Legal Challenges of Decentralized Identity (DID) within Iran's System of Official Documents

Ali Ahmadi
PhD Student, Private Law, Faculty of Humanities, Yasouj Branch, Islamic Azad University, Kohgiluyeh and Boyer-Ahmad, Iran. (Corresponding Author)
Email : a.ahmadi5667@iau.ac.ir

Dr. Hamidreza Rostami
Associate Professor, Department of Private Law, Faculty of Humanities, Yasouj Branch, Islamic Azad University, Kohgiluyeh and Boyer-Ahmad, Iran.
Email : hrostami1962@yahoo.com

Dr. Nazanin Abbaspoor ekder
PhD in Criminal Law and Criminology, Faculty of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
Email : nazanin.abbaspoorekder@iau.ir

Abstract:
Decentralized Identity (DID), grounded in Distributed Ledger Technology (DLT) and developed in accordance with standards promulgated by the World Wide Web Consortium (W3C)-notably Verifiable Credentials (VCs)-has the potential to precipitate a paradigm shift in Iran's regime governing official documentation and notarization. Notwithstanding its transformative promise, the practical deployment of this architecture encounters substantial and systemic legal impediments. Employing an analytical, comparative, and doctrinal methodology, this article first delineates and critically assesses the inherent tension between the principle of Self-Sovereign Identity (SSI), which constitutes the conceptual foundation of decentralized identification frameworks, and the doctrine of the state's exclusive authority over identity verification and document authentication within the Iranian legal order. This normative conflict finds its most explicit expression in Article 1287 of the Civil

Legal Innovation Quarterly
Legal Innovation Research Institute
Summer 2025, Volume 2, Issue 2
www.journallir.com

Code and Article 22 of the Law on the Registration of Deeds and Real Estate.
The study's core inquiries are directed toward the precise identification of the legal and fiqh-based constraints confronting DID and the formulation of localization strategies capable of reconciling this model with Shiite jurisprudence. The results of the combined legal and jurisprudential analysis demonstrate that, despite its notable capacity to enhance administrative efficiency and safeguard informational privacy, the DID paradigm faces fundamental obstacles arising from its incongruity with established standards of evidentiary authority (*ḥujjiyyat*) and formal authentication (*tawthīq*) in Shiite fiqh, as well as with the statute-driven architecture of Iran's system of official instruments. These challenges include the absence of clear judicial probative value, uncertainty in the allocation of civil liability-particularly in scenarios involving fault or negligence in the custody of private cryptographic keys, in light of Article 1 of the Civil Liability Act of 1960 and the fiqh doctrines of *itlāf* (direct causation of harm) and *tasbīb* (indirect causation)-and the strategic risk associated with reliance on foreign technological infrastructures in the context of international sanctions, contrary to the constitutional imperative of preserving national independence enshrined in Article 152 of the Constitution.
A comparative examination of established international practices, including the European Union's framework for electronic identification and trust services and Estonia's e-Residency system, underscores the feasibility of contextual adaptation through the development of hybrid governance models that retain the involvement of public authorities in the initial attestation of identity. On this basis, the article advances a set of policy and legislative recommendations, namely: revising the Registration Law to formally recognize an "official decentralized signature," instituting a regulatory

sandbox to enable controlled experimentation, enhancing judicial literacy in digital identity and blockchain-based evidence, and investing in the creation of a sovereign national blockchain infrastructure.

Keywords: Decentralized Identity (DID); official instruments; Iranian legal system; Self-Sovereign Identity (SSI); distributed ledger technology; Shiite jurisprudence.

Extended abstract

The accelerated evolution of Distributed Ledger Technology (DLT), and more specifically the emergence of Decentralized Identity (DID) architectures, has placed the traditional Iranian regime of official instruments-long predicated upon centralized oversight and state-based authentication-under significant normative strain. Iran's legal framework, which confers validity and official status upon documents executed before notarial authorities (Article 1287 of the Civil Code) and reserves the verification of ownership to the exclusive prerogative of the state (Article 22 of the Law on the Registration of Deeds and Real Estate), is structurally misaligned with the paradigm of Self-Sovereign Identity (SSI) and the disintermediated logic that underpins DID systems. The principal objective of this study is to identify with precision the salient legal and jurisprudential challenges posed by decentralized identity within Iran's system of official documentation and to advance localization models capable of reconciling DID with statutory law and Imamiyyah (Shiite) jurisprudence. The central research questions address: (i) the extent of DID's incompatibility with the foundational doctrines of the Registration Law and the Electronic Commerce Act; (ii) its conformity with Shiite fiqh and constitutional principles-most notably Article 152, which enshrines the preservation of national independence; and (iii) the legislative mechanisms required for the construction of hybrid governance models.

The working hypothesis advanced herein is that, notwithstanding its technological efficiencies and its contribution to enhanced informational privacy, DID confronts substantial impediments within Iran's prevailing legal order, particularly in relation to evidentiary admissibility and the indeterminacy of civil liability. Nonetheless, the study contends that convergence is attainable through incremental

legislative reform and the formulation of hybrid architectures that retain the involvement of sovereign institutions-such as the Organization for the Registration of Deeds and Properties-in the initial attestation of identity.

Research Methodology

This research adopts an analytical, comparative, and doctrinal framework, employing a descriptive–analytical method. The sources examined encompass Iranian statutory instruments (including the Civil Code, the Registration Law, the Electronic Commerce Act, civil liability legislation, and cybercrime statutes), international technical norms (most notably the standards promulgated by the World Wide Web Consortium (W3C)), and qualitative analyses of jurisprudential doctrines (including the fiqh principles of *itlāf* and *tasbīb*, as well as the foundations of evidentiary authority (*ḥujjiyyat*) and *bayyina*). In addition, a comparative approach is utilized to evaluate successful foreign experiences-such as the European Union's eIDAS regime and Estonia's digital identity framework-with the aim of distilling models adaptable to Iran's legal and jurisprudential environment.

Findings

The combined legal and jurisprudential assessment indicates that the DID model, owing to its discordance with established standards of probative authority and formal authentication in Shiite jurisprudence and with the statute-centered configuration of official instruments, is confronted with the following substantive challenges:

1. **Incompatibility with the Concept of the Official Instrument (Article 1287 of the Civil Code):** Decentralized identity mechanisms, which rely on user-controlled identifiers and private cryptographic keys rather than acts performed by a public officer, are fundamentally at odds with the statutory definition of an official document under Article 1287 of the Civil Code, as well as with the

requirement of physical and notarization prescribed by Article 29 of the Law on Notarial Offices. From an evidentiary perspective, instruments generated through DID lack prima facie probative force grounded in state authority and are therefore likely to be classified by Iranian courts as private documents.

2. **Indeterminacy of Civil and Criminal Responsibility:**
   The distributed and multi-actor configuration of DID infrastructures renders the attribution of harm particularly complex in cases involving falsification, unauthorized access (such as private key compromise), or systemic malfunction. This uncertainty complicates the application of Article 1 of the Civil Liability Act and the fiqh doctrines of *itlāf* and *tasbīb*, both of which presuppose the identification of a specific culpable agent. Consequently, the existing framework appears ill-suited to such scenarios and calls for the articulation of a theory of joint or shared liability responsive to distributed technological environments.
3. **National Sovereignty and Infrastructural Dependence:**
   The prospective reliance on foreign standards and platforms, including those developed under the auspices of the W3C, coupled with the risk of service disruption arising from international sanctions, places the operationalization of DID in tension with the constitutional mandate to safeguard national independence as articulated in Article 152 of the Constitution. This concern accentuates the necessity of developing a domestically governed blockchain infrastructure capable of hosting indigenous DID solutions.
4. **Jurisprudential Constraints:**
   From the standpoint of Shiite jurisprudence, authentication predicated exclusively on cryptographic trust requires either an expansive hermeneutic reinterpretation or authoritative

advisory opinions (*fatāwā*) to ensure compatibility with the doctrine of *ḥifẓ al-niẓām* (preservation of public order) and with the recognition of documentary evidence grounded in *bayyina* endorsed by sovereign authority. Absent such interpretive accommodation, DID-based instruments remain jurisprudentially contested.

5. **Prospects for Institutional Convergence:** Comparative analysis of international practices suggests that functional convergence is achievable through the integration of DID frameworks with existing domestic mechanisms-such as the Shahkar system for preliminary identity verification-and the deployment of Verifiable Credentials (VCs). Under such an arrangement, DID-enabled records could acquire the status of "official digital instruments," provided that the Organization for the Registration of Deeds and Properties continues to operate as the recognized authority for initial identity attestation.

Conclusion and Policy Recommendations

The foregoing analysis substantiates the existence of a paradigmatic tension between legal centralization and technological decentralization. Legal certainty within Iran's system of official documentation has historically been anchored in state-centric control, and the accommodation of DID necessitates a dynamic and evolutionary interpretation of existing statutes aimed at recognizing the intrinsic legal validity of digital instruments. Concurrently, DID's capacity for selective disclosure and enhanced privacy protection aligns with the guarantees enshrined in Article 22 of the Constitution and with emerging data governance norms.

In light of these findings, the study advances the following legislative and institutional recommendations to facilitate the localization of DID and to mitigate its attendant legal challenges:

1. **Statutory Reform of the Registration Law:** The enactment of supplementary provisions defining an "official decentralized signature" and a "digital

official instrument" grounded in DID identifiers and Verifiable Credentials, thereby conferring initial judicial probative value upon such records.

2. **Distributed Liability Framework:**
   The formulation of a statutory regime establishing joint and several liability among users, credential issuers, and the state-acting as the primary identity attester-in instances of security breaches or resulting harm, in conformity with the proposed Personal Data Protection legislation.
3. **Sovereign Technological Infrastructure:**
   The development and formal legal recognition of a national blockchain as the authoritative sovereign platform for hosting domestically issued DID identifiers, ensuring technological autonomy and resilience against sanctions-induced disruptions.
4. **Regulatory Sandbox Mechanism:**
   The establishment of a regulatory sandbox to permit the controlled experimentation and evaluation of DID-based registration and authentication services, insulated from the immediate risk of judicial invalidation.
5. **Judicial Capacity Building:**
   The systematic training of judges and forensic experts to enhance their competence in assessing advanced digital evidence, including zero-knowledge proofs (ZKPs) and Verifiable Credentials (VCs), within adjudicative processes.

