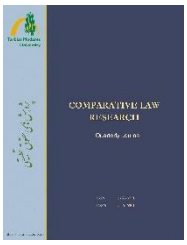


Comparative LawResearch Quarterly, Vol. 30, No.2, Summer 2026, Pp. 218-245

The Role of Blockchain Technology in the Protection of Trade Secrets and Its Admissibility in Judicial Proceedings

ARTICLE INFO
DOI: 10.48311/clr.2026.101687.0

Article Type
Research Article

Authors:
[1] Parsa Rezaee
ORCID: https://0009-0003-5197-1907
[2] Mahmoud Bagheri*
ORCID: https://0000-0002-0057-7534

Affiliation:
[1] M.A. in International Economic and Commercial Law, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran
[2] Assoiate Professor in Private Law, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran

Correspondence:
Email: mahbagheri@ut.ac.ir

Article History:
Received: 2025/08/03
Received in Revised form: 2026/01/02
Accepted: 2026/01/18

Abstract

Blockchain technology, as a secure, reliable, fast, decentralized, and peer-to-peer system, provides an appropriate platform for the storage and protection of trade secrets. Today, this technology is increasingly regarded worldwide as a novel solution for safeguarding and preserving trade secrets. With the rapid advancement of technology, the accelerated flow of information, and the growing mobility of employees between companies, traditional tools such as non-disclosure agreements or notarized undertakings no longer possess the necessary efficacy to prevent the disclosure of confidential information. This has led to an increase in the unauthorized dissemination of trade secrets, causing significant harm to their owners. Moreover, establishing ownership and meeting the legal requirements for trade secrets has become a serious challenge for rights holders, as conventional mechanisms lack the capacity to address these issues adequately. In this context, blockchain technology can offer an effective solution to these challenges. This article analyzes the capabilities of blockchain technology, assesses the feasibility of its application in the protection of trade secrets, and examines its admissibility as evidence in judicial proceedings. In doing so, it also explores the legal challenges posed by various legal systems and proposes solutions for enhancing the security of confidential information and establishing legal ownership. The findings of this study indicate that blockchain, by enhancing transparency and security, can serve as an effective tool for the protection and management of trade secrets in the digital age.

Keywords: Blockchain Technology, Intellectual Property, Exclusive Right, Trade Secrets, Admissibility

فصلنامه پژوهش‌های حقوق تطبیقی
دوره ۳۰، شماره ۲، تابستان ۱۴۰۵
صص ۲۱۸-۲۴۵
مقاله پژوهشی

Comparative Law Research Quarterly
Vol.30, No.2, Summer 2026
Pp 218-245
Original Article

نقش فناوری بلاکچین در حفاظت از اسرار تجاری و استنادپذیری آن در محاکم قضایی

پارسا رضایی[۱]، محمود باقری[۲*]

۱. کارشناسی ارشد حقوق تجاری اقتصادی بین‌المللی، گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

۲. دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

تاریخ ارسال: ۱۴۰۴/۰۵/۱۲ تاریخ بازنگری: ۱۴۰۴/۱۰/۱۲ تاریخ پذیرش: ۱۴۰۴/۱۰/۲۸

چکیده

فناوری بلاکچین به‌عنوان سامانه‌های امن، غیرمتمرکز و همتابه‌همتا، بستری مناسب برای ذخیره و صیانت از اسرار تجاری فراهم می‌آورد. با پیشرفت فناوری، شتاب انتقال اطلاعات و تحرّک کارکنان میان شرکت‌ها، ابزارهای سنتی نظیر قراردادهای عدم افشا و تعهدات محضری کارآیی لازم را برای جلوگیری از افشای اطلاعات محرمانه از دست داده‌اند. این امر نه‌تنها افشای اسرار تجاری را افزایش داده، بلکه اثبات مالکیت و شرایط حقوقی این دارایی‌ها را نیز به چالشی جدی تبدیل کرده است. این مقاله قابلیت بلاکچین را در حفاظت از اسرار تجاری و استنادپذیری آن به‌عنوان دلیل الکترونیکی در برخی محاکم بررسی می‌کند. یافته‌های پژوهش نشان می‌دهد که بلاکچین با ثبت غیرقابل‌تغییر و توزیع‌شده، راهکاری مؤثر برای مدیریت اسرار تجاری در عصر دیجیتال ارائه می‌دهد.

واژگان کلیدی: اموال فکری، حق انحصاری، فرمول سری، دانش فنی، هش

* نویسندهٔ مسئول مقاله: **Email: mahbagheri@ut.ac.ir**

۱. مقدمه

یکی از مهم‌ترین مصادیق اموال، اموال فکری بوده که در دنیای معاصر از اهمیت ویژه‌ای برخوردار است. کاربرد گسترده و فراگیری این نوع اموال، پیداش مفهوم «حقوق مالکیت فکری» را رقم زده است. حقوق مالکیت فکری، حقی است که قانون‌گذار در برابر تولید اندیشه و نوآوری‌های جدید به پدیدآورندگان اعطا می‌نماید (امامی، ۱۳۷۱: ۳). اموال فکری اَشکال متنوعی دارد و «اسرار تجاری» یکی از رایج ترین آن می‌باشد. اسرار تجاری شامل اطلاعات فنی یا شغلی، فرمول، برنامه کامپیوتری، فهرست مشتریان، دستور پخت غذا، نتایج آزمایشگاهی، کدهای دستوری و اطلاعات محرمانه قراردادها بوده که به‌دلیل محرمانه بودن، منفعت مادی و معنوی برای دارنده ایجاد می‌کند (European IP helpdesk, 2019: 29). یکی از تفاوت‌های کلیدی اسرار تجاری با سایر رژیم‌های حمایتی مالکیت فکری، در نحوه و مدت حمایت است. اسرار تجاری که شامل شرایط ثبت اختراع بوده، برای مدت ۲۰ سال حمایت می‌شود، اما صاحبان اغلب ترجیح می‌دهند اطلاعات را به‌صورت محرمانه «اسرار تجاری» نگهداری کنند (نعیمی و دیگران، ۱٤۰٤: ۱۱۷). حمایت از اسرار تجاری تا زمانی ادامه دارد که اطلاعات، افشانشده باقی بماند و تدابیر متعارف برای حفاظت از آن اتخاذ شود (باقری و گودرزی، ۱۳۸۸: ٤٤ و ٤۵). بنابراین، میان ثبت اختراع و حفظ اسرار تجاری به ماهیت اطلاعات، استراتژی شرکت و شرایط بازار بستگی دارد (Dyrhovden, 2021: 3). در اتحادیه اروپا، دستورالعمل ۹٤۳/۲۰۱٦ [1]به‌طور خاص به حمایت از دانش فنی و اطلاعات تجاری افشانشده پرداخته است. در ایالات متحده نیز قوانین متعددی از جمله قانون یکنواخت اسرار تجاری (UTSA)[2] و قانون حمایت از اسرار تجاری (DTSA)[3] وجود دارد. در حقوق ایران، قانون حمایت از مالکیت صنعتی در سال ۱٤۰۳ در فصل پنجم خود، برای اولین‌بار اسرار تجاری را

1. DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed

2. The Uniform Trade Secrets Act (UTSA) was published by the Uniform Law Commission (ULC) in 1979 and amended in 1985.

3. DEFEND TRADE SECRETS ACT OF 2016

به‌عنوان اموال فکری به رسمیت شناخت.

چالش‌های کنونی اسرار تجاری عبارت‌اند از: افشای غیرمجاز به رقبا و از دست رفتن حق انحصاری، ناتوانی روش‌های سنتی (گاوصندوق، تعهد محضری، قرارداد عدم افشا)، عدم اثبات مالکیت و تدابیر متعارف در دادگاه (Dyrhovden, 2021: 2). با توجه به چالش‌های مطروحه و نگرانی‌های موجود از جانب صاحبین اسرار تجاری، ما نیازمند یک روش جدید برای نگهداری این نوع آثار هستیم؛ به‌طوری که اولاً: این روش باید امن، سریع، قابل‌اعتماد باشد، ثانیاً: می‌بایست به‌وسیله آن بتوان مالکیت و شرایط نگهداری متعارف را در دادگاه یا محکمه در صورت بروز خسارت و طرح دعوای احتمالی ثابت کرد. پرسشی که مطرح می‌شود این است که در حال حاضر چه ابزاری می‌تواند به حل چالش‌های موجود کمک کند؟ در این چهارچوب فناوری بلاکچین به‌عنوان یک سازوکار ثبت توزیع‌شده و تغییرناپذیر، این ظرفیت را دارد که بخشی از خلأهای عملی در ثبت زمان‌مند و تمامیت داده را جبران کند. با این حال، بهره‌گیری از بلاکچین در حوزه اسرار تجاری تنها زمانی قابل دفاع است که با ماهیت محرمانگی تعارض پیدا نکند؛ به‌نحوی که به افشای مستقیم یا غیرمسقتیم اطلاعات منجر نشود.

