های نظامی به زیرساخت‌های قدیمی و غیرقابل ادغام با فناوری‌های جدید نیاز دارند. سرمایه‌گذاری اولیه و هزینه‌های پیاده‌سازی بلاکچین، تجزیه‌وتحلیل پیچیده‌ای را طلب می نماید. هزینه‌های بالای راه‌اندازی و نگهداری سیستم‌های بلاکچینی، مانع از پذیرش گسترده آن می گردد.

نتیجه‌گیری

فناوری بلاکچین در دهه‌های اخیر به‌عنوان یک نوآوری تحول‌آفرین در صنایع مختلف شناخته شده است و تأثیر خود را به‌ویژه در حوزه‌های امنیتی و دفاعی به وضوح نشان داده است. در دنیای امروز، تهدیدات سایبری به‌سرعت در حال افزایش هستند و حکومت‌ها به‌ویژه باید به نهادهای امنیتی امکان دهند تا در برابر چنین تهدیداتی واکنش سریع و مؤثری داشته باشند. بلاکچین، با ماهیت غیرمتمرکز و رمزنگاری شده‌اش، این امکان را فراهم می‌کند تا داده‌ها و اطلاعات مربوط به عملیات و استراتژی‌های نظامی نیز به‌صورتی امن و بدون احتمال دست‌کاری حفظ شوند. شفافیت به‌عنوان یکی از ابعاد اصلی بلاکچین، قادر است در سیاست‌های دفاعی نقش بسزایی ایفا کند. ایجاد پروتکل‌های بلاکچین در رویه‌های نظامی و دفاعی می‌تواند از فساد و سوءمدیریت جلوگیری کند و در عین حال به ایجاد اعتماد عمومی و بین‌المللی کمک شایانی نماید. چنین موضوعی به‌ویژه در زمان‌هایی که تحریم‌ها و فشارهای بین‌المللی بر کشورها اعمال می‌شود، اهمیت بیشتری پیدا می‌کند، زیرا شفافیت قادر است به کشورهای در حال توسعه یاری رساند تا اعتبار خود را در فضای بین‌المللی تقویت نمایند. مسئله حریم خصوصی و حفاظت از داده‌ها نیز یکی از چالش‌های جدی در زمینه استفاده از بلاکچین در سیاست‌های دفاعی است. با اینکه بلاکچین شفافیت را ارتقاء می‌دهد، نگرانی‌های مربوط به افشای اطلاعات حساس و حقوق حریم خصوصی همچنان وجود دارد. لذا ضروری است نهادهای دولتی و نظامی به طراحی و پیاده‌سازی استراتژی‌هایی بپردازند که ضمن حفظ شفافیت، از حقایق خصوصی و اطلاعات حساس نیز محافظت کند. در این راستا، پیدا کردن تعادل میان شفافیت و امنیت شخصی قادر است به موفقیت فناوری بلاکچین در سیاست دفاعی یاری رساند. یکی دیگر از نتایج کلیدی تحقیق، عدم وجود چارچوب‌های قانونی مشخص جهت استفاده از بلاکچین در سیاست‌های دفاعی است. عدم وجود چارچوب می‌تواند مناطق خاکستری قانونی را ایجاد کند که باعث عدم اطمینان و تعاملات ضعیف در حوزه سیاست دفاعی می‌شود. بنابراین، لازم است تا حکومت‌ها و نهادهای بین‌المللی به توسعه و تصویب قوانین و مقرراتی بپردازند که استفاده از فناوری بلاکچین در سیاست‌های دفاعی را ممکن و مشروط سازد. بنابراین، اگر چه بلاکچین می‌تواند به‌عنوان یک

