Received: 10 /10/2024
Review: 04/01/2025
Accepted: 10 /04/2025
DOI: 10.22054/jocl.2025.85062.1237

Journal of Cyber Law
No(1),Vol(2), 1-17.
ISSN: 0972-6934
www.jocl.ir

The Role of Cyber Law in Managing Security Risks of Blockchain-Based Electronic Elections

Rayan Keyhanifar [1], Saghar Niknamfar[2*]

1- Master's Student in Law, Payame Noor University, Mahedasht, Iran

2- Master's Student in Law, Payame Noor University, Mahedasht, Iran

ABSTRACT

The rapid advancement of information technologies and the widespread adoption of blockchain have led to significant transformations in political participation and electoral systems. One of the major concerns of electronic voting is ensuring security, transparency, and public trust in the outcomes. The central question of this study is how cyber law can contribute to managing the security risks of blockchain-based electronic elections. The importance of this research arises from the fact that despite blockchain's advantages—such as immutability, transparency, and decentralization—risks such as cyberattacks, vote manipulation, misuse of personal data, and international legal challenges remain. The purpose of this study is to examine the role of cyber law frameworks in identifying, preventing, and managing these risks. The research method is descriptive–analytical and based on document analysis, relying on legal, security, and technological sources. Findings indicate that cyber law plays a crucial role in mitigating threats and enhancing public trust through the establishment of binding regulations for data protection, criminalization of cyber electoral crimes, development of transparent dispute resolution mechanisms, and oversight of technical compliance with security standards. The novelty of this paper lies in combining legal and technological perspectives to propose an integrated framework for managing the security risks of blockchain-based elections, offering a practical model for countries transitioning to secure digital voting systems.

Keywords:
Cyber Law, Risk Management, Cybersecurity, Electronic Elections, Blockchain

How to Cite: keyhanifar, R. and niknamfar, S. (2025). The Role of Cyber Law in Managing Security Risks of Blockchain-Based Electronic Elections. Journal of Cyber Law (JOCL), 2(1), 1-17. doi: 10.22054/jocl.2025.85062.1237

* Corresponding Author: saghar.niknamfar@pnu.ac.ir

نشریه حقوق سایبری
شماره (۱) ۱-۱۷
دوره ۱٤۰٤

تاریخ دریافت: ۱٤۰۳/۰۷/۲۰
تاریخ اصلاح: ۱٤۰۳/۱۰/۱٤
تاریخ پذیرش: ۱٤۰٤/۰۱/۲۲

نقش حقوق سایبری در مدیریت ریسک‌های امنیتی انتخابات الکترونیک مبتنی بر بلاک‌چین

رایان کیهانی فر[۱]، ساغر نیک نام فر[۲]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور ماهدشت، ایران

۲ - دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور ماهدشت، ایران

چکیده

تحول فناوری‌های نوین اطلاعاتی و گسترش کاربرد بلاک‌چین در عرصه‌های مختلف، زمینه‌ساز تغییرات عمیقی در شیوه‌های مشارکت سیاسی و برگزاری انتخابات شده است. یکی از مهم‌ترین دغدغه‌های نظام‌های انتخاباتی الکترونیک، تأمین امنیت، شفافیت و اعتماد عمومی به نتایج است. پرسش اصلی این پژوهش آن است که حقوق سایبری چگونه می‌تواند به مدیریت ریسک‌های امنیتی انتخابات الکترونیک مبتنی بر بلاک‌چین کمک کند. اهمیت موضوع از آنجا ناشی می‌شود که با وجود مزایای بلاک‌چین همچون غیرقابل تغییر بودن داده‌ها، شفافیت و توزیع‌شدگی، همچنان تهدیداتی چون حملات سایبری، دستکاری در فرآیند رأی‌گیری، سوءاستفاده از داده‌های شخصی و چالش‌های حقوقی بین‌المللی وجود دارد. این پژوهش با هدف بررسی نقش چارچوب‌های حقوق سایبری در شناسایی، پیشگیری و مدیریت این ریسک‌ها انجام شده است. روش تحقیق به‌صورت توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی می‌باشد و با بهره‌گیری از منابع حقوقی، امنیتی و فناورانه به تحلیل ابعاد موضوع پرداخته است. نتایج نشان می‌دهد که حقوق سایبری از طریق تدوین مقررات الزام‌آور در حوزه حفاظت از داده‌ها، جرم‌انگاری جرایم انتخاباتی سایبری، ایجاد سازوکارهای شفاف برای حل‌وفصل اختلافات و نظارت بر انطباق فنی سیستم‌های انتخاباتی با استانداردهای امنیتی، نقشی کلیدی در کاهش تهدیدات و افزایش اعتماد عمومی دارد. نوآوری این مقاله در ترکیب دیدگاه‌های حقوقی و فناورانه برای ارائه چارچوبی یکپارچه جهت مدیریت ریسک‌های امنیتی انتخابات بلاک‌چینی است که می‌تواند الگویی کاربردی برای کشورها در مسیر گذار به انتخابات دیجیتال امن فراهم آورد.

