Jurisprudence and legal studies of media Journal
VOL. 6 / Autumn 2024 and Winter 2025 / NO. 2 (Serial 12)

Invocabling Smart Contracts in Iranian Courts

Seyed Mahdi Razavi[1]
Seyed Pedram Khandani[2]

Abstract

With the development of new technologies, smart contracts have become popular among people as a new type of legal contracts, and their use may cause disputes between the parties. the smart contract is the source of disputes between the parties once disputes arise from smart contracts between parties and they refer to the law court to resolve them accordingly. Additionally, it is considered one of the most important proofs of claim. Therefore, to accredit these contracts, the parties must be aware of their nature as a rationale. However, library studies, analyzing Iran's laws and regulations, and features and mechanisms of smart contracts indicate that the contracts, as electronic evidence, are essentially electronic documents with attributes such as being inscribed, invocable, and retaining a signature; it is, therefore, conceivable to refer/submit such instruments in law court given the requirements for invocable electronic evidence, such as authenticity, accessibility, and assignability, are implicated in the contracts. Consistent with the probative value, although they are potentially closer to the concept of secure electrical reason, but such contracts are likely to be considered standard electronic evidence, deniable and dubitable, or maybe secure electronic evidence, which is likely only to be claimed for falsification.

Keywords: Blockchain, Electronic Evidence, Invocable, Smart Contract.

1- Master of Private Law, Faculty of Humanities, Islamic Azad University Branch Azadshahr, Azadshahr, iran s.mahdi.razavi77@gmail.com
2- Assistant Professor of Private Law Department, Karaj Branch, Islamic Azad University, Karaj, Iran dr.khandani@gmail.com

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۶، شماره ۲ (پیاپی ۱۲)
پاییز و زمستان ۱۴۰۳
صص: ۱۸۱-۲۰۶

امکان‌سنجی استناد به قراردادهای هوشمند در محاکم دادگستری ایران

نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۳/۵/۱۷
تاریخ پذیرش: ۱۴۰۳/۷/۱۸

سیدمهدی رضوی[۱]
سیدپدرام خندانی[۲*]

چکیده

با گسترش فناوری‌های نوین، قراردادهای هوشمند به‌عنوان نوع جدیدی از قراردادهای حقوقی در میان مردم رواج یافته است و به‌تبع استفاده از آن‌ها ممکن است سبب ایجاد اختلافاتی میان متعاقدان آن گردد. در هنگام بروز اختلافات ناشی از قراردادهای هوشمند میان طرفین آن و رجوع آن‌ها به محاکم دادگستری جهت دادخواهی، یکی از مهم‌ترین ادله اثبات دعوی، خود قرارداد منشأ اختلاف می‌باشد و اشخاص برای آنکه بتوانند به این قراردادها استناد کنند باید از ماهیت آن‌ها به‌عنوان دلیل مطلع باشند. مطالعات کتابخانه‌ای، بررسی قوانین و مقررات ایران و تحلیل ویژگی‌ها و سازوکار قراردادهای هوشمند، نشان می‌دهد این قراردادها به‌عنوان دلیل الکترونیکی، با داشتن اوصافی مانند نوشته بودن، قابلیت استناد و دارای امضا بودن ماهیتا سند الکترونیکی هستند و چون شرایط استناد به ادله الکترونیکی، مانند اصالت، قابلیت دسترسی و قابلیت انتساب موجود است امکان استناد به آن‌ها در محاکم وجود دارد و بر اساس ارزش اثباتی، هرچند به‌صورت بالقوه به مفهوم دلیل الکتریکی مطمئن نزدیک‌تر هستند؛ اما حسب مورد می‌توانند دلیل الکترونیکی عادی، قابل‌انکار و تردید باشند یا می‌توانند دلیل الکترونیکی مطمئنی باشند که صرفاً ادعای جعل نسبت به آن ممکن است.

واژه‌های کلیدی

استنادپذیری، بلاکچین، دلیل الکترونیکی، قرارداد هوشمند.

---

۱. کارشناسی ارشد حقوق خصوصی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد آزادشهر، آزادشهر، ایران s.mahdi.razavi77@gmail.com
۲. استادیار گروه حقوق خصوصی، دانشکده حقوق، دانشگاه آزاد اسلامی واحد کرج، کرج، ایران
dr.khandani@gmail.com

مقدمه

با توسعه علوم رایانه‌ای و گسترش ارتباطات و معاملات الکترونیکی، نوع جدیدی از قراردادها با نام قراردادهای هوشمند[۳] پدیدار شده‌اند. این قراردادها مبتنی بر فناوری بلاکچین[٤] می‌باشند و به علت ویژگی‌های منحصربه‌فرد خود نظیر غیرمتمرکز بودن[٥]، خوداجرایی[٦]، رمزنگاری[۷]، شفافیت و برگشت‌ناپذیر بودن[۸]، موجب تسریع در معاملات تجاری، حذف واسطه‌ها، کاهش هزینه‌ها، تسهیل معاملات بین‌المللی و... می‌شوند و به همین جهت مورد استقبال عموم قرار گرفته‌اند؛ اما به موازات ایجاد این مزایا، وجود ویژگی‌های جدید و منحصربه‌فرد این قراردادها، باعث ایجاد چالش‌ها و مشکلاتی برای طرف‌های آن می‌شود که بخش عمده این چالش‌ها مرتبط با نحوه تبدیل قصد و اراده طرفین قرارداد از زبان مرسوم (زبان انسانی) به زبان تخصصی برنامه‌نویسی است *(Nguyen, 2023, p. 490)* که سبب بروز اختلافاتی حاصل تعارض اراده‌ها با یکدیگر یا عدم تطابق آثار قرارداد با اراده متعاقدان می‌شود *(Buchwald, 2020, p. 1387)* و لازم گردد تا متعاقدان جهت رفع اختلافات، اقدام حقوقی مورد نیاز را اعمال نمایند.

آنچه که باید مورد توجه قرار گیرد، این است که قراردادهای هوشمند به مانند قراردادهای سنتی به زبان انسانی و رسم‌الخط مرسوم نگارش نمی‌شوند *(Kerikmae & Rull, 2016, p. 126)* تا به سهولت بتوان با مذاکره متعاقدان یا رجوع به داوری سنتی[۹] اقدام به

---

3. Smart Contracts

٤. بلاکچین (Blockchain) یک سربرگ دیجیتالی غیرقابل تغییر است. بلاکچین متشکل از چندین بلوک است که هر بلوک حاوی اطلاعات خاصی مانند اعتبارات و بدهی‌ها یا مالکیت دارایی است و هر بلوک توسط تعداد زیادی رایانه در یک شبکه به نام گره (Node) تأیید می‌شود و سپس به بلوک‌های تأییده شده قبلی متصل می‌شود؛ این زنجیره از بلوک‌های داده به عنوان بلاکچین شناخته می‌شود *(Raskin, 2017, p. 318)*.

5. Decentralized

6. Self-executing

۷. رمزنگاری (Encryption) عبارت است از «مبهم نمودن اطلاعات به طریقی که از دید فرد غیرمجاز پنهان شود و در عین‌حال فرد مجاز قادر به مشاهده و استفاده از اطلاعات باشد» *(فضلی، ۱۳۸۸، ص.۳۰)*.

8. Irreversible

۹. دعاوی مرتبط با بلاکچین (و نوع خاص‌تر آن، دعاوی مرتبط با قراردادهای هوشمند) قابل ارجاع به داوری سنتی (مواد ٤٥٤ تا ٥٠١ قانون آیین دادرسی مدنی) نمی‌باشند؛ زیرا حل این اختلافات از طریق داوری سنتی، به

کشف اراده واقعی و حل اختلافات نمود. برخی معتقدند قراردادهای هوشمند، دستورالعمل‌های الکترونیکی هستند که در قالب کدهای رایانه‌ای پیش‌نویسی شده‌اند تا رایانه بتواند به این وسیله مفاد قرارداد را بخواند و اجرا نماید (O'Shields, 2017, p. 179) و برخی دیگر معتقدند قرارداد هوشمند پدیده‌ای دوگانه با هر دو مؤلفه فنی و حقوقی است؛ لذا نمی‌توان این دو مؤلفه قرارداد هوشمند را مستقل از هم در نظر گرفت (Niyazova & Askarbekova, 2022, p.144).

بنا به آنچه در بررسی ماهیت قرارداد هوشمند شرح داده خواهد شد، نظر اخیر صحیح‌تر است؛ اما آنچه در این‌باره مهم است، این است که این قراردادها به زبان تخصصی[۱۰] برنامه‌نویسی می‌شوند و در مقام حل اختلاف ضروری است به متخصصان فنی و حقوقی مراجعه نمود تا بتوانند معانی مفاد قرارداد هوشمند و اثرهای حقوقی آن‌ها را مشخص کنند؛ بنابراین به نظر می‌رسد در حال‌حاضر، مطمئن‌ترین مرجع جهت حل اختلافات ناشی از قراردادهای هوشمند رجوع به محاکم دادگستری، بر حسب صلاحیت آن‌ها در رسیدگی

علت ویژگی‌های خاص این دعاوی، بسیار زمان‌بر، پرهزینه و پیچیده است (Chevalier, 2021, p. 559). در مقابل دعاوی مرتبط با بلاکچین قابل ارجاع به نوع خاصی داوری غیرمتمرکز هستند که سازوکارهای منحصربه‌فردی دارد و این سازوکارها حتی در نخستین تعاریف و ایده‌های نیک سابو (خالق بلاکچین بیت‌کوین) از بلاکچین بیت‌کوین (Bitcoin) قابل مشاهده است (Ortolani, 2019, p. 34)؛ زیرا بلاکچین، بستری غیرمتمرکز است و باید شیوه حل اختلاف در آن نیز شیوه‌ای غیرمتمرکز و در عین‌حال تضمین‌کننده حقوق کاربران شبکه بلاکچین باشد؛ اما از آنجا که هنوز اطلاعات کمی درباره نحوه عملی کردن این سازوکارها وجود دارد (Ortolani, 2019, p. 435) و اجرایی نمودن آن با چالش‌هایی مانند فقدان مرجع داوری غیرمتمرکز، عدم وجود تمایل طرفین اختلاف جهت سازش با این شیوه و عدم پذیرش قانونی این نوع داوری، روبه‌روست (Ortolani, 2019, p. 568). تا زمان ایجاد سازوکاری مشخص جهت استفاده از این نوع داوری غیرمتمرکز برای حل اختلافات مرتبط با بلاکچین و نیز به‌رسمیت شناختن ارجاع به این نوع داوری به موجب قانون، لازم است تا کاربران بلاکچین از طریق محاکم دادگستری نسبت به حل اختلافات خود اقدام نمایند (Ortolani, 2019, p. 436). جهت مطالعه تفصیلی درباره سازوکار داوری غیرمتمرکز در دعاوی مرتبط با بلاکچین رجوع کنید به:

Chevalier, Maxime. (2021). From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order. *Journal of International Dispute Settlement*, 12(4), 558–584.

