دوره هجدهم، شماره بهار ۱۴۰۴

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://sanad.iau.ir/journal/ited

تحلیل کاربردها و چالش‌های پیش‌روی فناوری زنجیره‌بلوکی درحوزه مقررات حفاظت از داده‌های عمومی (GDPR)

مهدی سیدهاشمی[۱] حسن شاکری*[۲] ابوذر عرب‌سرخی[۳] رحیم خانی‌زاد[۴]

(۱) گروه مهندسی کامپیوتر، واحد سبزوار، دانشگاه آزاد اسلامی، سبزوار، ایران

(۲) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران*

(۳) پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

(۴) دانشکده مدیریت، اقتصاد و فناوری پیشرفت، دانشگاه علم و صنعت، تهران، ایران

(تاریخ دریافت: ۱۴۰۳/۰۵/۰۶ تاریخ پذیرش: ۱۴۰۳/۰۹/۰۴)

چکیده

رشد کاربرد فناوری‌های نوظهور در صنایع مختلف و افزایش حجم و سرعت تولید و انتشار داده‌ها باعث افزایش نگرانی‌ها در زمینه حفاظت از داده‌های شخصی شده است. دولت‌ها و نهادهای قانون‌گذار قوانینی در جهت صیانت از حریم خصوصی کاربران تدوین کرده‌اند که یکی از جامع‌ترین آنها GDPR است که توسط اتحادیه اروپا تدوین شده و مسئولیت‌ها و وظایفی را بر سازمان‌ها، کسب‌وکارها و نهادهای نظارتی تحمیل می‌کند تا از داده‌های شخصی کاربران محافظت شود. در میان فناوری‌های نوظهور، زنجیره‌بلوکی توجه بسیاری را در زمینه صیانت از حریم‌خصوصی و GDPR به خود جلب کرده‌است. زنجیره‌بلوکی به‌دلیل قابلیت ردیابی، شفافیت و امنیت، راه‌حل‌های نوآورانه‌ای در زمینه حفاظت از داده‌ها ارائه می‌کند. از سوی دیگر، معماری توزیع‌شده، تغییرناپذیری و عدم حداقل‌سازی فضای‌ذخیره‌سازی توسط زنجیره‌بلوکی، باعث ایجاد چالش‌هایی در زمینه انطباق این فناوری با الزامات GDPR شده است. در این مقاله به بررسی انطباق فناوری زنجیره‌بلوکی با چارچوب این قوانین از دو منظر معماری و قابلیتی و وارسی جزئی ویژگی‌های تسهیل‌گر و بازدارنده این فناوری با قوانین مذکور پرداخته‌ایم و تعدادی از راه‌حل‌های ارائه‌شده در جهت رفع بازدارندگی این فناوری در پیروی از GDPR، از جمله ذخیره‌سازی داده در خارج از زنجیره و استفاده از توابع درهم‌ساز را مورد تحلیل قرار داده‌ایم.

کلمات کلیدی: زنجیره‌بلوکی، GDPR، الزامات حفاظت از داده

*عهده‌دار مکاتبات:

حسن شاکری

نشانی: گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

پست الکترونیکی: shakeri@mshdiau.ac.ir

۱- مقدمه

در سال‌های اخیر، توسعه و گسترش فناوری اطلاعات و ارتباطات و معرفی و رشد فناوری‌های نوظهور، باعث توسعه و پیشرفت اقتصاد دیجیتال به همراه تاثیری شگرف بر روی آن‌ها بوده است. فناوری‌های نوظهور همانند زنجیره‌بلوکی[۱]، هوش‌مصنوعی[۲] و اینترنت اشیاء[۳] معرف کلید ایجاد تحول در تمامی ابعاد اقتصاد دیجیتالی و تقویت موج دیجیتالی‌شدن است [1] . با رهبری فناوری‌های جدید و ظهور صنعت ۴[۴] ما شاهد حرکت اقتصاد جهانی به سمت اقتصاد دیجیتالی هستیم. انقلابی که باعث تحول سازوکارهای کسب‌وکارها، مشتریان، سازمان‌ها و دیگر بازیگران این زیست‌بوم شده است [2]. ابعاد تاثیرگذاری انقلاب صنعتی چهارم تنها به اقتصاد ختم نمی‌شود، بلکه پتانسیل این فناوری‌های نوظهور برای حل چالش‌های بزرگ جهانی همانند فقر، نابرابری، تغییرات آب و هوایی و هدررفت منابع طبیعی وصف‌ناپذیر است [3].

در این میان، فناوری زنجیره‌بلوکی قرار دارد که در ابتدا به عنوان زیرساختی برای تولید اولین رمزارز شناخته شده دنیا [4] بیت‌کوین[۵] معرفی گردید [5]. حال به واسطه‌ی ویژگی‌های این فناوری نظیر ایمنی داده‌ها، شفافیت و اجتناب از تقلب، علاوه بر رمزارزها، کاربردهای بسیاری برای آن در حوزه‌های متفاوتی از جمله امور مالی، مدیریت دارایی، مدیریت زنجیره تامین و رأی‌گیری تعریف شده است [6]. علاوه بر موارد فوق، ماهیت امن، تغییرناپذیر، توزیع‌شده، و قابل ردیابی زنجیره‌بلوکی، باعث توسعه‌ی بسترهایی برپایه‌ی این فناوری برای مدیریت و حفاظت از داده‌ها، همچون مدیریت پرونده‌های الکترونیکی بیماران[۶] [7]، حفاظت از داده‌های شخصی به صورت توزیع‌شده [8] و ممیزی گواهی‌ها[۷] [9] گردیده است. علاوه‌براین، با توجه به امکان بهره‌برداری از زنجیره‌بلوکی به عنوان بستری زیرساختی، مطالعات بسیاری در زمینه امکان و چگونگی ترکیب آن با دیگر فناوری‌های نوظهور انجام شده که استفاده از زنجیره‌بلوکی به عنوان زیرساختی برای ارائه‌ی سرویس‌های اینترنت‌اشیاء بهره‌مند از هوش‌مصنوعی در لایه لبه از بهترین این موارد است [10, 11, 12, 13, 1, 14, 15, 16, 17].

---

۱ Blockchain
۲ Artificial Intelligence (AI)
۳ Internet of Things (IoT)
۴ Industry 4.0 (I4.0)
۵ Bitcoin
۶ Electronic Health Record (HER)
۷ Certificate Audit

به واسطه‌ی پتانسیل بی‌اندازه فناوری‌های نوظهور، آنها باعث رشد کسب‌وکارها و صنایع و حرکت آن‌ها به سمت تاثیر و مشارکت بیشتر [18] و رشد و افزایش نوآوری در مشاغل [19] شده‌اند. اما در مقابل، این فناوری‌ها، به دلیل تولید دریایی از داده‌ها شامل داده‌های حساس و شخصی [20] ملاحظات و چالش‌هایی امنیتی مرتبط با حریم خصوصی و امنیت داده‌ها را هم افزایش می‌دهند که اگر مدیریت نشوند، می‌توانند باعث مواجهه‌ی سازمان‌ها با مخاطرات جدی در حوزه حریم‌خصوصی و ایمنی داده‌ها شوند [18]. «داده، نفت جدید است و با نفت، هم آسایش و هم مصیبت همراه است» [20] . بنابراین استفاده از این فناوری‌ها، به نوعی همانند شمشیر دولبه می‌باشد، و ایجاد تعادل بین نوآوری و شفافیت، امنیت و نظارت اساساً فرآیندی دشوار است [21].

علیرغم فرصت‌های بی‌شماری که در اثر استفاده از این فناوری‌ها برای پیشرفت ایجاد می‌شود، پاسخ دولت‌ها و نهادهای نظارتگر به این فناوری‌ها براساس میزان مطابقت با الزامات امنیت داده، حریم خصوصی داده‌ها و سلامت شهروندان است. این پاسخ، در قالب طراحی و تدوین مقررات نظارتی در زمینه حفاظت از داده‌ها رخ داده است [22] . در همین راستا، قوانین بسیاری در کشورهای مختلف، برای حفاظت از داده‌های عمومی تدوین و اجرایی شده اند [23, 24, 25, 26, 27, 28, 29, 30, 31, 32] [33].

یکی از جامع ترین قوانین تدوین شده در جهت صیانت و حفاظت از داده‌ها، مقررات حفاظت از داده‌های عمومی[1] (GDPR) است [31]. این الزامات، که در سال ۲۰۱۶ تدوین و از ۲۵ مه سال ۲۰۱۸ اجرایی شده‌است. این مجموعه برای حفاظت از داده‌های شخصی شهروندان اتحادیه اروپا تدوین شده و شامل اصول و چارچوب‌هایی قابل اعمال برای هر سازمانی است که داده‌های شخصی و عمومی را پردازش می‌کنند. کسب‌وکارها هم به علت تحمیل قوانین توسط دولت‌ها، و همچنین جلب رضایت مشتریان و حتی کارمندان خود که داده‌هایی در این فضا دارند به پیروی از این قوانین روی آورده‌اند [20]. با حجم عظیم داده‌ها و چالش‌های تضمین پیروی از این الزامات، سازمان‌ها و نهادهای نظارتی به سمت استفاده از فناوری‌های نوظهور به عنوان بستری برای پشتیبانی از این مقررات حرکت نموده‌اند [34, 35, 36].