ابزار مؤثر در تقویت سیاست‌های دفاعی عمل کند، اما موانع مختلفی در پیش رو وجود دارد که توجه و اصلاح آن‌ها را می‌طلبد. بدین ترتیب، شناخت کامل فرصت‌ها و چالش‌های پیش روی بلاکچین در این حوزه، مهم‌ترین گام برای بهره‌برداری مؤثر از این فناوری‌های نوین به شمار می‌آید. تدوین یک چارچوب سه لایه قانون‌گذاری برای فناوری بلاکچین نیازمند یک رویکرد جامع و دقت در نظرگیری جوانب مختلف بلاکچین نوپا است. چارچوب باید به‌گونه‌ای طراحی شود که هم فرصت‌ها را شناسایی کرده و هم چالش‌ها و مشکلات بالقوه را مدیریت نماید. در این راستا، می‌توان این چارچوب را به سه لایه تقسیم کرد: لایه بنیادی، لایه تنظیمات ویژه و قانون‌گذاری صنعتی و لایه بین‌المللی و تعاملات جهانی. لایه اول) قوانین بنیادی و اصول اولیه: در نخستین مرحله، نیاز است که اصطلاحات کلیدی مرتبط با بلاکچین به شکلی دقیق تعریف شوند. به‌عنوان مثال، قوانین ابتدایی باید شامل تعاریف بلاکچین، قراردادهای هوشمند، توکن‌ها و ارزهای دیجیتال باشند. تعاریف، همچنین باید شامل یک توضیح مختصر از نحوه عملکرد بلاکچین‌ها و تأثیرات آن‌ها بر جوامع و اقتصادها باشد. برقراری اصول کلی نظیر شفافیت، غیردولتی بودن، عدم تمرکز و حریم خصوصی در این بخش حیاتی است. اصول مذکور، باید به‌طور مستمر در چارچوب‌های قانونی و مقرراتی اعمال شوند و به‌عنوان ارکان اساسی امنیت و اعتماد عمومی در فرآیندهای بلاکچینی عمل نمایند. با توجه به اینکه بسیاری از کاربردهای بلاکچین شامل ذخیره‌سازی و پردازش داده‌های شخصی است، نیاز به پیاده‌سازی قوانین مربوط به حریم خصوصی و حفاظت از داده‌ها احساس می‌شود. قوانین میبایست حقوق فردی نسبت به داده‌های خود را مشخص کنند و نحوه استفاده از این داده‌ها در بلاکچین را تحت نظارت قرار دهند. قوانین، به‌گونه‌ای تنظیم شوند که افراد بتوانند دسترسی و ویرایش اطلاعات شخصی خود را داشته باشند. قوانین مربوط به امنیت باید به طور خاص به پروتکل‌های بلاکچینی اشاره داشته باشند و الزامات امنیتی مشخصی را در نظر بگیرند تا از حملات سایبری و نقض داده‌ها جلوگیری شود. قوانین مذکور، مکانیزم‌های امنیتی را که می‌توانند به حفظ ایمنی شبکه‌های بلاکچینی کمک کنند، تنظیم نمایند. تعیین نهادهای مسئول نظارت بر اجرای قوانین و قواعد در زمینه بلاکچین لازم است. نهادها به ایجاد استانداردهای بین‌المللی در زمینه بلاکچین کمک می رسانند. طبقه‌بندی فعالیت‌های غیرقانونی در این فضا و جرم‌انگاری برخی رفتارها (مانند پول‌شویی یا تقلب) باید در این لایه مد