۱۰. قراردادهای هوشمند غالباً به زبان سالیدیتی (Solidity) برنامه‌نویسی می‌شوند. سالیدیتی، یک زبان برنامه‌نویسی شیءگرا و سطح بالا است که به‌طور خاص برای ایجاد و اجرای قراردادهای هوشمند در سکوهای مختلف مبتنی بر بلاک‌چین توسعه یافته است (Pluralsight, 2022).

به موضوع دعوا می‌باشد *(Kerikmae & Rull, 2016, p.137)* تا علاوه بر رسیدگی تخصصی به موضوع دعوا با ارجاع به کارشناسی یا سایر طرق پیش‌بینی شده در قوانین و مقررات جهت کشف حقیقت[۱۱]، بتوانند به قابل اعتمادترین روش قصد و اراده متعاقدان درخصوص قرارداد را کشف و حکم موضوع را تعیین نمایند و همچنین تا صدور حکم با أخذ تأمین متناسب از تضرر بیشتر متعاقدان جلوگیری کنند.

در مقام رسیدگی به اختلافات طرفین قراردادهای هوشمند، متعاقدان باید جهت اثبات حقوق، تعهدات و تکالیف خود به ادله مختلف استناد نمایند و یکی از مهم‌ترین ادله در اختلافات مورد بحث، خود قرارداد هوشمند می‌باشد. به هنگام استناد به دلایل مختلف در فرایند رسیدگی قضایی، ضروری است تا اصحاب دعوا و وکلای آن‌ها از ماهیت و نوع دلایل مورد استناد مطلع باشند تا بتوانند مطابق با قوانین و مقررات حاکم بر آن‌ها آیین ارائه و استناد به این دلایل، ارزش اثباتی و شیوه دفاع در برابر آن‌ها را به درستی تشخیص دهند که بتوانند به این وسیله اثبات حق نمایند. حال پرسش اصلی، این است که آیا این قراردادها به لحاظ تفاوتشان با قراردادهای الکترونیکی از منظر حقوق تجارت الکترونیکی، دلیل الکترونیکی محسوب می‌شوند و امکان استناد به آن‌ها در محاکم دادگستری وجود دارد؟ فرضیات نیز چنین است که قراردادهای هوشمند از نظر حقوق تجارت الکترونیکی، نوعی سند الکترونیکی هستند و به‌صورت بالقوه امکان استناد به آن‌ها در محاکم دادگستری وجود دارد. در ادامه با بررسی ماهیت و ویژگی‌های قراردادهای هوشمند و انطباق و تحلیل آن‌ها با تعاریف و ویژگی‌های ادله الکترونیکی و ارزش اثباتی در قانون و دکترین حقوقی، به تبیین موارد بیان شده خواهیم پرداخت.

۱. قراردادهای هوشمند

بحث درباره قراردادهای هوشمند نیازمند شناخت ماهیت و ویژگی‌های منحصربه‌فرد آن‌هاست. در ادامه به تبیین ماهیت قراردادهای هوشمند و مهم‌ترین ویژگی‌های این قراردادها خواهیم پرداخت.

---

۱۱. ماده ۱۹۹ قانون آیین دادرسی مدنی

۱-۱. ماهیت قراردادهای هوشمند

پژوهشگران حوزه سایبر تعاریف گوناگونی از این قراردادها ارائه نموده‌اند؛ اما به‌علت بدیع بودن این قراردادها و ناشناخته بودن ابعاد مختلف آن‌ها نمی‌توان تعریف جامعی رائه کرد. شاید بتوان بهترین تعریف در حال‌حاضر از قراردادهای هوشمند را چنین دانست: «قراردادهای هوشمند، کدهای ذخیره شده در بلاکچین هستند که مبین توافق طرفین قرارداد بر مفاد قرارداد بوده و پس از تحقق شروط قراردادی مفاد آن را به اجرا می‌گذارند» *(LukasK, 2017)*. ازآنجاکه قراردادهای هوشمند در بستری رمزنگاری شده منعقد می‌شوند[۱۲]، درنتیجه برای اینکه بتوان توافقات متعاقدان را در قالب قرارداد هوشمند منعقد نمود؛ لذا قرارداد باید در قالب زبان برنامه‌نویسی تخصصی مربوطه کدنویسی شود و برنامه‌نویس قراردادهای هوشمند علاوه بر تسلط کافی بر علم برنامه‌نویسی، باید یا با اثر حقوقی کدهای نوشته شده، آشنایی دقیق داشته باشد یا اینکه تحت نظارت یک حقوق‌دانان آشنا با فناوری قراردادهای هوشمند، کدنویسی نماید و به نحوی کدهای قرارداد را برنامه‌نویسی کند که اثر آن مطابق با قصد طرفین قرارداد باشد، چرا که اگر قرارداد هوشمند فاقد اثر حقوقی مدنظر طرفین آن باشد، نه‌تنها مطلوب ایشان نیست بلکه ممکن است سبب ورود ضرر به آن‌ها نیز گردد.

به‌منظور اجرای خودکار[۱۳] قراردادهای هوشمند که پس از انعقاد آن مطرح می‌شود، نیاز به فناوری‌ای است که قادر به انجام این فرایند باشد *(Kerikmae & Rull, 2016, p. 126)*. این فناوری در قراردادهای هوشمند مبتنی بر بلاکچین، با بازخوانی مفاد قرارداد توسط هوش مصنوعی[۱۴] تأمین می‌گردد و در صورت مطابقت مفاد قرارداد هوشمند با دستورالعمل‌های داده شده به هوش مصنوعی به‌صورت خودکار و مطابق با الگوریتم، خود به خود اجرا می‌شود *(Raskin, 2017, p. 306)*. بنا به آنچه بیان شد، قراردادهای هوشمند را می‌توان نسل جدید قراردادهای

---

۱۲. جهت مطالعه تفصیلی پیرامون سازوکار انعقاد قراردادهای هوشمند، رجوع کنید به:
ناصر، مهدی (۱۳۹۷). قراردادهای هوشمند (مطالعه تطبیقی حقوق ایران و آمریکا). تهران: مجد، صص.۱٤٥-۱۸۹.

13. Automaticity
14. Artificial Intelligence

الکترونیکی دانست[۱۵] *(Kerikmae & Rull, 2016, p. 136)* که دارای ویژگی‌های جدید و منحصربه‌فرد است. این سازوکار با تعریف مورد قبول در دکترین حقوقی از عقد[۱۶] مطابقت دارد و قراردادهای هوشمند نیز جهت انعقاد نیازمند ایجاب و قبول توسط حداقل دو اراده در بستر بلاکچین هستند *(Bohme et al, 2015, p. 214)*. همچنین با توجه به اینکه متعاقدان برای انعقاد قراردادهای هوشمند نیازمند برخورداری از امضائات دیجیتالی[۱۷] می‌باشند، اشخاصی که تحت چنین فرایندی مبادرت به انعقاد قراردادهای هوشمند می‌کنند، باید دارای تمامی شرایط مذکور از جمله صحت قصد و اهلیت بوده و در صورت فقدان یا مخدوش شدن هر یک از مقتضیات بیان شده، مجوز آن‌ها (کلید خصوصی تخصیص داده شده) باطل می‌شود (ناصر، ۱۳۹۷، ص.۱۲۵). همچنین در صورتی‌که این قراردادها از نظر قانونی و فنی صحیح منعقد شوند مفاد به‌صورت خودکار اجرا شده و اثر حقوقی ایجاد می‌کنند *(O'Shields, 2017, p. 190)*؛ بنابراین باید شرایط اساسی صحت قراردادها را دارا باشند[۱۸] *(Chevalier, 2021, p. 566)* و کلیه حقوق، قوانین

---

۱۵. نباید به اشتباه چنین پنداشت که قراردادهای هوشمند دقیقاً همان قرارداد الکترونیکی می‌باشند چرا که تفاوت‌های زیادی میان آن‌ها وجود دارد و صرف استفاده از سازوکارهای الکترونیکی نباید موجب یکی پنداشتن آن‌ها شود *(Nguyen, 2023, p. 490)*. بررسی تفاوت‌های قراردادهای هوشمند و قرارداد الکترونیکی، بحثی مفصل و خارج از حوصله این نوشتار است؛ اما اجمالاً می‌توان بیان داشت علاوه بر تفاوت در سازوکار انعقاد این قراردادها، کلیه ویژگی‌های قراردادهای هوشمند که در ادامه بررسی می‌شود صرفاً مختص به این نوع قراردادها بوده و در قراردادهای الکترونیکی وجود ندارد. جهت مطالعه تفصیلی درباره وجوه افتراق قراردادهای هوشمند و قراردادهای الکترونیکی رجوع کنید به:

Sapkota, Shrisha. (2022). The Difference Between E-contracts and Smart Contracts and How These Can Help the Legal Tech. https://goodlawsoftware.co.uk/law/the-difference-between-e-contracts-and-smart-contracts-and-how-these-can-help-the-legal-tech.

۱۶. «عقد، توافق دو یا چند اراده است که به منظور ایجاد آثار حقوقی انجام می‌شود» (کاتوزیان، ۱۴۰۱ب، ص.۲۱).