به دلیل ماهیت و ویژگی‌های زنجیره‌بلوکی، این فناوری یک فناوری محبوب در زمینه حکمرانی‌داده[2] محسوب می‌شود. به این دلیل، زنجیره‌بلوکی توجه بسیاری را به خود به عنوان بستری برای تضمین صیانت داده جلب کرده‌است [7] [37, 38, 39, 40, 41, 42, 43, 44, 45, 46]. در این تحقیق، به بررسی میزان انطباق این فناوری با اصول و الزامات مقررات حفاظت از داده‌های عمومی (GDPR) پرداخته خواهد شد. ساختار این تحقیق به این شرح است: در

[1] General Data Protection Regulation (GDPR)

[2] Data Governance

بخش ۲ مفاهیم و کاربردهای زنجیره‌بلوکی پرداخته خواهد شد؛ سپس در بخش ۳، درباره‌ی GDPR و اصول و الزامات آن صحبت می‌شود. در انتها، قابلیت انطباق ویژگی‌ها و معماری‌های مختلف زنجیره بلوکی به عنوان زیرساخت و بسترهای تأمین‌کننده الزامات GDPR در بخش ۴ مورد بررسی قرار خواهد گرفت.

۲- مفاهیم، مضامین و کاربردهای زنجیره‌بلوکی

ناوری زنجیره‌بلوکی، در ابتدا به عنوان زیرساختی برای توسعه‌ی رمز ارز بیت‌کوین توسط فرد، افرادی با نام مستعار ساتوشی ناکاموتو[۱] در سال ۲۰۰۸ معرفی شد [5]. از آن زمان، به دلیل ساختار توزیع شده و غیرمتمرکزش، توجهات بسیاری را به خود جلب کرد [39]. در پایه‌ای‌ترین نگاه، زنجیره‌بلوکی معرف یک پایگاه‌داده اشتراکی است که به صورت زنجیره‌ای از بلوک‌ها (گروه‌هایی از تراکنش‌ها) ذخیره می‌شود و داده به محض ورود و ثبت در زنجیره، غیرقابل تغییر خواهد شد [47]. این فناوری تعریف واحدی ندارد و از دیدگاه‌های مختلف، تعاریف متفاوتی پیرامون آن ارائه شده که تعدادی از آنها در قالب جدول (۱) ارائه شده است.

جدول ۱: تعاریف فناوری زنجیره‌بلوکی از دیدگاه‌های متفاوت

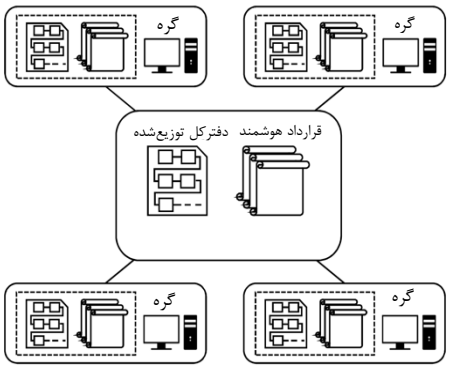
مولف	خلاصه تعریف	ویژگی‌های مهم	مؤلفه‌های کلیدی
دلویت[۲] [48]	زنجیره‌بلوکی معرف یک دفترکل دیجیتالی و توزیع‌شده از تراکنش‌ها است که به صورت بلادرنگ در شبکه‌ای از رایانه‌ها یا گره‌ها[۳] ثبت و تکرار می‌شود.	• توزیع شده • حذف نهادهای مرکزی • شبکه نظیر به نظیر • ایجاد اعتماد • اسناد تغییر ناپذیر	• دفترکل توزیع شده[۴] • سازوکار اجماع[۵] • بلوک • الگوریتم‌های رمزنگاری
آی‌بی‌ام[۶] [49]	زنجیره‌بلوکی معرف یک دفترکل[۷] اشتراکی و تغییرناپذیر[۸] است که فرآیند ثبت تراکنش‌ها و رهگیری دارایی‌ها در یک شبکه تجاری را تسهیل می‌کند.	• اسناد تغییر ناپذیر • توزیع شده • شبکه نظیر به نظیر	• دفترکل توزیع شده • قراردادهای هوشمند[۹] • بلوک‌ها

[۱] Satoshi Nakamoto
[۲] Deloitte
[۳] Node
[۴] Distributed Ledger
[۵] Consensus Mechanism
[۶] IBM
[۷] Ledger
[۸] Immutable
[۹] Smart Contracts

		• ایجاداعتماد، مسئولیت‌پذیری، شفافیت و امنیت بیشتر	
موسسه ملی فناوری و استانداردها[1] ایالات متحده[50]	زنجیره‌بلوکی معرف دفترکل‌هایی دیجیتالی آشکار و مقاوم در برابر دستکاری هستند که به صورت توزیع‌شده (به‌عنوان مثال، بدون مخزن مرکزی) و معمولاً بدون یک مرجع مرکزی (یعنی بانک، شرکت یا دولت) اجرا می‌شوند.	• حذف نهادهای مرکزی • مقاوم در برابر دستکاری • اسناد تغییر ناپذیر • توزیع شده	• دفترکل توزیع شده • بلوک‌ها • توابع درهم‌ساز[2] • الگوریتم‌های رمزنگاری
انجمن جهانی اقتصاد[3] [51]	زنجیره‌بلوکی، یک سیستم دفترکل توزیع‌شده دیجیتالی می‌باشد که سوابق رمزنگاری‌شده امن و تغییرناپذیر از هر تراکنش (از جمله تراکنش مالی، کالا، دارایی، کار، یا رأی) را ایجاد و نگه‌داری می‌کند.	• اسناد تغییرناپذیر • توزیع شده • شبکه نظیر به نظیر • امنیت	• دفترکل توزیع شده • قراردادهای هوشمند • الگوریتم‌های رمزنگاری

۲-۱- اجزای اصلی زنجیره‌بلوکی

همانگونه که بررسی شد، زنجیره‌بلوکی در دیدگاه‌های متفاوت، دارای تعاریف متفاوتی است و طبق هر تعریف شامل عناصر و اجزای متفاوتی خواهد بود. نمایی کلی از اجزای اصلی و مشترک یک شبکه زنجیره‌بلوکی (طبق تعاریف ارائه‌شده در جدول ۱) در قالب شکل (۱) ارائه شده است.



شکل ۱ : اجزای اصلی یک پلتفرم زنجیره‌بلوکی

[1] National Institue of Standards and Technology (NIST)

[2] Hash Functions

[3] World Economic Forum (WEF)

گره‌ها[۱]، گره‌ها اسکلت اصلی اجرای یک شبکه نظیربه‌نظیر همانند زنجیره‌بلوکی هستند [52] . به هر کامپیوتر و یا هر گونه دستگاهی که به عنوان یک عضو در یک شبکه‌ی زنجیره‌بلوکی است و یک کپی از زنجیره‌بلوکی را نگه‌داری می‌کند، گره می‌گویند [39]. به هر کامپیوتر و یا هر گونه دستگاهی که به عنوان یک عضو در یک شبکه‌ی زنجیره‌بلوکی است و یک کپی از زنجیره‌بلوکی را نگه‌داری می‌کند، گره می‌گویند. هر گره می‌تواند در شبکه نقش متفاوتی از جمله گره کامل[۲]، گره آرشیوی[۳]، گره تاییدگر[۴] ، گره سبک[۵] و یا گره استخراج‌گر[۶] را برعهده داشته باشند.

بلوک‌ها، همان‌گونه که پیش‌تر توضیح داده شد، تراکنش‌ها در قالب بلوک‌ها ذخیره می‌شوند. سپس این بلوک‌ها، در یک زنجیره قرار می‌گیرند و یک زنجیره‌بلوکی را ایجاد می‌کنند. بلوک‌ها اغلب شامل یک سربرگ[۷] و بدنه هستند. سربرگ بلوک‌ها شامل داده‌های مورد نیاز برای زنجیره‌سازی بلوک‌ها، زمان ایجاد بلاک، مقدار تابع درهم ساز[۸] برای بلوک قبلی و بلوک فعلی و ... است. در بدنه بلوک‌ها، تعداد و لیستی از تراکنش‌ها ذخیره می‌شود [53]. تراکنش‌ها شامل داده‌هایی نظیر فرستنده، گیرنده، مقدار دارایی منتقل‌شده و همچنین امضای دیجیتالی آن است. بلوک‌ها پس از فرآیند اجماع، به زنجیره بلوک‌های دفترکل توزیع‌شده اضافه می‌شوند [52] .

دفترکل توزیع‌شده، دفترکل توزیع‌شده معرف یک پایگاه داده است که مرتباً بین تمامی اعضای (گره‌های) شبکه، به اشتراک گذاشته شده و به‌روز می‌شود. برخلاف پایگاه‌داده‌ها و یا دفاترکل سنتی، این سازوکار به دلیل ماهیت توزیع‌شده آن‌ها، وابسته به یک موجودیت مرکزی برای تایید و به‌روزرسانی نیست و با استفاده از مکانیسم‌های متفاوت اجماع و از طریق اجماع بین اعضای شبکه بلوک‌ها را به‌روزرسانی می‌نماید و در تمامی کپی‌های آن بین تمام گره‌ها، اعمال می‌شود. دفترکل توزیع‌شده معرف مجموعه‌ای از بلوک‌ها است که به‌صورت زنجیره‌ای و با استفاده از تکنیک‌های رمزنگاری به یکدیگر متصل شده‌اند [53, 34, 52] .

قراردادهای هوشمند[۹]، قراردادهای هوشمند معرف پروتکل‌های تراکنش رایانه‌ای است که شرایط یک قرارداد را اجرا می‌کنند. آنها مجموعه‌ای از کُد و داده هستند که به وسیله‌ی تراکنش‌های رمزنگاری‌شده در شبکه زنجیره‌بلوکی

---

۱ Nodes
۲ Full Node
۳ Archival Node
۴ Validator Node
۵ Light Node
۶ Miner Node
۷ Header
۸ Hash Function
۹ Smart Contracts

بکارگیری می‌شوند. قراردادهای هوشمند توسط گره‌های درون شبکه قابل اجرا هستند. سنجش درستی قراردادهای هوشمند مستلزم آن است که خروجی همگی گره‌ها از اجرای یک قرارداد باید ثابت باشد، و این خروجی‌ها باید در دفترکل توزیع‌شده ثبت شوند [50].