کلیدواژه‌ها:

حقوق سایبری، مدیریت ریسک، امنیت سایبری، انتخابات الکترونیک، بلاک‌چین

نحوه استناد:

کیهانی فر, رایان و نیک نام فر, ساغر . (۱۴۰۴). نقش حقوق سایبری در مدیریت ریسک‌های امنیتی انتخابات الکترونیک مبتنی بر بلاک‌چین. حقوق سایبری, ۲(۱), ۱-۱۷

* ایمیل نویسنده مسئول: saghar.niknamfar@pnu.ac.ir

مقدمه

تحول فناوری‌های نوین اطلاعاتی و کاربرد بلاک‌چین در حوزه‌های مختلف، از جمله انتخابات الکترونیک، مسائل حقوقی و امنیتی پیچیده‌ای را مطرح کرده است (Belen-Saglam, Altuncu, Lu, & Li, ۲۰۲۳p,۳۰۲). مسئله اصلی این مقاله بررسی نقش حقوق سایبری در مدیریت ریسک‌های امنیتی سامانه‌های انتخاباتی مبتنی بر بلاک‌چین است. بلاک‌چین با ویژگی‌های توزیع‌شدگی، شفافیت و تغییرناپذیری، توانایی افزایش اعتماد عمومی و جلوگیری از تقلب را دارد، اما فقدان چارچوب‌های حقوقی جامع و استانداردهای فنی قابل راستی‌آزمایی می‌تواند زمینهٔ تهدیداتی مانند حملات سایبری، سوءاستفاده از داده‌های شخصی رأی‌دهندگان و مشکلات حقوقی بین‌المللی را فراهم کند (Godyn et al., ۲۰۲۲p,۵۰). اهمیت پرداختن به این موضوع از آن جهت است که حقوق شهروندان، از جمله حق رأی و حریم خصوصی، نیازمند حفاظت است و اعتماد عمومی به نتایج انتخابات باید تضمین شود (Taş, ۲۰۲۰p.,۱۳).

پژوهش‌های پیشین نشان می‌دهد که موضوع انتخابات الکترونیک و کاربرد بلاک‌چین در آن مورد توجه محققان زیادی قرار گرفته است. جافار، عبدالعزیز و شوکور (۲۰۲۲) نشان داده‌اند که سیستم‌های رأی‌گیری مبتنی بر بلاک‌چین قابلیت حسابرسی و امنیت بالایی دارند، اما چالش‌های فنی و عملی نیز قابل توجه است . سیستم‌های رمزنگاری شده‌ای مانند Helios را تحلیل کرده و محدودیت‌های قابلیت راستی‌آزمایی را بیان کرده است. پارک (۲۰۲۱, ص. ۲۱۵) به نقد سیستم‌های اینترنتی رأی‌گیری پرداخته و هشدار داده که راه‌حل‌های بلاک‌چینی ممکن است با مشکلات بنیادی مواجه شوند. همچنین، پژوهش‌های مروری و تجربی اخیر (Zhuk, ۲۰۲۵o.,۳۲؛ Kareklas & Chaleplioglou, ۲۰۲۵p.,۵۱) نشان داده‌اند که ترکیب جنبه‌های حقوقی و فنی هنوز به صورت یک چارچوب کامل انجام نشده است. مطالعات چائوم و همکاران (ص. ۸۹) نیز بر اهمیت رمزنگاری در تضمین صحت آراء تأکید کرده‌اند. این مجموعه پژوهش‌ها بیانگر این است که موضوع مسبوق به سابقه است، اما هنوز لبه‌های حقوقی و تعامل میان مقررات و معماری فنی به‌طور کامل تحلیل نشده است.