۱۷. امضائات دیجیتال (Digital Signatures) محصول علم رمزنگاری است. از نظر ریاضی فنون مشخصی برای ایجاد آن وجود دارد. در فرایند معمول امضا شخص امضاکننده از کلید خصوصی (Private Key) یا همان الگوریتم تبدیل‌کننده پیام به یک متن بی‌معنا (رمز) استفاده می‌کند. درحالی‌که یک کلید عمومی (Public Key) وجود دارد که از طریق آن، حسب مورد شخص ذینفع یا هر شخصی می‌تواند برای رمزگشایی امضا استفاده کند *(السان، ۱۴۰۰، ص.۱۴۱)*.

۱۸. «برای تشکیل قرارداد – اعم از الکترونیکی و غیره – وجود شرایط اساسی صحت معامله که در ماده ۱۹۰ به بعد قانون مدنی مذکور است، ضرورت دارد، دلیل این امر تبعیت قراردادهای الکترونیکی از قواعد

و مقررات مرتبط با قراردادها، مانند قوانین و مقررات مرتبط با قواعد عمومی قراردادها، عقود معین و قراردادهای الکترونیکی، شامل قراردادهای هوشمند نیز می‌گردد و رعایت این مقررات در انعقاد و اجرای آن‌ها ضروری است.

۱-۲. ویژگی‌های قراردادهای هوشمند

در این گفتار، به بررسی چند مورد از ویژگی‌های قراردادهای هوشمند که به تناسب مبحث این نوشتار، دارای اهمیت هستند پرداخته می‌شود تا با آن‌ها شناخت حاصل شود.

۱-۲-۱. رمزنگاری

قراردادهای هوشمند به مانند نسل‌های پیشین قراردادهای الکترونیکی از طریق کدهای الکترونیکی توسعه‌یافته و تشکیل می‌شوند، با این تفاوت که کدهای قراردادهای هوشمند با استفاده از کلید عمومی و کلید خصوصی[۱۹] به‌صورت رمزنگاری شده برنامه‌نویسی می‌شوند *(Kerikmae & Rull, 2016, p. 62)*. این امر سبب می‌شود تا برای درک مفاد قرارداد هوشمند راهی جز رمزگشایی اطلاعات موجود در بلاکچین وجود نداشته باشد و همین موضوع باعث شده هوش مصنوعی‌ای که با مجوز قانونی و فنی جهت اجرای مفاد قرارداد هوشمند استفاده می‌گردد پیشرفته‌ترین هوش مصنوعی حال حاضر، به نام سیستم خبره[۲۰] باشد *(ناصر، ۱۳۹۷، ص.۶۸)* چرا که برای اجرای این کدهای رمزنگاری شده و درک اراده متعاقدان دقت و قدرت استنتاج بالایی لازم است؛ بنابراین رمزنگاری کردن اطلاعات برای

عمومی قراردادهاست» *(رضایی، ۱۳۹۳، ص.۲۸)*.

۱۹. در رمزنگاری، کلید عمومی یک مقدار عددی بزرگ است که برای رمزگذاری داده‌ها استفاده می‌شود و می‌توان آن را توسط یک برنامه نرم‌افزاری تولید کرد؛ اما بیشتر اوقات توسط یک مرجع معتمد و تعیین شده ارائه می‌شود و از طریق یک منبع یا دستورالعمل در دسترس عموم در دسترس همه قرار می‌گیرد. کلید عمومی برای رمزگذاری پیام یا بررسی مشروعیت امضای دیجیتال استفاده می‌شود و با یک کلید خصوصی مرتبط همراه است که فقط برای صاحب آن شناخته شده است. کلیدهای خصوصی برای رمزگشایی پیام‌هایی که با کلید عمومی مربوطه ایجاد شده‌اند یا برای ایجاد امضا استفاده می‌شود. به عبارت‌دیگر، یک کلید عمومی داده‌ها را از استفاده غیرمجاز ایمن نگه می‌دارد، درحالی‌که یک کلید خصوصی برای باز کردن قانونی آن اطلاعات استفاده می‌شود *(Tech Target, 2021)*.

20. Expert System

حفاظت از حریم خصوصی کاربران و اطمینان از اعتبار مبادلات[۲۱] ضرورت دارد. با استفاده از رمزنگاری، تنها اشخاصی به اطلاعات حساس متعاقدان قرارداد هوشمند دسترسی دارند که مجوزهای لازم را در اختیار داشته باشند و این امر موجب افزایش ایمنی اطلاعات و اعتماد متعاقدان قرارداد هوشمند می‌شود.

مهم‌ترین اثر رمزنگاری، غیرقابل هک‌شدن اطلاعات است. از این‌رو برای اطمینان از صحت مبادلاتی که در بلاکچین انجام می‌شود، رمزنگاری اطلاعات بسیار حائز اهمیت است. در بلاکچین، هر بلوک دارای سه بخش داده[۲۲] ذخیره شده، هش بلوک[۲۳] و پیش هش بلوک[۲۴] است. هر هش بلوک برای بلوک مربوطه منحصربه‌فرد بوده و دربردارنده مشخصات دقیق و محتویات درون آن است که با فرایند رمزنگاری ایجاد شده است. هرگونه تغییر یا خدشه در یک بلوک منجر به تغییر هش بلوک آن می‌گردد چرا که تغییرات ایجاد شده سبب تغییر داده‌های بلوک و بی اعتباری هش بلوک می‌شود. پیش هش بلوک نیز به‌عنوان کدی کاربرد دارد که ارتباط میان بلوک‌های هر زنجیره بلوکی را برقرار می‌نماید. پیش هش بلوک به‌نوعی نماینده هش بلوک پیشین است که ارتباط میان بلوک‌های متصل به‌وسیله زنجیره بلوکی را فراهم می‌کند. در صورت تغییر یک هش بلوک در هر بلوک، بلوک مزبور تغییر کرده و هش بلوک آن با سایر هش بلوک‌ها تقارن خود را از دست می‌دهد و به این‌ترتیب می‌توان خرابی سیستم را به‌سادگی تشخیص داد *(ناصر، ۱۳۹۷، ص.۶۰)*. چنین سازوکاری امکان هک سیستم در اثر حملات سایبری را به حداقل می‌رساند *(Suvitha & Subha, 2021, p. 1536)*؛ زیرا به‌علت وجود فرایند رمزنگاری اطلاعات ذخیره شده اولاً، هکر نمی‌تواند از محل اصلی اطلاعات مدنظر خود در میان بلوک‌های بلاکچین مطلع شود و ثانیاً، بر فرض اطلاع یافتن از محل وجود اطلاعات، هرگونه دسترسی و تغییر اطلاعات منجر به تغییر هش بلوک گردیده و دسترسی وی به زنجیره بلوک‌ها قطع می‌شود. خود این امر در کنار ویژگی غیرمتمرکز بودن بلاکچین، سبب می‌شود تا سطح اعتماد بین متعاقدان قرارداد هوشمند افزایش یابد؛ زیرا اولاً، مفاد قرارداد به‌وسیله کدهای رمزنگاری شده و بدون

21. Transactions
22. Data
23. Hash Block
24. Previous Hash Block

دخالت شخص ثالث یا قدرت آمره مرکزی اجرا می‌گردد (Werbach, 2018, p. 495) و ثانیاً، اطمینان متعاقدان از تغییر نیافتن یا حذف نشدن کدهای دربردارنده مفاد قرارداد، این امنیت‌خاطر را در آن‌ها ایجاد می‌سازد که توافقاتشان به‌صورت دقیق اجرا می‌شود و پس از انعقاد قرارداد، احتمال دستکاری توافقات بسیار کم است.

۱-۲-۲. برگشت‌ناپذیر بودن

اجرای تمامی مفاد قرارداد هوشمند به‌صورت یک مبادله رمزنگاری شده در هش‌های بلوک‌های بلاکچین ذخیره می‌شود و پس از تکمیل و ثبت مبادلات، غیرقابل تغییر و برگشت‌ناپذیر می‌شوند (Rasure, 2024). این ویژگی اولاً ناشی از غیرمتمرکز بودن این قراردادها (Raskin, 2017, p. 318) و ثانیاً متأثر از ویژگی تغییرناپذیری[۲۵] این قراردادهاست. همان‌طور که پیش‌تر بیان شد، کدهای قرارداد هوشمند به‌علت سازوکار ویژه آن غیرقابل هک کردن می‌باشند، همچنین بنا به فرایند اثبات کار[۲۶] امکان تغییر مفاد قرارداد هوشمند به‌صورت یک‌جانبه میسر نیست و تنها در صورتی مبادلات قرارداد هوشمند تغییر می‌یابند که به‌موجب این فرایند تأیید شوند؛ بنابراین پس از نهایی شدن مبادلات قرارداد مزبور، امکان تغییر یا بازگشت یک‌جانبه آن مبادلات به حالت قبل، وجود نخواهد داشت و مبادلات انجام شده به همان شکل در شبکه بلاکچین به ثبت می‌رسد.

۱-۲-۳. قابلیت پیگیری مبادلات

قراردادهای هوشمند مبتنی بر بلاکچین هستند و بلاکچین یک دفتر کل توزیع شده[۲۷]

---

25. Immutability

۲۶. در فرایند اثبات کار (Proof of Work) مبادلات انجام یافته میان دو یا چند شخص در صورتی نهایی و ثبت می‌شوند که مفاد آن‌ها توسط همه طرفین آن مبادله مورد تأیید واقع گردد. در این‌صورت مبادله انجام شده قابلیت بررسی و ذخیره در هر بلوک را در قالب یک کد خواهد داشت (Demeyer, 2018, p. 16).