بنابراین، مسئله اصلی پژوهش حاضر صرفاً معرفی سازوکار فنی بلاکچین نیست؛ بلکه تببین این نکته است که بلاکچین در چه الگویی می‌تواند هم‌زمان در خدمت حفاظت از اسرار تجاری قرار گیرد، به‌نحوی که خروجی آن نیز در فرآیند رسیدگی قضایی به‌عنوان دلیل الکترونیکی قابل استناد باشد. بر همین اساس، این مقالبه با رویکرد تحلیلی - توصیفی و با اتکا به منابع کتابخآن‌های و اسنادی، ابتدا جایگاه و اهمیت اسرار تجاری و همچنین عدم کارکرد روشی‌های سنتی به‌منظور حفاظت و حمایت از اسرار تجاری را تبیین می‌کند؛ سپس امکان بهره‌برداری از بلاکچین برای مدیریت و صیانت از اسرار تجاری را همراه با شناسایی محدودیت‌ها و مخاطرات (از جمله ریسک افشا، چالش‌های امنیتی و نسبت آن با امکان ثبت اختراع) را مورد بررسی قرار می‌دهد. در گام بعد، استنادپذیری داده‌های مبتنی بر بلاکچین در رسیدگی قضایی با تمرکز بر سه نظام حقوقی منتخب (ایران، ایالات متحده آمریکا و چین) تحلیل می‌شود، تا مشخص گردد این فناوری در چه چهارچوبی می‌تواند به‌عنوان دلیل

الکترونیکی پذیرفته شود. همچنین بررسی می‌شود چه پیش نیازهای فنی و نهادی برای استفاده موثر از آن وجود دارد. نوآوری مقاله حاضر در این است که علاوه‌بر بیان امکانات بلاکچین، نقطه تعادل میان حفاظت و اثبات را در حوزه اسرار تجاری توضیح داده و الگوی عملی نگهداری راز خارج از زنجیره و ثبت هش[4] را به‌عنوان مسیر کم‌ریسک‌تر پیشنهاد می‌کند.

۲. اسرار تجاری و اهمیت حمایت از آن‌ها

۲-۱) اسرار تجاری

اسرار تجاری در منابع حقوقی به‌شرح زیر تعریف شده‌اند:

در فرهنگ حقوقی آکسفورد، اسرار تجاری به فرآیندها و محصولات خاصی اطلاق می‌شود که در اختیار بنگاه تجاری بوده و افشای آن‌ها به بنگاه آسیب می‌رساند (Martin, 2003). قانون یکنواخت‌سازی اسرار تجاری آمریکا[5]، اسرار تجاری را اطلاعاتی می‌داند که شامل فرمول، الگو، فراگرد، برنامه، ابزار، شیوه، فن یا فرآیندی است با ارزش اقتصادی مستقل و عموماً ناشناخته. موافقت‌نامه تریپس[6] نیز اسرار تجاری را اطلاعاتی سری با ارزش تجاری و اقدامات متعارف حفظ محرمانگی تعریف می‌کند. ماده ۱۲۲ قانون حمایت از مالکیت صنعتی ایران مصوب سال ۱٤۰۳ نیز اسرار تجاری را هر نوع اطلاعات تجاری با ارزش اقتصادی مستقل، بالقوه یا بالفعل عموماً ناشناخته و با تدابیر متعارف حفظ محرمانگی می‌شناسد (شبیری زنجانی و دیگران، ۱٤۰٤: ۱۸۰) و به سادگی این اسرار از طرق قانونی قابل دست‌یابی یا احراز نیست. پیش از تصویب قانون ۱٤۰۳، صرفاً مواد ٦٤ و ٦٥ قانون تجارت الکترونیک به اسرار تجاری در بستر الکترونیک اشاره داشت (رضوی، ۱٤۰۱: ٤)، اما قانون جدید حمایتی جامع ارائه کرد. در دکترین حقوقی ایران نیز تعاریفی از اسرار تجاری ارائه شده است: «اسرار تجاری، دانش فنی محرمانه و گردآوری اطلاعات مفید است، که در انجام فعالیت‌های خاص و

4. Hash

5. The Uniform Trade Secrets Act (UTSA) was published by the Uniform Law Commission (ULC) in 1979 and amended in 1985.

6. AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS

یا در توسعه فنون سودمند یک هدف صنعتی ضرورت دارد» (میرحسینی، ۱۳۹۶).

از برآیند تعاریف فوق، اسرار تجاری زمانی محقق است که سه شرط، همزمان وجود داشته باشد: ۱) محرمانه بودن، به این معنا که اطلاعات باید سری باشد و افراد غیر از دارنده آن قادر به شناسایی یا دسترسی به آن نباشند؛ ۲) ارزش اقتصادی، یعنی اطلاعات باید ارزش تجاری و اقتصادی برای دارنده خود داشته باشد؛ ۳) اقدامات متعارف، بدین معنا که دارنده اسرار تجاری باید اقدامات معقول و متعارفی برای حفظ محرمانگی اطلاعات انجام داده باشد (European IP helpdesk, 2019: 29). مثال عملی: شرکت کوکاکولا فرمول نوشیدنی خود را نزد تعداد محدودی از کارکنان با تدابیر امنیتی شدید حفظ می‌کند. افشای این فرمول، مزیت رقابتی شرکت را نابود می‌سازد.

۲-۲) بررسی ابزارهای سنتی حفاظت از اسرار تجاری و چالش‌های حقوقی آن

روش‌های سنتی حفاظت از اسرار تجاری هرچند رایج بوده، اما ناتوان از جلوگیری کامل از افشا هستند و چالش‌های حقوقی متعددی ایجاد می‌کنند (عبدالحمید و اسکندرنژاد، ۱۳۹۶: ۱۲۶). مهم‌ترین این روش‌ها عبارت‌اند از:

۲-۲-۱) قرارداد عدم افشا

قرارداد عدم افشا یا (NDA)[۷]، یکی از ابزارهای قراردادی برای حفاظت از اسرار تجاری و اطلاعات محرمانه است. این قرارداد میان اشخاص حقیقی یا حقوقی منعقد می‌گرد و طرفین را ملزم به عدم افشا و استفاده محدود از اطلاعات محرمانه در چهارچوب قرارداد می‌نماید. با این حال، قراردادهای عدم افشا با چالش‌هایی مواجه‌اند، از جمله: ۱) ابهام در دامنه اطلاعات محرمانه: گاهی اطلاعات به درستی تعریف نشده، و طرف مقابل ادعا می‌کند اطلاعات افشاشده، مشمول قرارداد نبوده است؛ ۲) دشواری در اثبات نقض: اثبات اینکه چه کسی و چه زمانی و چگونه اطلاعات را افشا یا سوءاستفاده کرده، در عمل بسیار دشوار است؛ ۳) مشکلات اثبات

7. Non-Disclosure Agreement

مالکیت و زمان‌بندی: اثبات اینکه اطلاعات از ابتدا متعلق به کدام طرف بوده و چه زمانی منتقل یا افشا شده، چالش‌برانگیز است!؛ محدودیت اجرایی در نظام‌های حقوقی مختلف، اجرای قرارداد در کشورهای مختلف یا در دعاوی بین‌المللی به‌سادگی امکان‌پذیر نیست (رهبری، ۱۳۹۲: ۱٦۷).

۲-۲-۲) اخذ تعهد محضری

در این روش، فرد یا سازمان با دسترسی به اطلاعات محرمانه، در دفترخانه اسناد رسمی تعهد عدم افشا امضا می‌کند. این سند رسمی قابلیت استناد قضایی دارد و در روابط با کارکنان کلیدی و شرکای تجاری کاربرد دارد. تعهد محضری به‌دلیل رسمیت و اعتبار قانونی بالای آن، می‌تواند نقش بازدارنده‌ای در جلوگیری از افشای اسرار تجاری ایفا کند. این روش عمدتاً در روابط کاری با کارمندان کلیدی، مدیران، مشاوران و حتی شرکای تجاری مورداستفاده قرار می‌گیرد؛ به‌ویژه زمانی که اطلاعاتی با اهمیت و حساسیت بالا در میان باشد. از مزایای این روش می‌توان به قابلیت استناد آسان در محاکم قضایی و امکان پیگیری حقوقی سریع‌تر در صورت نقض تعهد اشاره کرد. با این حال، علی‌رغم ویژگی‌های خاصی که در بحث استنادپذیری آن در محاکم وجود دارد، این روش خالی از ایراد نمی‌باشد و چالش‌های عنوان- شده در بند فوق‌الذکر را در خود دارد (السان، ۱۳۸٤: ۲۸۳ و ۲۸٤).