چالش‌های حقوقی احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران

(دریافت: ۱۴۰۳/۰۷/۱۷ پذیرش: ۱۴۰۴/۰۸/۲۶)

علی احمدی
دانشجوی دکتری حقوق خصوصی، دانشکدهٔ علوم انسانی، واحد یاسوج، دانشگاه آزاد اسلامی، کهگیلویه و بویراحمد، ایران. (نویسندهٔ مسئول)
Email : a.ahmadi5667@iau.ac.ir

دکتر حمیدرضا رستمی
استادیار، گروه حقوق خصوصی، دانشکدهٔ علوم انسانی، واحد یاسوج، دانشگاه آزاد اسلامی، کهگیلویه و بویراحمد، ایران.
Email : hrostami1962@yahoo.com

دکتر نازنین عباس‌پور ایکدر
دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
Email : nazanin.abbaspoorekder@iau.ir

چکیده:
احراز هویت غیرمتمرکز (DID)، که بر پایهٔ فناوری دفترکل توزیع‌شده (DLT) و استانداردهای کنسرسیوم جهانی وب (W3C) نظیر اعتبارات قابل تأیید (VC) توسعه یافته، نویدبخش یک تحول بنیادین در نظام اسناد رسمی و توثیق کشور ایران است. با این حال، اجرای این الگو با چالش‌های حقوقی عمیق و ساختاری مواجه است. این پژوهش با اتخاذ یک رویکرد تحلیلی ـ تطبیقی و مبنایی، ابتدا به تبیین و تحلیل تضاد بنیادین میان اصل حاکمیت هویتی شخص (SSI) به‌عنوان شالودهٔ احراز هویت غیرمتمرکز و اصل انحصار حاکمیت دولت در احراز هویت و توثیق اسناد در نظام حقوقی ایران می‌پردازد. این تعارض به‌طور خاص در مادهٔ ۱۲۸۷ قانون مدنی و مادهٔ ۲۲ قانون ثبت اسناد و املاک متبلور می‌شود. سؤالات محوری تحقیق بر

فصلنامه نوآوری حقوقی
پژوهشکده نوآوری حقوقی
تابستان ۱۴۰۴، دوره دوم، شماره ۲
www.journallir.com

شناسایی دقیق موانع حقوقی و فقهی DID و ارائهٔ مدل‌های بومی‌سازی جهت سازگاری آن با فقه شیعه متمرکز است. یافته‌های تحلیل فقهی و حقوقی نشان می‌دهد که الگوی DID، علی‌رغم توانایی در ارتقای کارایی و حفظ حریم خصوصی اشخاص، به‌دلیل عدم انطباق با معیارهای حجیت و توثیق در فقه شیعه و همچنین ساختار قانون‌محور اسناد رسمی، با موانع اساسی روبه‌روست. ازجمله این موانع می‌توان به عدم اعتبار قضائی، ابهام در تعیین مسئولیت حقوقی (به‌ویژه در فرض تقصیر در نگهداری کلید خصوصی، مطابق با مادهٔ ۱ قانون مسئولیت مدنی، ۱۳۳۹ و قواعد فقهی اتلاف و تسبیب) و ریسک وابستگی به زیرساخت‌های خارجی در صورت تحریم‌ها (با توجه به تأکید اصل ۱۵۲ قانون اساسی بر حفظ استقلال) اشاره کرد. تحلیل تطبیقی با مدل‌های موفق جهانی نظیر نظام احراز هویت الکترونیکی و خدمات اعتماد در اتحادیهٔ اروپا و اقامت الکترونیکی استونی، امکان بومی‌سازی را از طریق طراحی مدل‌های ترکیبی که نقش نهادهای رسمی را در تأیید اولیه هویت حفظ می‌کنند، تأیید می‌نماید. پیشنهادات شامل اصلاح قانون ثبت برای تعریف «امضای غیرمتمرکز رسمی»، ایجاد sandbox نظارتی، آموزش قضات و توسعهٔ بلاکچین ملی است.

واژگان کلیدی: احراز هویت غیرمتمرکز (DID)، اسناد رسمی، نظام حقوقی ایران، حاکمیت هویتی شخص (SSI)، دفتر کل توزیع‌شده، فقه شیعه.

مقدمه

تحولات شتابان فناوری‌های رقومی[1] در دهۀ اخیر، بنیان بسیاری از نهادهای سنتی حقوقی را با چالش‌های نوینی مواجه ساخته است. در این میان، فناوری دفترکل توزیع‌شده (DLT)[2] و سازوکار احراز هویت غیرمتمرکز (DID)[3] با ایجاد الگوهای نوینی از اعتماد، در حال بازتعریف روابط اجتماعی، اقتصادی و به‌ویژه حقوقی هستند. نظام اسناد رسمی ایران، که در حقوق ایران بر مبنای اعتبار و رسمیت ناشی از تنظیم در دفاتر رسمی و تحت نظارت حاکمیتی استوار است، اکنون با یک پرسش بنیادین مواجه است: آیا می‌توان سازوکار خودحاکمیتی هویت (SSI)[4] را در چارچوب ساختار متمرکز حقوقی و مبانی فقه امامیه ادغام کرد، بی‌آنکه اعتبار قضائی و امنیت عمومی مخدوش شود؟

احراز هویت غیرمتمرکز با فراهم آوردن امکان کنترل مستقیم داده‌های هویتی توسط اشخاص و حذف واسطه‌های نهادی (که در ادبیات حقوقی به مفهوم کاهش تصدی‌گری دولت نیز تعبیر می‌شود)، ظرفیت‌های قابل توجهی برای ارتقای حریم خصوصی (با تأکید بر حق کنترل فرد بر اطلاعات شخصی) و کاهش هزینه‌های اداری را در خود نهفته دارد. این ظرفیت‌ها به‌ویژه در حوزه‌هایی نظیر ثبت احوال، ثبت املاک و مستغلات و اسناد تجاری الکترونیکی اهمیتی مضاعف می‌یابد. با این حال، چارچوب حقوقی موجود ایران ـ که براساس مادۀ ۱۲۸۷ قانون مدنی، سند رسمی را به تنظیم نزد مأمور رسمی صالح محدود کرده و طبق مادۀ ۲۲ قانون ثبت اسناد و املاک مصوب ۱۳۱۰، اعتبار مالکیت را منوط به ثبت در دفاتر دولتی می‌داند ـ با ماهیت غیرمتمرکز[5] و عاری از مرجع واسط بودن احراز هویت غیرمتمرکز (DID) در تعارض ساختاری قرار می‌گیرد.

از منظر فقهی و حقوقی، اعتبار اثباتی اسناد در نظام حقوقی ایران بر مبانی‌ای همچون حجیت بیّنه، اصل صحت عقود و قاعدۀ ید مبتنی است. در حالی که احراز هویت غیرمتمرکز (DID) با حذف نقش مرجع رسمی توثیق و اتکای صرف به امضاهای رمزنگاری‌شده[6]، پرسش‌های نوینی را دربارۀ حجیت شرعی، قابل استناد بودن در محاکم و انطباق با قواعدی نظیر مبانی فقهی ضمان (مسئولیت) در صورت جعل یا سوءاستفاده ایجاد می‌کند. این موارد نیازمند تفسیر موسع از قواعد فقهی توثیق و مسئولیت است.

1. digital technologies
2. distributed ledger technology
3. decentralized identity
4. self-sovereign identity
5. permissionless
6. cryptographic signatures

در چنین بستری، مسئلهٔ محوری این پژوهش آن است که چالش‌های حقوقی کلیدی احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران کدام‌اند و آیا از طریق تفسیر هدفمند قوانین موجود و تدوین مقررات مکمل، امکان انطباق این الگو با قوانین موضوعه و اصول فقه امامیه وجود دارد یا خیر.

پرسش‌های اساسی بدین شرح‌اند:

نخست، تضاد احراز هویت غیرمتمرکز (DID) با اصول بنیادین قانون ثبت اسناد و املاک مصوب ۱۳۱۰ و مفاهیم «امضای مطمئن» و «سند الکترونیکی قابل استناد» در قانون تجارت الکترونیکی مصوب ۱۳۸۲ تا چه حد جدی است و چگونه می‌توان از طریق تفسیر حقوقی این تضاد را برطرف ساخت؟

دوم، آیا سازوکارهای غیرمتمرکز با مبانی فقه شیعه و اصول قانون اساسی ـ ازجمله اصل چهل و چهارم (۴۴) درخصوص نقش نظارتی دولت و اصل یکصد و پنجاه و دوم (۱۵۲) در حفظ استقلال ملی از زیرساخت‌های خارجی ـ سازگاری دارند؟

سوم، چه راهکارهای تقنینی یا اجرایی برای بومی‌سازی احراز هویت غیرمتمرکز (DID) و تدوین مدل‌های هیبریدی (ترکیبی) که متضمن نظارت حاکمیتی باشد، در ایران قابل تصور است؟

فرضیهٔ اصلی آن است که احراز هویت غیرمتمرکز (DID)، هرچند از منظر کارآمدی فنی و ارتقای حریم خصوصی مزایای انکارناپذیری دارد، اما در ساختار کنونی حقوقی و فقهی ایران با موانع بنیادینی همچون مشکل اثبات و عدم قابلیت پذیرش به‌عنوان دلیل رسمی در محاکم، ابهام در مسئولیت مدنی (ضمان) و چالش‌های ناشی از فقدان قانونگذاری صریح مواجه است. با وجود این، با اعمال اصلاحات تدریجی و مبتنی بر مصلحت در قوانین ثبت، تجارت الکترونیکی و مقررات حفاظت از داده‌ها، و نیز طراحی مدل‌های ترکیبی که تلفیقی از نظارت حاکمیتی (حفظ نقش سازمان ثبت اسناد) و آزادی کاربر باشد، می‌توان امکان همگرایی احراز هویت غیرمتمرکز (DID) با نظام اسناد رسمی ایران را فراهم ساخت.

اهداف این مقاله شامل: تبیین مبانی مفهومی احراز هویت غیرمتمرکز (DID)، تحلیل چالش‌های حقوقی عمیق آن در چارچوب قوانین ایران، بررسی تطبیقی تجربه‌های موفق جهانی (مانند مقررات احراز هویت الکترونیکی و خدمات اعتماد (eIDAS) در اتحادیهٔ اروپا و نظام هویت رقومی[1] استونی) و ارائهٔ پیشنهادات اجرایی و تقنینی برای بومی‌سازی این فناوری در ایران است. این اهداف با هدف پر کردن خلأ ادبیات حقوقی داخلی دربارهٔ DID دنبال می‌شود، چراکه اغلب پژوهش‌های موجود بر جنبه‌های صرفاً فنی تمرکز دارند.

1. digital identity

روش تحقیق مبتنی بر رویکرد توصیفی ـ تحلیلی است و از طریق مطالعهٔ قوانین ایران، اسناد فنی بین‌المللی (مانند اسناد فنی کنسرسیوم جهانی وب (W3C)) و تحلیل کیفی داده‌ها پیش می‌رود. همچنین از روش تطبیقی برای بررسی تجارب بین‌المللی و استخراج الگوهای سازگار با بستر حقوقی و فقهی ایران بهره گرفته می‌شود.

ساختار مقاله به شرح زیر تنظیم شده است: بخش دوم به مبانی نظری و فنی احراز هویت غیرمتمرکز (DID) اختصاص دارد؛ بخش سوم نظام حقوقی اسناد رسمی ایران و مبانی فقهی آن را مرور می‌کند؛ بخش چهارم چالش‌های حقوقی را براساس مواد قانونی تحلیل می‌کند؛ بخش پنجم تحلیل تطبیقی و الگوهای جهانی را ارائه می‌دهد؛ بخش ششم راهکارها و پیشنهادات تقنینی را مطرح می‌سازد؛ و درنهایت، نتیجه‌گیری به جمع‌بندی یافته‌ها و پیشنهاد مسیرهای آتی پژوهش می‌پردازد. این ساختار، انسجام منطقی از توصیف به تحلیل عمیق و ارائهٔ راهکار مبتنی بر قانون و فقه را تضمین می‌کند.

۱. مبانی نظری احراز هویت غیرمتمرکز (DID)

احراز هویت، همواره یکی از ارکان اساسی در برقراری روابط حقوقی و اقتصادی بوده است. در سنت حقوقی ایران و بسیاری از نظام‌های حقوقی مبتنی بر حقوق رومی ـ ژرمنی، این فرایند بر مبنای شناسایی فیزیکی اشخاص و استفاده از اسناد مکتوب یا رقومی[1] تحت نظارت و توثیق مراجع رسمی حاکمیتی استوار است (بی‌جانی و امینی‌نیا، ۱٤۰۰). با ظهور تحولات گسترده در فناوری‌های نوین، به‌ویژه دفاتر کل توزیع‌شده (DLT)، الگوهای جدیدی برای مدیریت هویت شکل گرفت که برجسته‌ترین و ساختارشکن‌ترین آن‌ها، احراز هویت غیرمتمرکز (DID) است.

۱-۱. تعریف و ماهیت احراز هویت غیرمتمرکز (DID): پارادایم تغییر حاکمیت

احراز هویت غیرمتمرکز (DID) به‌عنوان یک سازوکار نوین شناسایی، امکان مدیریت کامل هویت رقومی را بدون نیاز به واسطه‌های متمرکز یا نهادی واسط[2] فراهم می‌کند (Das et al., 2022). بر اساس این الگو، هر فرد یا نهاد حقوقی دارای یک شناسه غیرمتمرکز[3] است که بر بستر شبکه‌های توزیع‌شده و با استفاده از رمزنگاری کلید عمومی[4] ایجاد و مدیریت می‌شود.