۲۷ فناوری دفتر کل توزیع شده (Distributed ledger technology) یک سیستم دیجیتال برای ثبت مبادلات دارایی‌ها است که در آن مبادلات و جزئیات آن‌ها در چندین مکان به‌طور همزمان ثبت می‌شود. بر خلاف پایگاه داده‌های سنتی، دفتر کل توزیع شده هیچ ذخیره مرکزی داده یا عملکرد مدیریتی ندارند. به‌طور خاص به زیرساخت‌ها و دستورالعمل‌های فناوری اشاره دارد که امکان دسترسی، اعتبارسنجی و به‌روزرسانی

می‌باشد که کلیه مبادلات به‌طور عمومی و شفاف در آن ثبت می‌شود؛ البته ثبت عمومی مبادلات به‌معنی افشای اطلاعات متعاقدان قرارداد هوشمند برای اشخاص ثالث نیست بلکه بلاکچین به‌گونه‌ای طراحی شده است که متعاقدان ناشناس باقی بمانند *(O'Shields, 2017, p. 180)* و اشخاص ثالث از جزئیات مبادلات آگاه نشوند مگر آنکه دارای مجوزهای لازم باشند؛ ثبت عمومی اطلاعات و مبادلات در بلاکچین به این‌ترتیب است که متعاقدان می‌توانند ناشناس باقی بمانند و صرفاً نام مستعار آن‌ها نمایش داده شود *(Chevalier, 2021, p. 563)* ولی تاریخچه مبادلات آن‌ها از طریق تجزیه و تحلیل بلاکچین قابل پیگیری است *(Rosic, 2023)*. به این‌صورت که می‌توان با داشتن شناسه مبادله[۲۸] (شناسه تراکنش) در بستر بلاکچین و جستجوی آن از طریق جستجوگر[۲۹] مختص به آن بلاکچین، اطلاعاتی نظیر کیف پول[۳۰]های مرتبط با مبادله و نشانی[۳۱]های مبدأ و مقصد، زمان انجام مبادله و مقدار رمزارز منتقل‌شده را مشاهده نمود؛ به‌عنوان‌مثال با داشتن شناسه یک مبادله در بلاکچین بیت‌کوین می‌توان با مراجعه به تارنمای Blockchain.com و وارد نمودن شناسه در قسمت جستجوگر، اطلاعات کلی پیرامون آن مبادله در بلاکچین بیت‌کوین را مشاهده و رهگیری نمود و حتی با نمایش شناسه مبادلات بعد از این مبادله، امکان رهگیری آن مبادلات نیز از همین طریق

همزمان سوابق را که دفتر کل توزیع‌شده را مشخص می‌کنند، می‌سازد که بر روی یک شبکه رایانه‌ای پراکنده در چندین نهاد، مکان یا گره کار می‌کند. در یک دفتر کل توزیع شده، هر گره هر مورد را پردازش و تأیید می‌کند و درنهایت آن مورد را ثبت می‌کند و در مورد صحت آن اجماع ایجاد می‌شود. دفتر کل توزیع شده را می‌توان برای ثبت داده‌های ثابت مانند رجیستری و داده‌های پویا مانند مبادلات مالی استفاده کرد. بلاکچین نمونه‌ای شناخته شده از فناوری دفتر کل توزیع شده است *(Barney & Troy & Pratt, 2023)*.

۲۸ شناسه مبادله (Transaction ID یا به اختصار TXID) رشته‌ای از کاراکترهای متشکل از اعداد و حروف است که باعث تمایز و شناسایی هر مبادله تأیید شده در شبکه بلاکچین است و هنگامی که یک مبادله در شبکه بلاکچین آغاز می‌شود، آن مبادله، بلافاصله یک شناسه مبادله ایجاد می‌کند که ردیابی و شناسایی آن را در بلاکچین میسر می‌سازد (Ledger Academy, 2024)؛ به‌عنوان‌مثال، عبارت زیر، اولین شناسه مبادله ثبت شده در شبکه بلاکچین بیت‌کوین می‌باشد:

0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098

29. Explorer
30. Wallet
31. Address

میسر است؛ البته که این مورد تمثیلی است و فقط مختص به بلاکچین بیت‌کوین نیست و اغلب شبکه‌های بلاکچین[۳۲] دارای چنین خصوصیتی می‌باشند.

۴-۲-۱. محرمانه بودن داده‌پیام‌های ردوبدل‌شده[۳۳]

داده‌پیام‌های تبادل‌شده میان متعاقدان فقط تحت نظارت هوش مصنوعی و مرجع صلاحیت‌دار منتقل گردیده و هیچ شخص دیگری امکان دستیابی به داده‌پیام‌های تبادل شده را نخواهد داشت *(Kerikmae & Rull, 2016, p. 62)*. در بسترهای غیرمتمرکز به جهت برخورداری این بسترها از فرایند رمزنگاری داده‌ها امکان دسترسی به داده‌پیام‌ها از طریق حملات سایبری یا استفاده از بدافزارها تقریباً ناممکن است. چنین خصیصه‌ای تحت سازوکارهای شناسایی[۳۴]، تأیید اصالت اصل‌ساز[۳۵]، عدم رد داده‌پیام[۳۶] و تمامیت[۳۷]، قابلیت اجرایی در قرارداد هوشمند می‌یابد. باید توجه نمود قراردادهای هوشمند بستری شفاف هستند *(O'Shields, 2017, p. 180)* و همان‌طور که در گفتار قبل بیان شد مبادلات صورت گرفته در آن‌ها قابل مشاهده و رهگیری است ولی آنچه در این قراردادها محرمانه باقی می‌ماند مفاد مورد توافق متعاقدان قرارداد است که فقط توسط کلید عمومی و کلید خصوصی می‌توان به جزئیات آن دسترسی داشت.

---

۳۲. برخی از شبکه‌های بلاکچین مانند بلاکچین Zcash سوابق مبادلات را ذخیره نمی‌کنند و اطلاعات پرداخت را برای اهداف رعایت حریم خصوصی حفظ نمی‌کنند، درنتیجه قابلیت رهگیری مبادلات به‌وسیله شناسه مبادله را ندارند.

33. Confidentiality

34. Identification

۳۵. (Authentication) استفاده از کلید خصوصی جهت امضای قراردادهای هوشمند به‌منزله تأیید اصالت فردی است که نسبت به انجام مذاکرات قراردادی اقدام می‌نماید. این فرد با امضای قرارداد، مفاد قرارداد را مورد تأیید قرار داده و خود را ملزم به اجرا و پذیرش حقوق و تکالیف ناشی از قرارداد می‌داند *(ناصر، ۱۳۹۷، ص.۱۱۰)*.

36. Nonrepudiation

37. Integrity

۲. قرارداد هوشمند به‌عنوان دلیل در دادرسی

جهت پاسخ به این پرسش که آیا امکان استناد به قرارداد هوشمند در محاکم دادگستری به‌عنوان دلیل ممکن است یا خیر، لازم است ابتدا تعیین نماییم قرارداد هوشمند ماهیتاً دلیل سنتی است یا الکترونیکی، و پس از آن بررسی نماییم که این قراردادها بر اساس ویژگی‌هایشان جزء کدام نوع از دلایلی است که قانون استناد به آن‌ها را در محاکم دادگستری معتبر دانسته است.

۲-۱. قرارداد هوشمند به‌عنوان دلیل الکترونیکی

اصحاب دعوا، جهت اثبات ادعا یا دفاع در برابر ادعای مطرح شده طرف مقابل، به مواردی استناد می‌نمایند، که به آن‌ها «دلیل» گفته می‌شود[۳۸]. ادله اثبات دعوا از یک حیث به دو نوع دلایل سنتی و دلایل الکترونیکی دسته‌بندی می‌شوند[۳۹]. دلیل الکترونیکی، هر داده‌پیامی است که اصحاب دعوا برای اثبات یا دفاع از دعوا به آن استناد می‌نمایند *(شهبازی‌نیا و عبدالهی، ۱۳۸۹، ص.۱۹٤)*. از این‌رو، ادله الکترونیکی شامل هر نوع اطلاعات یا دستورهایی است که در حافظه رایانه یا از طریق سامانه‌های رایانه‌ای یا مخابراتی، مبادله، پردازش، بازیافت یا تولید می‌شود *(السان، ۱٤۰۰، ص.۱٥٤)*. این موضوع از بند «الف» ماده ۲ قانون تجارت الکترونیکی نیز قابل استنباط است. همچنین با توجه به اینکه در ماده ۱۲ قانون تجارت الکترونیکی، به امکان وجود ادله اثبات دعوی به‌صورت داده‌پیام اشاره نموده، نشان‌دهنده این است که قانون‌گذار دلایل الکترونیکی را مورد پذیرش قرار داده است. برخی از حقوق‌دانان در دسته‌بندی ادله الکترونیکی، آن‌ها را به سه دسته تقسیم می‌نمایند: دسته اول، محاسبات و تجزیه و تحلیل‌های خود رایانه را شامل می‌شود که از طریق پردازش نرم‌افزاری و وصول اطلاعات از دستگاه‌های دیگر انجام می‌دهد، دسته دوم، اطلاعاتی را

---

۳۸. ماده ۱۹٤ قانون آیین دادرسی مدنی

۳۹. جهت مطالعه تفصیلی تفاوت‌های دلایل سنتی و الکترونیکی رجوع کنید به:

شهبازی‌نیا، مرتضی و عبدالهی، محبوبه (۱۳۸۹). دلیل الکترونیک در نظام ادله اثبات دعوا. *فصلنامه حقوق*، دوره ٤۰، شماره ٤، صص ۱۹٥ و ۱۹٦.

شامل می‌شود که به‌وسیله انسان به رایانه وارد شده است و دسته سوم، ترکیبی از دو دسته فوق است، بدین‌معنا که داده‌های ناشی از پردازش خودکار و نیز فعل انسان، دلیل خاصی را به وجود می‌آورد *(السان، ۱٤۰۰، ص.۱٥٦)*.