مکانیسم‌های اجماع، به دلیل معماری غیرمتمرکز و حذف فرآیندهای مرکزی، نیاز به مکانیسمی برای توافق درباره‌ی وضعیت فعلی دفترکل و جلوگیری از ناسازگاری بین گره‌ها است. مکانیسم‌های اجماع معرف فرآیندهایی هستند که در آن، گره‌های درون یک شبکه در مورد وضعیت دفترکل، به توافق می‌رسند و در صورت نیاز، حالت آن را به‌روزرسانی می‌کنند [53] [39] . مکانیسم‌های اجماع پرکاربرد دربرگیرنده اثبات‌کار[۱]، اثبات‌سهم[۲] و تحمل خطای بیزانسی کاربردی[۳] هستند [53].

۲-۲- انواع زنجیره بلوکی

به‌طورکلی و بر اساس نگاه کنترلگران شبکه، می‌توان شبکه‌های زنجیره‌بلوکی را به ۲ دسته کلی بدون‌مجوز[۴] (یا عمومی[۵]) و مجوزمحور[۶] تقسیم نمود [1, 50, 37, 45, 55, 54]. البته در بسیاری از مطالعات، زنجیره‌های بلوکی مجوزمحور هم خود به دو دسته خصوصی[۷] و کنسرسیومی[۸] تقسیم می‌شوند. بنابراین بسیاری از متخصصان پلتفرم‌های زنجیره‌بلوکی را به ۳ دسته تقسیم می‌کنند [56, 55, 36, 54, 53, 52, 51, 50].

به صورت خلاصه، زنجیره‌بلوکی عمومی برای همگان قابل دسترس است. از این‌رو، همه گره‌ها در فرآیند اجماع مشارکت دارند و شبکه توسط یک شخص یا سازمان کنترل نمی‌شود. زنجیره‌های بلوکی مجوزمحور قابل دسترس عمومی نیستند و برای ورود به شبکه نیاز به مجوز کنترلگران پلتفرم است. شبکه‌های زنجیره‌بلوکی خصوصی توسط یک سازمان و شبکه‌های زنجیره‌بلوکی کنسرسیومی توسط گروهی از سازمان‌ها (کنسرسیوم) کنترل می‌شود [53]. قابلیت‌های این ۳ دسته از زنجیره‌های بلوکی به صورت مشروح در قالب جدول (۲) مقایسه شده است.

جدول ۲- مقایسه قابلیت‌های شبکه‌های مختلف زنجیره‌بلوکی

[۱] Proof-of-Work (PoW)
[۲] Proof-of-Stake (PoS)
[۳] Practical Byzantine Fault Tolerance (PBFT)
[۴] Permissionless
[۵] Public Blockchain
[۶] Permissioned
[۷] Private Blockchain
[۸] Consortium Blockchain

	بدون مجوز	مجوز محور	
ویژگی / نوع شبکه	عمومی	کنسرسیومی	خصوصی
شرکت‌کنندگان [56, 53, 50]	بدون مجوز اعضای ناشناس[1] شرکت‌کنندگان می‌توانند مخرب باشند (احتمال حملاتی نظیر حمله ۵۱ درصد)	مجوزمحور اعضای شناخته‌شده از یک سازمان شرکت‌کنندگان همگی قابل اعتماد هستند	مجوزمحور اعضای شناخته شده از چند سازمان شرکت‌کنندگان همگی قابل اعتماد هستند.
مکانیسم اجماع [57, 53]	مکانیسم‌های همگانی مانند اثبات‌کار یا اثبات‌سهم مصرف زیاد انرژی همه اعضاء می‌توانند در فرآیند اجماع شرکت نمایند	الگوریتم های سبک‌تر و سریع‌تر (همانند PBFT) مصرف کم انرژی اعضای انتخاب شده در فرآیند اجماع شرکت دارند	الگوریتم‌های سبک‌تر و سریع‌تر (همانند PBFT) مصرف کم انرژی اعضای انتخاب شده در فرآیند اجماع شرکت دارند
نرخ گذرداد [53, 58]	▪ پایین (در بیت‌کوین برابر با ۷ تراکنش در ثانیه)	▪ بالا	▪ بالا
دسترسی به دفترکل [59]	خواندن و نوشتن بدون نیاز به مجوز	خواندن مجوزمحور یا بدون مجوز است نوشتن نیاز به مجوز دارد	خواندن مجوزمحوز یا بدون مجوز است نوشتن نیاز به مجوز دارد
سرعت [57, 58]	▪ کُند (به دلیل عمومی بودن)	▪ سریع	▪ سریع
امنیت [50]	▪ مکانیسم‌های اجماع، امنیت شبکه را تامین می‌کنند.	▪ امنیت به دلیل شرکت‌کنندگان از قبل تایید شده است	▪ امنیت به دلیل شرکت‌کنندگان از قبل تایید شده است
موارد استفاده [60, 46, 61, 62, 63]	▪ رمزارزها معرف بستری برای توسعه نرم‌افزار است	▪ تراکنش‌های میان بانکی، مدیریت زنجیره تأمین، اشتراک داده‌های میان سازمانی	▪ تراکنش‌های درون‌بانکی، معاملات و امور مالی

۳-مفاهیم و الزامات مقررات حفاظت از داده‌های عمومی (GDPR)

همانگونه که پیش‌تر توضیح داده‌شد، ارزش و پتانسیل بی‌مانند فناوری‌های نوظهور همانند زنجیره‌بلوکی بر اساس حجم داده‌های انبوه و ظرفیت پردازش آنها مشخص می‌شود. به همین دلیل، امروزه با رشد استفاده از این فناوری‌ها توسط سازمان‌ها و در نتیجه رشد پردازش داده‌های شخصی و حساس توسط آنها، نهادهای نظارتی به سمت وضع قوانینی برای اعمال کنترل و حفاظت از داده‌های افراد حرکت نموده‌اند. در نتیجه این اقدامات، کشورها قوانین و الزاماتی

[1] Anonymouse

را برای حمایت از حریم‌خصوصی و داده‌های شخصی شهروندان خود تدوین کرده‌اند که تعدادی از مهم‌ترین آنها در قالب جدول (۳) مقایسه شده‌اند.

جدول ۳ : مقایسه قوانین حفاظت داده در کشورها (به جز اتحادیه اروپا)

قانون / ویژگی‌ها	آمریکا (CCPA) [64]	آمریکا (HIPAA) [65]	چین (PIPL) [66]	چین (DSL) [27]	روسیه (قانون فدرال -152 FZ) [67]	ژاپن (APPI) [28]	کانادا (PIPEDA) [25]
جامعیت و قلمرو	منطقه ای (ایالت کالیفرنیا)	صنفی (حوزه سلامت)	جامع (داده‌های شخصی)	جامع (انواع داده، بخصوص داده‌های حساس)	جامع	جامع	جامع (به غیر از مناطق و مشاغل خاص)
الزام به محلی‌سازی داده‌ها	خیر	خیر	لازم برای یکسری از داده‌ها	لازم	لازم برای یکسری از داده‌ها	خیر	خیر
حقوق موضوع‌داده	دسترسی، تصحیح، پاک‌سازی	دسترسی، تصحیح	دسترسی، تصحیح، پاک‌سازی	به طور واضح مشخص نشده	دسترسی، تصحیح، پاک‌سازی	دسترسی، تصحیح، پاک‌سازی	دسترسی، تصحیح، پاک‌سازی
نهاد مجری	دادستان کل کالیفرنیا	وزارت بهداشت و خدمات انسانی[1]	اداره فضای‌مجازی چین[2]	اداره فضای‌مجازی چین	خدمت‌فدرال نظارت بر ارتباطات، فناوری اطلاعات و رسانه‌های جمعی	PPC	دفتر کمیسیون حریم خصوصی
الزام به اخذ مجوز از موضوع‌داده	لازم	لازم	لازم	به طور واضح مشخص نشده	لازم	لازم	لازم

در نگاهی اجمالی و با شروع برخی از فعالیت‌ها از سال ۱۳۵۸ و اصل بیست و دوم در و همچنین بیست و پنجم قانون اساسی جمهوری اسلامی ایران می‌توان به سابقه‌ای از قوانین مطرح شده در راستای حفاظت از حریم‌خصوصی و

[1] Department of Health and Human Services (HHS)

[2] Cyberspace Adminstration of China (CAC)

داده‌های شخصی افراد در کشور ایران پرداخت [68]. نمایه‌ای از مهم‌ترین این موارد در قالب جدول (۴) ارائه شده است.