1. digital
2. intermediaries
3. decentralized identifier
4. public key cryptography

تفسیر حقوقی ماهیت احراز هویت غیرمتمرکز (DID): این شناسه، مستقل از نهادهای صادرکنندهٔ سنتی هویت (مانند سازمان ثبت احوال) عمل می‌کند و مالک آن،[1] اختیار تام و انحصاری در کنترل داده‌های هویتی و اشتراک‌گذاری انتخابی آن‌ها را دارد. بدین ترتیب، احراز هویت غیرمتمرکز (DID) از یک سو به اصل «خودحاکمیتی هویت (SSI)»[2] تحقق می‌بخشد و از سوی دیگر، وابستگی حقوقی و عملیاتی به نهادهای ثبت مرکزی را کاهش می‌دهد. این انتقال حاکمیت از دولت به فرد، اصلی‌ترین منبع تعارض احراز هویت غیرمتمرکز (DID) با نظام متمرکز اسناد رسمی ایران است.

۱-۲. اصول بنیادین احراز هویت غیرمتمرکز (DID) و تعارض آن با مبانی توثیق دولتی

اصول کلیدی احراز هویت غیرمتمرکز (DID) که در استانداردهای بین‌المللی مانند کنسرسیوم جهانی وب (W3C)[3] تدوین شده‌اند، بنیان‌های چالش‌های حقوقی را شکل می‌دهند:

۱.کنترل کاربر بر داده‌ها (مالکیت داده): افراد مالک نهایی داده‌های هویتی خود بوده و می‌توانند تصمیم بگیرند چه اطلاعاتی را، در چه زمانی و با چه شخصی به اشتراک بگذارند (Shitharth et al., 2023). این اصل با رویکرد حاکمیتی بر داده‌ها در قوانین ایران، نظیر مقررات سازمان ثبت اسناد و املاک، که داده‌های هویتی و مالکیتی را جزو اسناد عمومی و تحت حفاظت دولت می‌داند، تضاد دارد (یعقوبی و همکاران، ۱۴۰۳).

۲.غیرمتمرکز بودن (عدم وجود مرجع توثیق): صدور، مدیریت و ابطال هویت به‌جای تمرکز در دست نهادهای مرکزی، بر بستر شبکه‌های توزیع‌شده صورت می‌گیرد. این اصل با تعریف سند رسمی در مادهٔ ۱۲۸۷ قانون مدنی که منوط به تنظیم نزد «مأمور رسمی» است و همچنین با مبانی فقهی «توثیق» که نیازمند مرجعیت یا بیّنهٔ مورد تأیید حاکمیت است، مستقیماً تعارض می‌یابد.

۳. قابلیت تأیید رمزنگاری‌شده (جایگزینی امضای مرجع با رمز): اصالت داده‌ها و هویت از طریق امضاهای رمزنگاری و الگوریتم‌های رمزنگاری تضمین می‌شود (Saeidi Aghdam et al., 2023)، نه از طریق مُهر و امضای مأمور رسمی. اگرچه قانون تجارت الکترونیکی ۱۳۸۲، امضای الکترونیکی مطمئن را به رسمیت شناخته است (مستنبط از مواد ۷ و ۱۰)، اما احراز هویت غیرمتمرکز (DID)، یک قدم فراتر رفته و مرجعیت صادرکننده را نیز غیرمتمرکز می‌کند که این امر، اعتبار اثباتی (حجیت)

1. subject
2. self-sovereign identity
3. world wide web consortium

آن را در مواجهه با مادۀ ۱۲۹۱ قانون مدنی زیر سؤال می‌برد.

٤.حفظ حریم خصوصی (افشای انتخابی): کاربران می‌توانند صرفاً بخش‌های ضروری و حداقلی از داده‌های خود را افشا کنند[1]؛ مثلاً تنها تأیید کنند که بالای ۱۸ سال دارند، بدون اینکه تاریخ تولد دقیق خود را فاش نمایند. این امر ریسک نقض حریم خصوصی را به‌شدت کاهش می‌دهد.

۱-۳. جایگاه احراز هویت غیرمتمرکز (DID) در معماری هویت دیجیتال

احراز هویت غیرمتمرکز (DID) نمایانگر آخرین مرحلۀ تحول در معماری هویت رقومی است که شامل مدل‌های زیر می‌شود:

۱. مدل متمرکز: هویت کاملاً توسط دولت یا نهادهای دولتی صادر و کنترل می‌شود (مانند ثبت احوال یا سیستم‌های بانکی سنتی).

۲. مدل فدرال یا توزیع‌شدۀ نسبی: هویت توسط نهادهای خصوصی یا دولتی صادر می‌شود، اما تحت یک استاندارد یکپارچه، قابلیت انتقال و استفاده بین نهادها را دارد (مانند نظام‌های ورود واحد[2]).

۳. مدل غیرمتمرکز: حداکثر اختیار و کنترل به شخص واگذار می‌شود و زیرساخت توثیق، غیرمتمرکز است.

این گذار نشان‌دهندۀ یک رقابت پارادایمی میان حق دولت در احراز هویت عمومی و حق فرد در کنترل داده‌های شخصی است.

۱-۴. مزایا و چالش‌های ذاتی احراز هویت غیرمتمرکز (DID)

مزایای اصلی احراز هویت غیرمتمرکز (DID) که از نظر حقوقی قابل توجه‌اند، شامل: افزایش اعتماد در تراکنش‌های دیجیتال، کاهش هزینه‌های بوروکراتیک و اداری، مقابلۀ مؤثرتر با جعل اسناد و هویت، و تسهیل تبادلات فرامرزی[3] است. در حوزۀ اسناد رسمی، احراز هویت غیرمتمرکز (DID) می‌تواند به‌عنوان ابزاری قدرتمند برای اعتبارسنجی دیجیتال سریع و تکمیل فرایند ثبت سنتی عمل کند.

چالش‌های حقوقی ذاتی احراز هویت غیرمتمرکز (DID): در کنار مزایا، احراز هویت غیرمتمرکز (DID) دارای چالش‌های حقوقی عمیق است که نیازمند پاسخ‌های قانونی است؛ ازجمله:

---

1. selective disclosure
2. single sign-on
3. cross-border transactions

۱. عدم وجود چارچوب حقوقی شفاف: فقدان قانون صریح درخصوص اعتبار شناسهٔ غیرمتمرکز به عنوان دلیل اثباتی.

۲. ابهام در مسئولیت مدنی (ضمان): عدم وضوح درمورد مسئولیت مدنی در صورت بروز خطا، جعل یا نقض امنیت. از آنجا که مرجع مرکزی وجود ندارد، تعیین مسبب و انتساب تقصیر براساس مادهٔ ۱ قانون مسئولیت مدنی دشوار خواهد بود.

۲. نیاز به زیرساخت‌های فنی و قضائی پیشرفته: نیاز به آموزش قضات و کارشناسان در پذیرش ادلهٔ دیجیتال پیچیده (لطیف‌زاده و قبولی درافشان، ۱۴۰۲).

جمع‌بندی این بخش آن است که احراز هویت غیرمتمرکز (DID) نه صرفاً یک فناوری، بلکه یک پارادایم حقوقی ـ اجتماعی نوین در مدیریت هویت است که اصول آن با مفروضات تمرکزگرا و قواعد فقهی سنتی توثیق در نظام اسناد رسمی ایران در تعارض بنیادین قرار دارد. لذا، بررسی دقیق این مبانی، پیش‌شرط تحلیل چالش‌های حقوقی و سازوکارهای بومی‌سازی در بخش‌های آتی است.

۲. مروری بر نظام حقوقی و مبانی فقهی اسناد رسمی در ایران

نظام حقوقی اسناد رسمی در ایران یکی از ستون‌های اصلی تضمین امنیت معاملات و تثبیت حقوق مالکیت محسوب می‌شود. این نظام، بر پایهٔ قوانین مدنی و ثبتی و با تأکید صریح بر نظارت متمرکز دولتی بنا شده است. هدف بنیادین این ساختار، پیشگیری از تعارض مالکیت‌ها، جلوگیری از جعل و حمایت از اعتبار اسناد است که از منظر فقهی با هدف قطع نزاع و تأمین عدالت همسوست. با وجود این، ورود فناوری‌های نوین و الزامات جهانی، به‌ویژه پس از قانون الزام به ثبت رسمی معاملات اموال غیرمنقول (مصوب ۱۴۰۴/۱۴۰۳)، این نظام را به سمت رقومی شدن[1] و تحول نهادی سوق داده است.

۲-۱. مبانی قانونی و استنادات حقوقی

زیربنای حقوقی نظام اسناد رسمی ایران از سه منبع اصلی تشکیل شده که هر سه با فلسفهٔ تمرکز در توثیق در تعارض جدی با احراز هویت غیرمتمرکز (DID) هستند:

۱. قانون ثبت اسناد و املاک (مصوب ۱۳۱۰ با اصلاحات)

این قانون، به‌ویژه در مادهٔ ۲۲، اصل «اعتبار مطلق مالکیت ثبت‌شده» را مستقر کرده است. این حکم به این معناست که مالکیت رسمی تنها از طریق ثبت در دفتر املاک (که مرجعی رسمی و دولتی است) محقق می‌شود.

1. digitalization

این رویکرد در مبانی فقهی «حجیت بیّنه» و «اصالت سند مکتوب» ریشه دارد که جایگزین شهادت شفاهی در اثبات مالکیت شده است. هدف اصلی، عمل به قاعدهٔ فقهی «منع غرر» و تقویت «قاعدهٔ لزوم» در معاملات است تا امنیت اقتصادی جامعه تضمین شود. تمرکز حاکمیتی بر ثبت، لازمهٔ اعتبار سند رسمی است.

۲. قانون مدنی (مصوب ۱۳۰۷ با اصلاحات) و قانون دفاتر اسناد رسمی (مصوب ۱۳۵۴)

این قوانین، جایگاه سردفتران را به‌عنوان مأموران عمومی (نه واسطهٔ خصوصی) تثبیت کرده و تنظیم اسناد رسمی را منوط به حضور آنان و رعایت تشریفات خاص می‌دانند. مادهٔ ۱۲۸۷ قانون مدنی بر تعریف سند رسمی به‌عنوان سندی که توسط مأموران رسمی در حدود صلاحیت» تنظیم شده، تأکید می‌کند. در این چارچوب، اسنادی که فاقد امضا و مهر سردفتر هستند، سند عادی تلقی شده و حجیت و اعتبار اثباتی (مادهٔ ۱۲۹۱ ق.م.) کم‌تری دارند. این ساختار نقش واسط حاکمیتی (سردفتر) را حیاتی می‌داند، در حالی که احراز هویت غیرمتمرکز (DID) این واسط را حذف می‌کند.

۳. قانون تجارت الکترونیک (مصوب ۱۳۸۲)

این قانون پلی میان حقوق سنتی و فضای رقومی ایجاد کرده و برای نخستین‌بار امضای الکترونیکی مطمئن را در کنار امضای دستی معتبر شناخته است (مادهٔ ۷ و مادهٔ ۱۰). هرچند این قانون گامی در جهت پذیرش فناوری است، اما اعتبار امضای الکترونیکی در آن به زیرساخت‌های متمرکز (مانند مراکز صدور گواهی امضای الکترونیکی) وابسته است. درنتیجه، کاربرد آن در حوزهٔ اسناد رسمی ملکی به‌دلیل الزامات حضور فیزیکی و تشریفات خاص توثیق، محدود باقی مانده است. احراز هویت غیرمتمرکز (DID) با زیر سؤال بردن مرکز صدور، از چارچوب مادهٔ ۱۰ قانون تجارت الکترونیک فراتر می‌رود.

۲-۲. چالش‌های ساختاری: تعارض اصول کلیدی نظام اسناد رسمی با احراز هویت غیرمتمرکز (DID)

اصول بنیادین حاکم بر نظام اسناد رسمی ایران، که در حقوق خصوصی متمرکز و فقه امامیه ریشه دارند، به‌طور مستقیم چالش‌های ساختاری عمیقی را در برابر پذیرش احراز هویت غیرمتمرکز (DID) ایجاد می‌کنند. این تعارضات، نشان‌دهندهٔ تفاوت بنیادین میان تشریفات توثیق سنتی و مکانیزم اثبات رمزنگاری‌شده در فناوری احراز هویت غیرمتمرکز (DID) است.