بنا به آنچه که در گفتار ۱-۱ درباره ماهیت قرارداد هوشمند تشریح گردید، قراردادهای هوشمند به‌وسیله رایانه، کدنویسی و سپس در بستر بلاکچین پیاده‌سازی و اجرا می‌شوند و در آن بستر توسط هوش مصنوعی (که خود نوعی سامانه رایانه‌ای هوشمند است *(Soyer & Tettenborn, 2023, p. 385)*) پردازش و آنگاه کدهای رمزنگاری شده قرارداد هوشمند در عالم حقیقی دارای اثر می‌شود، حال می‌توان نتیجه گرفت که قراردادهای هوشمند، داده-پیام‌های رمزنگاری شده‌اند که برنامه‌نویسی، اجرا، پردازش و مبادله آن‌ها توسط سامانه-های رایانه‌ای هوشمند انجام می‌گیرد؛ بنابراین دارای همه شرایطی که بتوان آن‌ها را به‌عنوان دلیل الکترونیکی محسوب نمود، هستند. همچنین با توجه به اینکه این قراردادها، هم کدهای رمزنگاری نگارش شده توسط انسان‌ها، هم اطلاعات دریافتی از اوراکل[٤۰]های متصل به قرارداد هوشمند (به‌عنوان اطلاعات ارسالی از دستگاه دیگر) و هم اطلاعات پردازش‌شده توسط هوش مصنوعی را اجرا می‌نمایند، دلایل الکترونیکی ناشی از قرارداد هوشمند می‌تواند شامل هر یک از سه نوع دلیل الکترونیکی بیان شده در بند فوق باشد.

۲-۲. سندیت داشتن قراردادهای هوشمند

دلیل الکترونیکی، فارق از محتوای آن، در هر شکلی قابلیت بروز دارد و یکی از مهم‌ترین دلایل الکترونیکی، دلایلی است که در قالب سند الکترونیکی[٤۱] می‌باشد. در نظر برخی حقوق‌دانان *(کریمی و جوادی، ۱٤۰۲، ص.۱۲۲)* ارزش «سند» (به‌معنای عام آن که شامل اسناد کاغذی و اسناد الکترونیکی می‌شود) به‌علت رایج بودن استناد به سند در قریب به اتفاق دعاوی در دادگاه‌ها، به‌قدری زیاد است که سند را جزء ارزشمندترین دلایل برمی‌شمارند.

---

٤۰. اوراکل‌ها (Oracle) سیستم‌های اطلاعاتی خارج از بلاکچین می‌باشند و واسطه‌ای میان بلاکچین و اطلاعات خارجی محسوب می‌شوند که این اطلاعات خارجی را به‌صورت برخط و به‌سرعت در اختیار بلاکچین قرار می‌دهند و از این طریق بر عملکرد قراردادهای هوشمند تأثیر می‌گذارند *(Chevalier, 2021, p. 559)*.

41. Electronic Document

طبق ماده ۱۲۸٤ قانون مدنی «سند عبارت است از هر نوشته که در مقام دعوی یا دفاع قابل استناد باشد». بر اساس این تعریف می‌توان ارکان تشکیل‌دهنده سند را شامل سه مورد دانست: سند نوشته باشد، در مقام دفاع یا دعوا قابل استناد باشد و دارای امضا باشد *(کاتوزیان، ۱٤۰۱الف، ص.۲۷٦)*؛ بنابراین اگر دلیلی فاقد هر یک از این سه رکن باشد نمی‌توان آن را سند دانست.

۲-۲-۱. نوشته بودن

هر رسم و اثر انسانی (در مقابل رسم و اثر طبیعی مثل اثر زلزله و سیل) که بر روی شیء ایجاد شود، نوشته محسوب می‌شود *(کریمی و جوادی، ۱٤۰۲، ص.۱۲۵)*. ادله الکترونیکی از آن جهت که در جایی ذخیره شده و یا قابل چاپ هستند و نیز اغلب به‌صورت مستند می‌توان آن‌ها را ارائه داد، به نوشته شباهت بسیاری دارند *(السان، ۱٤۰۰، ص.۱٥٤)*. بر این‌اساس، قراردادهای هوشمند رکن «نوشته بودن» اسناد را دارا هستند؛ زیرا این قراردادها به‌وسیله کدهای رمزنگاری‌شده در بستر بلاکچین نگاشته می‌شوند، درواقع در این قراردادها توافقات متعاقدان به‌صورت کد رمزنگاری شده نوشته *(O'Shields, 2017, p. 181)* و در بستر بلاکچین به اجرا گذاشته می‌شود. نوع نوشته در این حالت به‌صورت داده‌پیام است و این امر مستند به ماده ٦ قانون تجارت الکترونیکی مانع از پذیرش اعتبار داده‌پیام به‌عنوان نوشته نیست *(السان، ۱٤۰۲، ص.۲٥٦)*. علاوه بر آن بنا به آنچه در گفتار ۱-۲-۳ بیان شد، می‌توان با مراجعه به پایگاه‌های مرتبط با هر بلاکچین، مبادلات صورت گرفته در آن‌ها را مشاهده کرد و به‌صورت مکتوب ذخیره یا چاپ نمود.

۲-۲-۲. قابلیت استناد

نوشته‌ای که به منظور تحقق بخشیدن و اثبات واقعه حقوقی تنظیم می‌شود، در اصطلاح حقوقی سند نامیده می‌شود؛ بنابراین هدف از تنظیم سند فراهم آوردن امکان استناد به آن است *(کاتوزیان، ۱٤۰۱الف، ص.۲۷۷)*. قابلیت استناد به این معناست که نوشته دلیلیت داشته باشد و برای اینکه سند دلیلیت داشته باشد و بتوان به آن استناد کرد باید حاوی دلیلی موضوعی برای اثبات حق مورد ادعا باشد *(کریمی و جوادی، ۱٤۰۲، ص.۱۲۵)*؛ بنابراین قابلیت

استناد فقط ناظر به مرحله اثبات است و به آثار حقوقی و ماهوی عمل حقوقی توجه ندارد *(کاتوزیان، ۱۴۰۱الف، ص.۲۸۵)*.

در قراردادهای هوشمند مطابق توضیحات بیان شده در گفتار ۱-۲ کلیه اطلاعات، مبادلات و روابط میان طرفین در بستر بلاکچین به ثبت می‌رسد و امکان تغییر یا هک آن‌ها تقریباً ناممکن است؛ بنابراین اطلاعات قراردادهای هوشمند به هنگام بروز اختلاف میان متعاقدان می‌تواند به‌عنوان یک دلیل موضوعی مورد استناد قرار گیرد تا طرفین به‌وسیله این اطلاعات بتوانند ادعاهای خود را ثابت کرده یا مقابل ادعاهای طرف مقابل دفاع نمایند. همچنین دادگاه، به‌عنوان مرجع فصل خصومت، می‌تواند با بررسی این اطلاعات به‌طور تخصصی، به حقیقت آنچه میان طرفین رخ داده پی ببرد و حل اختلاف نماید.

۲-۲-۳. دارای امضا بودن

نوشته منتسب به اشخاص در صورتی قابل استناد است که دارای امضا *(کاتوزیان، ۱۴۰۱الف، ص.۲۷۸)* اثر انگشت یا مهر شخصی باشد *(شمس، ۱۳۹۰، ص.۸۰)*. امضا، نشان‌دهنده تأیید اعلام‌های مندرج در سند و پذیرش تعهدهای ناشی از آن است و پیش از آن، نوشته را باید طرحی به حساب آورد که تحت مطالعه و تدبر است و هنوز تصمیم نهایی درباره آن گرفته نشده است *(کاتوزیان، ۱۴۰۱الف، ص.۲۷۹)*. امضا یک سند، به‌عنوان متعهد بر چهار چیز دلالت دارد: انتساب، انجام تشریفات، تصدیق و قدرت اجرایی *(السان، ۱۴۰۰، ص.۱۳۳)*؛ بنابراین سند، زمانی علیه شخص سندیت می‌یابد که ذیل سند امضا شده باشد *(بهزادی، ۱۳۹۷، ص.۵۶)*. امضای سنتی به مفهوم اعم هرگونه علامت انحصاری شخصی است که زیر نوشته ترسیم یا گذاشته شده و دلالت بر هویت امضاکننده و تأیید متن نوشته توسط او بنماید *(شمس، ۱۳۹۰، ص.۹۰)*؛ اما قراردادهای هوشمند با امضائات دیجیتالی منعقد می‌شوند و امضائات دیجیتالی نوع خاصی از امضاهای الکترونیکی[۴۲] هستند که برای مشخص کردن هویت یک پیام یا برای علامت‌گذاری یک متن به‌کار می‌رود *(ناصر، ۱۳۹۷، ص.۵۶)*. طبق ماده ۷ قانون

۴۲. بند «ی» ماده ۲ قانون تجارت الکترونیکی در تعریف امضای الکترونیکی (Electronic Signature) بیان می‌دارد: «عبارت است از هر نوع علامت منضم شده یا به نحو منطقی تبدیل شده به داده‌پیام است که برای شناسایی امضاکننده داده‌پیام مورد استفاده قرار می‌گیرد».

تجارت الکترونیکی: «هرگاه قانون وجود امضا را لازم بداند امضای الکترونیکی مکفی است»؛ بنابراین در انعقاد قراردادهای هوشمند وجود امضای دیجیتالی از نظر قانونی معتبر است و قرارداد، امضا شده محسوب می‌شود. درنتیجه اگر قرارداد هوشمندی دارای امضا دیجیتالی باشد علاوه بر آنکه می‌توان امضا را به متعاقدان منتسب کرد تا اصالت سند مشخص شود، اماره‌ای است بر تصدیق مفاد قرارداد توسط آن‌ها که امکان الزام متعاقدان به اجرای تعهدات به‌واسطه آن ایجاد می‌شود، ضمن آنکه بنا بر سازوکار امضائات دیجیتال که در گفتار ۱-۱ توضیح داده شد امکان هک یا تغییر مفاد قرارداد دارای امضای دیجیتال وجود ندارد. در حقوق کشور ما از سیاق مواد ٦، ۱۲ و ۱۳ قانون تجارت الکترونیکی و به‌ویژه مفهوم مخالف ماده ۱۵ قانون تجارت الکترونیکی می‌توان دریافت که امضا، اعتبار و ارزش اثباتی امضای عادی را داراست مگر اینکه امضا یا داده‌پیام از نوع «مطمئن»[۴۳] باشد که در این‌صورت دارای اعتبار امضای رسمی است *(السان، ۱٤۰۰، ص.۱۳۹)*. در کشورهای توسعه‌یافته امضائات دیجیتالی با طی تشریفات خاصی به اشخاص اعطا می‌شود و اشخاص پس از مراجعه به مراجع صالح، در صورت داشتن شرایط قانونی و اهلیت لازم، پس از بررسی مدارک مورد نیاز، برایشان امضائات دیجیتالی اختصاص داده می‌شود *(ناصر، ۱۳۹۷، ص.٥٦)*. در ایران، اشخاص می‌توانند با مراجعه به دفاتر خدمات صدور گواهی امضای الکترونیکی[٤٤] یا تارنمای مرکز صدور گواهی الکترونیکی عام[٤٥] و ارائه مدارک مورد نیاز و طی تشریفات خاصی، امضای دیجیتالی اختصاصی دریافت نمایند. امضا دیجیتالی تخصیص یافته به اشخاص، فقط توسط همان شخص می‌تواند مورد استفاده قرار گیرد و در صورت اعمال هرگونه تغییر در مفاد نوشته پس از امضای آن، امضای دیجیتال در آن نوشته، از اعتبار می‌افتد *(Zaremba, 2003, p. 481)* و الحاق مجدد

---

۴۳. ماده ۱۰ قانون تجارت الکترونیکی: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد: الف) نسبت به امضاکننده منحصربه‌فرد باشد. ب) هویت امضاکننده داده‌پیام را معلوم نماید. ج) به‌وسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد. د) به‌نحوی به یک داده‌پیام متصل شود که هر تغییری در آن داده‌پیام قابل تشخیص و کشف باشد».