جدول ۴ : قوانین و مقررات اصلی حفاظت از داده در ایران

ردیف	عنوان	موضوع کلیدی مطرح شده
۱	اصل بیست و دوم قانون اساسی (۱۳۵۸)	تعرض غیرقانونی به حیثیت، جان، مال، حقوق، شغل و مسکن اشخاص را مد نظر قرارداده است.
۲	اصل بیست و پنجم قانون اساسی (۱۳۵۸)	دسترسی غیرمجاز به داده‌های شخصی مردم و نیز افشای آن را مدنظر قرار داده است.
۳	مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب شورای‌عالی انقلاب فرهنگی (۱۳۸۰)	وظایف سرویس‌دهنده‌های اینترنتی که دربرگیرنده حریم‌خصوصی کاربران و تعیین جرایم افشاء است.
۴	قانون تجارت الکترونیکی (۱۳۸۲)	حمایت از داده پیام‌های شخصی را مدنظر قرار داده است.
۵	قانون جرائم رایانه‌ای (۱۳۸۸)	دسترسی غیرمجاز به اطلاعات را مدنظر قرار داده است.
۶	منشور حقوق شهروندی (۱۳۹۵)	بند ۱- تفکیک حریم عمومی از حریم‌خصوصی و نهادینه کردن خدمت در هر دو حریم را مدنظر قرار داده است که متاسفانه جزئیاتی پیرامون آن اشاره نشده‌است.
۷	قانون انتشار و دسترسی آزاد به اطلاعات	بند «ب» ماده ۱ قانون- اطلاعات شخصی معرف اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.
۸	ماده ۱۳۰ قانون برنامه چهارم توسعه (۱۳۸۳)	لایحه «حفظ و ارتقاء حقوق شهروندی و حمایت از حریم‌خصوصی افراد، در راستای اجرای اصل بیستم قانون اساسی جمهوری اسلامی ایران» توسط قوه قضائیه تدوین می‌شود.
۹	قانون برنامه پنجم توسعه (۱۳۹۴-۱۳۹۰)	▪ تبصره ماده ۲۰۶- عدم افشاء اطلاعات ▪ بند الف ماده ۳۵- صیانت از اطلاعات پزشکی
۱۰	بند «ب» اساسنامه سازمان بیمه سلامت ایران	تشکیل و صیانت از پرونده الکترونیکی سلامت افراد مدنظر است.
۱۱	بند ۴ ماده ۱۲ دستورالعمل تشکیل بانک اطلاعات هویت ژنتیک ایران	دستورالعمل حفاظت از اطلاعات ژنتیکی در آزمایشگاه‌ها را مدنظر قرار داده‌است.
۱۲	مصوبه شورای‌عالی اداری در خصوص منشور حقوق شهروندی (۱۳۹۵)	تمهیدات فنی و قانونی لازم را برای حفظ حریم‌خصوصی افراد و تأمین امنیت داده‌های شخصی آنان توسط قوه قضائیه مدنظر قرار دهد.
۱۳	لوایح وزارت اطلاعات و فناوری اطلاعات	▪ پیش‌نویس لایحه حمایت از داده‌ها و حریم‌خصوصی در فضای مجازی (دی ماه ۱۳۹۶) ▪ پیش‌نویس صیانت و حفاظت از داده‌های شخصی (تیرماه سال ۱۳۹۷)

اما یکی از جامع‌ترین قوانین تدوین شده در جهت صیانت از داده‌های شخصی کاربران [69]، مجموعه الزاماتی به نام «مقررات حفاظت از داده‌های عمومی» یا همان GDPR است، که در ماه آوریل سال ۲۰۱۶ وضع و پس از دو سال اجرای آزمایشی، سرانجام از ماه مه سال ۲۰۱۸، در کشورهای عضو اتحادیه اروپا اجرایی گردید. GDPR معرف مجموعه‌ای از الزامات و اقدامات تدوین شده در ۱۱ بخش و ۹۹ ماده، در جهت حفظ و حمایت از حریم‌خصوصی و داده‌های شخصی در سطح کشورهای عضو اتحادیه اروپا است که بر هر سازمان و نهادی (در هر نقطه از جهان) که داده‌های شخصی شهروندان اتحادیه اروپا را پردازش می‌کنند، قابل اعمال است. این الزامات شامل ۷ اصل کلیدی برای پردازش داده‌ها است که در قالب جدول (۵) ارائه شده است. پس از معرفی اصول، باقی بخش‌های GDPR در قالب مجموعه‌ای از حقوق و الزامات پیرامون بازیگران متفاوت در زنجیره پردازش اطلاعات بیان شده است. نقش‌های هدف اصلی این الزامات در قالب جدول (۶) معرفی و در ادامه آن خلاصه‌ای از حقوق و مسئولیت‌های متوجه هر کدام از آنها بیان شده است.

جدول ۵ : اصول پردازش داده‌ها در GDPR

ردیف	موضوع اصل پردازش	موضوع کلیدی مطرح شده
۱	قانونی بودن، انصاف و شفافیت[۱]	پردازش اطلاعات کاملاً قانونی، منصفانه و همراه با شفافیت و با رضایت کامل موضوع داده (افراد) همراه است.
۲	محدودیت در اهداف پردازش[۲]	داده برای اهداف مشخص، صریح و قانونی جمع‌آوری شده و به صورتی پردازش نشود که ناسازگار با این اهداف است. پردازش بیشتر برای دستیابی به اهداف مربوط به منافع عمومی، اهداف علمی، تحقیقات تاریخی یا اهداف آماری باید ناسازگار با اهداف اولیه تلقی نشود.
۳	حداقل‌سازی داده‌ها[۳]	فقط داده‌های لازم و کافی، مرتبط و محدود به آنچه برای هدف لازم است مورد پردازش قرار گیرد و میزان داده‌های موردنیاز در پردازش به حداقل برسد.
۴	دقت[۴]	داده‌های افراد دقیق و در صورت لزوم به‌روز باشد. در این راستا باید هر اقدام معقول انجام شود تا اطمینان حاصل گردد که داده‌های شخصی دقیق هستند و با توجه به اهداف پردازش آن‌ها، بدون تأخیر به‌روزرسانی، پاک یا اصلاح می‌شوند.

[۱] Lawfulness, fairness and transparency

[۲] Purpose limitation

[۳] Data minimisation

[۴] Accuracy

۵	محدودسازی فضای ذخیره‌سازی[۱]	داده‌ها به شکلی نگهداری می‌شوند که امکان شناسایی سوابق داده را برای بیش از اهداف پردازش داده‌های شخصی فراهم نکند. در مواردی که داده‌های شخصی صرفاً برای اهداف عمومی، علمی-پژوهشی، تاریخی و یا آماری ذخیره و برای مدت طولانی نگهداری گردد باید مصادیق و موارد موردنیاز به منظور پاسداری از حقوق و آزادی‌های موضوع داده تبیین شوند.
۶	یکپارچگی و محرمانگی[۲]	داده‌ها باید به روشی پردازش شوند که یک سطح امنیتی مناسب برای داده‌های شخصی نظیر محافظت در برابر پردازش غیرمجاز یا غیرقانونی و از بین رفتن تصادفی، تخریب یا آسیب به داده‌ها با استفاده از اقدامات فنی و سازمانی کارآمد تضمین شود.
۷	مسئولیت‌پذیری[۳]	کنترل‌کننده باید مسئولیت انطباق موارد فوق‌الذکر را بر عهده داشته و بتواند سازگاری با اصول حفاظ از داده را اثبات نماید.

جدول ۶ : بررسی تعریف، حقوق و مسئولیت‌های نقش‌های اصلی تعریف‌شده در GDPR

نقش	تعریف نقش	حقوق و مسئولیت‌ها
موضوع داده	به هر فرد مشخصی اطلاق می‌شود که به‌طور مستقیم یا غیرمستقیم از طریق شناسه‌ای مانند نام، شماره شناسنامه، داده‌های محل یا از طریق فاکتورهای اختصاصی جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و یا هویت اجتماعی شناسایی شود (ماده ۴- بند ۱).	▪ حق دسترسی به داده‌ها ▪ حق تصحیح داده‌ها ▪ حق فراموش‌شدن ▪ حق محدودسازی پردازش داده ▪ حق انتقال داده‌ها ▪ حق اعتراض ▪ حق رضایت برای پردازش ▪ حق لغو مجوز پردازش داده ▪ حق شکایت به نهاد نظارتگر
کنترلرگر داده	شخص حقیقی یا حقوقی، مرجع عمومی، سازمان یا نهاد دیگر است که به تنهایی یا به طور مشترک با دیگران اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کند (ماده ۴- بند ۷).	▪ اطمینان از پردازش داده تنها در چارچوب تعیین شده توسط خود و پردازشگران ▪ رعایت اصول پردازش مندرج در GDPR ▪ استفاده از پردازشگرها برای پردازش داده‌ها در چارچوب تعیین شده ▪ حق انتقال داده‌های به شرکت ثالث (با چارچوب‌های امنیتی مشخص) ▪ جمع‌آوری داده‌های موضوع داده با پیروی از GDPR و عدم نقض آن ▪ طراحی و پیاده‌سازی ساختاری ایمن جهت پردازش داده‌ها

[۱] Storage limitation

[۲] Integrity and confidentiality

[۳] Accountability

نقش	تعریف نقش	حقوق و مسئولیت‌ها
		▪ نگه‌داری سوابق پردازش‌داده‌ها ▪ همکاری با نهادهای نظارتی ▪ برگزاری آزمون‌های مداوم در جهت اطمینان از امنیت پردازش داده‌های حساس
پردازشگر داده	شخص حقیقی یا حقوقی، مقامات دولتی، سازمان یا نهاد دیگری است که داده‌های شخصی را از طرف کنترل کننده پردازش می‌کند (ماده ۴- بند ۸).	▪ پردازش داده تنها در چارچوب تعیین شده توسط کنترلگر ▪ رعایت اصول پردازش مندرج در GDPR ▪ دخالت‌دادن پردازشگرهای دیگر در امر پردازش و در چارچوب مشخص شده توسط کنترلگر، تنها با مجوز کتبی آن ▪ طراحی و پیاده‌سازی ساختاری امن جهت پردازش‌داده‌ها و انتقال داده‌ها ▪ دفاع در دعاوی قانونی در مقابل دادگاه یا نهادهای نظارتگر از پردازش قانونی ▪ اطلاع بلادرنگ در هنگام افشای اطلاعات ▪ همکاری با نهادهای نظارتی ▪ برگزاری آزمون‌های مداوم در جهت اطمینان از امنیت پردازش داده‌های حساس
نهاد نظارتگر	هر کشور عضو باید یک یا چند نهاد نظارتگر دولتی مستقل را با مسئولیت نظارت بر کاربرد این مقررات، با هدف حفظ حقوق و آزادی اشخاص حقیقی در ارتباط با پردازش و تسهیل جریان آزاد داده‌های فردی، در سراسر اتحادیه، معرفی کند (ماده ۵۱- بند ۱).	▪ نظارت و صدور اخطار، توبیخ و ابلاغ دستورات به کنترلگران و پردازشگران در چارچوب GDPR و یا در صورت تخطی ▪ حق بازرسی و انجام تحقیقات نسبت به کنترلگران، پردازشگران و (در صورت وجود) نمایندگان آنان برای بررسی پیروی از الزامات و احتمال تخطی از آنها ▪ دسترسی به تمام داده‌های شخصی و پردازش‌های انجام شده روی آنها ▪ اعمال محدودیت‌ها و یا منع پردازش به صورت موقت یا دائمی ▪ منع انتقال داده به کشورهای ثالث یا شرکت‌های بین‌المللی ▪ ارجاع نقض قوانین توسط هر یک از نهادها به مراجع قضایی ▪ مشاوره و نظارت بر پیاده‌سازی سازوکارهای پیرو اصول GDPR توسط کنترلگران و پردازشگران ▪ افزایش آگاهی عمومی نسبت به حقوق موضوع‌داده