نظر قرار گیرد. به‌عنوان مثال، باید راهکارهایی برای شناسایی و مدیریت فعالیت‌های غیرمجاز در فضاهای بلاکچینی طراحی شود. لایه دوم) قوانین ویژه و تنظیمات صنعت: قوانین خاصی که بر صنعت مالی و بانکداری دیجیتال تأثیر می‌گذارد، باید تدوین شود. قوانین مذکور، میبایست به جنبه‌های مختلفی نظیر صدور ارزهای دیجیتال و استفاده از آن‌ها در پرداخت‌ها، مدیریت ریسک‌های مالی و معیارهای مربوط به تأمین مالی و تضمین‌های لازم بپردازند. به‌ویژه، باید دامنه و محدودیت‌های قانونی را بر اساس نوع فعالیت‌ها تعیین کرد. تدوین چارچوب‌های قانونی برای تعیین اعتبار و اجرایی بودن قراردادهای هوشمند و نحوه حل و فصل اختلافات ناشی از آن‌ها، در این لایه مورد توجه قرار می گیرد. ایجاد الزامات و استانداردهای فنی برای پشتیبانی از نوآوری در بلاکچین، شامل نیازهای سخت‌افزاری و نرم‌افزاری، پروتکل‌ها و APIهای مرتبط، باید در نظر گرفته شود. تعریف استانداردهای کمی و کیفی در حوزه بلاکچین، به تسهیل نوآوری و توسعه فناوری‌های جدید می انجامد. ایجاد فضای قانونی مشخص برای استارتاپ‌ها و نوآوران در حوزه بلاکچین، از جمله طرح‌های آزمایشی (sandbox)، به آن‌ها اجازه می دهد تا بدون درگیری‌های قانونی، فناوری‌های جدید را آزمایش کنند. توسعه معیارها و ارتباطات برای شفاف‌سازی ریسک‌های مرتبط با سرمایه‌گذاری در ارزهای دیجیتال و جلوگیری از استثمار سرمایه‌گذاران غیرحرفه‌ای، در این لایه لحاظ می شود. به‌عنوان مثال، قوانین مربوط به تبلیغات و اطلاع‌رسانی در زمینه ارائه محصولات مالی باید تنظیم شوند تا اطمینان حاصل شود که اطلاعات کافی به سرمایه‌گذاران ارائه می‌شود. تدوین راهکارهایی برای مدیریت ریسک‌های اجتماعی و اقتصادی ناشی از عدم جبران خسارت در موارد نقض حقوق میبایست به‌طور خاص در نظر گرفته شود. سازوکارهایی برای جبران خسارات ناشی از کلاهبرداری‌های مالی یا نواقص در پروژه‌های بلاکچینی تدوین می گردد. لایه سوم) مقررات تعاملات بین‌المللی: ایجاد توافقات همکاری میان کشورها برای شفافیت و هماهنگی در قوانین بلاکچینی و تبادل اطلاعات با هدف ایجاد یک چارچوب قانونی مشترک برای تجارت و مالیات آنلاین، بسیار مؤثر است. توافقات به‌گونه‌ای طراحی می شوند که به تبادل دانش، تجارب و استانداردها در سطح جهانی بپردازند. ایجاد شبکه‌های نظارتی و ارزیابی تحت نظارت سازمان‌های بین‌المللی به‌منظور رصد فعالیت‌های بلاکچین در سطوح بین‌المللی، مدنظر قرار می گیرد. تضمین اطمینان از اینکه هیچ‌یک از

فعالیت‌های مرتبط با بلاکچین سبب نقض حقوق بشر نمی‌شود و حتی ارتقا آن‌ها بر مبنای افـزایش شفافیت و دسترسی به اطلاعات باید از جمله اهداف کلیدی این لایه محسوب شـوند. بـه‌ویـژه، در پروژه‌های بلاکچینی که به نحوی با اطلاعات حساس انسـانی در ارتبـاط هسـتند، ایـن نکتـه بسـیار اهمیت دارد. اقداماتی که به افزایش شمولیت اجتماعی و مالی کمـک مـی‌کننـد، ماننـد اسـتفاده از بلاکچین برای تسهیل دسترسی به خدمات مالی برای افرادی که به‌طـور سـنتی بـه آن‌هـا دسترسـی ندارند، نیز باید بررسی شوند. توسعه احکام و الزامات تطبیق با پیشرفت‌های فناوری‌های نوظهـور و نوآوری‌هایی چون اینترنت اشیا (IoT)، هوش مصنوعی (AI) و سایر تولیدات دیجیتالی بـا هـدف هم‌افزایی قانون‌گذاری باید به‌صورت مستمر در نظر گرفته شود. فرهنگ حقوقی به مجموعـه‌ای از باورها، ارزش‌ها و رویه‌های قانونی اطلاق می‌شود که در یک سازمان یا جامعه خاص شکل گرفته است. فرهنگ حقوقی، نه‌تنها به شیوه‌های برخـورد بـا قـوانین و حقـوق بشـر اشـاره دارد، بلکـه بـر تعاملات اجتماعی و سیاسی نیز تأثیرگذار است. فرهنگ حقوقی، بر نحـوه تصـمیم‌گیـری، اجـرای قوانین و نظارت بر فعالیت‌ها تأثیر می گذارد. در نیروهای مسلح و نهادهای امنیتی، فرهنگ حقوقی نقشی حیاتی دارد. هرگونه انحراف از چنین اصولی سبب نقض حقوق بشر و بـی‌اعتمـادی عمـومی می گردد. ادغام فناوری‌های نوین همچون بلاکچـین در نهادهـای مـوردنظر، راهکارهـای مـؤثری برای تقویت فرهنگ حقوقی ارائه مـی دهـد. بلاکچـین خـود بـه‌عنـوان یـک فنـاوری غیرمتمرکـز اطلاعات به‌طور درون‌زا و با استفاده از رمزنگـاری امنیـت داده‌هـا را تضـمین مـی‌کنـد. سیسـتم بـه گونه‌ای طراحی شده که همه داده‌ها به‌صورت عمـومی و غیرقابـل تغییـر ثبـت مـی‌شـوند. فنـاوری بلاکچین به‌طور خاص به پیگیری و ردیابی اطلاعات یاری می رساند. به‌عنوان مثال، ثبت اطلاعات مربوط به تأمین مالی تجهیزات نظامی، عملیات‌ها و تعاملات با دیگر کشورها، در بلاکچین ثبـت و مدیریت می شود. کاربرد غیرمتمرکز بلاکچین، به آن معناست که هیچ نهاد واحدی نمی‌توانـد بـر اطلاعات کنترل مطلق داشته باشد. استفاده از فناوری بلاکچین، به افزایش شفافیت در فعالیت‌هـای نظامی و امنیتی می انجامد. اطلاعات را مـی‌تـوان بـه‌صـورت عمـومی در دفترکـل‌هـای بلاکچینـی نگهداری کرد، که این امر از ظرفیت‌های حسابرسی و نظارت حمایت می نماید. اطلاعات مربـوط به عملیات‌های نظامی، تأمین منابع مالی و استفاده از تجهیـزات نظـامی بـه‌طـور مـؤثر و دقیـق ثبـت خواهد شد. بلاکچین، راهکارهایی برای تقویت حقوق بشر در زمینه‌های امنیتی فراهم می کنـد. بـا