٤٤. ماده ۳۱ قانون تجارت الکترونیکی

45. https://www.gica.ir

امضای دیجیتال به نوشته تغییر یافته منوط به آن است که مالک تغییرات صورت گرفته تا تایید نماید؛ بنابراین می‌توان نتیجه گرفت که امضائات دیجیتالی که طبق فرایند بیان شده به اشخاص اعطا شوند بنابر ماده ۱۵ قانون تجارت الکترونیکی دارای اعتبار امضای رسمی هستند و صرفاً ادعای جعل نسبت به آن‌ها مسموع است و هرگونه تردید یا انکار نسبت به آن‌ها مسموع نخواهد بود.

بنا به آنچه تا این‌جا شرح داده شد، مشاهده می‌شود که قراردادهای هوشمند همه ویژگی‌های اسناد را دارا هستند و حتی در برخی از این ویژگی‌ها، مانند غیرقابل هک بودن اطلاعات و غیرقابل تغییر بودن مفاد قراردادی بدون توافق متعاقدان، نسبت به اسناد دیگر برتری دارند؛ بنابراین می‌توان قراردادهای هوشمند را دلیل الکترونیکی، از نوع سند الکترونیکی، محسوب نمود.

۳. امکان‌سنجی استناد به قراردادهای هوشمند

بیان شد که قراردادهای هوشمند، نوعی سند الکترونیکی می‌باشند؛ لکن جهت آن که بتوان در دعاوی گوناگون به‌عنوان دلیل به این قراردادها استناد کرد، باید مقررات و شرایط خاصی رعایت گردد و نیز ارزش اثباتی آن‌ها در حالات مختلف بررسی شود تا به‌درستی بتوان به این قراردادها به‌عنوان دلیل استناد نمود.

۳-۱. شرایط استناد به قراردادهای هوشمند

تضمین امنیت، اعتبار و اصالت داده‌ها پیش‌شرط تعیین‌کننده امکان استناد به قراردادهای هوشمند (به‌عنوان دلیل الکترونیکی) در محاکم است *(مؤذن‌زادگان، سلیمان‌دهکردی و یوشی، ۱۳۹٤، ص.۷۰)*. طبق ماده ١٤ قانون تجارت الکترونیکی، قراردادهای هوشمند در صورتی در محاکم قابل استناد هستند که به طریق مطمئن ایجاد و نگهداری شوند و در صورتی به‌عنوان داده‌پیام مطمئن تلقی می‌شوند که طبق بند «ح» ماده ۲ قانون تجارت الکترونیکی، توسط یک سیستم اطلاعاتی مطمئن با شرایط زیر ایجاد شوند: «۱- به نحوی معقول در برابر سوءاستفاده و نفوذ محفوظ باشد. ۲- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد. ۳- به نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و

سازماندهی شده باشد. ٤- موافق با رویه ایمن[٤٦] باشد». بنا به آنچه پیرامون سازوکار بلاکچین، به‌عنوان بستر انعقاد قراردادهای هوشمند، با استفاده از فرایند اثبات کار و سازوکار هش و پیش هش بلوک‌های بلاکچین در گفتار ۱-۲-۱ و ۱-۲-۲ تشریح شد، قراردادهای هوشمند در برابر سوءاستفاده و نفوذ محفوظ هستند و از سطح دسترسی معقولی نیز برخوردارند؛ زیرا این قراردادها، طبق توضیحات گفتار ۱-۲-۱، با استفاده از سازوکار کلید عمومی و کلید خصوصی ایجاد می‌شوند و در این سازوکار، به جهت رمزنگاری بودن آن امکان دسترسی اشخاص غیرمجاز به حداقل‌ترین میزان ممکن می‌رسد *(مؤذن‌زادگان، سلیمان‌دهکردی و یوشی، ۱۳۹٤، ص.۸۷)*. می‌توان چنین بیان داشت که قراردادهای هوشمند متناسب با انتظارات مدنظر متعاقدان آن پیکربندی و توسعه یافته‌اند. همچنین نظر به اینکه مفاد قراردادی در قراردادهای هوشمند به‌صورت رمزنگاری ایجاد و ذخیره می‌شود و طبق توضیحات گفتارهای ۱-۲-۱ و ۱-۲-۳، این اطلاعات به صورت دائمی در بستر بلاکچین باقی می‌مانند و متعاقدان می‌توانند با استفاده از کلیدهای عمومی و خصوصی خود این اطلاعات را در جستجوگرهای بلاکچین مرتبط با قرارداد هوشمند، مشاهده و بررسی نمایند. درنتیجه قراردادهای هوشمند مطابق با رویه ایمن نیز هستند و به‌صورت کامل دارای شرایط بیان شده در ماده ١٤ قانون تجارت الکترونیکی می‌باشند و می‌توان به‌عنوان دلیل الکترونیکی به آن‌ها استناد کرد؛ البته باید توجه داشت این موضوع نشان می‌دهد قراردادهای هوشمند به‌صورت بالقوه می‌توانند یک سیستم مطمئن تلقی شوند و شاید دارای استثنائاتی هم باشند؛ زیرا همان‌طور که پیش‌تر بیان شد امکان هک بلاکچین و قراردادهای هوشمند مبتنی بر آن، «تقریباً غیرممکن» است و علی‌رغم ارتقای سطح امنیت قراردادهای هوشمند به‌صورت مستمر توسط توسعه‌دهندگان بلاکچین، ممکن است در فرض نادر، مانند آنچه در سال ۲۰۱٦ در هک قرارداد هوشمند The DAO اتفاق افتاد

---

٤٦. بند «ط» ماده ۲ قانون تجارت الکترونیکی: «رویه‌ای است برای تطبیق صحت ثبت داده‌پیام، منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره‌سازی داده‌پیام از یک زمان خاص. یک رویه ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود».

(Werbach, 2018, p. 496; Kolber, 2018, p. 202). بنا به ملاحظات مختلف، اگر قرارداد هوشمند هر یک از ویژگی‌های سیستم مطمئن را از دست دهد پس ضرورت دارد در استناد به این قراردادها، محاکم اصل را بر عادی بودن سیستم انعقاد قراردادهای هوشمند بگذارند و در فرض ادعای یکی از اصحاب دعوی بر مطمئن بودن سیستم قرارداد هوشمند، بار اثبات آن را بر دوش مدعی بگذارند.

همچنین بنا به ماده ۵۰ قانون جرائم رایانه‌ای، اصالت[۴۷] قرارداد هوشمند و انکارناپذیری مفاد آن را هم باید جزء شرایط قابلیت استناد به این گونه قراردادها دانست. مستفاد از این ماده، اصل را باید بر عدم اعتبار ادله الکترونیکی گذارد و اثبات اعتبار آن برعهده استنادکننده خواهد بود *(السان، ۱٤۰۰، ص.۱٦۹)*. در ادله الکترونیکی با توجه به گمنامی اشخاص در فضای سایبر امکان اصالت‌سنجی به‌راحتی میسر نیست ولی رمزنگاری اطلاعات در قراردادهای هوشمند می‌تواند صحت و اصالت داده‌پیام‌ها را حفظ نماید *(مؤذن‌زادگان، سلیمان‌دهکردی و یوشی، ۱۳۹٤، ص.۷۱)*؛ بنابراین استنادکننده به قراردادهای هوشمند با توجه به اینکه اطلاعات رمزنگاری شده در این قراردادها به‌صورت برگشت ناپذیر و غیرقابل تغییر می‌باشد (گفتار ۱-۲-۲) و صرفاً دارندگان کلید عمومی و خصوصی به این اطلاعات دسترسی دارند، می‌تواند با استفاده از این کلیدها، داده‌پیام‌های مرتبط با قرارداد هوشمند را به مقام قضایی ارائه نموده و اصالت این اطلاعات و تغییر نیافتن آن‌ها بعد از ایجاد را اثبات نماید.

از دیگر ویژگی‌های لازم جهت استناد به قراردادهای هوشمند، قابلیت انتساب آن‌ها می‌باشد *(مؤذن‌زادگان، سلیمان‌دهکردی و یوشی، ۱۳۹٤، ص.۷٤)*. بیان شد که قراردادهای هوشمند، نوعی سند الکترونیکی هستند و هر سندی را برای آن که بتوان به شخصی منتسب کرد باید به امضای وی رسیده باشد *(شمس، ۱۳۹۰، ص.۹۸)*. با امضای دیجیتالی قرارداد هوشمند، اصالت قرارداد و انتساب آن به امضاکننده، اثبات می‌شود *(بهزادی، ۱۳۹۷، ص.٥٦)* و این الحاق امضای دیجیتال به قرارداد به نحو منطقی اشاره به سازوکار امضا با کلید خصوصی و

---

٤٧. «اصالت»، به معنای واقعی بودن و تنظیم بدون قصد و غرض (با صداقت) داده‌پیام می‌باشد *(السان، ۱٤۰۰، ص.۱٦۰)*.