با وجود این پیشینه ، خلأ پژوهش روشن است: اغلب مطالعات یا بر جنبه‌های فنی تمرکز کرده‌اند یا تحلیل‌های حقوقی کلی ارائه داده‌اند، اما ترکیب چارچوب حقوق سایبری با الزامات فنی سامانه‌های بلاک‌چینی برای مدیریت ریسک‌های امنیتی انتخابات هنوز تدوین نشده است (Belen-Saglam et al., ۲۰۲۳p.,۳۱۰). این خلأ به ویژه در زمینهٔ تعیین تکلیف حقوقی بازیگران خصوصی، شفافیت قراردادهای هوشمند و اعمال مقررات منطقه‌ای و بین‌المللی آشکار است (Godyn et al., ۲۰۲۲, ۱۰p.).

پرسش‌های اصلی این تحقیق عبارت‌اند از: «حقوق سایبری چه ابزارها و مکانیسم‌هایی در اختیار دارد تا ریسک‌های امنیتی سامانه‌های انتخابات الکترونیک مبتنی بر بلاک‌چین را شناسایی، کاهش و مدیریت نماید؟» و «چگونه می‌توان چارچوبی حقوقی—فنی تدوین کرد که هم حفاظت داده رأی‌دهندگان را تضمین کند و هم امکان حسابرسی و شفافیت لازم برای مشروعیت انتخاباتی را فراهم آورد؟» اهداف مقاله شامل (۱) شناسایی انواع ریسک‌های امنیتی مرتبط با انتخابات بلاک‌چینی، (۲) بررسی مقررات و رویه‌های موجود در حقوق سایبری و حفاظت داده که قابلیت تسری به این سامانه‌ها را

دارند، (۳) ارائه چارچوب حقوقی—فنی یکپارچه برای مدیریت ریسک و (۴) ارائه توصیه‌های سیاستی برای قانون‌گذاران و مجریان انتخاباتی در سطوح ملی و بین‌المللی است .

روش پژوهش در این مقاله توصیفی—تحلیلی و تطبیقی است؛ یعنی گردآوری و تحلیل اسنادی متون حقوقی، مقالات فنی و گزارش‌های موردی و سپس مقایسه چارچوب‌های حقوقی موجود با الزامات فنی سامانه‌های بلاک‌چینی صورت می‌گیرد . تحلیل حقوقی شامل بررسی و طبقه‌بندی مواد قانونی، مقررات و رویه‌های قضایی است و بخش فناورانه با مرور انتقادی مطالعات تجربی و مروری تکمیل می‌شود؛ سپس این دو تحلیل برای ارائه چارچوب مدیریت ریسک تلفیق می‌شوند.این روش به پژوهش اجازه می‌دهد هم واقعیت‌های فنی را مدنظر قرار دهد و هم توصیه‌های حقوقی و سیاست‌گذاری ارائه نماید.