۲-۲-۳) قرارداد عدم رقابت

این قرارداد متعهد را از فعالیت مشابه یا همکاری با رقبا برای مدت و محدوده جغرافیایی معین منع می‌کند. در صنایع دانش‌محور با اطلاعات حساس، قرارداد عدم رقابت کاربردهای زیادی دارد. برای نمونه، یک شرکت فناوری ممکن است با کارمندان کلیدی خود قرارداد عدم رقابت امضا کند تا پس از ترک شرکت، دانش فنی یا اسرار تجاری را به شرکت رقیب منتقل نکنند یا خودشان کسب‌وکاری مشابه راه‌اندازی ننمایند. در بسیاری از نظام‌های حقوقی، اعتبار و قابلیت اجرای این قراردادها بستگی به متعارف بودن شرایط آن دارد. از چالش‌های رایجی که

در رابطه با قراردادهای عدم رقابت می‌توان عنوان کرد: ۱) ابهام گستردگی بیش از حد بوده؛ لذا اگر دامنه زمانی، جغرافیایی یا موضوع قرارداد بیش از حد وسیع باشد، ممکن است دادگاه‌ها آن را غیرقابل اجرا بدانند، زیرا آزادی شغلی افراد را به‌طور ناموجه، محدود می‌کند. ۲) مشکلات اثبات نقض؛ اثبات اینکه کارمند یا شرکت سابق دقیقاً چه اطلاعاتی را منتقل یا استفاده کرده و آیا واقعاً وارد رقابت شده، در عمل دشوار است. ۳) تعارض با حقوق بنیادین؛ در برخی کشورها (مانند فرانسه یا برخی ایالت‌های آمریکا) محدودیت‌های شدید بر قراردادهای عدم رقابت وجود دارد و این قراردادها فقط در شرایط خاص و با رعایت حقوق بنیادین فرد (آزادی شغل و حرفه) معتبر هستند. ٤) عدم توازن منافع؛ اگر قرارداد به‌طور یک‌طرفه به نفع کارفرما باشد و هیچ مزایای مالی یا شغلی برای کارمند در نظر نگیرد، احتمال ابطال آن توسط دادگاه افزایش می‌یابد. ٥) تعارض با منافع عمومی؛ اگر اجرای قرارداد منجر به کاهش رقابت سالم در بازار یا محرومیت مشتریان از خدمات شود، ممکن است باطل شود. ٦) محدودیت اجرایی فرامرزی؛ اجرای این قراردادها در سطح بین‌المللی یا در کشورهای مختلف با چالش‌های حقوقی جدی روبه‌رو است و ممکن دارد در همه کشورها به رسمیت شناخته نشود (Roush, 2011: 288).

از سوی دیگر، صرف‌نظر از ایراداتی که روش‌های فوق‌الذکر دارند، تحقیقات اخیر نشان می‌دهد دعاوی افشای اسرار تجاری در ایالات متحده رو به افزایش است (Dyrhovden, 2021: 4)؛ درحالی‌که این مسئله تنها محدود به آمریکا نیست، بلکه در ایران نیز افشای اطلاعات محرمانه از طریق ابزارهای الکترونیکی به یک مشکل تبدیل شده و آراء متعددی در این زمینه در محاکم قضایی صادر شده است[8]. روش‌های سنتی (تعهد محضری، قرارداد عدم افشا و عدم رقابت) به‌دلیل ضعف در اثبات، اجرا و مقاومت در برابر فناوری‌های نوین، کارآیی کافی ندارند و از این رو نیاز به راهکار امن، غیرمتمرکز و قابل اثبات احساس می‌شود.

---

۸. شرکت گسترش خدمات تجارت الکترونیک ایرانیان در مقابل خانم م. ال. دادنامه شماره ۱۳۲۳ مورخ ۱۳۹۲/۱۱/۲٦، شعبه ۱۰٤۳ دادگاه عمومی تهران و دادنامه شماره ۹۳۰۹۹۷۰۲۲۳۹۰۰۱۷ مورخ ۱۳۹۳/۰۲/۲٤ شعبه ۳۹ دادگاه تجدیدنظر استان تهران، سامانه ملی آراء قضایی.

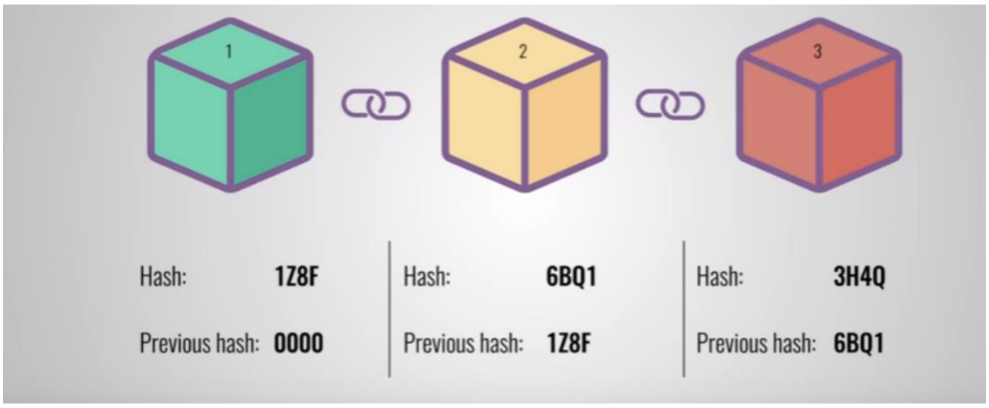
۳. نحوه کارکرد فناوری بلاکچین در حمایت از اسرار تجاری

همان‌گونه که در گفتار پیشین تبیین شد، فناوری بلاکچین ظرفیت رفع چالش‌های حفاظت از اسرار تجاری را دارا است. پرسش اصلی این است که بلاکچین چگونه این کار را انجام می‌دهد؟ و صاحبان اسرار تجاری چگونه از آن بهره می‌برند؟ در این گفتار، کارکرد عملی بلاکچین و برتری آن نسبت به روش‌های سنتی تحلیل می‌شود. در حال حاضر فناوری بلاکچین داده‌ها را به‌صورت توزیع‌شده، قابل اعتماد و غیرقابل‌تغییر ذخیره می‌کند و در حوزه حقوق کاربرد گسترده‌ای یافته است (Hauck, 2021: 18). علاوه‌بر ذخیره اسرار تجاری در بستر بلاکچین، یکی دیگر از مهم‌ترین کاربردهای این فناوری، قراردادهای هوشمند[9] می‌باشد که از طریق این تکنولوژی، تعهدات قراردادی[10] به‌وسیله نرم‌افزار از طریق سیستم برنامه‌نویسی در بستر فناوری بلاکچین بدون دخالت انسان اجراشده و تأثیرات شگرفی در اجرای تعهدات طرفین قرارداد ایجاد می‌نماید (De Filippi et al., 2021: 2-3).

۳-۱) تعریف بلاکچین

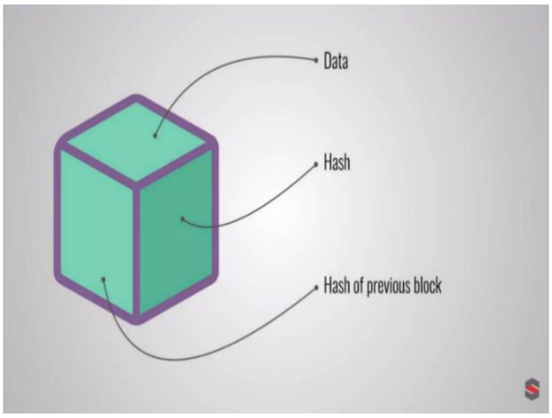
فناوری بلاکچین ابداع ساتوشی نکاموتو، دفتر کل توزیع‌شده است که اطلاعات را به‌صورت غیرمتمرکز در گره‌های جهانی ذخیره می‌کند. برخلاف سیستم‌های متمرکز، بلاکچین به‌صورت همتابه‌همتا عمل کرده و نیازی به واسطه (بانک، شرکت و دولت) ندارد (Balamurali, 2018: 9,10 &13).

9. Smart Contracts
10. Intelligence Performance of Contract



شکل ۱: ساختار بلاکچین{۱}

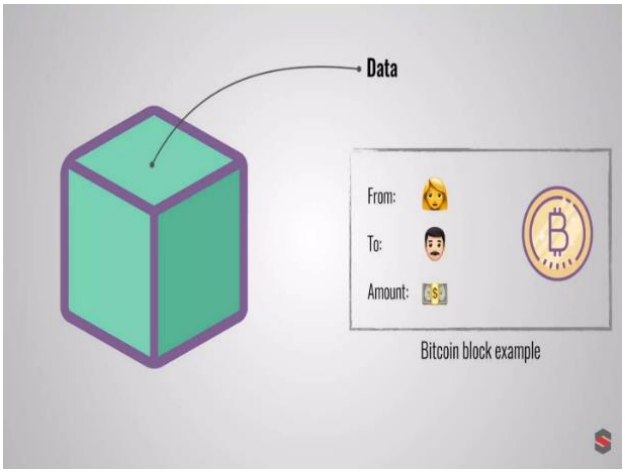
فناوری بلاکچین که ماشین اعتماد نامیده می‌شود، در قلب بسیاری از چشم‌اندازهای هیجان‌انگیز قرار دارد که هدف آن بهبود کارآیی، شفافیت و امنیت در انواع معاملات تجاری است (De Filippi et al., 2020: 2). همان‌طور که از نام بلاکچین پیدا است (زنجیره بلاک)، این فناوری متشکل از یک مجموعه یا زنجیره‌ای است که هر زنجیره در این ساختار از تعداد غیرمحدودی بلاک تشکیل می‌شود (Dyrhovden, 2021: 7) {۱}.