محرمانه دارد که پس از رمزنگاری فقط با کلید عمومی قابل رمزگشایی است *(بهزادی، ۱۳۹۷، ص.۵۸)*. در نتیجه استنادکننده به قرارداد هوشمند می‌تواند با در اختیار گذاشتن کلید خصوصی خود نزد مقام قضایی مطابق با مقررات آیین‌نامه شیوه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳ و تحلیل مبادلات و کدهای قراردادی توسط کارشناسان مورد اعتماد مقام قضایی، انتساب قرارداد هوشمند به مدعی علیه را اثبات نماید؛ البته زمانی که امضای دیجیتالی توسط دفاتر خدمات صدور گواهی امضای الکترونیکی، گواهی شده باشد، امکان انتساب آن با سهولت بیشتری ممکن است و انکار آن سخت‌تر می‌شود؛ اما در مواردی که امضای دیجیتالی شخص به گواهی مقامات رسمی نرسیده باشد نیز می‌توان با استفاده از ویژگی پیگیری مبادلات انجام شده در بستر بلاکچین و تحلیل کلیه مبادلات صورت گرفته از هویت دارنده آن امضا اطلاع پیدا کرد. چرا که موضوع قراردادهای هوشمند تعهدات مالی است *(O'Shields, 2017, p. 178)* و درنتیجه آن رمزارزها به کیف پول دیجیتالی اشخاص منتقل می‌شود و ایشان جهت تبدیل کردن آن‌ها به وجه رایج باید به صرافی‌های رمزارزها مراجعه نماید و ازآنجایی‌که اکثر این صرافی‌ها از روش‌های مختلف هویت‌سنجی مثل روش KYC[۴۸] استفاده می‌کنند نهایتاً می‌توان به هویت شخص پی برد و امضای دیجیتال را به او نسبت داد؛ البته در صورت عدم وقوع فرض اخیر، کارشناسان حوزه برنامه‌نویسی بلاکچین می‌توانند با تحلیل مبادلات صورت گرفته با آن امضای دیجیتالی، قرائن و اماراتی را به دست آورند که نشان دهد دارنده آن امضای دیجیتالی چه شخصی می‌باشد. لازم به ذکر است برای آنکه امضای دیجیتالی را بتوان به‌طور معتبر به مدعی علیه منتسب نمود بایستی به‌گونه‌ای عمل شود که تدابیر معقول را برای ممانعت از هرگونه استفاده غیرمجاز از داده‌های مرتبط با تولید امضا به عمل آورد *(بهزادی، ۱۳۹۷، ص.٦٤)* و همان‌طور که پیش‌تر بیان شد این موضوع به‌طور بالقوه

---

۴۸. KYC مخفف "Know Your Customer" و به معنی «مشتری‌ات را بشناس» است و به احراز هویت اجباری مشتری، معمولاً توسط یک مؤسسه مالی اشاره دارد و شامل اطلاعاتی است که می‌تواند برای تأیید هویت مشتری استفاده شود، مانند کارت شناسایی معتبر، آدرس منزل و غیره. مشتریان معمولاً در هنگام افتتاح حساب، ملزم به ارائه اطلاعات احراز هویت هستند *(Chen, 2024)*.

در سازوکار قراردادهای هوشمند فراهم است ولی لازم است تا هنگامی که جهت کشف حقیقت و انجام تحقیقات، کلید خصوصی متعاقدان قرارداد در اختیار مقام قضایی یا کارشناسان قرار می‌گیرد، مقام قضایی مطابق ماده ۱۸ آیین‌نامه شیوه جمع‌آوری و استنادپذیری ادله الکترونیکی، اقدامات لازم جهت حفظ محرمانگی، صحت و اعتبار داده-پیام‌های مرتبط با قرارداد هوشمند را لحاظ نماید.

قابلیت ارائه *(مؤذن‌زادگان، سلیمان‌دهکردی و یوشی، ۱۳۹٤، ص.۷٤)*، از دیگر ویژگی‌های قرارداد هوشمند قابل استناد، یعنی آنکه بتوان مفاد و اطلاعات مورد نیاز مقام قضایی درباره قرارداد هوشمند را با رعایت ماده ۱۸ آیین‌نامه شیوه جمع‌آوری و استنادپذیری ادله الکترونیکی به مقام قضایی تحویل داد. ارائه اطلاعات مرتبط با قراردادهای هوشمند را طبق توضیحات گفتار ۱-۲-۱ و ۱-۲-۳، نه‌تنها می‌توان از طریق چاپ داده‌های مربوط به مبادلات قرارداد هوشمند در حافظه جانبی، لوح فشرده و... ذخیره کرد بلکه می‌توان با در اختیار گذاشتن کلیدهای عمومی و خصوصی نزد مقام قضایی دسترسی‌های لازم را برای بررسی مفاد قرارداد هوشمند ایجاد کرد.

۳-۲. ارزش اثباتی

با بررسی قانون تجارت الکترونیکی، ادله الکترونیکی را می‌توان به دو نوع عادی و مطمئن تقسیم نمود *(شهبازی‌نیا و عبدالهی، ۱۳۸۹، ص.۱۹٦)*. مستند به ماده ۱۵ قانون تجارت الکترونیکی، ادله الکترونیکی عادی، قابل‌انکار و تردید و ادعای جعل هستند؛ اما ادله الکترونیکی مطمئن از ارزش اثباتی بالاتری برخوردارند و فقط ادعای جعل نسبت به آن‌ها مسموع است. اصل بر عادی بودن ادله الکترونیکی است *(شهبازی‌نیا و عبدالهی، ۱۳۸۹، ص.۲۰۳)* مگر آنکه استنادکننده به دلیل الکترونیکی بتواند ثابت کند آن داده‌پیام توسط سیستم مطمئن با شرایط بند «ح» ماده ۲ قانون تجارت الکترونیکی به‌وجود آمده است که در گفتار قبل بیان شد و این امر به طور بالقوه در قراردادهای هوشمند قابل اثبات است.

در قراردادهای هوشمند، به‌عنوان نوعی سند الکترونیکی، برخی معتقدند ارزش اثباتی اسناد الکترونیکی به اعتبار حقوقی امضای مندرج در آن بستگی دارد چرا که اسناد

الکترونیکی تحقق نمی‌یابند مگر اینکه امضای الکترونیکی معتبر و لازم‌الاجرا داشته باشند *(ساعی و باباخانی، ۱۳۹۱، ص.۱۷۵)*؛ اما در مقابل برخی دیگر، برخلاف امضا در اسناد عادی، امضا در اسناد الکترونیکی را رکن سند ندانسته و صرفاً وسیله‌ای برای ارتقای امنیت سند می‌دانند و در تأیید نظرشان به بند «ح» ماده ۲ قانون تجارت الکترونیکی استناد می‌نمایند و بیان می‌دارند در این مقرره قانونی امضای الکترونیکی جزء شرایط سیستم اطلاعاتی مطمئن ذکر نشده است *(السان، ۱٤۰۰، ص.۱۷٤)*؛ اما به نظر مؤلف، نظر اخیر حداقل درباره قراردادهای هوشمند صدق نمی‌کند؛ زیرا از آنجا که در این قراردادها ممکن است متعاقدان به‌طور کلی یکدیگر را نشناسند و همان‌طور که در گفتار ۱-۱ نیز بیان شد، اهلیت آن‌ها با استفاده از سازوکار اعطای کلید عمومی و خصوصی سنجیده می‌شود و به‌نوعی اشخاص با اعمال امضای دیجیتال خود از طریق کلیدهای عمومی و خصوصی در این قراردادها، قصد خود را بروز می‌دهند و نیز اصالت داده‌پیام‌های قرارداد هوشمند توسط امضای دیجیتال آن سنجیده می‌شود (گفتار ۱-۲-٤ و ۳-۱)؛ لذا برای تعیین ارزش اثباتی قرارداد هوشمند لازم است تا صحت امضای دیجیتال آن مطابق ماده ۱۰ قانون تجارت الکترونیکی مورد بررسی قرار گیرد.

طبق آنچه درباره سازوکار امضای دیجیتالی قرارداد هوشمند در گفتار ۲-۲-۳ بیان گردید این امضاها صرفاً توسط شخص دارنده آن امضا می‌تواند مورد استفاده قرار گیرد و با توجه به رمزنگاری شدن امضا امکان هک آن‌ها کم است مگر آنکه خود دارنده امضای دیجیتال مرتکب اهمال شود و کدهای آن را در اختیار دیگران قرار دهد یا در دام کلاهبرداران یا هکرها بیافتد و کدهای آن را افشا کند. از سوی‌دیگر امضای دیجیتال صرفاً مختص به دارنده آن می‌باشد؛ زیرا کدهای کلید عمومی و خصوصی آن امضا با حساب کاربری وی در بلاکچین متصل و مرتبط است و جهت شناسایی هویت حقیقی دارنده امضا نیز می‌توان از طرقی که در گفتار قبل ذکر شد استفاده کرد. درنهایت با توجه به قابلیت برگشت‌ناپذیری و پیگیری مبادلات در قراردادهای هوشمند (گفتارهای ۱-۲-۲ و ۱-۲-۳) امضائات دیجیتالی قرارداد هوشمند متصل به مفاد قرارداد است و به علت شفافیت اطلاعات در بستر بلاکچین به‌راحتی کارشناسان حوزه بلاکچین می‌توانند تشخیص دهند که تغییرات صورت گرفته در

قرارداد با تأیید دارنده امضای دیجیتال صورت گرفته است یا خیر. کمااینکه علی رغم خوداجرایی قراردادهای هوشمند، لازم است تا کلیه کدهای این قرارداد ابتدا به توافق و امضای طرفین قرارداد برسد و سپس توسط هوش مصنوعی این قرارداد به اجرا درآید، در غیر این‌صورت کدهای قراردادی بدون امضای متعاقدان به اجرا در نخواهد آمد و به‌صورت معلق باقی می‌ماند؛ بنابراین قراردادهای هوشمند می‌توانند به‌عنوان دلیل الکترونیکی مورد استناد قرار گیرند ولی اصل بر آن است که از نوع عادی هستند و جهت بهره‌مندی از مزایای دلیل الکترونیکی مطمئن لازم است تا مطابق ماده ۱۰ قانون تجارت الکترونیکی ثابت نماید که این قرارداد دارای شرایط امضای الکترونیکی مطمئن می‌باشد.