ثبت اطلاعات و روندهای قانونی در بلاکچین، نهادهای امنیتی، ردیابی و نظارت بر رفتارهای خود را از طریق فرآیندهای شفاف‌تری انجام می دهند. فناوری بلاکچین، باعث تسهیل همکاری و هماهنگی میان نهادهای نظامی و امنیتی مختلف می گردد. توسعه و گنجاندن بلاکچین در سیاست‌های امنیتی، به نهادهای نظامی کمک می نماید تا روش‌های بهتری برای سازمان‌دهی اقدامات خود در برابر چالش‌های معاصر پیدا کنند. چنین بحثی، به تضمین انطباق با حقوق بشر، شفافیت و افزایش پاسخگویی در میان نهادها منجر می شود. تغییر فرهنگ حقوقی، به‌ویژه در نهادهای نظامی، معمولاً با موانع و مقاومت‌هایی مواجه است. بسیاری از افرادی که در این بخش‌ها کار می‌کنند ممکن است به تغییرات، به‌ویژه در زمینه‌های فناوری، به راحتی واکنش نشان ندهند. وجود خلاهای قانونی در زمینه بلاکچین و کاربرد آن، موانع جدی برای پذیرش بلاکچین در نهادها ایجاد می کند. خلاها، گاهاً موجب عدم امنیت حقوقی و افزایش تعارضات می‌شود، به‌خصوص در مواقعی که اطلاعات ثبت‌شده باعث دعاوی قانونی می‌گردد. گروه G20، به‌طور منظم نشست‌هایی را برای بررسی و تبادل نظر در مورد مسائل اقتصادی و مالی جهانی برگزار می‌کند. فناوری بلاکچین به‌عنوان یکی از موضوعات کلیدی در این نشست‌ها مطرح شده است. اعضای G20 به‌خوبی آگاه هستند که بلاکچین، به‌عنوان ابزاری برای تسهیل گردش مالی، تقویت امنیت سایبری و انجام معاملات بین‌المللی به کار می رود. در نشست‌های سالانه G20، نمایندگان کشورهای مختلف به بحث در مورد مزایا و چالش‌های بلاکچین پرداخته و به لزوم ایجاد همکاری‌های بین‌المللی برای تنظیم و نظارت بر کاربردهای بلاکچین تأکید می‌کنند. همکاری‌ها در اینخصوص شامل تبادل اطلاعات، به اشتراک‌گذاری بهترین شیوه‌ها و ایجاد استانداردهای جهانی برای فناوری بلاکچین می باشد. گروه G20 با تأکید بر مزایای اقتصادی بلاکچین، به‌طور خاص به موارد گوناگونی اشاره کرده است، که مهم ترین آن ها، عبارت اند از: بلاکچین قادر است با ایجاد یک سیستم غیرمتمرکز، هزینه‌های مربوط به معاملات را بسیار کاهش دهد. چنین موضوعی به نفع کسب‌وکارها و مصرف‌کنندگان خواهد بود. با استفاده از بلاکچین، تمام تراکنش‌ها به‌طور دائمی و غیرقابل تغییر ثبت می‌شوند، که این مورد، شفافیت را در تجارت افزایش می‌دهد. شفافیت به‌نوبه خود، به کاهش فساد و تقلب در معاملات تجاری می انجامد. با این حال، G20 به خطرات و چالش‌های مرتبط با استفاده از بلاکچین نیز توجه نموده است. عدم وجود