۴-بررسی و تحلیل پیروی از الزامات GDPR در بستر زنجیره بلوکی

با رشد روزافزون فناوری‌های نوظهور و امکانات بسیاری که با استفاده از آنها در اختیار اصناف و مشاغل مختلف قرار می‌گیرد، شرکت‌ها به سمت بهره‌برداری از این فناوری‌ها حرکت می‌نمایند. طبق بند ۲۵ مقررات GDPR مبنی بر «حفاظت داده با طراحی و به صورت پیش‌فرض»، کنترل‌گران داده الزام دارند تا از طراحی‌ها و ساختارهایی به‌روز و مناسب برای حفاظت از داده‌ها استفاده کنند. این بند، کنترلگران و پردازشگران داده را به سمت استفاده از زنجیره‌بلوکی به واسطه داده‌ها رمزگذاری شده، امن و بدون نقطه شکست[۱] سوق می‌دهد. علی ایحال، با تبیین الزامات حفاظت از داده‌های شخصی همانند GDPR سازمان‌ها به پیروی از آن‌ها الزام دارند. از این‌رو، در بخش حاضر به بررسی قابلیت انطباق بین زنجیره‌بلوکی با مقررات حفاظت از داده‌های عمومی پرداخته خواهد شد.

با بررسی الزامات GDPR پی خواهید برد که تمرکز این الزامات، بر یک محیط متمرکز به جای یک محیط غیرمتمرکز است. در واقع، کل این مقررات وجود یک کنترلگر داده را فرض می‌کند که اهداف و ابزار پردازش داده‌ها را تعیین می‌کند و همچنین قادر به شناسایی، ارائه مجوز و نظارت دائمی بر پردازشگرهای داده است. GDPR به موضوع داده این حق را می دهد که اطلاعات شخصی خود را پاک کند یا در صورت لزوم اصلاح کند و تغییراتی را در آن ایجاد کند. بنابراین چنانچه شرکتی داده‌های مشتریان خود را در شبکه‌ی زنجیره‌بلوکی ذخیره کند، در تامین این دسته از الزامات دچار ناسازگاری با قوانین و مقررات حفاظت از داده خواهد شد [43]. البته این فناوری، مزیت‌هایی هم دارد که به پیروی و اطاعت از الزامات GDPR کمک شایانی می‌کند. در ادامه از دو دیدگاه معماری نوع زنجیره بلوکی و قابلیت‌های فناوری به سنجش میزان انطباق این فناوری با الزامات GDPR پرداخته خواهد شد.

۴-۱- زنجیره‌بلوکی و پیروی از الزامات GDPR از منظر معماری فناوری

به‌طورکلی مشکلاتی نظیر ناشناس‌سازی داده‌های شخصی، اصل به حداقل رسانی داده‌ها، در هر دو نوع معماری‌های زنجیره‌بلوکی وجود دارد و به‌عنوان یک عامل بازدارنده در پیروی از الزامات GDPR مطرح است. البته این امر با استفاده از معماری مناسب و ملاحظات خاص قابل حل است. در ادامه به بررسی مجموعه این ملاحظات پرداخته خواهد شد.

معماری زنجیره‌بلوکی بدون‌مجوز (عمومی) و الزامات GDPR استفاده از یک بستر زنجیره‌بلوکی با معماری بدون‌مجوز (عمومی) توانایی انطباق بالایی را با قوانین و مقررات GDPR ندارد. به‌عنوان مثال، یکی از عوامل بازدارنده مهم زنجیره‌بلوکی (به‌خصوص زنجیره‌بلوکی عمومی) در حوزه الزامات GDPR به مشکل حق فراموشی اظهار شده در حقوق موضوع داده مربوط می‌شود. این بازدارندگی به‌خاطر ماهیت تغییرناپذیر دفترکل در معماری زنجیره‌بلوکی است.

[۱] Single point of failure

از دیگر مشکلات مختص به معماری زنجیره‌بلوکی عمومی، انتقال داده به کشورهای ثالث خارج اتحادیه اروپا و دیگر پردازشگران است؛ چرا که به‌صورت کلی، تمامی گره‌های شبکه، یک کپی از تمام زنجیره‌بلوکی را دارند [39]. از سوی دیگر، در زنجیره‌های بلوکی عمومی، علیرغم اینکه یکپارچگی و محرمانگی داده می‌تواند حفظ شود، اما در برقراری امنیت داده مشکلاتی وجود دارد [45]. علاوه‌براین، یکی دیگر از مشکلاتی که در معماری‌های زنجیره‌بلوکی بدون‌مجوز (عمومی) همانند بیت‌کوین با آن مواجه هستیم، عدم توانایی تمایز واضح و مشخص بین نقش‌های موضوع داده و کنترلگر/ پردازشگر داده است [54]. در زنجیره‌های بلوکی عمومی، به دلیل عدم توانایی تمایز بین نقش‌ها، امکان مسئولیت‌پذیری و پاسخگویی هم میسر نیست؛ چرا که موجودیت کنترلگر یا پردازشگر به‌راحتی قابلیت شناسایی نیستند [70].

معماری زنجیره‌بلوکی مجوزمحور (خصوصی و کنسرسیومی) و الزامات GDPR تفاوت اصلی معماری مجوزمحور با معماری عمومی، حضور گره‌ها با مجوز قبلی است. یکی از برتری‌های این نوع معماری به امکان اعمال محدودیت‌ها و اعمال نظارت با سطح بالاتر برای خواندن و نوشتن و دسترسی به داده‌ها مربوط می‌شود [62]. علاوه‌براین، کنترلگر داده نسبت به پردازش داده تنها در چاچوب تعیین شده توسط خود و پردازشگران پاسخگو است. این اصل در زنجیره بلوکی خصوصی و مجوزمحور رعایت می‌شود و زنجیره‌بلوکی عمومی و بدون مجوز با این اصل GDPR انطباقی ندارد [71]. طبق ماده ۱۶ از GDPR، موضوع داده این حق را دارد که درخواست اصلاح و تصحیح داده‌های نادرست را به کنترلگر داده ارسال نماید و نتیجه‌ی این اصلاح را از کنترلگر داده بدون تاخیر اضافی دریافت کند. بنابراین، موضوع داده این حق را دارد که داده‌های ناقص را از طریق ارائه بیانیه تکمیلی، اصلاح نماید. این در حالی است که در فناوری زنجیره‌بلوکی، داده‌ها در دفاترکل توزیع‌شده و تغییرناپذیر ذخیره می‌شوند. به‌صورت‌کلی زنجیره‌بلوکی نمی‌تواند قابلیت برگشت‌پذیری را پوشش دهد [72]. البته زنجیره‌بلوکی خصوصی و مجوز محور می‌تواند از طریق تغییر سابقه تراکنش‌های مربوطه به درهم‌سازی مجدد بلوک‌های بعدی، از چنین درخواست‌هایی پشتیبانی نماید [37]. همانطور که در معماری عمومی گفته شد، مشکل عدم توانایی تمایز نقش‌ها در معماری زنجیره‌بلوکی عمومی، در زنجیره‌بلوکی خصوصی و مجوزدار به‌راحتی قابل حل است [54]. لازم به ذکر است که استفاده از شبکه‌های زنجیره‌بلوکی مجوزمحور همانند هایپِرلجِر فبریک[1] برای جلوگیری از جعل هویت کاربران توسط عوامل و موجودیت‌های ناشناس و تایید نشده موثر است؛ که این امر سبب نظارت بر شبکه و پایداری بیشتر آن خواهد بود. این ویژگی با اصول «استفاده از مکانیزم‌های امنیتی مناسب توسط کنترلگران و پردازشگران» منطق است [43]. علاوه بر موارد ذکر شده، به دلیل احراز هویت

[1] Hyperledger Fabric

موجودیت‌های وارد شده در زنجیره‌بلوکی مجوزمحور، امکان پیاده‌سازی قابلیت حق فراموش‌شدن توسط موضوع داده با استفاده از تکنیک‌هایی نظیر ذخیره‌سازی خارج زنجیره با فعال‌سازی این قابلیت برای گره‌های مورد تایید قابل پیاده‌سازی است [34]. برخلاف زنجیره‌بلوکی عمومی، در زنجیره‌های بلوکی کنسرسیومی و یا خصوصی به دلیل احراز هویت پیش از ورود به شبکه نقش‌ها قابل تمایز هستند و امکان فراهم‌سازی اصل مسئولیت‌پذیری در آنها فراهم است [70].

مقایسه‌ای از میزان تطبیق و بازدارندگی انواع مختلف زنجیره‌بلوکی نسبت به اصول و حقوق موضوع‌داده در GDPR در قالب جدول (۷) ارائه شده‌است.