شکل ۲: ساختار کامل هر بلاک{۲}

هر بلاک مشتکل از سه بخش می‌باشد (Dyrhovden, 2021: 7) {۲}:

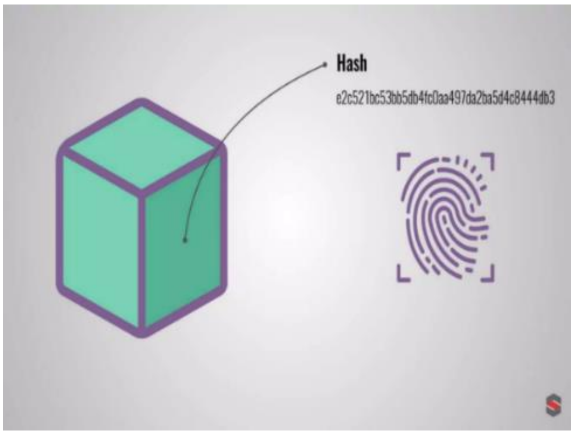
اطلاعات[11]: در بخش اطلاعات مواردی همچون ارسال‌کننده، دریافت‌کننده، تاریخ تراکنش در بستر بلاک وجود دارد یا مثلاً فرض کنید فردی از طریق قرارداد هوشمند در بستر بلاکچین منزل جدیدی خریداری کرده، در بخش اطلاعات مواردی همچون صاحب جدید منزل، صاحب قدیمی آن، تاریخ انتقال و موارد دیگر وجود دارد یا زمانی که سرّ تجاری در بلاک ذخیره می‌شود. در این بخش مواردی همچون نام دارنده آن سرّ، تاریخ ثبت و موارد دیگر در بلاک وجود دارد (Balamurali, 2018: 10-11) {۳}.



شکل ۳: اطلاعات {۳}

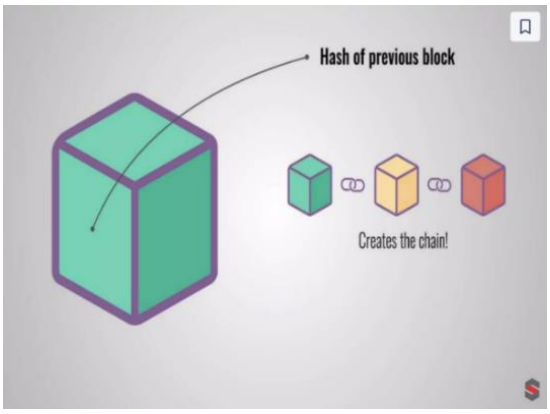
هَش[12]: هر بلوک دارای یک اثر انگشت می‌باشد که به آن هش می‌گویند. در واقع هش یک نوع تابع ریاضی است که تمامی اطلاعات موجود در بلاک را به یک رشته ثابت و کوتاه تبدیل می‌کند. این رشته معمولاً به‌صورت یک کد منحصربه‌فرد بوده و اگر اطلاعات هر بلاک تغییر کند، هش آن بلاک هم تغییر می‌کند (Balamurali, 2018: 10-11) {٤}.

11. Information
12. Hash



شکل۴: هَش {۴}

هَش قبلی[۱۳]: هر بلاک علاوه‌بر اطلاعات خود، حاوی اطلاعات بلاک قبلی خود نیز می‌باشد. بدین شکل که هر عملی که در بلاک قبلی رخ داده است، اعم از تراکنش ارزی یا انعقاد قرارداد هوشمند، به هش تبدیل شده و به بلاک بعدی منتقل می‌شود (Balamurali, 2018: 10-11) {۵}.



شکل ۵ : هش قبلی {۵}

13. Hash of Previous Block

مطابق شکل {۱}، اطلاعات هر بلاک در قالب هش، به بلاک بعدی منتقل می‌شود و مطابق شکل {۲}، در بخش هش قبلی ذخیره می‌شود. این چرخه به همین شکل در بلاک‌های بعدی هم اتفاق می‌افتد. بدین منظور که هر بلاک مجموعه از هش‌های قبلی هر بلاک را ذخیره می‌کند و با استفاده از هش بلاک‌های قبلی، هش خود را تولید می‌کند.

۳-۲) مراحل عملی استفاده از بلاکچین در ثبت اسرار تجاری

همان‌گونه که بیان شد، بلاکچین یک دفترکل توزیع‌شده و غیرقابل‌تغییر است که داده‌ها را به‌صورت زنجیره‌ای از بلوک‌ها ذخیره می‌کند. در حوزه اسرار تجاری، این فناوری زمانی کارآمد است که نه خودِ سرّ، بلکه «نمایه رمزنگاری‌شده» آن (هش) و داده‌های مربوط به مالکیت و زمان ایجاد، بر روی بلاکچین ثبت شود. فرآیند استفاده از بلاکچین برای حفاظت اسرار تجاری را می‌توان در چند گام عملی تبیین کرد:

مرحله اول - آماده‌سازی و رمزنگاری سرّ تجاری:

در گام نخست، صاحب سرّ تجاری، اطلاعات محرمانه مانند فرمول تولید، کدمنبع نرم‌افزار، فهرست مشتریان یا نتایج تحقیقاتی را در محیطی خارج از زنجیره و در یک سامانه امن نگهداری می‌کند. سپس با استفاده از الگوریتم‌های رمزنگاری، از این داده‌ها یک «هش» تولید می‌شود که در حکم اثر انگشت دیجیتال سرّ تجاری است؛ به‌گونه‌ای که با هر تغییر در محتوای اطلاعات، هش نیز تغییر خواهد کرد.

مرحله دوم - ثبت هش و داده‌های هویتی بر روی بلاکچین:

در مرحله بعد، هش تولیدشده به همراه اطلاعاتی نظیر شناسه مالک، زمان دقیق ایجاد یا ثبت، نوع سرّ تجاری و در صورت لزوم شناسه قراردادهای مرتبط (مانند قرارداد عدم افشا یا لیسانس) در یک بلاک جدید ثبت می‌شود. این ثبت بر بستر بلاکچین باعث می‌گردد که زمان و انتساب سرّ تجاری به دارنده آن، به‌صورت غیرقابل‌تغییر و در یک شبکه توزیع‌شده، ذخیره شود. در نتیجه، در صورت بروز اختلاف، صاحب سرّ می‌تواند با ارائه نسخه اصلی اطلاعات و تطبیق آن با هش ثبت‌شده، تقدم زمانی مالکیت خود را اثبات نماید.

مرحله سوم - ثبت تغییرات و استفاده‌های مجاز:

اسرار تجاری در طول زمان ممکن است توسعه یابند، به‌روزرسانی شوند یا موضوع قراردادهای مختلفی مانند لیسانس، NDA یا قرارداد عدم رقابت قرار گیرند. هر یک از این وقایع (به‌روزرسانی اطلاعات، انعقاد یا خاتمه قرارداد، اعطای مجوز استفاده به شخص ثالث) می‌تواند در قالب هش‌های جدید در بلوک‌های بعدی ثبت شود. به این ترتیب، زنجیره‌ای از سوابق ایجاد می‌شود که نشان می‌دهد دارنده سرّ، به‌طور مستمر اقدامات متعارفی برای حفظ محرمانگی انجام داده و دسترسی اشخاص ثالث را در قالب قراردادهای مشخص مدیریت کرده است.

مرحله چهارم - استفاده از سوابق بلاکچین در فرآیند دادرسی:

در صورت طرح دعوا به سبب افشای غیرمجاز یا سوءاستفاده از سرّ تجاری، صاحب سرّ می‌تواند با ارائه سوابق بلاکچین، سه امر اساسی را اثبات کند: نخست آنکه اطلاعات مورد نزاع، پیش از تاریخ ادعایی طرف مقابل، در مالکیت او بوده است؛ دوم، اطلاعات واجد شرایط محرمانگی بوده و ناشناخته برای عموم محسوب می‌شده است؛ سوم، وی اقدامات متعارف برای حفظ محرمانگی را انجام داده و این اقدامات در قالب ثبت مستمر روی بلاکچین قابل ردیابی است.

غیرمتمرکز بودن و غیرقابل‌تغییر بودن ساختار بلاکچین، ارزش اثباتی این سوابق را افزایش می‌دهد و می‌تواند نواقص روش‌های سنتی مانند اسناد کاغذی، تعهدات محضری و قراردادهای دوطرفه را تا حد زیادی برطرف سازد. با توجه به ویژگی‌های منحصر به فرد بلاکچین، دیگر صاحبان اسرار تجاری هیچ‌گونه نگرانی در رابطه با چالش‌های عنوان‌شده در مطالب پیشین ندارند. زیرا نخست: با توجه به امنیت و شفافیت بالای بلاکچین، صاحبین این نوع اموال با خیال راحت نسبت به نگهداری اسرار خود اقدام می کنند؛ دوم: از آنجایی که تمامی اطلاعات اعم از نام و نام‌خانوادگی ثبت‌کننده اطلاعات، تاریخ دقیق ثبت اطلاعات و موارد مرتبط با ذخیره‌سازی اطلاعات سرّی در بستر بلاکچین در بخش دیتا، ثبت و جای‌گذاری می‌شود، دیگر صاحبان اسرار تجاری هیچ‌گونه مشکلی در رابطه با اثبات مالکیت خود مبنی

بر این اموال ندارند؛ سوم: از آنجایی که نحو عملکرد فناوری بلاکچین به‌صورت همتابه‌همتا و همچنین غیرمتمرکز است و اطلاعات در گره‌های متفاوت و گوناگون در سراسر دنیا ثبت می‌شود، این موضوع می‌تواند یکی از بحث‌برانگیزترین چالش‌های موجود، یعنی انجام اقدامات متعارف به‌منظور حفظ و نگهداری این نوع اموال را از بین ببرد و این فناوری، هم به صاحبان اسرار تجاری و هم به محاکم، کمک می‌کند تا علی‌رغم نبود یک سیستم یکپارچه، صاحبان آن از حمایت لازم و کافی برخوردار شوند.