۲-۲-۱. اصل لزوم حضور فیزیکی و احراز قصد و رضای طرفین

نظام اسناد رسمی ایران بر لزوم حضور فیزیکی طرفین معامله در محل دفترخانه و ابراز ایجاب و قبول در حضور سردفتر تأکید دارد. این تشریفات، در فقه معاملات و اصل «لزوم ایجاب و قبول لفظی یا فعلی در عقود» ریشه دارد که هدف غایی آن، احراز قطعی و بدون شبهۀ قصد و رضای آزاد متعاملین است. سردفتر به عنوان مأمور رسمی، نه‌تنها وجود اراده، بلکه صحت اراده را نیز گواهی می‌دهد. احراز هویت غیرمتمرکز (DID) این فرایند را به تأیید صرفاً رمزنگاری‌شده[1] و کاملاً غیرحضوری تقلیل می‌دهد. در این مدل، اثبات هویت و ارادۀ صرفاً از طریق کلید خصوصی کاربر انجام می‌شود. اگرچه این مکانیزم از نظر فنی غیرقابل انکار است، اما از منظر تشریفات قانونی ایران، فقدان گواهی حضور فیزیکی سردفتر، صحت و قطعیت اراده (قصد و رضا) را زیر سؤال می‌برد، زیرا احراز هویت غیرمتمرکز (DID)جایگزینی برای تشریفات فقهی ـ حقوقی نظیر حضور فیزیکی ارائه نمی‌دهد. بنابراین، حذف حضور فیزیکی می‌تواند سند رقومی مبتنی بر احراز هویت غیرمتمرکز (DID) را از درجۀ سند رسمی به سند عادی تنزل دهد.

۲-۲-۲. اصل امضای رسمی و حجیت ناشی از نظارت دولتی

دومین اصل بنیادین، حجیت قانونی سند است که مستقیماً از امضای مأمور رسمی (سردفتر) نشئت می‌گیرد. این امضا، سند را براساس مادۀ ۱۲۸۷ قانون مدنی رسمیت می‌بخشد و آن را از نظر اثباتی به قوۀ قهریۀ دولتی متصل می‌کند (مادۀ ۱۲۹۱ قانون مدنی: اسناد رسمی حجت هستند). این امر با قواعد فقهی نظیر «امارۀ ید» و «أصاله‌ی الصحه» هم‌پوشانی دارد؛ سند رسمی امارۀ صحت و مالکیت تلقی می‌شود و بار اثبات نقض آن بر دوش مدعی است. احراز هویت غیرمتمرکز (DID) اساساً این حجیت ناشی از نظارت دولتی را حذف کرده و آن را به یک توثیق شبکه‌ای مبتنی بر اعتماد رمزنگاری‌شده تبدیل می‌کند. در سیستم DID/SSI، اعتبار از طریق صادرکننده‌ها[2] توزیع می‌شود، نه یک مقام متمرکز حاکمیتی. حذف امضای مأمور رسمی به معنای حذف «حجت دولتی» است. درنتیجه، سند تولیدشده در زیرساخت احراز هویت غیرمتمرکز (DID)، در نظام حقوقی ایران فاقد جایگاه اثباتی رسمی است و صرفاً به‌عنوان یک دلیل الکترونیکی (مطابق مادۀ ۷ قانون تجارت الکترونیک) پذیرفته می‌شود که اعتبار آن در صورت انکار، نیازمند اثبات مضاعف در محاکم خواهد بود؛ در حالی که سند رسمی نیازی به اثبات اولیه ندارد.

---

1. cryptographic
2. issuers

۲-۲-۳. اصل مسئولیت مدنی و کیفری متمرکز و قابل انتساب

نظام اسناد رسمی ایران، چارچوب قوی برای مسئولیت متمرکز فراهم می‌کند. هرگونه جعل، تزویر یا تنظیم ناصحیح سند، علاوه بر مسئولیت مدنی برای جبران خسارت (بر اساس مادهٔ ۱ قانون مسئولیت مدنی، ۱۳۳۹)، مستوجب مجازات کیفری است (مواد ۵۲۳ به بعد قانون مجازات اسلامی)، در اینجا، سردفتر یا عامل خسارت یک شخص حقیقی یا حقوقی مشخص است که تقصیر مستقیماً به او قابل انتساب می‌باشد. ساختار توزیع‌پذیر[1] زیرساخت احراز هویت غیرمتمرکز (DID)، تعیین مسبب و انتساب تقصیر را در صورت بروز جعل (مانند هک کلید خصوصی کاربر) یا خطا در زیرساخت بلاکچین، بسیار دشوار می‌کند (عاکفی قاضیانی و همکاران، ۱۴۰۱). برای اجرای مادهٔ ۱ قانون مسئولیت مدنی، اثبات رابطهٔ سببیت و انتساب تقصیر به یک شخص حقوقی یا حقیقی معین، امری ضروری است. در شبکهٔ احراز هویت غیرمتمرکز (DID)، مسئولیت می‌تواند میان کاربر (به‌دلیل حفظ ناصحیح کلید)، صادرکنندهٔ اعتبار، یا حتی توسعه‌دهندهٔ پلتفرم توزیع شود. این ابهام در تعیین «عامل خسارت»، بزرگ‌ترین چالش را در جبران خسارت کاربران آسیب‌دیده ایجاد می‌کند و نیازمند تعریف یک نظریهٔ جدید مسئولیت مشترک[2] متناسب با فناوری توزیع‌شده است.

۲-۳. نقش نهادها و تحولات اخیر (تمرکزگرایی در مقابل غیرمتمرکزسازی)

نهادهای کلیدی ایران، یک نظام کاملاً متمرکز و سلسله‌مراتبی ایجاد می‌کنند که با فلسفهٔ غیرمتمرکز احراز هویت غیرمتمرکز (DID)، در تعارض بنیادین است:

سازمان ثبت اسناد و املاک کشور: با نقش محوری در تثبیت مالکیت و حرکت به سمت حدنگاری[3] و الکترونیکی شدن کامل فرایندها تا سال ۱۴۰۴، همچنان بر نظارت کامل دولتی تأکید دارد.

سازمان ثبت احوال کشور: به‌عنوان مرجع انحصاری اسناد هویتی، مبنای اولیهٔ احراز هویت طرفین معاملات را فراهم می‌آورد.

قوهٔ قضائیه: از طریق نظارت بر دفاتر و حل دعاوی ثبتی، ضمانت اجرای قضائی برای اعتبار رسمی اسناد فراهم می‌کند.

گرچه قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۱) با تأکید بر محرمانگی و امنیت داده‌ها، بستر

---

1. distributed
2. joint liability
3. cadastre

حقوقی برای حفاظت از داده‌های شخصی را فراهم کرده و سامانه‌هایی نظیر ثنا در قوهٔ قضائیه از امضای رقومی استفاده می‌کنند، اما این تحولات همچنان در چارچوب مدل متمرکز حاکمیتی عمل می‌کنند. محدودیت جدی آنجاست که امضای دیجیتال در اسناد رسمی ملکی به‌طور کامل جایگزین امضای فیزیکی و حضور سردفتر نشده و خلأ قانونی در پذیرش الگوی احراز هویت غیرمتمرکز (DID)، به عنوان سند دارای حجیت رسمی همچنان پابرجاست.

جمع‌بندی این بخش، تأکیدی دوباره بر این حقیقت است که نظام اسناد رسمی ایران، با تکیه بر قوانین سنتی و اصول فقهی، امنیت حقوقی را در چارچوب تمرکزگرایی دولتی تضمین می‌کند، اما ورود فناوری‌های غیرمتمرکز مانند احراز هویت غیرمتمرکز (DID)، چالش‌های اساسی را متوجه این ساختار می‌سازد. تقابل میان «تمرکزگرایی حقوقی» و «غیرمتمرکزگرایی فناورانه» نقطهٔ کانونی بحث است که در بخش‌های بعدی (تحلیل چالش‌ها) مورد تحلیل عمیق قرار خواهد گرفت.

۳.کاربردهای بالقوهٔ احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران

احراز هویت غیرمتمرکز (DID)، به‌عنوان یک چارچوب حقوقی ـ فناوری مبتنی بر اصول خودحاکمیتی هویت (SSI)، پتانسیل تحول‌آفرینی در نظام اسناد رسمی ایران را دارد. چالش‌های سنتی این نظام، مانند تمرکزگرایی و ریسک جعل، در مواجهه با این فناوری به چالش کشیده می‌شوند.

احراز هویت غیرمتمرکز (DID)، می‌تواند بر پایهٔ نظریهٔ «اعتبار ذاتی سند»[1] عمل کند. اگرچه مادهٔ ۱۲۸۷ قانون مدنی سند رسمی را به تنظیم توسط «مأمور رسمی» محدود می‌کند، اما یک تفسیر موسع و تحولی از این ماده می‌تواند «اعتبارات قابل تأیید(VCs)»[2] را به‌مثابهٔ «سند یا امضای مأمور رقومی»[3] معتبر سازد. تحلیل حقوقی نشان می‌دهد که کاربرد احراز هویت غیرمتمرکز (DID)، با مادهٔ ۲۲ قانون ثبت اسناد و املاک مصوب ۱۳۱۰ (اعتبار مطلق مالکیت ثبت‌شده) همخوانی دارد، زیرا اثبات‌های رمزنگاری‌شدهٔ[4] آن، اصل «غیرقابل انکارپذیری»[5] را تقویت می‌کند. با این حال، تعارض با نظریهٔ «نظارت انحصاری دولتی بر اسناد» در فقه شیعه (نظیر فتاوای فقها در تحریرالوسیله، ۲/ ۴۵۶ مبنی بر

1. intrinsic validity of documents
2. verifiable credentials
3. digital agent
4. cryptographic proofs
5. non-repudiation

اعتبار سند بر پایهٔ شهادت و توثیق مأمور رسمی یا عادل) نیازمند تفسیر قضائی دیوان عالی کشور است تا احراز هویت غیرمتمرکز (DID)، را به عنوان مکمل، نه جایگزین، نظارت دولتی بپذیرد.

۳-۱. سناریوهای عملی: احراز هویت در ثبت ازدواج، املاک و گواهی‌های هویتی

سناریوهای عملی احراز هویت غیرمتمرکز (DID)، در نظام اسناد رسمی با نظریهٔ حقوقی «کارایی معاملات» در حقوق خصوصی همسوست که بر کاهش هزینه‌ها و تسریع فرایندها تأکید دارد.

۳-۱-۱. ثبت ازدواج و رضایت آگاهانه

در ثبت ازدواج، احراز هویت غیرمتمرکز (DID)، امکان احراز هویت غیرحضوری را از طریق اعتبارات قابل تأیید (مانند گواهی تجرد صادرشده توسط ثبت احوال) فراهم می‌کند. این تأیید با استفاده از اثبات‌های دانش صفر (ZKP)[1] و بدون افشای داده‌های حساس (مانند سن دقیق یا سابقه) صورت می‌گیرد.

رضایت آگاهانه را از طریق امضای رقومی[2] اثبات می‌کند که با مادهٔ ۷ قانون تجارت الکترونیک مصوب ۱۳۸۲ (اعتبار امضای الکترونیکی معادل دستی) همخوانی دارد. با این حال، تفسیر سخت‌گیرانه مادهٔ ۱۲۹۰ قانون مدنی (اعتبار اسناد رسمی در عقود) در کنار مادهٔ ۲۹ قانون دفاتر اسناد رسمی مصوب ۱۳۵۴ (لزوم حضور در دفتر ازدواج)، حاکی از تعارض است، زیرا عدم حضور فیزیکی می‌تواند سند را «عادی» تلقی کند.

براساس نظریهٔ «اعتبار خارجی سند» [3] که بر اثبات‌پذیری تأکید دارد، احراز هویت غیرمتمرکز (DID)، می‌تواند با ادغام در سامانهٔ ثبت ازدواج الکترونیک، این تعارض را حل کند و ریسک جعل (مذکور در مادهٔ ۵۲۳ قانون مجازات اسلامی) را کاهش دهد.