جدول ۷ : تطبیق مقررات، اصول و حقوق موضوع‌داده در GDPR با انواع زنجیره‌بلوکی (دیدگاه معماری)

	اصول، مقررات و حقوق / نوع	عمومی	خصوصی	کنسرسیوم
مقررات	امنیت	✗	✓	✓
	تمایز نقش‌ها و مسئولیت‌ها (کنترلگر و پردازشگر داده)	✗	✓	✓
اصول	قانونی بودن، انصاف و شفافیت	شفافیت ✓	شفافیت ✓	شفافیت ✓
	محدودیت در اهداف پردازش	✗	✓	✓
	حداقل‌سازی داده‌ها	–	–	–
	دقت	✗	✗	✗
	محدودسازی فضای ذخیره‌سازی	✗	✗	✗
	یکپارچگی و محرمانگی	یکپارچگی ✗	یکپارچگی ✓	یکپارچگی ✓
		محرمانگی ✓	محرمانگی ✓	محرمانگی ✓
	مسئولیت‌پذیری	✗	✓	✓
حقوق موضوع‌داده	حق دسترسی	✓	✓	✓
	حق تصحیح	✗	✓	✓
	حق فراموش‌شدن (پاک‌کردن)	✗	✓	✓
	حق محدودیت پردازش	✗	✗	✗
	حق انتقال داده	✗	✗	✗
	حق رضایت	✓	✓	✓

۴-۲-زنجیره‌بلوکی و پیروی از الزامات GDPR از منظر قابلیت‌های فناوری

مجموعه‌ای از قابلیت‌ها به صورت ذاتی در زنجیره‌بلوکی وجود دارند که در برخی از موارد باعث انطباق در پیروی از الزامات GDPR می‌شوند و گاهی اوقات هم باعث بازدارندگی در پیروی درست از این الزامات گردیده‌اند. در ادامه، مهم‌ترین ویژگی‌های زنجیره‌بلوکی و میزان انطباق آن‌ها با الزامات GDPR بررسی خواهند شد.

قرارداد هوشمند و الزامات GDPR، در توسعه سامانه‌های هماهنگ با GDPR در بستر زنجیره‌بلوکی دارای قرارداد هوشمند، نویسندگان این قراردادها به عنوان کنترلگر و خود قرارداد هوشمند به عنوان پردازشگر داده شناسایی می‌شوند. بر این اساس، می‌توان از انتقال داده بین کنترلگر و پردازشگر طبق قرارداد تعیین‌شده، عدم تخطی از آن و نیز مشخص‌سازی نقش‌ها و عملکرد درست آنها اطمینان حاصل نمود [40]. استفاده از قراردادهای هوشمند و ذخیره‌سازی داده‌ها در فضاهای خارج از زنجیره‌بلوکی (همانند سیستم فایل جهانی[1])، می‌تواند سازوکار زنجیره‌بلوکی را به نحوی تنظیم کند که امکان تغییر در داده و حذف آن فراهم شود [73]. علاوه‌براین، قراردادهای هوشمند را می‌توان به گونه‌ای نوشت که تمام حقوق دسترسی را لغو کند و یا محتویات (یعنی شرایط دسترسی و داده های شخصی موجود در آن) را پس از یک دوره زمانی معین حذف و اطلاعات شخصی را غیرقابل دسترس نماید.

همچنین با استفاده از قراردادهای هوشمند می‌توان از پردازش در چارچوب تعیین شده و عدم تخطی از دستورالعمل‌های پردازش (همانند الزامات اصل‌های ۲۵، ۲۸، ۲۹ و حقوق موضوع‌داده نظیر بندهای a، b، f از اصل ۵-۱ و اصل ۵-۲)، اطمینان حاصل نمود.

ساختاری توزیع‌شده و الزامات GDPR، پایگاه‌داده در زنجیره‌بلوکی معرف یک پایگاه‌داده توزیع شده است که به توزیع مسئولیت در همه طرف‌های درگیر می‌انجامد. از طرفی توزیع داده‌ها در یک دفترکل مشترک، با جمع‌آوری هدفمند داده، حداقل‌سازی داده‌ها و محدودیت‌های ذخیره‌سازی -که در اصول مندرج در GDPR ذکر شده است منطق نمی‌باشد. به‌طورکلی، GDPR دید متمرکز نسبت به معماری سامانه دارد، ولی همانطور که پیش‌تر گفته شد، زنجیره‌بلوکی یک دفترکل توزیع‌شده است که دید غیرمتمرکز نسبت به تمامی گره‌ها دارد که با GDPR منطبق نیست و این مشکل باید با دیگر قابلیت‌های فناوری نظیر الگوریتم‌های اجماع و یا معماری متمرکز حل شود.

الگوریتم‌های اجماع و الزامات GDPR، از الگوریتم‌های اجماع برای ارائه یک شبکه‌ی ایمن و تایید تراکنش‌های درست در یک معماری غیرمتمرکز استفاده می‌شود. رمزنگاری، الگوریتم‌های اجماع (همانند اثبات‌کار و اثبات‌سهم)، امضای ناشناس، فضای ذخیره‌سازی خارج از زنجیره و اثبات‌های دانش صفر[2] سبب می‌شود تا الزامات و ویژگی‌های مفاهیم اعتبار، ناشناس بودن و شفافیت تامین گردد [74]. در صورتی که شبکه‌ی زنجیره‌بلوکی عمومی (بدون عضو

[1] Interplanetary File System (IPFS)

[2] Zero-knowledge-proofs (ZKPs)

خطاکار) و یا ترکیبی (که از هویت افراد مطمئن بوده ولی زنجیره‌بلوکی عمومی هم پیاده‌سازی شده است) استفاده شود، امکان استفاده از قوانین تایید همه‌گانی قبل از تایید هر تراکنش با پیاده‌سازی و استفاده از الگوریتم‌ها و مکانیزم‌های اجماع مناسب وجود دارد. این امر به پیاده‌سازی سیاست‌های تایید تراکنش به منظور پیروی تراکنش‌ها از قوانین شفاف و نیز اجرای تراکنش‌های قانون‌مند و در راستای اصول پردازش، کمک شایانی می‌نماید [75].

ذخیره‌سازی خارج از زنجیره[1] و الزامات GDPR، یکی از دلایل بازدارندگی توسعه بستری بر پایه زنجیره‌بلوکی برای پیروی از الزامات GDPR به اصل ۱۷ این مقررات مبنی بر حق فراموشی برای موضوعات داده مربوط می‌شود. این مشکل با استفاده از تکنیک ذخیره‌سازی داده‌های اصلی خارج از زنجیره‌بلوکی و استفاده از مقادیر نگاشتی با تابع درهم‌سازی، قابل حل است [76]. البته همانطور که در بخش‌های قبلی توضیح داده‌شد، اصل ۱۶ از الزامات GDPR به حق اصلاح اطلاعات اشاره دارد، که با استفاده از این تکنیک، قابل حل است [71]. علاوه‌براین، یکی دیگر از ویژگی‌های زنجیره‌بلوکی که باعث پشتیبانی از حقوقی نظیر شفافیت، اعتبار و ناشناس بودن می‌شود، استفاده از ذخیره‌سازی خارج از زنجیره است [74] که باعث رعایت اصل حداقل‌سازی فضای ذخیره‌سازی نیز می‌گردد. همان‌گونه که در بخش قراردادهای هوشمند بیان شد، با استفاده از فضاهای ذخیره‌سازی خارج از زنجیره (همانند IPFS)، می‌توان حق تصحیح و فراموشی موضوع‌داده را برقرار نمود [73].

رمزنگاری و توابع درهم‌سازی و الزامات GDPR، یکی از مشکلاتی که رمزنگاری و مقادیر توابع درهم‌سازی حل می‌کنند، مشکل مستعارسازی است. یکی از راه‌های حفاظت از داده‌ها استفاده از نام مستعار است. طبق ماده (۴) از الزامات GDPR، استفاده از نام مستعار به این معنی است که پردازش داده‌ها باید به گونه‌ای انجام گیرد که امکان نسبت دادن داده خصوصی و شخصی به موضوع داده خاص بدون استفاده از اطلاعات اضافی وجود نداشته باشد. این خواسته زمانی محقق می‌شود که نام و شناسه‌های موضوع داده با یک نام مستعار جایگزین شود. استفاده از نام مستعار به این معنی نیست که شخص حقیقی دیگر قابل شناسایی نیست، بلکه اطلاعات هویتی وی همچنان به عنوان داده شخصی در نظر گرفته می‌شود [42]. به‌طورکلی در زنجیره‌بلوکی، استفاده از مقادیر توابع درهم‌سازی به‌عنوان یک تکنیک نام مستعار در نظر گرفته می‌شود. براین اساس، ناشناس‌سازی داده به معنی تغییر داده‌های شخصی است که منجر به عدم وجود پیوند بین داده و فرد می‌شود [44].