۳-۳) چالش‌ها، محدودیت‌ها و مخاطرات استفاده از بلاکچین در حفاظت از اسرار تجاری

با وجود مزیت‌های بلاکچین در ثبت زمان‌مند و غیرقابل‌تغییر داده‌ها، استفاده از آن در حوزه اسرار تجاری بدون توجه به ماهیت «محرمانگی»، می‌تواند به خطای تحلیلی یا حتی نقض هدف اصلی حمایت، منجر شود. از همین رو، تمایز میان «ثبتِ خودِ راز» و «ثبتِ اثر انگشت دیجیتال (هش) از سرّ» ضروری است؛ زیرا در رویکرد صحیح، سرّ تجاری روی زنجیره قرار نمی‌گیرد، بلکه تنها هشِ داده یا شاخص‌های حداقلی آن ثبت می‌شود تا امکان اثبات وجود و تقدم زمانی فراهم باشد و اصل محرمانگی خدشه‌دار نشود.

الف) آیا قرار دادن سر در زنجیره، افشا محسوب می‌شود؟

اگر داده‌ی خامِ سر (متن کامل فرمول، نقشه فنی، کدمنبع، لیست مشتریان و...) مستقیماً در بلاکچین عمومی منتشر شود، این اقدام می‌تواند در عمل به «افشا» نزدیک شود؛ چون شبکه به صورت گسترده قابل دسترسی است و برگشت‌پذیر هم نیست. راه‌حل حقوقی و فنی این است که به‌جای درج محتوا، فقط «هش» یا شناسه رمزنگاری‌شده و نیز زمان ثبت، در بلاکچین ثبت گردد و محتوای اصلی در مخزن امن خارج از زنجیره نگهداری شود.

ب) چالش‌های فنی- امنیتی (اینترنتی) و شیوه کنترل آن‌ها

مهم‌ترین ریسک عملی در استفاده از بلاکچین برای اسرار تجاری، نه خودِ ساختار بلاکچین، بلکه «مدیریت کلید خصوصی»، امنیت سامانه‌های ذخیره خارج از زنجیره، و نقاط اتصال به اینترنت (کیف پول‌ها، سرورها، ایمیل‌ها، فضای ابری) است. بنابراین، حتی اگر هش

روی زنجیره تغییرناپذیر باشد، سرقت کلید یا نفوذ به مخزن داده، می‌تواند موجب دسترسی غیرمجاز به سر شود. راهکار پیشنهادی استفاده از سیاست‌های امنیتی مانند چندامضائی، کنترل دسترسی لایه‌بندی‌شده، ثبت رویدادها و الزام به استانداردهای امنیت اطلاعات در سازمان‌ها است.

ج) مخاطره تعارض با ثبت اختراع

یکی از پرسش‌های مهم آن است که آیا ثبت داده یا هش در بلاکچین، امکان ثبت اختراع بعدی را از بین می‌برد یا خیر؟ پاسخ به نحوه اجرای سامانه، وابسته است. اگر اطلاعات افشاشونده به‌حدی باشد که «محتوای فنی» اختراع را آشکار کند، می‌تواند در ارزیابی تازگی (Novelty) مشکل ایجاد کند. اما اگر صرفاً هش ثبت شود و محتوای فنی آشکار نگردد، اصولاً ثبت اختراع بعدی با مانع ذاتی ناشی از بلاکچین مواجه نیست (البته نیازمند ارزیابی موردی است).

د) محدودیت‌های حقوقی و اثباتی در دادرسی

در فرآیند دادرسی، ثبت هش به‌تنهایی همیشه کافی نیست؛ زیرا دادگاه باید بتواند ارتباط میان هش ثبت‌شده و سند یا داده خارج از زنجیره را احراز کند و همچنین زنجیره نگهداری رعایت شده باشد. بنابراین، برای اینکه بلاکچین واقعاً کارآمد شود، علاوه‌بر ثبت هش، باید فرآیند تولید هش، نگهداری نسخه اصلی و نحوه ارائه آن به کارشناس یا دادگاه روشن و قابل ردیابی باشد.

۴. رویکرد برخی نظام‌های حقوقی نسبت به استنادپذیری فناوری بلاکچین به‌عنوان دلیل الکترونیکی

پس از تبیین کارکرد عملی بلاکچین در حمایت از اسرار تجاری، در این گفتار به این پرسش پرداخته می‌شود که آیا علی‌رغم ظرفیت‌های گسترده فناوری بلاکچین در حفظ و نگهداری اسرار تجاری، این فناوری در محاکم به‌عنوان دلیل الکترونیکی یا دیجیتال قابل استناد است یا خیر؟ به‌جای بررسی «محاکم سراسر دنیا»، تمرکز بر سه نظام حقوقی منتخب یعنی ایران، ایالات متحده آمریکا و چین است که هر یک در سطحی متفاوت، رویکرد خود را نسبت به

استنادپذیری ادله مبتنی بر بلاکچین شکل داده‌اند.

۴-۱) ادله الکترونیکی

ادله الکترونیکی، مدارک دیجیتالی تولیدشده توسط ابزارهای الکترونیکی، مانند رایانه‌ها، گوشی‌های هوشمند و شبکه‌های اینترنتی، ایجاد و ذخیره می‌شوند (السان، ۱۳۹۷: ۳۰). این نوع ادله می‌تواند شامل انواع مختلفی از داده‌ها باشد که در فرآیندهای مختلف قضایی، تجاری یا مدیریتی به‌کار می‌روند. برخی از نمونه‌های ادله الکترونیکی عبارت‌اند از: ایمیل‌ها، اسناد دیجیتال، پایگاه داده، پیام‌های متنی و غیره.

در ادبیات حقوق فناوری[14] باید بین دیجیتال و الکترونیک تفاوت قائل شد؛ الزاماً هر ادله‌ای که دیجیتال است، الکترونیکی هم قلمداد می‌شود، اما هر ادله‌ای که الکترونیکی هست لزوماً دیجیتالی نیست؛ به‌طوری که اگر از یک سیستم رمزنگاری، برای ذخیره اطلاعات استفاده شود، آن ادله، ادله دیجیتال می باشد، اما اگر برای ذخیره اطلاعات از یک سیستم رمزنگاری استفاده نشود، این نوع ادله، ادله الکترونیکی می‌باشد، مانند ایمیل یا پیامک (حبیب‌زاده، ۱۳۹۹). بنابراین، بلاکچین جزو ادله دیجیتالی محسوب می‌شود.

۴-۲) استنادپذیری بلاکچین در مراجع قضایی

مسئله‌ای که در این بخش به آن پرداخته می‌شود، این است که استنادپذیری ادله الکترونیکی در برخی محاکم دنیا به چه شکل می‌باشد؟ آیا ادله الکترونیکی همچون بلاکچین، به استناد قوانین موضوعه و رویه قضایی محاکم قابلیت استناد به‌عنوان یک ادله محکمه‌پسند به‌منظور اثبات دعوا را دارند یا خیر؟ از این رو، سیستم‌های حقوقی ایران و آمریکا و چین مورد بحث قرار می گیرد تا کم‌وکیف این موضوع مشخص شود.

14. Legal Technolegy (legal Tech)

۴-۲-۱) استنادپذیری بلاکچین در محاکم ایران

ماده ۱۲ قانون تجارت الکترونیک ایران مقرر می دارد: «اسناد و ادله اثبات دعوا ممکن است به صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی (داده‌پیام) را صرفاً به‌دلیل شکل و قالب آن رد کرد». همچنین به موجب ماده ۲ قانون تجارت الکترونیک ایران، داده‌پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. ماده ٤٧ آیین‌نامه استنادپذیری ادله الکترونیک (۱۳۹۳)، داده‌پیام را تنها منحصر به ابزارهای الکترونیکی نکرده است؛ بنابراین، هر ابزاری اعم از تلگرام، تلکس، ابزارهای نوری و دیگر ابزارهای ناشی از فناوری اطلاعات نیز دلیل الکترونیکی محسوب می‌شود. با توجه به تعریف وسیع و پویایی که قانون تجارت الکترونیک ارائه داده است، تمام ابزارهای موجود از قبیل تلگرام، ابزارهای دیجیتالی همچون فناوری بلاکچین می‌توانند منشأ ایجاد دلیل الکترونیکی باشد (لاشکی، ١٤٠٢: ۱۸۳) و بر این اساس، صاحبان اسرار تجاری به استناد مواد فوق می‌توانند فناوری بلاکچین را به‌عنوان یک دلیل الکترونیکی قانونی به‌عنوان ادله اثبات دعوای خود مطرح کنند.