بلاک‌چین

بلاک‌چین یک فناوری دفتر کل توزیع‌شده است که امکان ذخیره‌سازی داده‌ها به‌صورت غیرقابل تغییر و شفاف را فراهم می‌آورد (Hajian Berenjestanaki, ۲۰۲۳ p. ,۱۸). این فناوری به گونه‌ای طراحی شده است که هر تراکنش یا تغییر در سیستم، به‌صورت زنجیره‌ای ثبت می‌شود و پس از تایید شبکه، امکان تغییر یا حذف آن تقریباً غیرممکن است. این ویژگی، بلاک‌چین را به ابزاری بسیار مطمئن برای ثبت اطلاعات حساس، مانند رأی‌دهی الکترونیک، تبدیل می‌کند (Belen-Saglam, Altuncu, Lu, & Li, ۲۰۲۳ p. ,۳۰۲).از نظر ساختاری، بلاک‌چین شامل بلوک‌هایی است که هر بلوک حاوی مجموعه‌ای از تراکنش‌ها و یک هش منحصر به فرد است. هر بلوک جدید با استفاده از هش بلوک قبلی به زنجیره اضافه می‌شود، که این امر موجب ایجاد یک ساختار غیرقابل تغییر می‌شود و امکان دستکاری داده‌ها را بسیار کاهش می‌دهد (Zhuk, ۲۰۲۵ p. ,۴۲). این ویژگی باعث شده است که بلاک‌چین به‌عنوان یکی از ابزارهای کلیدی در تضمین شفافیت و صحت اطلاعات در سامانه‌های رأی‌گیری دیجیتال شناخته شود (Taş, ۲۰۲۰ p. ,۱۳۳۰).ویژگی غیرمتمرکز بودن بلاک‌چین، دیگر مزیت مهم آن است. در سامانه‌های سنتی، داده‌ها در یک سرور مرکزی ذخیره می‌شوند و آسیب‌پذیری در مقابل حملات سایبری بالاست. اما در بلاک‌چین، داده‌ها به‌صورت توزیع‌شده در شبکه‌ای از گره‌ها ذخیره می‌شوند و هر گره یک نسخه از داده‌ها را در اختیار دارد. بنابراین، نفوذ یا دستکاری تنها در یک گره، تاثیری بر کل سیستم ندارد و امنیت سامانه به‌طور قابل توجهی افزایش می‌یابد (Jafar, Juzaiddin Ab Aziz, & Shukur, ۲۰۲۲ p. ,۷۷۰۶).شفافیت، یکی دیگر از ویژگی‌های مهم بلاک‌چین است. در این فناوری، هر تراکنش قابل رهگیری است و هر کاربر شبکه می‌تواند صحت اطلاعات ثبت‌شده را بررسی کند، بدون آنکه نیاز به اعتماد به یک نهاد مرکزی باشد (Zafar, ۲۰۲۵ p. ,۱۲). این ویژگی به ویژه در انتخابات الکترونیک اهمیت دارد، زیرا باعث افزایش اعتماد عمومی به صحت فرآیند رأی‌گیری می‌شود و امکان حسابرسی مستقل توسط ناظران را فراهم می‌کند (موسوی، ۲۰۲۳، ص. ۴۷).علاوه بر مزایای امنیتی و شفافیت، بلاک‌چین امکان استفاده از قراردادهای هوشمند (Smart Contracts) را نیز فراهم می‌کند. قراردادهای هوشمند، پروتکل‌های برنامه‌ریزی‌شده‌ای هستند که به صورت خودکار شرایط مشخصی را

اجرا می‌کنند. در انتخابات، این قراردادها می‌توانند فرآیندهای جمع‌آوری و شمارش آراء را خودکار کنند و احتمال خطای انسانی یا دستکاری داده‌ها را کاهش دهند (Kareklas & Chaleplioglou, ۲۰۲۵, p. ۵۱).

با توجه به این ویژگی‌ها، بلاک‌چین می‌تواند به کاهش ریسک‌های امنیتی در انتخابات کمک کند، از جمله تقلب در ثبت رأی، تغییر نتایج، و دسترسی غیرمجاز به داده‌های رأی‌دهندگان (Godyn et al., ۲۰۲۲, p. ۱۰). با این حال، پیاده‌سازی موفق نیازمند هماهنگی با چارچوب‌های حقوقی و مقررات حفاظت داده‌ها است تا هم امنیت فنی و هم حفاظت حقوق شهروندان تضمین شود (Belen-Saglam et al., ۲۰۲۳, p. ۳۱۰).