همانطور که در بخش‌های پیشین هم گفته شد، برخی از قابلیت‌ها و ویژگی‌های زنجیره‌بلوکی مستقل از معماری و ویژگی‌های پیاده‌سازی‌شده رابطه‌ای در تضاد یا در راستای الزامات GDPR دارند. به‌عنوان مثال، حق فراموشی توسط

[1] Off-chain storage

موضوع‌داده یکی از موضوعات مطالعاتی در زمینه‌ی انطباق زنجیره‌بلوکی با الزامات GDPR است، چرا که به دلیل تغییرناپذیری، زنجیره‌بلوکی حقوق فراموش‌شدن و تصحیح اطلاعات را به طور پیش‌فرض تامین نمی‌کند. هر چند با استفاده از تکنیک‌هایی نظیر ذخیره‌سازی داده خارج از زنجیره، می‌توان این امکان را فراهم آورد. از طرف دیگر، ماهیت تغییرناپذیر زنجیره‌بلوکی، قابلیت ذخیره‌ی سابقه‌ی مجوزهای موضوعات‌داده را فراهم می‌آورد. که از آنجایی که این داده غیرقابل تغییر و قابل ردیابی است، این محیط به بستری مناسب برای ذخیره‌ی سابقه‌ی مجوزهای گرفته شده از موضوع‌داده طبق اصول GDPR تبدیل می‌شود [78] [77]. پیاده‌سازی مکانیزمی برای ارائه سابقه پردازش‌ها به نهادهای نظارتگر مستلزم ماهیت توزیع‌شده و تغییرناپذیر این فناوری است که موجب انطباق زنجیره بلوکی با این اصل GDPR شده است [34]. در مقابل این مورد، اصل‌های دقت و حداقل‌سازی حافظه در GDPR معرف مشکلاتی است که هر ۳ نوع عمومی، خصوصی و کنسرسیومی زنجیره‌بلوکی با آن روبه‌رو هستند. دلیل این امر آن است که تصحیح داده‌های تراکنش‌های ذخیره شده در زنجیره‌بلوکی امری غیرممکن است. علاوه‌براین، داده‌های بلااستفاده، قابل پاک کردن نیستند. بنابراین مشکل حداقل‌سازی حافظه همواره وجود دارد و زنجیره‌های بلوکی با آن روبه‌رو هستند[70].

نتایج بررسی تطبیقی قابلیت‌های زنجیره‌بلوکی با اصول، مقررات و حقوق موضوع‌داده در GDPR در قالب جدول (۸) ارائه شده است.

جدول ۸ : تطبیق مقررات، اصول و حقوق موضوع‌داده در GDPR با قابلیت‌های زنجیره‌بلوکی

	اصول، مقررات و حقوق / نوع	قراردادهای هوشمند	ساختار توزیع‌شده	ذخیره‌سازی خارج زنجیره	مکانیزم‌های اجماع	رمزنگاری و درهم‌سازی
مقررات	حریم خصوصی					✓
	امنیت	✓	✓			✓
	تمایز نقش‌ها و مسئولیت‌ها (کنترلگر و پردازشگر داده)	✓	×		✓	
اصول	قانونی بودن، انصاف و شفافیت	✓				
	محدودیت در اهداف پردازش	✓	×		✓	
	حداقل‌سازی داده‌ها		×			
	دقت و صحت			✓		✓
	محدودسازی فضای ذخیره‌سازی		×	✓ (می‌تواند مساعدت کند)		✓ (می‌تواند مساعدت کند)

	اصول، مقررات و حقوق / نوع	قراردادهای هوشمند	ساختار توزیع‌شده	ذخیره‌سازی خارج زنجیره	مکانیزم‌های اجماع	رمزنگاری و درهم‌سازی
	یکپارچگی و محرمانگی	✓	یکپارچگی ×			✓
	مسئولیت‌پذیری		×			
حقوق موضوع‌داده	حق دسترسی	✓			✓	
	حق تصحیح	✓		✓		✓
	حق فراموش‌شدن (پاک‌کردن)	✓		✓		✓
	حق محدودیت پردازش		×			
	حق انتقال داده	✓			✓	
	حق رضایت	✓			✓	

۵- نتیجه‌گیری

طراحی بستری منطبق با GDPR بر پایه‌ی زنجیره‌بلوکی، فرصت‌ها و همینطور چالش‌های قابل توجهی را با خود به همراه دارد. ماهیت امن، شفاف و غیرقابل دستکاری زنجیره‌بلوکی، می‌تواند آن‌را به گزینه‌ای محبوب و قدرتمند برای طراحی بسترهای منطبق بر قوانین صیانت از حریم‌خصوصی کاربران تبدیل کند. در این مطالعه، به بررسی قابلیت انطباق این فناوری نوظهور، با چارچوب قوانین GDPR پرداختیم و این انطباق را به صورت مشروح از منظر معماری و ویژگی‌های زنجیره‌بلوکی، مورد تحلیل قرار دادیم. در نتیجه، به طور کلی می‌توان قوانین GDPR را از منظر امکان انطباق با ویژگی‌ها معماری‌های زنجیره‌بلوکی، به ۳ دسته اصلی تقسیم کرد:

۱- قوانینی که با ماهیت زنجیره‌بلوکی منطبق می‌باشند (از جمله امنیت و شفافیت).

۲- قوانینی که با ماهیت زنجیره‌بلوکی در تضاد می‌باشند (از جمله حق فراموشی و حق تصحیح).

۳- قوانینی که با گروهی از ویژگی‌ها معماری‌های زنجیره‌بلوکی منطبق و با گروهی دیگر در تضاد می‌باشند (از جمله تمایز بین نقوش و حق رضایت موضوع‌داده).

همچنین در بخش (۴) این مطالعه، با واکاوی نقشه‌راه‌ها و بسترهای ارائه‌شده در مطالعات اخیر، به ارائه راه‌حل‌هایی برای تضمین انطباق با قوانین دسته (۲) و (۳) پرداختیم. از راه‌کارهای ارائه شده، می‌توان به استفاده از تکنیک ذخیره‌سازی خارج زنجیره و توابع درهم‌ساز به هدف ارائه راه‌حلی مناسب برای حل تضاد بین زنجیره‌بلوکی و حقوق فراموشی و تصحیح از GDPR اشاره کرد. علاوه‌براین، امکان اعمال محدودیت‌هایی در دسترسی، پردازش و اشتراک‌گذاری داده‌ها با استفاده از معماری مجوزمحور و قراردادهای هوشمند، مورد بررسی قرار داده‌شد.

فضای تقاطع زنجیره‌بلوکی و GDPR، علیرغم نیاز به حل چالش‌هایی اساسی در زمینه انطباق، ابزارهای قدرتمندی در زمینه‌ی صیانت از حریم‌خصوصی کاربران در اختیار سازمان‌ها و کسب‌وکارها قرار می‌دهد. همانطور که بسترهای نظارتی هم‌راستا با رشد فناوری‌های نوظهور در حال تکامل هستند، ضرورت طراحی راه‌حل‌های خلاقانه در جهت حل چالش‌های این تقاطع و استفاده از پتانسیل کامل زنجیره‌بلوکی در پیروی از مقررات حفاظت از داده‌های شخصی، طراحی بسترهای ایمن‌تر و حفاظت از داده‌های شخصی در موج عظیم تولیددادەها در انقلاب چهارم صنعتی، غیرقابل انکار می‌باشد.

منابع

[1] P. Sandner, J. Gross and R. Richter, "Convergence of Blockchain, IoT and AI," *Frontiers in Blockchain*, vol. 3, 2020.

[2] A. Mottaeva, Z. Khussainova and Y. Gordeyeva, "Impact of the digital economy on the development of economic systems," *E3S Web of Conferences*, vol. 381, 2023.

[3] World Economic Forum, PWC, "Unlocking Technology for the Global Goals," World Economic Forum, 2020.

[4] P. Treleaven, R. G. Brown and D. Yang, "Blockchain Technology in Finance," *Computer*, vol. 50, no. 9, pp. 14-17, 2017.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[6] M. Javaid, A. Haleem, R. P. Singh, S. Khan and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain: Research and Applications*, vol. 2, no. 4, 2021.

[7] L. Yang, "The blockchain: State-of-the-art and research challenges," *Journal of Industrial Information Integration*, vol. 15, pp. 80-90, 2019.

[8] E. Karafiloski and A. Mishev, "Blockchain Solutions for Big Data Challenges: A Literature Review," in *17th International Conference on Smart Technologies*, Ohrid, Macedonia, 2017.

[9] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji and R. Du, "Certchain: Public and efficient certificate audit based on blockchain for tls connections," in *IEEE Conference on Computer Communications*, Honolulu, 2018.

[10] H. F. Atlam, M. A. Azad, A. G. Alzahrani and G. Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data and Cognitive Computing,* vol. 4, 2020.

[11] Z. Zheng, Y. Zhang and H.-N. Dai, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 8076-8094, 2019.

[12] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2188-2204, 2019.

[13] A. K. Das, B. Bera, S. Saha, N. Kumar, I. You and H.-C. Chao, "AI-Envisioned Blockchain-Enabled Signature-Based Key Management Scheme for Industrial Cyber–Physical Systems," *IEEE Internet of Things Journal,* vol. 9, no. 9, pp. 6374-6388, 2022.

[14] S. K. Singh, S. Rathore and J. H. Park, "BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence," *Future Generation Computer Systems,* vol. 110, pp. 721-743, 2020.

[15] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li and Z. Ming, "Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach," *IEEE Internet of Things Journal,* vol. 8, no. 4, pp. 2226-2237, 2021.

[16] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh and A. Tselykh, "Sustainable Smart Cities: Convergence of Artificial Intelligence and Blockchain," *Sustainability,* vol. 13, no. 23, 2021.

[17] S. M. Alrubei, E. Ball and J. M. Rigelsford, "A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer," *IEEE Access,* vol. 10, pp. 18583-18595, 2022.

[18] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors,* vol. 23, 2023.

[19] L.-P. Dana, A. Salamzadeh, S. Mortazavi and M. Hadizadeh, "Investigating the Impact of International Markets and New Digital Technologies on Business Innovation in Emerging Markets," *Sustainability,* vol. 14, 2022.

[20] V. Mone and C. Sivakumar, "An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies," *Legal Information Management,* vol. 22, no. 3, pp. 166-174, 2022.

[21] N. Goyal, M. Howlett and A. Taeihagh, "Why and how does the regulation of emergingtechnologies occur? Explaining the adoption of the EUGeneral Data Protection Regulation using the multiplestreams framework," *Regulation & Governance,* vol. 15, pp. 1020-1034, 2021.