۴-۲-۲) استنادپذیری بلاکچین در محاکم آمریکا

در نظام حقوقی آمریکا، پذیرش ادله مبتنی بر بلاکچین عمدتاً از مسیر «قواعد ادله و احراز اصالت» و همچنین قوانین ایالتی که به‌طور خاص به داده‌های مبتنی بر بلاکچین پرداخته‌اند، تقویت شده است. نمونه شاخص، قانون ایالت ورمونت[15] است که اشعار می‌دارد «رکورد دیجیتالِ ثبت‌شده در بلاکچین» در صورت همراه بودن با اظهارنامه کتبیِ شخص واجد صلاحیت، می‌تواند «خوداحراز (self-authenticating) تلقی شده و برای احراز اصالت، جزو اماره قانونی محسوب گردد. بر اساس همین مقرره، اماره‌هایی مانند «اصالت رکورد»، «زمان ثبت در بلاکچین» و «هویت شخص ثبت‌کننده» نیز به‌عنوان مفروضات قابل‌استناد پیش‌بینی

15. Vermont Statutes, 12 V.S.A. § 1913 (Blockchain enabling; self-authentication of blockchain records).

شده و طرف مقابل برای تضعیف آن باید دلیل متقن ارائه کند. افزون بر ورمونت، قانون ایالت آریزونا[۱۶] نیز به‌صراحت بیان می‌کند، امضا و «رکورد یا قراردادی که از طریق بلاکچین ایمن شده باشد، در حکم امضای الکترونیکی و رکورد الکترونیکی محسوب می‌گردد. لذا از حیث اثر حقوقی نمی‌توان صرفاً به‌دلیل استفاده از بلاکچین، آن را بی‌اعتبار دانست. همچنین قانون آریزونا تصریح می‌کند، شخصی که اطلاعاتی را که مالک آن است با بلاکچین ایمن می‌کند، «حقوق مالکیت یا حق استفاده» خود را نسبت به آن اطلاعات حفظ کرده است. این گزاره برای پیوند دادن بحث «مالکیت» با بحث «ثبت و اثبات» در دعوای اسرار تجاری قابل‌استناد است. در کنار این قوانین ناظر بر «ادله»، برخی ایالت‌ها مانند تگزاس[۱۷] نیز با شناسایی امکان استفاده شرکت‌ها از «سامانه‌های داده الکترونیک» شامل بلاکچین برای نگهداری سوابق و دفاتر، مسیر اتکای عملی به سوابق مبتنی بر بلاکچین را در محیط تجاری تقویت نموده‌اند.

۴-۲-۳) استنادپذیری بلاکچین در محاکم چین

یکی دیگر از کشورهای پیشگام در حوزه استنادپذیری فناوری بلاکچین، کشور چین می‌باشد. بدین منظور، اولین دادگاه اینترنتی جهان در سال ۲۰۱۷ در هانگژو چین افتتاح شد. هدف این نوع دادگاه‌ها رسیدگی به اختلافات حقوقی در بستر اینترنت می‌باشد. در همین حین، پس از افتتاح این دادگاه پرونده‌ای با موضوع نقض چاپ تکثیر آنلاین در این نوع دادگاه ها مطرح شد.[۱۸] خواهان، وب سایب متخلف و کدمنبع آن‌ها را ضبط کرده و داده‌ها را در یک پلتفرم بلاکچین آپلود کرد. این پرسش که آیا مدارک بلاکچین باید پذیرفته شود یا خیر به دادگاه عالی چین کشیده شد.[۱۹] دادگاه عالی اعلام کرد: « دادگاه‌های اینترنتی، داده‌های دیجیتالی را که

16. Arizona Revised Statutes, A.R.S. § 44-7061 (Signatures and records secured through blockchain technology; smart contracts).

17. Texas Senate Bill 1859 (2019) (recognizing “electronic data systems” including blockchain/DLT for entity recordkeeping

18. Hangzhou Huatai Yimei Culture Media Co., Ltd v Shenzhen Daotong Technology Development Co., Ltd. (Case No.: 055078 (2018) Zhe 0192 No. 81)

19. The Supreme People’s Court of The People’s Republic of China, Statement on the admissibility of blockchain evidence (2018).

به‌عنوان مدرک ارائه می‌شوند، در صورتی که از هش یا از طریق یک پلتفرم سپرده دیجیتال جمع‌آوری و ذخیره شده باشد، شناسایی و می‌توانند صحت چنین اطلاعاتی را ثابت کنند. بنابراین، دادگاه ماهیت غیرقابل‌دستکاری فناوری بلاکچین را تأیید می‌کند. این پرونده مؤید این بوده که فناوری بلاکچین به‌عنوان دلیل الکترونیکی در محاکم چین مورد پذیرش قرار گرفته است.

با توجه به رویکرد قوانین موضوعه و رویه قضایی در نظام‌های حقوقی ایران، ایالات متحده و چین، می‌توان گفت که فناوری بلاکچین در این کشورها در قالب «داده‌پیام»، «مدرک الکترونیکی» یا «داده دیجیتال غیرقابل‌دستکاری» مورد پذیرش قرار گرفته و اصولاً قابلیت استناد در محاکم را دارد. با این حال، استنادپذیری بلاکچین به‌تنهایی کافی نیست. به علت پیچیدگی‌های فنی این فناوری، رسیدگی قضایی به چنین دعاوی مستلزم وجود قضات یا مراجع تخصصی آشنا با فناوری‌های نوین و بهره‌گیری از کارشناسان خبره در حوزه ادله الکترونیکی است. این وضعیت نشان می‌دهد که برای استفاده مؤثر از بلاکچین در اثبات دعاوی مرتبط با اسرار تجاری، علاوه‌بر پذیرش قانونی، توسعه زیرساخت‌های فنی و ارتقای دانش تخصصی مراجع قضایی نیز ضرورت دارد؛ امری که در بخش نتیجه‌گیری به‌صورت پیشنهادهای تقنینی و اجرایی برای نظام حقوقی ایران مطرح می‌شود.

۵. نتیجه‌گیری و پیشنهاد

مطالعه تطبیقی سه نظام حقوقی ایران، ایالات متحده و چین نشان داد که فناوری بلاکچین، علاوه‌بر کارکرد فنی در حفظ و ثبت اسرار تجاری، به‌تدریج در سطح ادله الکترونیکی نیز در محاکم این کشورها پذیرفته شده است؛ هرچند بهره‌گیری کامل از این ظرفیت، نیازمند تکمیل چهارچوب‌های قانونی و تقویت زیرساخت‌های فنی و تخصصی است. فناوری بلاکچین در کشورهای توسعه‌یافته برای حفاظت از اسرار تجاری مورد استفاده قرار می‌گیرد. یافته‌های این مقاله نشان داد که این فناوری می‌تواند به‌عنوان ابزاری کارآمد برای مقابله با چالش‌های ناشی از افشای غیرمجاز اطلاعات محرمانه به‌کار گرفته شود. بلاکچین با ایجاد یک سیستم

ثبت غیرقابل‌تغییر و غیرمتمرکز، این امکان را فراهم می‌کند که سوابق مربوط به اسرار تجاری به شکلی شفاف، ایمن و غیرقابل‌دستکاری ثبت شوند. این ویژگی‌ها نه‌تنها اثبات مالکیت را برای صاحبان اسرار تسهیل می‌کند، بلکه از نظر حقوقی نیز به استنادپذیری این اطلاعات در مراجع قضایی کمک می‌نماید.

در کشورهای توسعه‌یافته، فناوری بلاکچین به‌عنوان جایگزینی برای روش‌های سنتی حفاظت از اسرار تجاری پذیرفته شده و نتایج مثبتی به همراه داشته است. همان‌طور که در این مقاله نشان داده شد، روش‌های متداول نظیر قراردادهای عدم افشا و تعهدات محضری، به‌دلیل ضعف در قابلیت اجرا، دشواری اثبات نقض و هزینه‌های اضافی، نتوانسته‌اند امنیت کافی را برای اشخاص تأمین کنند. در مقابل، استفاده از بلاکچین می‌تواند علاوه‌بر کاهش این هزینه‌ها، از طریق ایجاد شفافیت و افزایش قابلیت اثبات، مانع از سوءاستفاده‌های احتمالی شود.

بنابراین دستاورد اصلی پژوهش این است که بلاکچین به‌عنوان ابزار ثبت و اثبات، تنها در الگوی نگهداری سرّ به صورت ثبت هش می‌تواند با ماهیت محرمانگی اسرار تجاری سازگار باشد؛ در غیر این صورت ممکن است به افشا یا تضعیف حمایت منجر گردد. بر این اساس، پیوند میان حفاظت و استنادپذیری در این پژوهش یک پیوند ماهوی است، زیرا اگر ابزار فنی حفاظت نتواند در مرحله اختلاف و رسیدگی قضایی به کار آید، حمایت از اسرار تجاری ناقص خواهد بود. از همین رو، الگوی پیشنهادی مقاله بر «نگهداری سرّ خارج از زنجیره و ثبت هش بر زنجیره» استوار شده است.

با توجه به شرایط و مقتضیات نظام حقوقی ایران، برای تقویت حمایت از اسرار تجاری و بهره‌گیری مؤثر از فناوری بلاکچین، پیشنهادهای زیر ارائه می‌شود:

۱. تدوین و تصویب قانون جامع حمایت از اسرار تجاری:

با توجه به خلأ قانون خاص در قوانین جاریه ایران، ضروری است قانون‌گذار با الگوبرداری از استانداردهای بین‌المللی، قانونی جامع و کامل برای حمایت از اسرار تجاری تدوین نماید.