یک چارچوب قانونی مشخص برای فناوری بلاکچین سبب بی‌نظمی‌های حقوقی می شود. کشورهای مختلف به قوانین و مقررات متفاوتی برای حاکمیت بلاکچین نیاز دارند. افزایش استفاده از بلاکچین، به نگرانی‌های مربوط به حریم خصوصی می انجامد. از آنجایی که بلاکچین به‌طور عمومی اطلاعات را ذخیره می‌کند، باید اطمینان حاصل شود که حریم خصوصی کاربران به‌خوبی حفظ شود. کمیسیون حقوق تجارت بین‌الملل ملل متحد (UNCITRAL) مسئول ایجاد و توسعه چارچوب‌های قانونی بین‌المللی است که به تسهیل تجارت جهانی کمک می‌کنند. UNCITRAL در اواخر سال ۲۰۲۰ گزارشی درباره فناوری بلاکچین منتشر کرد که به‌طور خاص بر تأثیر آن بر حقوق تجارت و الزامات قانونی تأکید داشت. کمیسیون به بررسی چگونگی تأثیر بلاکچین بر قراردادهای تجاری، نام تجاری و دیگر جنبه‌های حقوقی پرداخته و پیش‌بینی کرده که باید استانداردهایی برای اعتبار، شفافیت و مسئولیت ناشی از استفاده از بلاکچین تدوین شود. کمیسیون حقوق تجارت بین‌الملل ملل متحد، بر اهمیت شفافیت و قابلیت اعتماد در استفاده از بلاکچین تأکید می‌کند. UNCITRAL بر ضرورت پژوهش و توسعه در زمینه بلاکچین تأکید دارد تا اطمینان حاصل کند که بلاکچین قادر است به‌طور مؤثر در راستای تسهیل تجارت بین‌المللی مورد استفاده قرار گیرد.

فهرست منابع

اسماعیلی عطاآبادی، عقیل و فتحی زاده، امیرهوشنگ (۱۳۹۸، الف). جنبه های حقوقی برنامه های کاربردی قراردادهای هوشمند، اولین کنفرانس بین المللی مدیریت دانش، بلاکچین و اقتصاد، تهران.

اسماعیلی عطاآبادی، عقیل و فتحی زاده، امیرهوشنگ (۱۳۹۸، ب). روابط قراردادی هوشمند در تجارت الکترونیک: مفاهیم حقوقی مبادلات انجام شده در بلاکچین، اولین کنفرانس بین المللی مدیریت دانش، بلاکچین و اقتصاد، تهران.

آقایی طوق، مسلم و ناصر، مهدی (۱۳۹۸). سازوکار و چالش های پیاده سازی بستر بلاکچیندر توسعه دولت الکترونیکی و آثار آن بر نظام مالیاتی، فصلنامه حقوق اداری، ۶(۱۹)، ۹-۳۳.

حدادی، شهرزاد و مظفری، مصطفی (۱۴۰۱). درآمد حقوقی بر عرضه عمومی اولیه توکن های رمزنگاری شده بر بستر بلاکچین، فصلنامه پژوهش های حقوق اقتصادی و تجاری، ۱(۱)، ۱۲۵-۱۵۶.