در نتیجه، بلاک‌چین نه تنها فناوری‌ای برای ثبت و نگهداری داده‌هاست، بلکه یک ابزار کلیدی برای تحقق شفافیت، امنیت و اعتماد در سامانه‌های الکترونیک به ویژه انتخابات دیجیتال محسوب می‌شود (موسوی، ۲۰۲۳، ص. ۴۸). ترکیب ویژگی‌های فنی بلاک‌چین با چارچوب‌های حقوقی مناسب می‌تواند امکان پیاده‌سازی انتخابات امن، شفاف و پاسخ‌گو را فراهم آورد و از حقوق اساسی شهروندان حفاظت کند.

انتخابات الکترونیک

انتخابات الکترونیک به کاربرد فناوری‌های دیجیتال در تمامی مراحل فرآیند رأی‌گیری، از ثبت‌نام داوطلبان تا شمارش و اعلام نتایج، اطلاق می‌شود. این نوع انتخابات می‌تواند شامل رأی‌گیری از طریق اینترنت، دستگاه‌های الکترونیکی (Electronic Voting Machines) یا سامانه‌های مبتنی بر بلاک‌چین باشد (Ohize, ۲۰۲۵, p. ۴۵؛ موسوی، ۲۰۲۳، ص. ۴۶).استفاده از فناوری‌های دیجیتال در انتخابات، مزایای قابل توجهی دارد که از جمله آن‌ها می‌توان به افزایش سرعت شمارش آراء، کاهش خطاهای انسانی، امکان مشارکت از راه دور و دسترسی آسان به داده‌ها اشاره کرد (Jafar & Ab Aziz, ۲۰۲۲, p. ۷۷۰۷). با این حال، این فناوری‌ها ریسک‌های امنیتی و قانونی جدیدی نیز به همراه دارند؛ از جمله خطر حملات سایبری، دستکاری داده‌ها، افشای اطلاعات محرمانه رأی‌دهندگان و تهدید به شفافیت فرآیند رأی‌گیری (Taş, ۲۰۲۰, p. ۱۳۳۰).در سامانه‌های مبتنی بر بلاک‌چین، مزیت اصلی، افزایش شفافیت و قابلیت رهگیری تراکنش‌هاست. هر رأی ثبت‌شده در شبکه بلاک‌چین قابل رهگیری و تأیید توسط ناظران انتخاباتی است، بدون اینکه امنیت یا محرمانگی رأی‌دهندگان به خطر بیفتد (Belen-Saglam et al., ۲۰۲۳, p. ۳۱۰). این قابلیت موجب تقویت اعتماد عمومی به فرآیند انتخابات و افزایش مشروعیت نتایج می‌شود (Hajian Berenjestanaki, ۲۰۲۳, p. ۱۹).انتخابات الکترونیک، علاوه بر مزایای فنی، آثار حقوقی مهمی نیز دارد. قوانین موجود در ایران، مانند قانون انتخابات مجلس شورای اسلامی و قانون جرائم رایانه‌ای، چارچوبی کلی برای برگزاری انتخابات و مقابله با جرائم سایبری فراهم کرده‌اند، اما این قوانین هنوز به‌طور خاص کاربرد فناوری‌های نوین مانند بلاک‌چین را پوشش نمی‌دهند (موسوی، ۲۰۲۳، ص. ۴۸). بنابراین، توسعه چارچوب قانونی مشخص و به‌روز برای انتخابات الکترونیک ضروری است تا هم امنیت داده‌ها تضمین شود و هم حقوق شهروندان محفوظ بماند (Zafar, ۲۰۲۵, p. ۱۲).