نتیجه‌گیری

قراردادهای هوشمند ماهیتاً نسل جدیدی از قراردادهای الکترونیکی می‌باشند که با دارا بودن ویژگی‌های اسناد الکترونیکی، می‌توان در محاکم دادگستری ایران به‌عنوان دلیل الکترونیکی به آن‌ها استناد کرد. بنابر ماده ۱۲ قانون تجارت الکترونیکی، محاکم نمی‌توانند صرف شکل رمزنگاری بودن کدهای قراردادهای هوشمند آن‌ها را به‌عنوان دلیل نپذیرند و اشخاص می‌توانند در مواردی که اثبات حق یا دفاع در برابر امری منوط به ارائه دلیل است، با اثبات شرایط ذکر شده در ماده ١٤ قانون تجارت الکترونیکی و ماده ٥٠ قانون جرائم رایانه‌ای، به این قراردادها استناد نمایند. اثبات اصالت، محرمانگی، قابلیت انتساب و انکارناپذیری داده‌پیام‌های قرارداد هوشمند، به کمک سازوکار کلیدهای عمومی و خصوصی، امضائات دیجیتالی منعقدکننده قرارداد هوشمند و قابلیت پیگیری مبادلات در بستر بلاکچین، می‌تواند با سهولت و سرعت بیشتری انجام گیرد به‌خصوص در مواردی که امضائات دیجیتال اشخاص توسط مقامات رسمی مورد گواهی قرار گرفته باشد. ارزش اثباتی قراردادهای هوشمند نزد محاکم دادگستری ایران منوط به اثبات شرایط مندرج در مواد ۱۳ و ١٤ قانون تجارت الکترونیکی است که غالباً بلاکچین و قرارداد هوشمند مبتنی بر آن، می‌توانند به‌صورت بالقوه دارای این شرایط باشند و اثبات آن‌ها به جهت ویژگی‌های بیان شده‌ی قراردادهای هوشمند و شفافیت اطلاعات برای متعاقدان قرارداد می‌تواند توسط

استنادکننده به قرارداد هوشمند صورت گیرد تا با اثبات مطمئن بودن قرارداد هوشمند، ادعای انکار و تردید آن‌ها نیز منتفی شود؛ بنابراین این قراردادها نه‌تنها می‌توانند مطابق قوانین و مقررات، به‌عنوان دلیل در محاکم دادگستری استفاده شوند بلکه به‌علت داشتن ویژگی‌های منحصربه‌فردشان نظیر شفاف بودن اطلاعات در بلاکیچن برای متعاقدان، برگشت‌ناپذیری مبادلات انجام شده، محدودیت دسترسی به کدهای قراردادی به متعاقدان قرارداد و... می‌توانند در اثبات امور مختلف در محاکم دادگستری راهگشاتر از سایر دلایل الکترونیکی باشند.

منابع

السان، مصطفی. (۱٤۰۲). *حقوق تجارت الکترونیکی*. تهران: سمت.

السان، مصطفی. (۱٤۰۰). *حقوق فضای مجازی*. تهران: شهر دانش.

بهزادی، ایرج. (۱۳۹۷). قابلیت انتساب ادله الکترونیک. *فصلنامه پژوهش‌های حقوقی*، دوره ۱۷، شماره ۳٤، ۵۵-۷۰، https://doi.org/10.48300/jlr.2018.67510.

رضایی، علی. (۱۳۹۳). *حقوق تجارت الکترونیکی*. تهران: میزان.

ساعی، سید محمدهادی؛ باباخانی، رضا. (۱۳۹۱). بررسی ارزش اثباتی اسناد الکترونیک در حقوق ایران. *پژوهش‌نامه حقوق اسلامی*، دوره ۱۳، شماره ۱، ۱۵۷-۱۸۸.

شمس، عبدالله. (۱۳۹۰). *ادله اثبات دعوا، حقوق ماهوی و شکلی*. تهران: دراک.

شهبازی‌نیا، مرتضی؛ عبدالهی، محبوبه. (۱۳۸۹). دلیل الکترونیک در نظام ادله اثبات دعوا. *فصلنامه حقوق*، دوره ٤۰، شماره ٤، ۱۹۳-۲۰۵.

فضلی، مهدی. (۱۳۸۸). *مسئولیت کیفری در فضای سایبر*. تهران: خرسندی.

کاتوزیان، ناصر. (۱٤۰۱الف). *اثبات و دلیل اثبات*. تهران: میزان.

کاتوزیان، ناصر. (۱٤۰۱ب). *دوره حقوق مدنی: قواعد عمومی قراردادها*. تهران: گنج دانش.

کریمی، عباس؛ جوادی، سهیلا. (۱٤۰۲). *ادله اثبات دعوا*. تهران: میزان.

مؤذن‌زادگان، حسنعلی؛ سلیمان‌دهکردی، الهام؛ یوشی، مهشید. (۱۳۹٤). حفظ صحت و استنادپذیری ادله‌ی الکترونیک با استفاده از بیومتریک و رمزنگاری. *پژوهش حقوق*

کیفری، دوره ٤، شماره ۱۲، ٦۹–۹۷، https://doi.org/10.22054/jclr.2015.1782.

ناصر، مهدی. (۱۳۹۷). *قراردادهای هوشمند (مطالعه تطبیقی حقوق ایران و آمریکا)*. تهران: مجد.

Barney, Nick; Troy, Sue; Pratt, Mary K. (September 2023). *Distributed Ledger Technology (DLT)*. https://www.techtarget.com/searchcio/definition/distributed-ledger. – 22/4/2024.

Bohme, Rainer; Christin, Nicolas; Edelman, Benjamin; Moore, Tyler. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, *29*(2), 213-238. https://doi.org/10.1257/jep.29.2.213.

Buchwald, Michael. (2020). Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration. *University of Pennsylvania Law Review*, *168*(5), 1369-1424.

Chen, James. (Updated 15 January 2024). *Know Your Client (KYC): What Means, Compliance Requirements*. https://www.investopedia.com/terms/k/knowyourclient.asp.

Chevalier, Maxime. (2021). From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order. *Journal of International Dispute Settlement*, *12*(4), 558-584. https://doi.org/10.1093/jnlids/idab025.

Demeyer, Maurice. (2018). *Blockchain Technology and Smart Contracts from a Financial Law Perspective*. Faculty of Law and Criminology.

Kerikmae, Tanel; Rull, Addi. (2016). *The Future of Law and eTechnologies*. Springer. https://doi.org/10.1007/978-3-319-26896-5.

Kolber, Adam. (2018). Not-So-Smart Blockchain Contracts and Artificial Responsibility. *Stanford Technology Law Review*, *21*(2), 198-234.

Ledger Academy. (Updated 29 May 2024). *Blockchain Transaction ID Meaning*. https://www.ledger.com/academy/glossary/transaction-id-txid.

LukasK. (2017). *What is Blockchain and Smart Contracts?*. https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-1-3328afca62ab - 21/4/2024.

Nguyen, Son. (2023). Consumer Protection Against Unfair Contract Terms in the Age of Smart Contracts. *Federal Law Review*, *51*(4), 487-508.

Niyazova, Anara; Askarbekova, Aksana. (2022). Legal Nature of Smart Contracts. *Repozytorium Uniwersytetu W Bialymstoku*, *1*(4), 143-149. https://doi.org/10.15290/IPF.2022.13.

Ortolani, Pietro. (2019). The impact of blockchain technologies and smart contracts on dispute resolution. Arbitration and court litigation at the crossroads. *Uniform Law Review*, *24*(2), 430-448. https://doi.org/10.1093/ulr/unz017.

O'Shields, Reggie. (2017). Smart Contracts Legal Agreements for the Block Chain. *North Carolina Banking Institute*, *21*(1), 177-194.

Pluralsight. (2022). *Solidity & Smart Contracts: A quick introduction*. https://www.pluralsight.com/blog/software-development/what-is-solidity-smart-contracts. – 21/4/2024.

Raskin, Max. (2017). The Law and Legality of Smart Contracts. *Georgetown Law*

Technology Review, *1*(2), 305-341.

Rasure, Erika. (2024). *What Are Smart Contracts on the Blockchain and How Do They Work?*. https://www.investopedia.com/terms/s/smart-contracts.asp - 22/4/2024.

Rosic, Ameer. (27 November 2023). *Are Blockchain Transactions Traceable? You Will De Surprised*. https://blockgeeks.com/are-bitcoin-transactions-traceable/#:~:text=Every%20transaction%20made%20on%20the,through%20analysis%20of%20the%20blockchain. – 22/4/2024.

Sapkota, Shrisha. (2022). *The Difference Between E-contracts and Smart Contracts and How These Can Help the Legal Tech*. https://goodlawsoftware.co.uk/law/the-difference-between-e-contracts-and-smart-contracts-and-how-these-can-help-the-legal-tech.

Soyer, Baris; Tettenborn, Andrew. (2023). Artificial Intelligence and Civil Liability: Do We Need a New Regime. *International Journal of Law and Information Technology*, *30*(4), 385-397. https://doi.org/10.1093/ijlit/eaad001.

Suvitha, M; Subha, R. (2021). *A Survey on Smart Contract Platforms and Features*. 7th International Conference on Advanced Computing & Communication Systems (ICACCS), 1536-1539.

Tech Target. (June 2021). *Public Key*. https://www.techtarget.com/searchsecurity/definition/public-key.

Werbach, Kevin. (2018). Trust, But Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, 33(2), 487-550.

Zaremba, Jochen. (2003). International Electronic Transaction Contracts between U.S. and EU Companies and Customers. *Connecticut Journal of International Law*, *18*, 479-512.