شیرانی، مسعود و طلاکش، ملیکاسادات (۱۳۹۹). قانونگذاری بلاکچین در ایران، چین و انگلستان، تمدن حقـوقی، ۳(۷)، ۱۷۵-۱۸۵.

صادقی، محسن، مولاپناه، سارا و صفری، مائده (۱۴۰۲). کاربرد بلاکچین در حفاظت از حقـوق مالکیـت فکـری و ابعاد کاربردی آن، مجله حقوق خصوصی، ۲۰(۱)، ۳۱-۴۴.

نصیری اقدم، علی (۱۳۹۹). فناوری زنجیره بلوک، قراردادهای هوشمند و آینـده علـم حقـوق، فصـلنامه مطالعـات حقوق خصوصی، ۵۰(۳)، ۶۰۹-۶۲۵

Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2022). Transforming business using digital innovations: The application of AI, Blockchain, cloud and data analytics. Annals of Operations Research, 308, 7–39.

Bhutta, M.N., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M., Song, H.H., Alshamari, M.A., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution. Architecture and Security, 9, 61048-61073.

Charles, V., Emrouznejad, A., & Gherman, T. (2023). A critical analysis of the integration of blockchain and artificial intelligence for supply chain. Annals of Operations Research, 327 (1), 7–47.

Cohen, Alan, Travis West & Chelsea Parker, (2017), Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids, 1 GEO. L. TECH. REV.

Daley, S. (2020), "Wallets, hospitals and the Chinese military: 19 examples of blockchain cybersecurity at work" [online], Built In, published on January 7, 2020, available at: https:// builtin.com/blockchain/blockchain-cybersecurity-uses [last accessed on 13/08/2024].

Dyèvre, A. and Mc Namara, S. (2018), "blockchain: Enjeux, usages et contraintes pour la Défense", Les notes stratégiques, CEIS, septembre 2018.

Eckel, M. (2019), "How Much Did Russian Spy Agencies Rely On Bitcoin? New Hints In Leaked Recordings" [online], Radio Free Europe, published on November 28, 2019, available at: https://www.rferl.org/a/how-mch-did-russian-spy-agencies-rely-on-bitcoin-new-hints-inleaked-recordings-/30297083.html [last accessed on 12/03/2020].

Hamilton, D. (2018), "DARPA blockchain Programs" [online], Coin Central, published on October 1st, 2018, available at https://coinntral.com/darpa-blockchain-programs/, [lastaccessed on 11/09/2024].

Hebblethwaite, C. (2017), "Defence blockchain study authorised by Trump" [online], The Block, published on on December 13, 2017, available at: https://www.blockchaintechnology-ws. com/2017/12/13/defence-blockchain-study-authorised-trump/ [last accessed on 13/09/2024].

Huumo, Yli-, J., Ko, D., Choi, S., Park, S., & Smolander, K.(2016), Where is current research on blockchain technology?—A systematic review. PLoS One, 11(10), e0163477.

Marwala, T., & Xing, B. (2018). Blockchain and artificial intelligence.arXiv preprint. arXiv:1802.04451

Muhati, E., Rawat, D. B., & Sadler, B. M. (2022). A new cyber-alliance of arti-ficial intelligence, internet of things, blockchain, and edge computing. IEEE Internet of Things Magazine, 5(1), 104–107.

Muheidat, F., & Tawalbeh, L. A. (2021). Artificial intelligence and blockchain for cybersecurity applications. Artificial intelligence and blockchain for future cybersecurity applications (pp. 3–29). Springer International.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2020). Blockchain. Business & Information Systems Engineering, 59, 183-187.

Sivarethinamohan, R., Jovin, P., & Sujatha, S. (2022). Unlocking the potential of (AI-powered) blockchain technology in environment sustainability and social good. In Applied Edge AI (pp. 193–213). Auerbach Publications.

Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. (2018) “blockchain Technology Overview”, National Institute of Standards and Technology, US Department of Commerce.

Young ,Steven, (2017), Enforcing Constitutional Rights Through Computer Code, 26 CATH. U. J. L. &TECH 1