یکی دیگر از مزایای مهم انتخابات الکترونیک، امکان استفاده از قراردادهای هوشمند (Smart Contracts) در فرآیند رأی‌گیری است. این قراردادها می‌توانند شمارش آراء و پردازش داده‌ها را به‌صورت خودکار انجام دهند و از خطاها و دستکاری‌های انسانی جلوگیری کنند (Kareklas & Chaleplioglou, ۲۰۲۵, p. ۵۱). با پیاده‌سازی صحیح فناوری و چارچوب حقوقی مناسب، انتخابات الکترونیک می‌تواند فرآیندی امن، شفاف و قابل اعتماد برای رأی‌دهندگان فراهم آورد.به طور خلاصه، انتخابات الکترونیک یک راهکار نوین برای بهبود کارایی و شفافیت فرآیندهای دموکراتیک است،

اما موفقیت آن مستلزم ترکیب فناوری پیشرفته با چارچوب‌های قانونی و حفاظت داده‌های دقیق است (Godyn et al., ۲۰۲۲, p. ۱۰؛ Taş, ۲۰۲۰, p. ۱۳۳۳). این ترکیب موجب کاهش ریسک‌های امنیتی، افزایش اعتماد عمومی و تضمین حقوق رأی‌دهندگان خواهد شد.

حقوق سایبری

حقوق سایبری شاخه‌ای از حقوق عمومی است که به تنظیم و نظارت بر استفاده از فناوری‌های اطلاعات و ارتباطات می‌پردازد. این حوزه شامل مسائل مربوط به حریم خصوصی، امنیت داده‌ها، مالکیت معنوی، حفاظت از اطلاعات شخصی و مسئولیت‌های قانونی در فضای مجازی است (موسوی، ۲۰۲۳، ص. ۴۹).در زمینه انتخابات الکترونیک، حقوق سایبری نقش مهمی در تعیین چارچوب قانونی استفاده از فناوری‌ها و جلوگیری از نقض حقوق شهروندان دارد. قوانین داخلی ایران، از جمله قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قانون انتخابات، پایه‌ای برای حمایت از حقوق رأی‌دهندگان فراهم می‌کنند، اما این قوانین هنوز به‌طور خاص کاربرد فناوری‌های نوین مانند بلاک‌چین را پوشش نمی‌دهند (موسوی، ۲۰۲۳، ص. ۵۰).حقوق سایبری شامل تنظیم مقررات برای حفظ امنیت سامانه‌ها، جلوگیری از دستکاری داده‌ها، جلوگیری از افشای اطلاعات محرمانه و ایجاد مسئولیت‌های قانونی برای مجرمان سایبری است (Hajian Berenjestanaki, ۲۰۲۳, 22p.). همچنین، رعایت حقوق سایبری باعث می‌شود فرآیند انتخابات الکترونیک شفاف، قابل حسابرسی و مشروع باشد و اعتماد عمومی به نتایج افزایش یابد (Ohize, ۲۰۲۵, p. ۱۲۸).

علاوه بر آن، حقوق سایبری به ایجاد سازوکارهای نظارتی و رویه‌های قانونی برای حفاظت از داده‌های رأی‌دهندگان و تضمین محرمانگی آراء کمک می‌کند. این حوزه همچنین با استانداردهای بین‌المللی حفاظت داده‌ها مانند GDPR همسو است و می‌تواند چارچوبی برای توسعه انتخابات الکترونیک امن و پاسخ‌گو فراهم کند (Belen-Saglam et al., ۲۰۲۳, p. ۳۱۰).در نتیجه، حقوق سایبری نه تنها ابزاری برای حفاظت قانونی از کاربران در فضای مجازی است، بلکه پایه و اساس تضمین امنیت و شفافیت در سیستم‌های انتخاباتی دیجیتال محسوب می‌شود و امکان پیاده‌سازی انتخابات مبتنی بر فناوری بلاک‌چین را با رعایت اصول حقوقی و اخلاقی فراهم می‌کند (Kusi, ۲۰۲۵, p. ۴؛ موسوی، ۲۰۲۳، ص. ۵۱).