۳-۱-۲. انتقال املاک و تثبیت مالکیت

در انتقال املاک، احراز هویت غیرمتمرکز (DID)، توکن‌سازی[4] سند مالکیت را امکان‌پذیر می‌سازد، جایی که تغییرات مالکیت بر بستر دفتر کل توزیع‌شده ثبت شده و غیرقابل‌انکار است. این امر با نظریهٔ «تثبیت مالکیت»[5] در حقوق ملکی ایران و مادهٔ ۲۲ قانون ثبت سازگار است. تفسیر هدفمند مادهٔ ۱

1. zero-knowledge proofs
2. digital signature
3. extrinsic validity
4. tokenization
5. property stabilization theory

قانون ثبت (الزام ثبت رسمی برای نقل و انتقال) نشان می‌دهد که اعتبارات احراز هویت غیرمتمرکز (DID) می‌توانند به‌عنوان «سند رسمی رقومی» عمل کنند، مشروط به اتصال به سامانهٔ حدنگاری سازمان ثبت.

تعارض با مادهٔ ۲۲ قانون دفاتر اسناد رسمی مصوب ۱۳۵٤ (مسئولیت سردفتر در اعتباربخشی) نیازمند تفسیر اصل «مسئولیت توزیع‌شده»[1] در حقوق مدنی است. سردفتر در این مدل، صرفاً به‌عنوان «تأییدکنندهٔ هویت غیرمتمرکز» باقی مانده و مسئولیتش ذیل مادهٔ ۱ قانون مسئولیت مدنی مصوب ۱۳۳۹، متناسب با نقش جدید او در تأیید شناسهٔ DID تعریف می‌شود. اعتبارات احراز هویت غیرمتمرکز (DID)، می‌تواند دعاوی ابطال سند (مادهٔ ۱۹۰ قانون مدنی) را کاهش دهد و با قانون الزام به ثبت رسمی معاملات اموال غیرمنقول مصوب ۱۴۰۳ (مادهٔ ۱: ممنوعیت اعتبار اسناد عادی) همخوانی کامل داشته باشد.

۳-۱-۳. گواهی‌های هویتی و حریم خصوصی

برای گواهی‌های هویتی (مانند شناسنامهٔ الکترونیک)، احراز هویت غیرمتمرکز (DID)، اصل خودحاکمیتی را محقق می‌سازد که با نظریهٔ «حقوق شخصی هویت»[2] و اصل ۲۲ قانون اساسی (امنیت حقوق افراد) همسوست.

تحلیل مادهٔ ۱ قانون ثبت احوال مصوب ۱۳۵۵ (الزام ثبت هویت ملی) حاکی از آن است که احراز هویت غیرمتمرکز (DID)، می‌تواند گواهی‌ها را به صورت قابل تأیید[3] صادر کند. با این حال، تفسیر مادهٔ ٦ قانون جرائم رایانه‌ای (مسئولیت در نقض داده‌های هویتی) نشان می‌دهد که بدون حفاظت اثبات‌های دانش صفر، تعارض با اصل «حریم خصوصی» (مادهٔ ۴ قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱) ایجاد می‌شود. براساس نظریهٔ فقهی «حفظ نظام» (نظیر دیدگاه امام خمینی در الرساله، ۱/ ۲۹۸)، احراز هویت غیرمتمرکز (DID)، می‌تواند با فتوای مراجع (مانند آیت‌الله مکارم شیرازی، ۱۴۰۳ در جواز امضای رقومی در هویت) سازگار شود، زیرا حفظ هویت برای حفظ نظم اجتماعی یک ضرورت شرعی است که احراز هویت غیرمتمرکز (DID)، آن را با کارایی بیشتر تأمین می‌کند.

---

1. distributed liability
2. personal identity rights
3. verifiable

۳-۲. همگرایی با فناوری‌های موجود: بلاکچین ملی ایران و سامانهٔ شاهکار[۱]

همگرایی احراز هویت غیرمتمرکز (DID) با فناوری‌های موجود، بر پایهٔ نظریهٔ «ادغام فناوری ـ حقوق»[۲] استوار است که بر قابلیت تعامل[۳] برای حفظ اعتبار حقوقی تأکید دارد.

۱. بلاکچین ملی ایران: بلاکچین ملی، که در برنامهٔ ملی مربوطه تعریف شده، پتانسیل میزبانی احراز هویت غیرمتمرکز (DID) را دارد. تفسیر مادهٔ ۱ قانون تجارت الکترونیک (اعتبار سیستم‌های الکترونیکی ملی) نشان می‌دهد که این ادغام با اصل ۴۴ قانون اساسی (گسترش بخش خصوصی در اقتصاد) همخوانی دارد، زیرا بلاکچین ملی را می‌توان به‌عنوان «نهاد توثیق تعاونی» تفسیر کرد. تفسیر مادهٔ ۱۵۲ قانون اساسی (سیاست خارجی مستقل) حاکی از ضرورت مقابله با تحریم‌ها و عدم وابستگی به زیرساخت‌های خارجی است. از این رو، تعریف قانونی «بلاکچین ملی» به عنوان «سامانهٔ معتبر حاکمیتی»، برای رفع تعارض با مادهٔ ۱۲۹۲ قانون مدنی (اثبات اسناد خارجی) یک ضرورت تقنینی است.

۲. سامانهٔ شاهکار: سامانهٔ شاهکار که برای احراز هویت متمرکز عمل می‌کند، می‌تواند احراز هویت غیرمتمرکز (DID) را با تأمین هویت اولیه (تطبیق کد ملی و شمارهٔ موبایل) ادغام کند. از دیدگاه نظریهٔ «حفاظت داده‌های شخصی»[۴]، مشابه مقررات عمومی حفاظت داده‌های اتحادیهٔ اروپا (GDPR)، این ادغام با مادهٔ ۴ قانون مدیریت داده‌ها سازگار است، زیرا احراز هویت غیرمتمرکز (DID) از حداقل افشاگری[۵] استفاده می‌کند. تحلیل مادهٔ ۲۵ قانون جرائم رایانه‌ای (مجازات نقض داده‌ها) نشان می‌دهد که مسئولیت دولت (به عنوان صادرکنندهٔ اولیه) باید به مدل حاکمیت هویتی شخص (SSI) منتقل شود، که نیازمند تفسیر اصل «مسئولیت تضامنی» (مادهٔ ۱۳۵ قانون تجارت) است تا هم دولت و هم صادرکننده احراز هویت غیرمتمرکز (DID) در صورت نقض امنیتی، مسئول شناخته شوند. لایحهٔ حفاظت از داده‌های شخصی این همگرایی را تسهیل می‌کند.

---

۱. شبکهٔ احراز هویت کاربران، یک لایهٔ امنیتی قوی در دنیای دیجیتال است که با تطبیق دقیق اطلاعات هویتی، تأیید می‌کند که شخصی که از یک سرویس خاص استفاده می‌کند، دقیقاً همان فردی است که ادعا کرده است. از همین رو از بروز کلاهبرداری به روش‌های مختلف جلوگیری می‌کند. این سامانه به تدریج در اختیار دستگاه‌های اجرایی، سازمان‌ها و کسب‌وکارهای مختلف قرار گرفته و به‌عنوان یک ابزار ضروری برای احراز هویت و ایجاد اعتماد در فضای دیجیتال شناخته می‌شود.

2. techno-legal integration theory

3. interoperability

4. data protection theory

5. minimal disclosure

۳-۳. مزایای حقوقی احراز هویت غیرمتمرکز (DID)

مزایای حقوقی احراز هویت غیرمتمرکز (DID) بر پایهٔ نظریه «خصوصی‌سازی حقوق»[1] در حقوق اقتصادی استوار است که انتقال کنترل از دولت به افراد را توجیه می‌کند.

۱.افزایش کارایی و اقتصاد مقاومتی: افزایش کارایی با مادهٔ ۷ قانون تجارت الکترونیک (تسریع معاملات رقومی) همخوانی دارد و تحلیل نشان می‌دهد که احراز هویت غیرمتمرکز (DID) اصل «اقتصاد مقاومتی» (بند ۱۹ سیاست‌های ابلاغی ۱۳۹۲: بهره‌وری) را محقق می‌سازد. با این حال، تفسیر مادهٔ ۱ قانون اجرای سیاست‌های کلی اصل ۴۴ (جلوگیری از انحصار) حاکی از ضرورت نظارت بر پلتفرم‌های احراز هویت غیرمتمرکز (DID) برای جلوگیری از رقابت ناعادلانه است.

۲.کاهش فساد و شفافیت: کاهش فساد از طریق شفافیت دفتر کل توزیع‌شده با نظریهٔ «شفافیت در حقوق عمومی»[2] سازگار است و مادهٔ ۵۲۳ قانون مجازات اسلامی (جعل اسناد) را تقویت می‌کند. اما تعارض با اصل «حفظ نظام» در فقه (نظیر آیت‌الله سیستانی، منهاج‌الصالحین، ۲/ ۳۴۲) نیازمند فتوای مشورتی است که حدود نظارت حاکمیت در بلاکچین را مشخص سازد.

۳.همخوانی با اصل ۴۴: همخوانی با اصل ۴۴، احراز هویت غیرمتمرکز (DID) را به‌عنوان ابزاری برای خودحاکمیتی در حوزهٔ فناوری توجیه می‌کند و خصوصی‌سازی فناوری را تقویت می‌نماید؛ با وجود این، بدون اصلاح قانون و تعریف مسئولیت توزیع‌شده، ریسک‌های مدنی (مادهٔ ۱ قانون مسئولیت مدنی) افزایش می‌یابد.

۴. چالش‌های حقوقی احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران

ادغام احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران، علی‌رغم مزایای چشمگیر، با چالش‌های حقوقی عمیقی مواجه است. این چالش‌ها در تضاد ساختاری میان اصول غیرمتمرکزسازی فناوری و ساختار متمرکز و سنتی حقوق خصوصی ایران ریشه دارد.

تحلیل نظریهٔ دوگانگی[3]: این چالش‌ها بر پایهٔ نظریهٔ دوگانگی در حقوق رقومی قابل تحلیل است که بر تعارض میان اختیار فردی[4] و خودحاکمیتی هویتی[5] با قیمومت دولتی[6] و نظارت متمرکز بر اعتبار

1. privatization of rights theory
2. transparency theory
3. duality theory
4. autonomy
5. self-sovereign identity
6. paternalism

اسناد تأکید دارد. مادۀ ۱۲۸۷ قانون مدنی که سند رسمی را منوط به تنظیم نزد «مأمورین رسمی در حدود صلاحیت و طبق مقررات قانونی»می‌داند، پایه‌ای برای این تضاد فراهم می‌کند، زیرا احراز هویت غیرمتمرکز (DID) فاقد «مأمور رسمی» مرکزی است و بر اثبات رمزنگاری‌شده[1] تکیه دارد. تفسیر حقوقی این ماده، بر اساس دکترین تفسیر مُضیّق (تنگ) در حقوق مدنی ایران (ملهم از فقه امامیه)، احراز هویت غیرمتمرکز (DID) را به‌عنوان سند عادی تلقی می‌کند مگر آنکه با اصلاحات تقنینی (مانند لایحۀ پیشنهادی هویت رقومی) به سطح رسمی ارتقا یابد.