[22] A. Taeihagh, M. Ramesh and M. Howlett, "Assessing the regulatory challenges of emerging disruptive technologies," *Regulation & Governance*, vol. 15, pp. 1009-1019, 2021.

[23] A. Kateifides, A. Potter, H. C. Keshawna Campbell, V. Prescott, S. Medvedev and S. Rumyantsev, "Comparing privacy laws: GDPR v. Russian Law on Personal Data," OneTrust DataGuidance, Gorodissky & Partners, 2022.

[24] H. W. Caming, "Protection of personal data in the United States," *The Information Society*, vol. 3, no. 2, pp. 113-130, 1984.

[25] Office of the Privacy Commissioner of Canada, [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. [Accessed 01 May 2024].

[26] C. Bennett, C. A. Parsons and A. Molnar, "Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies," *SSRN Electronic Journal*, 2013.

[27] R. Creemers, "China's emerging data protection framework," *Journal Of Cybersecurity*, 2022.

[28] I. Kaori, "Advancements in the Personal Information Protection System in Japan," *Global Privacy Law Review ,* 2020.

[29] S. Saeki, "Impact of the “Amendments to the Act of the Protection of Personal Information” to Global Health Research Conducted in Japanese Medical Facilities," Journal of Epidemiology, 2022.

[30] A. Savelyev, "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?," *Computer Law & Security Review*, 2016.

[31] The European Parliament, The Council, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," *Official Journal of the European Union*, 2016.

[32] N. P. Terry, "Existential challenges for healthcare data protection in the United States," *Ethics, Medicine and Public Health*, 2017.

[33] X. Li, Y. Cong and R. Liu, "Research Under China’s Personal Information Law," *Science*, 2022.

[34] N. B. Truong, K. Sun, G. M. Lee and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746-1761, 2019.

[35] J. Kingston, "Using artificial intelligence to support compliance with the general data protection regulation," *Artificial Intelligence and Law ,* vol. 25, p. 429–443, 2017.

[36] M. Barati, G. S. Aujla, J. T. Llanos, K. A. Duodu, O. F.Rana, M. Carr and R. Ranjan, "Privacy-Aware Cloud Auditing for GDPR Compliance Verification in Online Healthcare," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 7, pp. 4808-4819, 2022.

[37] S. S. Fateminasaba, S. Memarian, S. R. K. Tabbakha and M. Romero-Ternero, "A Review on Open Data Storage and Retrieval Techniques in Blockchain-based Applications," in *10th International Conference on Web Research (ICWR)*, Tehran, Iran, Islamic Republic of, 2024.

[38] European Parliamentary Research Service, "Blockchain and The General Data Protection Regulation," July 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. [Accessed May 2024].

[39] P. Hristov and W. Dimitrov, "The blockchain as a backbone of GDPR compliant frameworks," in *8th International Multidisciplinary Symposium*, Romania, 2018.

[40] R. Belen-Saglam, E. Altuncu, Y. Lu and S. Li, "A systematic literature review of the tension between the GDPR and public blockchain systems," *Blockchain: Research and Applications,* vol. 4, no. 2, 2023.

[41] R. Dutta, A. Das, A. Dey and S. Bhattacharya, "Blockchain vs GDPR in Collaborative Data Governance," in *17th International Conference on Cooperative Design, Visualization and Engineering (CDVE)*, Bangkok, 2020.

[42] S. R. Niya, J. Willems and B. Stiller, "A Case Study of a Blockchain-GDPR Adaptation," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Shanghai, 2022.

[43] D. Matsson, "GDPR, Blockchain & Personal data," [Online]. Available: https://gupea.ub.gu.se/bitstream/handle/2077/70713/gupea_2077_70713_1.pdf;jsessionid=7AFBC5B34FA395A4F932D4AC69545D44?sequence=1. [Accessed May 2024].

[44] IBM Security, "Blockchain and GDPR," March 2018. [Online]. Available: https://iapp.org/media/pdf/resource_center/blockchain_and_gdpr.pdf. [Accessed May 2024].

[45] CMS Law, "The tension between GDPR and the rise of blockchain technologies," January 2019. [Online]. Available: https://cms.law/en/media/international/files/publications/publications/the-tension-between-gdpr-and-the-rise-of-blockchain-technologies. [Accessed May 2024].

[46] A. B. Haque, S. Hyrynsalmi, B. Naqvi, K. Smolander and A. Najmul Islam, "GDPR Compliant Blockchains–A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 50593-50606, 2021.

[47] Y. Piao, K. Ye and X. Cui, "A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain," *Future Internet*, vol. 13, no. 8, 2021.

[48] Google Cloud, "Blockchain Node Engine terminology," 3 June 2024. [Online]. Available: https://cloud.google.com/blockchain-node-engine/docs/terms. [Accessed 5 June 2024].

[49] Deloitte Insight, "Blockchain: A Technical Primer," Deloitte, 2018.

[50] IBM, "What is Blockchain?," IBM, [Online]. Available: https://www.ibm.com/topics/what-is-blockchain. [Accessed May 2024].

[51] National Institute of Standards and Technology, "Blockchain Technology Overview," U.S. Department of Commerce, Washington, D.C., 2018.

[52] World Economic Forum, PWC, Stanford Woods Institute for the Environment, "Building Block(chain)s for a Better Planet," World Economic Forum, Geneva, 2018.

[53] H. R. Andrian, N. B. Kurniawan and Suhardi, "Blockchain Technology and Implementation : A Systematic Literature Review," in *International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, 2018.

[54] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *IEEE 6th International Congress on Big Data*, 2017.

[55] T. Buocz, T. Ehrke-Rabel, E. Hödl and I. Eisenberger, "Bitcoin and the GDPR: Allocating responsibility in distributed networks," *Computer Law & Security Review*, vol. 35, no. 2, pp. 182-198, 2019.

[56] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027-1038, 2017.

[57] J. J. Xu, "Are blockchains immune to all malicious attacks?," *Financial Innovation*, vol. 2, 2016.

[58] J. Yusoff, Z. Mohamad and M. Anuar, "A Review: Consensus Algorithms on Blockchain," *Journal of Computer and Communications*, vol. 10, pp. 37-50, 2022.

[59] K. Wüst and A. Gervais, "Do you Need a Blockchain?," in *Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, 2018.

[60] E. Zamani, Y. He and M. Phillips, "On the Security Risks of the Blockchain," *Journal of Computer Information Systems*, vol. 60, no. 6, p. 495–506, 2020.

[61] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi and K.-L. Tan, "BLOCKBENCH: A Framework for Analyzing Private Blockchains," in *ACM International Conference on Management of Data*, Association for Computing Machinery, New York, NY, United States, 2017.

[62] Stanford Online, "Popular blockchain use cases across industries," Stanford University, [Online]. Available: https://online.stanford.edu/popular-blockchain-use-cases-across-industries. [Accessed June 2024].

[63] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities," *Computers & Security*, 2019.

[64] J. Polge, J. Robert and Y. L. Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229-233, 2021.

[65] State of California Department of Justice, "California Consumer Privacy Act (CCPA)," 13 March 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa. [Accessed 9 June 2024].

[66] U.S Department of Health and Human Services, "Health Information Privacy," [Online]. Available: https://www.hhs.gov/hipaa/index.html. [Accessed 9 June 2024].

[67] Deloitte, "The China Personal Information Protection Law (PIPL)," Deloitte, 2021.

[68] Russian Federation, "Federal Law On Personal Data (152-FZ)," 27 July 2006. [Online]. Available: https://pd.rkn.gov.ru/docs/Federal_Law_On_personal_data.doc. [Accessed 9 June 2024].

[69] فاطمه قناد و الهام شریف، «مطالعهٔ اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا»، *حقوق فناوری های نوین، دوره ۲، شماره ۴، صفحه ۱-۲۲، ۱۴۰۰*.

[70] T. Linden, R. Khandelwal, H. Harkous and K. Fawaz, "The Privacy Policy Landscape After the GDPR," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020.

[71] F. Zemler and M. Westner, "Blockchain and GDPR: Application Scenarios and Compliance Requirements," in *Portland International Conference on Management of Engineering and Technology (PICMET)*, Portland, 2019.

[72] M. Foy, D. Martyn, D. Daly, A. Byrne, C. Aguneche and R. Brennan, "Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis," *Procedia Computer Science*, vol. 198, pp. 662-669, 2022.

[73] J. Bacon, J. D. Michels, C. Millard and J. Singh, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers," *Richmond Journal of Law and Technology,* vol. 25, no. 1, 2018.

[74] E. Politou, E. Alepis, C. Patsakis, F. Casino and M. Alazab, "Delegated content erasure in IPFS," *Future Generation Computer Systems,* vol. 112, 2020.

[75] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage and J. Platts, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Computer Science,* vol. 3, 2022.

[76] A. Mahindrakar and K. P. Joshi, "Automating GDPR Compliance Using Policy Integrated Blockchain," in *IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2020.

[77] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst and Y. Qiao, "Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective," *IEEE Access,* vol. 7, 2019.

[78] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials,* 2017.

[79] J. Ahmed, S. Yildirim, M. Nowostaki, R. Ramachandra, O. Elezaj and M. Abomohara, "GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach," in *3rd International Conference on Information and Computer Technologies (ICICT),* 2020.

[80] S. S. F. Nasab, D. Bahrepour and S. R. K. Tabbakh, "A Review on Secure Data Storage and Data Sharing Technics in Blockchain-based IoT Healthcare Systems," in *12th International Conference on Computer and Knowledge Engineering (ICCKE 2022)*, Mashhad, Iran, Islamic Republic of, 2022.

[81] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266-2277, Nov. 2019