۲. پذیرش ادله مبتنی بر بلاکچین در محاکم قضایی:

لازم است در قوانین آیین دادرسی مدنی و کیفری، اسناد و سوابق ثبت‌شده در بلاکچین به‌عنوان ادله معتبر و قابل استناد در اثبات مالکیت، افشا یا سوءاستفاده از اسرار تجاری مورد پذیرش قرار گیرد.

۳. ایجاد زیر ساخت‌های فنی و سامانه‌های ملی بلاکچین:

دولت و نهادهای ذی‌ربط باید با همکاری بخش خصوصی، سامانه‌های ملی مبتنی بر بلاکچین برای ثبت و نگهداری اسرار تجاری راه‌اندازی کنند تا صاحبان کسب‌وکار بتوانند اطلاعات محرمانه خود را به‌صورت ایمن و شفاف ثبت و مدیریت نمایند.

٤. آموزش و فرهنگ‌سازی در میان فعالان اقتصادی و حقوقی:

لازم است دوره‌های آموزشی و کارگاه‌هایی برای آشنایی مدیران شرکت ها، وکلا و قضات با فناوری بلاکچین و کاربرد آن در حفاظت از اسرار تجاری برگزار شود.

۵. تدوین مقررات حمایتی ویژه برای استارتاپ‌ها و شرکت‌های دانش‌بنیان:

با توجه به نقش کلیدی این شرکت‌ها در اقتصاد دانش‌بنیان، باید حمایت‌های خاصی برای حفاظت از اسرار تجاری آن‌ها با استفاده از فناوری‌های نوین پیش‌بینی شود.

در نهایت، اتخاذ رویکردی مبتنی بر بلاکچین نه‌تنها موجب افزایش امنیت اطلاعات محرمانه و کاهش هزینه‌های شرکت‌ها خواهد شد، بلکه می‌تواند به ارتقای سطح اعتماد در فضای کسب‌وکار و توسعه اقتصادی کشور نیز کمک کند. امید است با اصلاح قوانین و ایجاد زیرساخت‌های لازم، نظام حقوقی ایران بتواند همگام با تحولات جهانی، حمایت مؤثرتری از دارایی‌های فکری و اسرار تجاری فعالان اقتصادی به عمل آورد.

۶. منابع

۶-۱) منابع فارسی

الف) کتاب‌ها

۱. امامی، نورالدین (۱۳۷۱). *حقوق مالکیت فکری* ، ج ۲ و ۳، تهران: رهنمون نشریه مدرسه عالی شهید مطهری.

۲. امامی، نورالدین (بی.تا). حقوق *مالکیت صنعتی*، تهران: نشر میزان.
۳. رهبری، ابراهیم (۱۳۹۲). حقوق *اسرار تجاری*، چاپ دوم، تهران: انتشارات سمت.
٤. کاتوزیان، ناصر (١٤٠١). *دوره مقدماتی حقوق مدنی (اموال و مالکیت)*، تهران: نشر میزان.
٥. میرحسینی، حسن (١٣٩٦). *مقدمه‌ای بر حقوق مالکیت معنوی*، تهران: نشر میزان.

ب) مقالات

٦. احمدی لاشکی، حمیدرضا، ابهری، حمید و عباس مقدری امیری (١٤٠٢). «ادله الکترونیکی اثبات دعوا در دادرسی اداری و مدنی در ایران و فقه امامیه»، *نشریه پژوهش‌های نوین حقوق اداری*، شماره ١٦، صص ١٧٩-٢٠٢. Doi: 10.22034/mral.2023.1972392.1403
۷. السان، مصطفی و محمدرضا منوچهری (۱۳۹۷). «ارزیابی اصالت ادله الکترونیکی و ارزش اثباتی آن‌ها»، *نشریه مطالعات حقوقی*، دوره ۱۰، شماره ۲، صص ۳۰ – ۵۱. DOI: 10.22099/jls.2018.28058.2765
۸. السان، مصطفی (۱۳۸٤). «حقوق اسرار تجاری در عصر فناوری اطلاعات»، *مجله حقوقی دادگستری*، دوره ٦٩، شماره ٥٠ و ٥١، صص ٢٧٣ – ٣١٢.
۹. انصاری، باقر (١٤٠١). «حمایت از اسرار تجاری در برابر افشای غیر مجاز»، *نشریه پژوهش حقوق خصوصی*، شماره ٤١، صص ٤٢ – ٨٢.
۱۰. باقری، محمود و مریم گودرزی (۱۳۸۸). «مقایسه نظام حمایتی اسرار تجاری و نظام حق اختراع»، *نشریه مطالعات حقوق خصوصی*، سال ۳۹، شماره ۱، صص ٤١ – ٦٢.
۱۱. رضوی، سید مهدی (١٤٠١). «اسرار تجاری درحقوق استارت‌آپ‌ها»، *هفتمین همایش بین‌المللی فقه، حقوق، وکالت و علوم اجتماعی*، تهران.
۱۲. شبیری زنجانی، سید حسن، دهقانی، سید احمد و رضا سلطانی (١٤٠٤). «حمایت از ایده‌ها در چهارچوب نظام حقوق اسرار تجاری»، *فصلنامه پژوهش‌های حقوق تطبیقی*، دوره ۲۹، شماره ٤، صص ۱۸۳ – ۲۲۰.
۱۳. شیاسی، ملیحه (١٤٠٣). «چالش‌های قانونی درحفاظت از اسرارتجاری در ایران»، *سیویلیکا*.
١٤. کلته، عبدالحمید و طاهر اسکندرنژاد (١٣٩٦). «بررسی حقوق اسرار تجاری در روابط قراردادی

و غیر قراردادی در حقوق ایران با نگاه تطبیقی در حقوق آمریکا»، *نشریه پژوهش در هنر و علوم انسانی*، سال ۲، شماره ۵، صص ۱۲۳ – ۱۳٤.

١٥. نعیمی، سید مرتضی و مهین سبحانی (١٤٠٤). «اثر مشترک یا انحصاری؟ حق مالکیت فکری در پارساهای دانشگاهی ایران و دستاورد های پژوهشی ناشی از آن با نگاهی تطبیقی»، *فصلنامه پژوهش‌های حقوق تطبیقی*، دوره ۲۹، شماره ٤، صص ۱۱۹ – ١٤٦.

پ) اسناد آموزشی

١٦. حبیب زاده، طاهر (۱۳۹۹). مدرسه حقوق، دوره آموزشی قراردادهای هوشمند.

قراردادهای هوشمند – (Smart Contracts) مدرسه حقوق

١٧. حبیب زاده، طاهر (۱۳۹۹). مدرسه حقوق، دوره آموزشی محورهای کلیدی قرارداد انتقال فناوری.

دوره آموزشی محورهای کلیدی قرارداد انتقال فناوری

https://schooloflaw.ir/product/%d9%85%d8%ad%d9%88%d8%b1%d9%8‌7%d8%a7%db%8c-%da%a9%d9%84%db%8c%d8%af%db%8c-%d9%82%d8%b1%d8%a7%d8%b1%d8%af%d8%a7%d8%af%d9%87%d8%a7%db%8c-%d8%a7%d9%86%d8%aa%d9%82%d8%a7%d9%84-/%d9%81%d9%86%d8%a7%d9%88

ت) آرای قضایی

١٨. شرکت با مدیریت آقای ع. در مقابل آقای م. دادنامه شماره ۹۰۰۹۹۷۰۲۳۰۶۰۰۱۷٤ مورخ۱۳۹۰/۰٦/۰۸، شعبه ۱۰۸۳ دادگاه عمومی تهران و دادنامه شماره ۹۱۰۹۹۷۰۲۲۳۸۰۱۷۱۵مورخ ۱۳۹۱/۱۲/۲۰ شعبه ۳۹ دادگاه تجدیدنظر استان تهران، سامانه ملی آرای قضایی.

١٩. شرکت گسترش خدمات تجارت الکترونیک ایرانیان در مقابل خانم م. ال. دادنامه شماره ۱۳۲۳ مورخ۱۳۹۲/۱۱/۲٦، شعبه ۱۰٤۳ دادگاه عمومی تهران و دادنامه شماره ۹۳۰۹۹۷۰۲۲۳۹۰۰۱۷مورخ ۱۳۹۳/۰۲/۲٤ شعبه ۳۹ دادگاه تجدیدنظر استان تهران، سامانه ملی آرای قضایی.

ث) قوانین

۲۰. آیین‌نامه استنادپذیری ادله الکترونیکی (۱۳۹۳)

۲۱. قانون حمایت از مالکیت صنعتی (۱۴۰۳)

۲۲. قانون تجارت الکترونیک (۱۳۸۲)

۶-۲) منابع انگلیسی

A) Books

23. Elizabet, A. Martin (2003). *Dictionary of Law*, Oxford University Press.
24. Roush. C (2011). *Show Me the Money*, Routledge, 2nd Edition.
25. Your Guide to IP in Europe (2019). European IP helpdesk, United Nations,1-31.