۴-۱. چالش اعتبار و اثبات‌پذیری: تضاد با اصل «اسناد رسمی»

تضاد احراز هویت غیرمتمرکز (DID) با اصل «اسناد رسمی» در مادۀ ۱۲۸۷ قانون مدنی؛ چالش اصلی اعتبار و اثبات‌پذیری احراز هویت غیرمتمرکز (DID) در تضاد میان اصل غیرمتمرکز آن (عدم وابستگی به واسطۀ مرکزی) و الزام قانونی به گواهی رسمی ریشه دارد. مادۀ ۱۲۸۷ قانون مدنی اعتبار اسناد رسمی را بر پایۀ تنظیم توسط مأمور رسمی (سردفتر یا ثبت) استوار می‌سازد. اعتبارات قابل تأیید (VCs)[2] در احراز هویت غیرمتمرکز (DID) بر پایۀ کلیدهای خصوصی کاربران تولید می‌شوند، نه نهاد دولتی. براساس نظریۀ اثبات‌پذیری[3] اثبات احراز هویت غیرمتمرکز (DID) هرچند از طریق اثبات‌های دانش صفر (ZKP) غیرقابل انکار باشد، در محاکم ایران (که مادۀ ۱۲۹۱ قانون مدنی صرفاً اسناد رسمی را حجت می‌داند)، فاقد قوۀ اثباتی اولیه (حجت دولتی) است. از دیدگاه فقهی، براساس نظریۀ «سند معتبر» در فقه شیعه، احراز هویت غیرمتمرکز (DID)می‌تواند با شرط «علم اجمالی» (دانش غیرمستقیم حاکمیت از طریق زیرساخت ملی) معتبر شود. با این حال، مادۀ ۲۲ قانون ثبت اسناد و املاک (۱۳۱۰)، این اعتبار را محدود کرده و الزام ثبت مرکزی را تحمیل می‌کند، زیرا فقها حفظ نظام را مقدم بر آزادی فردی در توثیق می‌دانند.

این چالش نیازمند تفسیر گستردۀ مادۀ ۱۲۸۴ (براساس اصل سوم (۳) قانون اساسی: عدالت) است تا احراز هویت غیرمتمرکز (DID) را به عنوان «سند رسمی رقومی» بپذیرد. عدم انجام این مهم، ریسک ابطال قضائی اسناد مبتنی بر احراز هویت غیرمتمرکز (DID) را طبق مادۀ ۱۹۰ قانون مدنی (شرایط صحت معامله) افزایش می‌دهد.

1. cryptographic proof
2. verifiable credentials
3. evidentiary theory

۴-۲. مسائل حریم خصوصی و حفاظت داده‌ها: تناقض با اصول خودحاکمیتی

تناقض احراز هویت غیرمتمرکز (DID) با قانون جرائم رایانه‌ای (۱۳۸۸) و اصول حفاظت داده؛ مسائل حریم خصوصی درDID، که بر پایهٔ اصل خودحاکمیتی استوار است، با چارچوب حفاظت داده‌های ایران تناقض دارد.

مادهٔ ۱۶ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ (ممنوعیت دسترسی غیرمجاز به داده‌ها)، حفاظت را بر پایهٔ کنترل مرکزی دولت تعریف می‌کند، در حالی که حاکمیت هویتی شخص (SSI) کنترل را به کاربران واگذار می‌سازد. براساس نظریهٔ حریم خصوصی اطلاعاتی[1]، افشای انتخابی[2] در DID با اصول مقررات عمومی حفاظت داده‌های اتحادیهٔ اروپا (GDPR) همخوانی دارد. اما در ایران، مادهٔ ۲۵ قانون جرائم رایانه‌ای، مسئولیت نقض داده را بر عهدهٔ «دارندهٔ سیستم» می‌گذارد که در DID (که سیستم توزیع‌شده است) مبهم است (کاربر، صادرکنندهٔ اولیه، یا شبکه؟).

تفسیر حقوقی مادهٔ ۴ قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱ (حفاظت از داده‌های شخصی با رعایت امنیت ملی) حاکی از آن است کهDID، با ریسک حملات پیوندزنی هویت‌ها[3] در صورت عدم اجرای دقیق ZKP، می‌تواند به تعارض با اصل ۲۲ قانون اساسی (حقوق مالکانهٔ افراد بر داده‌ها) منجر شود.

براساس نظریهٔ «حرمت تجسس» (ملهم از فقه شیعه، و منعکس‌شده در مادهٔ ۵۸۳ قانون مجازات اسلامی)، DID حریم خصوصی را تقویت می‌کند. اما فقدان مقررات خاصی که چگونگی اِعمال کنترل دولتی بر زیرساخت غیرمتمرکز را مشخص کند، همچنان یک خلأ فقهی ـ قانونی ایجاد می‌کند.

۴-۳. مسئولیت مدنی و کیفری: ابهام در تعیین «عامل خسارت»

چالش مسئولیت مدنی و کیفری در صورت نقص DID؛ مسئولیت مدنی و کیفری درDID، به‌دلیل ماهیت توزیع‌شدهٔ[4] آن، نظریهٔ مسئولیت مشترک[5] را به‌چالش می‌کشد.

مادهٔ ۱ قانون مسئولیت مدنی مصوب ۱۳۳۹، مسئولیت را بر عهدهٔ «عامل خسارت» می‌گذارد. اما در DID، نقص (مانند ازدست رفتن کلید خصوصی توسط کاربر) می‌تواند به کاربران، صادرکنندگان

1. informational privacy theory
2. selective disclosure
3. correlation attacks
4. distributed nature
5. joint liability theory

اولیه یا پلتفرم‌های دفترکل توزیع‌شده نسبت داده شود، نه دفاتر اسناد سنتی (مادۀ ۲۲ قانون دفاتر اسناد رسمی، ۱۳۵۴). تحلیل براساس دکترین سَبَبِیَت [1]در حقوق مدنی نشان می‌دهد که اثبات سَبَبِیَت در بستر بلاکچین دشوار است، زیرا تراکنش‌ها شبه‌ناشناس [2] هستند. این امر با مادۀ ۵۲۳ قانون مجازات اسلامی (جعل اسناد) تعارض دارد، زیرا جعل در DID ممکن است به هک کلیدها نسبت داده شود و تعیین مجرم سخت باشد.

۴-۴. چالش‌های قضائی و اجرایی: خلأ مقررات خاص و تحریم‌ها

چالش‌های DID از عدم وجود مقررات خاص و موانع بین‌المللی؛ چالش‌های قضائی و اجرایی DID از خلأ نظارتی [3] ناشی می‌شود که با اصل ۱۶۷ قانون اساسی (لزوم استنباط حکم از منابع فقهی در نبود قانون) تعارض دارد. مادۀ ۷ قانون تجارت الکترونیک اثبات در دادگاه‌ها را برای اسناد الکترونیکی تسهیل می‌کند، اما DID فاقد «امضای معتبر» مرکزی است و تفسیر مادۀ ۱۲۵۸ قانون مدنی (اثبات ادعا با سند) آن را به عنوان «سند عادی» طبقه‌بندی می‌کند. تحلیل براساس نظریۀ اثبات قضائی [4] نشان می‌دهد که اثبات‌های دانش صفر در محاکم ایران (که بر شهادت و سند فیزیکی تکیه دارند) نیاز به کارشناس متخصص دارد که طبق مادۀ ۲۵۷ قانون آیین دادرسی مدنی، فرایندی زمان‌بر و پرهزینه است. تحریم‌های بین‌المللی (مانند محدودیت دسترسی به زیرساخت‌ها و استانداردهای کنسرسیوم جهانی وب) اجرای DID را مختل می‌کند. تفسیر اصل ۱۵۲ قانون اساسی (عدم تعهد به معاهدات مغایر شرع و منافع ملی) ضرورت ایجاد بلاکچین ملی بومی برای میزبانی DID را تقویت می‌کند تا از ریسک‌های خارجی و تحریمی جلوگیری شود.

۴-۵. موانع فرهنگی ـ حقوقی: مقاومت سنتی در برابر غیرمتمرکزسازی

مقاومت سنتی و تأثیر فقه شیعه بر اسناد؛ موانع فرهنگی ـ حقوقی DID در مقاومت سنتی و تأثیر فقه شیعه ریشه دارد، جایی که اصل غیرمتمرکز با نظریۀ «امانت‌داری دولتی» [5] در فقه تعارض دارد. مادۀ ۱۰۵۹ قانون مدنی (شرط صحت عقد: رضایت) در اسناد رسمی به‌طور سنتی با شرط حضور و شهود

1. causation
2. pseudonymous
3. regulatory Gap
4. judicial proof theory
5. trusteeship theory

تضمین می‌شود. DID فاقد این تشریفات سنتی است. تفسیر فقهی (نظیر فتوای آیت‌الله سیستانی در لزوم شاهد در معاملات) آن را نامعتبر نمی‌داند، اما نیازمند جایگزینی فناورانه برای احراز کامل قصد و اراده است.

تحلیل براساس نظریهٔ فرهنگی حقوقی[1] نشان می‌دهد که مقاومت سنتی (مانند ترجیح حضور فیزیکی) با اصل ۴۴ قانون اساسی (خصوصی‌سازی تدریجی) تعارض دارد و نیازمند استنباط فقهی نوین (اجتهاد پویا در فناوری) است تا «توثیق شرعی» را در فضای رقومی به رسمیت بشناسد (پاسبان و میلانی، ۱۴۰۲).

با توجه به مطالب ارائه‌شده، چالش‌های حقوقی DID در ایران عمدتاً ساختاری و تقنینی هستند. حل این چالش‌ها نیازمند خروج از تفسیر مُضیّق قوانین سنتی (م. ۱۲۸۴ ق.م.) و تدوین فوری مقررات ناظر بر مسئولیت توزیع‌شده (م. ۱ ق.م.م.) و اعتبار اثباتی شناسه غیرمتمرکز در محاکم است تا این فناوری در چارچوب اصول فقهی و قانون اساسی بومی‌سازی شود.

۵. تحلیل تطبیقی چالش‌ها (رویکرد همگرایی حقوقی)

تحلیل تطبیقی چالش‌های حقوقی احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران، بر پایهٔ رویکرد تطبیقی حقوق و با الهام از نظریهٔ همگرایی حقوقی[2] به بررسی تجربیات بین‌المللی می‌پردازد تا درس‌هایی برای بومی‌سازی در چارچوب فقه شیعه و قوانین ایران استخراج شود. این تحلیل، تضاد میان مدل‌های غیرمتمرکز غربی (مانند نظام احراز هویت الکترونیکی اتحادیهٔ اروپا) و ساختار متمرکز ایرانی را برجسته می‌سازد، جایی که مادهٔ ۱۲۸۷ قانون مدنی (تعریف سند رسمی بر پایهٔ مأمور رسمی) با اصول خودحاکمیتی هویتی (SSI) تعارض بنیادین دارد. تفسیر حقوقی این ماده براساس دکترین تفسیر سیستمی[3] نشان می‌دهد که تطبیق نیازمند اصلاحات تقنینی است.

۵-۱. تجربیات بین‌المللی: نظام احراز هویت الکترونیکی اتحادیهٔ اروپا و مدل استونی

تجربیات جهانی، به‌ویژه در اتحادیهٔ اروپا و استونی، الگوهایی موفق برای مدیریت هویت رقومی ارائه می‌دهند که می‌تواند برای ایران نقش راهنما داشته باشد.

---

1. cultural legal theory
2. convergence theory
3. systematic interpretation

۵-۱-۱. مدل نظام احراز هویت الکترونیکی اتحادیهٔ اروپا (eIDAS 2.0)

مقررات احراز هویت الکترونیکی و خدمات اعتماد (eIDAS 2.0)[1]، که به‌طور تدریجی تا سال ۲۰۲۶ الزام به ارائهٔ کیف پول هویتی رقومی اروپایی (EUDI Wallet)[2]را برای کشورهای عضو تحمیل می‌کند، بر اصول قابلیت تعامل‌پذیری،[3] خدمات اعتماد[4] و اعتبارات قابل تأیید (VCs)[5] استوار است (Hussain et al., 2024). این مدل براساس نظریهٔ حاکمیت رقومی[6]، چالش اعتبار را با تعریف امضای الکترونیکی واجد شرایط (QES)[7] حل کرده است. این راه‌حل مشابه مادهٔ ۷ قانون تجارت الکترونیک ایران (۱۳۸۲) (اعتبار امضای الکترونیکی) است، اما eIDAS 2.0 با تمرکز بر غیرمتمرکزسازی، حریم خصوصی (مطابق مادهٔ ۵ مقررات عمومی حفاظت داده‌های اروپا) را تقویت می‌کند.

در مقایسه با ایران، جایی که مادهٔ ۱۲۸۷ قانون مدنی الزام به مأمور رسمی دارد، eIDAS 2.0 از طریق مقررات اجرایی خود، مدل ترکیبی[8] را معرفی کرده که واسطه‌های متمرکز را کاهش می‌دهد، اما نظارت دولتی را حذف نمی‌کند. این مدل می‌تواند برای تفسیر گستردهٔ مادهٔ ۲۲ قانون ثبت اسناد و املاک (الزام ثبت رسمی) مفید باشد؛ به این صورت که ثبت دولتی به عنوان تأییدکنندهٔ نهایی عمل کند، اما فرایند احراز هویت توسط DID انجام شود.

eIDAS 2.0 اثبات‌پذیری را از طریق اثبات‌های دانش صفر (ZKP) تضمین می‌کند (Wadhwa et al., 2024). این مکانیزم علمی می‌تواند در حقوق ایران با مادهٔ ۱۲۹۱ قانون مدنی (حجت اسناد رسمی) تطبیق یابد، مشروط به پذیرش ادلهٔ علمی و اعتبار علمی در لایحهٔ هویت رقومی ایران.

۵-۱-۲. برنامهٔ اقامت الکترونیکی استونی

برنامهٔ اقامت الکترونیکی استونی[9]، نمونه‌ای عملی از کاربرد DID در خدمات کسب‌وکار است (Dwivedi et al., 2024). این برنامه با صدور شناسنامهٔ رقومی معتبر برای غیرمقیمان، چالش مسئولیت را با مدل توزیع‌شده حل کرده که از نظر اقتصادی مشابه اصل چهل و چهارم (۴۴) قانون اساسی ایران

1. regulation (EU) 2024/1183
2. european digital identity wallet
3. interoperability
4. trust services
5. verifiable credentials
6. digital sovereignty theory
7. qualified electronic signatures
8. hybrid model
9. e-residency

(خصوصی‌سازی) است. اعتبارات قابل تأیید در استونی برای ثبت شرکت و بانکداری استفاده می‌شوند و اثبات‌پذیری آن بالاتر از اسناد سنتی است. این مدل می‌تواند برای تفسیر مادهٔ ۱ قانون ثبت احوال (۱۳۵۵) در ایران مفید باشد، به نحوی که شناسنامهٔ رقومی DID نیز به‌عنوان یک سند معتبر اولیهٔ هویت پذیرفته شود. با این حال، تفاوت کلیدی در نظارت است؛ استونی بر پایهٔ مقررات اتحادیهٔ اروپا عمل می‌کند، در حالی که ایران با مادهٔ ۴ قانون مدیریت داده‌ها (۱۴۰۱) نیاز به حفاظت و کنترل مرکزی بر داده‌های ملی دارد.

ایران می‌تواند مدل اقامت الکترونیکی را برای ثبت املاک ترکیبی بومی‌سازی کند، اما بدون اصلاح مادهٔ ۴۸ قانون ثبت اسناد (الزام ثبت مرکزی برای نقل و انتقال)، چالش اجرایی باقی می‌ماند.

۵-۲. تطبیق تجربیات بین‌المللی با شریعت و اصول فقهی در ایران

درس‌های تجربیات بین‌المللی برای ایران، باید بر تطبیق DID با فقه شیعه تمرکز کند.

نظریهٔ اجتهاد پویا و فتوای مراجع: براساس نظریهٔ اجتهاد پویا،[1] فقهای معاصر می‌توانند فناوری‌های نوین را با اصول شریعت همخوان کنند. فتاوای مراجع تقلید درمورد امضای رقومی، پایه‌ای برای این تطبیق فراهم می‌کند، برای مثال فتوای آیت‌الله مکارم شیرازی (۱۴۰۰) امضای رقومی را معتبر می‌داند مشروط به «علم و یقین» به اصالت، که با اثبات رمزنگاری‌شدهٔ DID همخوانی دارد.

تحلیل فقهی ـ قانونی: مادهٔ ۷ قانون تجارت الکترونیک نشان می‌دهد که DID می‌تواند با فقه امامیه (مانند اصل «المؤمنون عند شروطهم») سازگار شود، زیرا افشای انتخابی[2] حریم خصوصی را حفظ می‌کند (مطابق با مادهٔ ۵۸۳ قانون مجازات اسلامی: حرمت تجسس).

تفسیر فقهی تعارض: درس کلیدی از eIDAS 2.0 این است که ادغام فقهی می‌تواند چالش اعتبار را حل کند، برای مثال فتوای آیت‌الله سیستانی (۱۴۰۱) درمورد معاملات رقومی که می‌تواند شرط «شهود» را با اثبات رقومی جایگزین کند.

نیاز به استنباط جدید: مادهٔ ۱۲۸۸و ۱۲۸۷ قانون مدنی و مادهٔ ٢٤ قانون حمایت از خانواده (اعتبار اسناد رسمی در ازدواج) می‌تواند با تفسیر فقهی به DID گسترش یابد، اما نیازمند استنباط جدید از اصل یکصد و شصت و هفتم (۱۶۷) قانون اساسی (استنباط از فقه) است.

نتیجه‌گیری فقهی: تطبیق نیازمند ایجاد استانداردهای فقهی برای DID است که حدود دخالت حاکمیت را در زیرساخت غیرمتمرکز، منطبق با قاعدهٔ لاضرر و حفظ نظام مشخص سازد تا مسئولیت مدنی (مادهٔ ۱ قانون مسئولیت مدنی، ۱۳۳۹) مبهم باقی نماند.

1. dynamic ijtihad theory

2. selective disclosure

۵-۳. ریسک‌های ژئوپلیتیک: تأثیر تحریم‌ها بر دسترسی به استانداردها

ریسک‌های ژئوپلیتیک DID در ایران، عمدتاً از تحریم‌های بین‌المللی ناشی می‌شود که دسترسی به فناوری‌های دفترکل توزیع‌شده را محدود می‌کند و نظریهٔ وابستگی ژئوپلیتیک[1] را برجسته می‌سازد. تحریم‌های ایالات متحده (مانند محدودیت دسترسی به شبکه‌های جهانی) دسترسی به استانداردهای کنسرسیوم جهانی وب (W3C) را محدود می‌کند که اجرای مادهٔ ۶ قانون جرائم رایانه‌ای (۱۳۸۸) (همکاری بین‌المللی) را مختل می‌سازد. تفسیر اصل یکصد و پنجاه و دوم (۱۵۲) قانون اساسی (سیاست خارجی مستقل) حاکی از آن است که ایران باید برای جلوگیری از ریسک‌های خارجی و تحریمی، به توسعهٔ بلاکچین ملی و استانداردهای بومی برای DID بپردازد. مادهٔ ۱ قانون تجارت الکترونیک (اعتبار معاملات رقومی) در صورت وابستگی به پلتفرم‌های جهانی محدود، با ریسک نقض و عدم دسترسی مواجه است.

بنابراین، تحریم‌ها اجرای DID را به یک چالش امنیتی ـ اقتصادی تبدیل کرده است. تفسیر اصل چهل و سوم (۴۳) قانون اساسی (اقتصاد مستقل) ضرورت بومی‌سازی کامل زیرساخت DID را برای حفظ امنیت حقوقی و استقلال ملی توجیه می‌کند و چالش‌های اجرایی (مادهٔ ۲۵ قانون جرائم رایانه‌ای: مسئولیت در نقص داده‌ها) را کاهش می‌دهد.

۶. پیشنهادها و راه‌حل‌های حقوقی (نقشهٔ راه تقنینی و اجرایی)

برای غلبه بر چالش‌های حقوقی احراز هویت غیرمتمرکز (DID) در نظام اسناد رسمی ایران، پیشنهادات زیر بر پایهٔ تحلیل حقوقی ارائه می‌شود که در نظریه‌های عدالت توزیعی[2] و اجتهاد پویا[3] ریشه دارد. این پیشنهادات، با استناد به مفاد قانونی جاری (مانند مادهٔ ۱۲۸۷ قانون مدنی و مادهٔ ۷ قانون تجارت الکترونیک)، به دنبال تعادل میان نوآوری فناوری و امنیت حقوقی هستند. تحلیل نشان می‌دهد که با تفسیر سیستمی[4] از اصل چهل و چهارم (۴۴) قانون اساسی (خصوصی‌سازی)، می‌توان DID را به‌عنوان ابزار تحول رقومی بومی‌سازی کرد تا تضعیف نظارت دولتی رخ ندهد.

1. geopolitical dependency theory
2. distributive justice theory
3. dynamic ijtihad theory
4. systematic interpretation

۶-۱. اصلاحات تقنینی: پیشنهاد لایحه برای ادغام DID در قانون ثبت اسناد

اصلاحات تقنینی کلیدی‌ترین راه‌حل است که بر پایهٔ نظریهٔ قانون‌گذاری پویا[1] پیشنهاد می‌شود تا قوانین سنتی را با فناوری همخوان کند.

تدوین لایحه‌ای برای اصلاح قانون ثبت اسناد و املاک (۱۳۱۰)، که «امضای غیرمتمرکز رسمی» را به‌عنوان جایگزین امضای مأمور رسمی تعریف کند، مشروط به اثبات رمزنگاری‌شده[2] و اتصال به پایگاه داده‌های ملی.

مادهٔ ۲۲ قانون ثبت (اعتبار مطلق مالکیت ثبت‌شده) نشان می‌دهد که DID می‌تواند این اعتبار را تقویت کند، زیرا غیرقابل انکار است، اما نیازمند گسترش مادهٔ ۴۸ (الزام ثبت رسمی) به مدل‌های رقومی توزیع‌شده است.

تفسیر موسع مادهٔ ۱۲۸۷ قانون مدنی اجازه می‌دهد DID به عنوان «سند رسمی» پذیرفته شود، اگر توسط نهادهای حاکمیتی (مانند سازمان ثبت اسناد در مدل ترکیبی) تأیید نهایی شود.

لایحه باید شرط «عدم ضرر عقلایی» را برای DID بگنجاند تا با فقه شیعه همخوانی داشته باشد (براساس قاعدهٔ لاضرر و فتوای مراجع درمورد مالیت فناوری‌های نوین).

تصویب این لایحه، مسئولیت مدنی (مادهٔ ۱ قانون مسئولیت مدنی، ۱۳۳۹) را از سردفتران به کاربران توزیع‌شده منتقل می‌کند که نیازمند تعریف جدید مسئولیت مشترک[3] یا مسئولیت تضامنی است.

۶-۲. چارچوب‌های فنی ـ حقوقی: ایجاد محیط آزمون نظارتی (فضای شن)

چارچوب‌های فنی ـ حقوقی مانند محیط آزمون نظارتی[4] یا فضای شن می‌تواند پلی برای آزمایش DID باشد، بر پایهٔ نظریهٔ آزمون و خطا. ایجاد یک فضای شن برای DID در ثبت احوال، با همکاری شورای عالی فضای مجازی و سازمان ثبت احوال، برای آزمایش اعتبارات قابل تأیید در محیط کنترل‌شده.

مادهٔ ۴ قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۱) نشان می‌دهد که این فضا می‌تواند ریسک حریم خصوصی را مدیریت کند، زیرا آزمایش محدود است و با مادهٔ ۲۵ قانون جرائم رایانه‌ای (۱۳۸۸) (مسئولیت در نقص داده) همخوانی دارد.

---

1. dynamic legislation theory
2. cryptographic proof
3. joint liability
4. regulatory sandbox

تفسیر اصل ۱۶۷ قانون اساسی (استنباط از فقه) اجازه می‌دهد که نتایج عملی فضای شن، در قالب نظر کارشناسی شرعی، به فتاوای مراجع منتقل شود تا سازگاری DID با قواعد شرعی (مانند حرمت تجسس) احراز شود و تسهیل در ثبت هویت (مادۀ ۱ قانون ثبت احوال) صورت پذیرد.

بنابراین، ایجاد این محیط توسط قوۀ مجریه (اصل ۶۰ قانون اساسی) می‌تواند نوآوری را بدون ریسک سیستماتیک پیش ببرد.

۶-۳. آموزش و ظرفیت‌سازی: نقش قوۀ قضائیه و دانشگاه‌ها

آموزش و ظرفیت‌سازی، بر پایۀ نظریۀ سرمایۀ انسانی[1] در حقوق، برای غلبه بر مقاومت فرهنگی ـ حقوقی ضروری است.