B) Articles

26. Aparnaa Balamurali (2018). "Blockchain Vs. The Law: Can Blockchain And Data Privacy Co-Exist?", *King's College London,* pp. 1-53. Microsoft Word - Aparnaa Balamurali Mostert_Y23437_60.docx
27. David R. Hannah (2006). "keeping trade secrets secret, MIT Sloan Management Review", https://www.researchgate.net/profile/David-Hannah-4/publication/291767953_Keeping_trade_secrets_secret/links/56cd50b908ae4d8d6496ca0e/Keeping-trade-secrets-secret.pdf
28. De Filippi, Primavera; Wray, Chris; Sileno, Giovanni (2021). "Smart contracts", *Internet Policy Review*, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, 10(2), pp.1-9. DOI: https://doi.org/10.14763/2021.2.1549
29. Dominique Guegan (2017). "Public Blockchain versus Private Blockchain", *Hal Open Science,* pp. 1-8,https://shs.hal.science/halshs-01524440v1/document
30. Dyrhovden Sindre (2021). "Blockchain and Trade Secrets: A Match Made in Heaven?", *Kings College London,* pp. 1-47. BlockchainandTradeSecretsAMatchMadeinHeaven.pdf
31. Elias.Strehle (2020). "Public Versus Private Blockchains", *Blockchain Research Lab*, Max-Brauer-Allee 46, 22765, pp. 1-8. https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf
32. Hauck, Ronny (2021). "Blockchain, Smart Contracts and Intellectual Property.Using distributed ledger technology to protect, license, and enforce intellectual property rights, Legal Issues in the Digital Age", *Research Gate*, pp. 17-41.

DOI:10.17323/2713-2749.2021.1.17.41
33. Primavera De Filippi, Morshed Mannan, Wessel Reijers (2020). "Blockchain as a confidence machine: The problem of trust & challenges of governance", *ScienceDirect*, pp. 1-14. https://doi.org/10.1016/j.techsoc.2020.101284
34. Rui Zhang, Rui Xue, and Ling Liu (2019). "Security and Privacy on Blockchain", *ACM Comput. Surv*, 52(3), Article 51.

B) Judicial Decisions
35. Hangzhou Huatai Yimei Culture Media Co., Ltd v Shenzhen Daotong Technology Development Co., Ltd. (Case No.: 055078 (2018) Zhe 0192 No. 81)
36. The Supreme People's Court of The People's Republic of China, Statement on the admissibility of blockchain evidence (2018).

C) Acts
37. AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS
38. An act relating to miscellaneous economic developments provisions H.868 (Act 157) § 1913(1) Sec. 1.1.12 (2016).
39. Arizona Revised Statutes, A.R.S. § 44-7061 (Signatures and records secured through blockchain technology; smart contracts).
40. DEFEND TRADE SECRETS ACT OF 2016.
41. DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
42. Electronic Signatures in Global and National Commerce Act(ESIGN).
43. Texas Senate Bill 1859 (2019) (recognizing "electronic data systems" including blockchain/DLT for entity recordkeeping)
44. The Economic Espionage Act of 1996.
45. The Uniform Trade Secrets Act (UTSA) was published by the Uniform Law Commission (ULC) in 1979 and amended in 1985.
46. Uniform Electronic Transactions Act(UETA).
47. Vermont Statutes, 12 V.S.A. § 1913 (Blockchain enabling; self-authentication of blockchain records).

[In Persian]:
A) Books
48. Emami, N. (1992). *Hoqooq-e Malkiyat-e Fekri*, Vol. 2 & 3. Tehran: Rahnamoon

Nashr-e Madrese-ye ‘Ali-ye Shahid Motahhari. [In Persian]
49. Emami, N. (n.d.). *Hoqooq-e Malkiyat-e San’ati*. Tehran: Nashr-e Mizan. [In Persian]
50. Katouzian, N. (2022). *Dore-ye Moghaddamati-ye Hoqooq-e Madani (Amval va Malkiyat)*. Tehran: Nashr-e Mizan. [In Persian]
51. Mirhosseini, H. (2017). *Moqaddame-i bar Hoqooq-e Malkiyat-e Ma’navi*. Tehran: Nashr-e Mizan. [In Persian]
52. Rahbari, E. (2013). *Hoqooq-e Asrar-e Tejari* (2nd ed.). Tehran: SAMT Publications. [In Persian]

B) Articles

53. Ahmadi Lashaki, H., Abhari, H., & Moghadari Amiri, A. (2023). *Adelle-ye Elektroniki-ye Esbat-e Da’va dar Daderesi-ye Edari va Madani dar Iran va Feqh-e Emamiyeh* [Electronic Evidence in Administrative and Civil Procedure in Iranian Law and Imamiyyah Jurisprudence]. *Modern Research in Administrative Law*, 16, 179–202. https://doi.org/10.22034/mral.2023.1972392.1403. [In Persian]
54. Alsan, M., & Manouchehri, M. (2018). *Arzyabi-ye Asalat-e Adelle-ye Elektroniki va Arzesh-e Esbati-ye Anha* [Authenticity Assessment and Evidentiary Value of Electronic Evidence]. *Journal of Legal Studies*, 10(2), 30–51. https://doi.org/10.22099/jls.2018.28058.2765. [In Persian]
55. Alsan, M. (2005). *Hoqooq-e Asrar-e Tejari dar Asr-e Fanavari-ye Ettela’at* [Trade Secrets Law in the Information Technology Era]. *Judicial Law Journal*, 69(50–51), 273–312. [In Persian]
56. Ansari, B. (2022). *Hemayat az Asrar-e Tejari dar Barabar-e Afsha-ye Gheyr-e Mojaz* [Protection of Trade Secrets Against Unauthorized Disclosure]. *Private Law Research*, 41, 42–82. [In Persian]
57. Bagheri, M., & Goodarzi, M. (2009). *Moghayese-ye Nezam-e Hemayati-ye Asrar-e Tejari va Nezam-e Hoqooq-e Ekhtara’* [Comparing Trade Secret Protection and Patent Systems]. *Journal of Private Law Studies*, 39(1), 41–62. [In Persian]
58. Kollateh, A., & Eskandarnezhad, T. (2017). *Barrasi-ye Hoqooq-e Asrar-e Tejari dar Ravabet-e Gharardadi va Gheyr-e Gharardadi dar Hoqooq-e Iran ba Negah-e Tatbighi bar Hoqooq-e Amrika* [Trade Secret Law in Contractual and Non-contractual Relations in Iranian Law Compared to U.S. Law]. *Journal of Research in Art and Humanities*, 2(5), 123–134. [In Persian]
59. Naeimi, S. M., & Sobhani, M. (2025). *Asar-e Moshtarak ya Enhesari? Hoqooq-e Malkiyat-e Fekri dar Parsaha-ye Daneshgahi-ye Iran va Dastavard-haye Pazhooheshi-ye Nashe az An ba Negah-e Tatbighi* [Shared or Exclusive Effect? Intellectual Property Rights in Iranian University Parks and the Resulting Research Outputs: A Comparative View]. *Faslname-ye Pazhoohesh-haye Hoquq-e Tatbighi*

(Comparative Legal Research Quarterly), 29(4). [In Persian]
60. Razavi, S. M. (2022). *Asrar-e Tejari dar Hoqooq-e Start-upha* [Trade Secrets in Start-up Law]. *The 7th International Conference on Jurisprudence, Law, Advocacy and Social Sciences*, Civilica. [In Persian]
61. Shiasi, M. (2024). *Chaleshha-ye Qanouni dar Hefazat az Asrar-e Tejari dar Iran* [Legal Challenges in Protecting Trade Secrets in Iran]. Civilica, 1–6. [In Persian]
62. Shobiri, S. H., Dehqani, S. A., & Soltani, R. (2025). *Hemayat az Ideha dar Charchoob-e Nezam-e Hoquq-e Asrar-e Tejari* [Protection of Ideas within the Framework of Trade Secrets Law]. *Faslname-ye Pazhoohesh-haye Hoquq-e Tatbighi* (Comparative Legal Research Quarterly), 29(4). [In Persian]

C) Educational Sources
63. Habibzadeh, T. (2020). *Madrese-ye Hoqooq, Dore-ye Amoozeshi-ye Gharardadha-ye Hoshmand (Smart Contracts)* [Smart Contracts Educational Course]. School of Law. [In Persian]
64. Habibzadeh, T. (2020). *Madrese-ye Hoqooq, Dore-ye Amoozeshi-ye Mahvar-haye Kelidi-ye Gharardad-e Enteghal-e Fanavari* [Key Elements of Technology Transfer Contracts]. School of Law. https://schooloflaw.ir/product/محورهای-کلیدی-قراردادهای-انتقا/. [In Persian]

D) Judicial Decisions
65. Company represented by Mr. A. v. Mr. M. (2011). Judgment No. 9009970230600174 (Branch 1083, Tehran General Court) & Judgment No. 9109970223801715 (Branch 39, Tehran Court of Appeal). *National Judicial Rulings Database*. [In Persian]
66. Gostaresh-e Khadamat-e Tejarat-e Elektronik Iranian Co. v. Ms. M. L. (2014). Judgment No. 1323 (Branch 1043, Tehran General Court) & Judgment No. 930997022390017 (Branch 39, Tehran Court of Appeal). *National Judicial Rulings Database*. [In Persian]

E) Laws
67. Ayin-nameh-ye Estenad-Paziri-ye Adelle-ye Elektroniki (2014), Article 47. [In Persian]
68. Electronic Commerce Act (2003), Articles 2, 12, 64, 65. [In Persian]
69. Qanoun-e Hemayat az Malkiyat-e San'ati (2024), Chapter 5, Articles 122–128. [In Persian]