قوۀ قضائیه (با استناد به مادۀ ۲۹ قانون آیین دادرسی مدنی: آموزش قضات) برنامه‌های آموزشی تخصصی درمورد دفترکل توزیع‌شده و DID برگزار کند. همچنین دانشگاه‌ها دوره‌های حقوقی ـ فناوری را در مقاطع عالی حقوق بگنجانند. مادۀ ۲۵۷ قانون آیین دادرسی مدنی (نیاز به کارشناس) نشان می‌دهد که آموزش قضات می‌تواند وابستگی به کارشناسان را کاهش دهد و اثبات DID در دادگاه‌ها (مادۀ ۱۲۹۱ قانون مدنی) را تسهیل کند، زیرا قضات خود به سطح بالاتری از دانش قضائی ـ فناورانه مجهز می‌شوند.

آموزش می‌تواند با فقه شیعه ادغام شود، مانند بررسی فتواهای مراجع درمورد معاملات رقومی برای ایجاد یک فرهنگ قضائی مبتنی بر اجتهاد پویا که به توثیق شرعی رقومی باور داشته باشد.

۶-۴. مدل ترکیبی برای حفظ امنیت ملی و حقوقی

مدل ترکیبی متمرکز ـ غیرمتمرکز، بر پایۀ نظریۀ تعادل[2] در حقوق رقومی، پیشنهاد می‌شود تا هم امنیت ملی حفظ شود و هم مزایای DID حاصل گردد.

DID با نظارت مرکزی (مانند استفاده از سامانۀ شاهکار یا بلاکچین ملی ایران) ادغام شود. در این مدل، ثبت احوال یا سازمان ثبت اسناد به عنوان صادرکنندۀ اولیۀ هویت[3] عمل کرده، اما کنترل کلید خصوصی و افشای داده به کاربر واگذار می‌شود.

---

1. human capital theory
2. balance theory
3. issuer

این مدل با اصل ۱۵۲ قانون اساسی (سیاست خارجی مستقل) همخوانی دارد و ریسک تحریم‌ها را کاهش می‌دهد. تفسیر مادۀ ۴ قانون مدیریت داده‌ها حاکی از آن است که هیبرید حفاظت داده‌ها را تقویت می‌کند، زیرا حاکمیت نظارت را بر زیرساخت حفظ می‌کند. همچنین، این مدل با فتوای مراجع درمورد لزوم شاهد دیجیتال سازگاری دارد.

این مدل، چالش مسئولیت را با توزیع مسئولیت حل می‌کند (مادۀ ۱۲۰ قانون آیین دادرسی مدنی)؛ به این صورت که مرجع صادرکننده مسئول صحت داده‌های اولیه است و کاربر مسئول حفاظت از کلید خصوصی خود.

این پیشنهادات، یک نقشۀ راه جامع برای قانون‌گذاری، اجرا و آموزش ارائه می‌دهند تا DID بتواند در چارچوب اصول فقهی و حقوقی جمهوری اسلامی ایران، به ابزاری قدرتمند برای تحول رقومی تبدیل شود.

نتیجه‌گیری

احراز هویت غیرمتمرکز (DID)، به‌عنوان یک پارادایم فناوری خودحاکمیتی، پتانسیل چشمگیری برای افزایش کارایی معاملاتی و تقویت حریم خصوصی در نظام اسناد رسمی ایران دارد. با این حال، یافته‌های این پژوهش به‌طور قاطع نشان می‌دهد که ادغام این فناوری با موانع ساختاری عمیق حقوقی و فقهی مواجه است که ناشی از تضاد ماهوی میان غیرمتمرکزسازی فناوری و تمرکزگرایی حاکمیتی در توثیق اسناد است.

فرضیهٔ اصلی مقاله که DID علی‌رغم مزایا، با چالش‌های ساختاری بنیادین مواجه است، کاملاً تأیید می‌شود. ریشهٔ این چالش‌ها در نظریهٔ دوگانگی حقوقی (تعارض اختیار فردی و نظارت دولتی) نهفته است::

نتایج نشان داد که DID به‌طور مستقیم با مادهٔ ۱۲۸۷ قانون مدنی (لزوم مأمور رسمی) و مادهٔ ۲۲ قانون ثبت (الزام ثبت مرکزی) در تضاد است. این تضاد، قوای اثباتی DID در محاکم را براساس مادهٔ ۱۲۹۱ قانون مدنی (حجت اسناد رسمی) تضعیف می‌کند.

همچنین ماهیت توزیع‌شدهٔ DID، تعیین «عامل خسارت» را طبق مادهٔ ۱ قانون مسئولیت مدنی (۱۳۳۹) دشوار می‌سازد و ریسک عدم جبران خسارت را افزایش می‌دهد.

از طرفی DID با فقه شیعه قابل تطبیق است، مشروط بر آنکه اصالت و یقین (مانند فتوای آیت‌الله مکارم شیرازی درمورد امضای رقومی) حفظ شود. با این حال، سازگاری آن با اصول قانون اساسی (نظیر اصل ۱۵۲: سیاست خارجی مستقل) مستلزم توسعهٔ زیرساخت ملی بومی است.

راه‌حل‌های تقنینی و اجرایی در گرو توسعهٔ مدل‌های ترکیبی (هیبریدی) است که در آن، حاکمیت نقش صادرکنندهٔ اولیهٔ هویت و تأییدکننده نهایی را حفظ می‌کند، اما کنترل داده به فرد واگذار می‌شود.

چشم‌انداز آینده DID در تحول رقومی ایران، به‌ویژه در پرتو سند تحول دولت الکترونیک (مصوب ۱۴۰۲)، امیدوارکننده است. تحلیل حقوقی این سند نشان می‌دهد که DID می‌تواند یک ابزار قدرتمند برای تحقق اصل چهل و چهارم (۴۴) قانون اساسی (خصوصی‌سازی و تعاونی‌سازی فناوری) باشد.

استفاده از اثبات‌های رمزنگاری‌شده در DID می‌تواند به‌طور مؤثر ریسک جعل اسناد (مادهٔ ۵۲۳ قانون مجازات اسلامی) را کاهش دهد و روند الکترونیکی کامل شدن سازمان ثبت اسناد در ۱۴۰۴ را تسریع بخشد. این امر، تحقق عدالت توزیعی در دسترسی به خدمات را امکان‌پذیر می‌سازد.

برای غلبه بر ریسک‌های ژئوپلیتیک (نظیر تحریم‌های بین‌المللی بر زیرساخت‌های دفترکل

توزیع‌شده)، تفسیر اصل یکصد و پنجاه و دوم (۱۵۲) قانون اساسی توجیه می‌کند که ایران باید بلاکچین ملی خود را برای میزبانی DID توسعه دهد و از این طریق، ضمن حفظ استقلال فناوری، به هاب منطقه‌ای تبدیل شود. این امر نیازمند تدوین یک چارچوب حقوقی ـ فناوری بومی و مستقل از استانداردهای صرفاً خارجی است.

برای پر کردن خلأ جدی ادبیات حقوقی در ایران، انجام تحقیقات آتی در مسیرهای زیر ضروری است:

مطالعهٔ موردی اثبات‌پذیری قضائی: انجام تحقیقات موردی بر کاربرد DID در ثبت املاک با تمرکز بر نظریه اثبات‌پذیری قضائی این مطالعات باید به‌طور تطبیقی، نحوهٔ انطباق مکانیزم‌های eIDAS 2.0 با قانون آیین دادرسی مدنی ایران را بررسی کنند.

مسئولیت توزیع‌شده و فقه پویا: تحلیل تأثیر فقه پویا بر تعریف جدید مسئولیت توزیع‌شده و جبران خسارت (مادهٔ ۱۲۰ قانون آیین دادرسی مدنی) در ساختارهای غیرمتمرکز.

حقوق داده‌ها و لایحهٔ حفاظت داده‌ها: بررسی نقش لایحهٔ حفاظت از داده‌های شخصی در تسهیل پذیرش SSI و تضمین حقوق مالکانهٔ افراد بر داده‌هایشان.

این تحقیقات می‌توانند مبنای سیاست‌گذاری مبتنی بر شواهد باشند تا DID به‌عنوان ابزاری کارآمد در تحقق عدالت رقومی در نظام حقوقی ایران به‌کار گرفته شود.

منابع

۱. اسکندریان، حسن، آقایی بجستانی، مریم و روحانی مقدم، محمد (۱٤۰۲)، «امکان‌سنجی حمایت حقوقی از داده‌های توالی دیجیتال»، پژوهش‌های سلولی و مولکولی (مجلهٔ زیست‌شناسی ایران)، ۳٦ (۲)، ۱۹۲-۲۱۱.

۲. بی‌جانی، بهاره، و امینی‌نیا، عاطفه (۱٤۰۰)، «ارتقای محرمانگی در تجارت الکترونیک: مسائل حقوقی استفادهٔ بین‌المللی از روش‌های احراز هویت و امضای الکترونیک»، فصلنامهٔ مطالعات حقوق، ٦ (۲۲)، ٤۱٥_ ٤٤۲.

۳. پاسبان، محمدرضا و میلانی، جمیل (۱٤۰۲)، «جایگاه ادارهٔ کل ثبت شرکت‌ها و مؤسسات غیرتجاری در هویت بخشی و تثبیت شخصیت اشخاص حقوقی»، فصلنامهٔ تحقیق و توسعه در حقوق تطبیقی، ٦(۱۸)، ۱۱٦_ ۱٤۰.

٤. عاکفی قاضیانی، موسی، سیدمصطفی میلانی و وحید عاکفی قاضیانی (۱٤۰۱)، «متاورس و چالش‌های حقوقی در حوزهٔ حقوق اموال»، حقوق فناوری‌های نوین، ۳(٦)، ۱٤۳-۱٥۳.

٥. لطیف‌زاده، مهدیه و قبولی درافشان، سید محمد مهدی (۱٤۰۲). «معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل»، مطالعات حقوق خصوصی، ٥۳(۲)، ۳٤۹-۳۷۲.

٦. هوشیدری فراهانی، فاطمه (۱۳۹٥)، تبیین بسترهای پیاده‌سازی قانون انتشار و دسترسی آزاد به اطلاعات در ایران، پایان‌نامهٔ کارشناسی ارشد، دانشکدهٔ مدیریت و اقتصاد، دانشگاه تربیت مدرس.

۷. یعقوبی، محدثه، جعفری، علی و سلمان‌زاده، جعفر (۱٤۰۳)، «بررسی نقاط قوت و ضعف قانون انتشار و دسترسی آزاد به اطلاعات از دیدگاه حقوق‌دانان»، مجلس و راهبرد، ۳۱(۱۱۷)، ٤۹۷-٥۲۸.

References

1. Dwivedi, S. K., Amin, R., Das, A. K., Leung, M. T., Choo, K. K. R., & Vollala, S. (2022), "Blockchain-based vehicular Ad-Hoc networks: A comprehensive survey", *Ad-Hoc networks*, *137*, 102980.
2. Hussain, S., Tahir, S., Masood, A., & Tahir, H. (2024). "Blockchain-enabled secure communication framework for enhancing trust and access control in the internet of vehicles (IoV)", *IEEE access*, *12*, 110992-111006.
3. Saeidi Aghdam, M., Komiak, S. Y. X., Amiri, M., & Bahiraie, A. (2025), "Developing an e-commerce trust model in crowdfunding by integrating blockchain and edge computing using fuzzy technique", *Journal of fuzzy extension and applications*, *6*(3), 424–447.
4. Shitharth, S., Manoharan, H., Shankar, A., Alsowail, R. A., Pandiaraj, S., Edalatpanah, S. A., & Viriyasitavat, W. (2023), "Federated learning optimization: A computational blockchain process with offloading analysis to enhance security", *Egyptian informatics journal*, *24*(4), 100406.
5. Wadhwa, D., Gupta, D., Saini, S., & Bathla, R. (2021), "Blockchain for iot security and privacy", *2021 9th international conference on reliability, infocom technologies and optimization (Trends and future directions)(ICRITO)* (pp. 1–5). IEEE.