ریسک‌های امنیتی

ریسک‌های امنیتی در انتخابات الکترونیک به تهدیداتی اطلاق می‌شود که می‌تواند بر صحت، محرمانگی و یکپارچگی فرآیند رأی‌گیری تأثیر بگذارد. این تهدیدات شامل حملات سایبری، دستکاری داده‌ها، افشای اطلاعات شخصی و نقض حریم خصوصی رأی‌دهندگان می‌باشد (Jafar & Ab Aziz, ۲۰۲۲, p. ۷۷۰۶؛ موسوی، ۲۰۲۳، ص. ۵۲).حملات سایبری می‌تواند شامل نفوذ به سامانه رأی‌گیری، تغییر نتایج آراء، ایجاد اختلال در فرآیند رأی‌گیری و سرقت اطلاعات محرمانه رأی‌دهندگان باشد (Ohize, ۲۰۲۵, p. ۱۳۰). دستکاری داده‌ها یا تغییر غیرمجاز نتایج رأی‌گیری، یکی از جدی‌ترین ریسک‌هاست که می‌تواند مشروعیت انتخابات را به شدت تحت تأثیر قرار دهد (Taş, ۲۰۲۰, p. ۱۳۳۴).

افشای اطلاعات شخصی رأی‌دهندگان، از جمله هویت و انتخاب رأی‌دهنده، می‌تواند به نقض حریم خصوصی و اعتماد عمومی منجر شود (Zafar, ۲۰۲۵, p. ۱۴). علاوه بر آن، حملات ترکیبی که از ضعف‌های امنیتی نرم‌افزار و خطای

انسانی بهره می‌برند، ریسک امنیتی را افزایش می‌دهند و نیازمند پیاده‌سازی سازوکارهای حفاظتی چندلایه هستند (Hajian Berenjestanaki, ۲۰۲۳, p. ۲۵).

یکی از راهکارهای کاهش این ریسک‌ها، استفاده از فناوری بلاک‌چین است. بلاک‌چین با ویژگی‌های غیرمتمرکز بودن، شفافیت و غیرقابل تغییر بودن داده‌ها، می‌تواند امنیت و یکپارچگی اطلاعات رأی‌گیری را تقویت کند (Kusi, ۲۰۲۵, p. ۳). همچنین، استفاده از قراردادهای هوشمند در سامانه‌های رأی‌گیری، امکان خودکارسازی فرآیند جمع‌آوری و شمارش آراء را فراهم کرده و احتمال خطای انسانی یا دستکاری داده‌ها را کاهش می‌دهد (Shaikh et al., ۲۰۲۵, p. ۲۲۳).به‌علاوه، ترکیب فناوری با چارچوب‌های حقوقی و رویه‌های نظارتی، می‌تواند ریسک‌های امنیتی را به حداقل برساند و اطمینان از صحت، شفافیت و محرمانگی انتخابات الکترونیک را تضمین کند (Belen-Saglam et al., ۲۰۲۳, p. ۳۱۰ و(موسوی، ۲۰۲۳، ص. ۵۳). در نتیجه، مدیریت ریسک‌های امنیتی انتخابات دیجیتال نیازمند هم‌آهنگی بین فناوری، حقوق سایبری و سیاست‌های نظارتی است تا حقوق رأی‌دهندگان حفظ و اعتماد عمومی تقویت شود.

مبانی فلسفی

از منظر فلسفی، انتخابات به‌عنوان یکی از ارکان اساسی دموکراسی، باید بر اصولی نظیر آزادی، برابری، شفافیت و عدالت استوار باشد. آزادی رأی‌دهندگان در انتخاب نمایندگان و عدم دخالت غیرمجاز در نتایج، یکی از مهم‌ترین شاخص‌های مشروعیت انتخابات است (Ohize, ۲۰۲۵). اصل برابری نیز مستلزم این است که همه رأی‌دهندگان از حق برابر در مشارکت برخوردار باشند و هیچ تبعیضی در فرآیند رأی‌گیری اعمال نشود. بلاک‌چین با ایجاد یک سامانه غیرمتمرکز و یکپارچه، امکان ثبت آراء به صورت شفاف و یکسان برای تمامی رأی‌دهندگان را فراهم می‌کند و این اصل را تقویت می‌نماید (Hajian Berenjestanaki, ۲۰۲۳, p. ۲۱).شفافیت، به‌عنوان یکی دیگر از مبانی فلسفی، تضمین می‌کند که فرآیند رأی‌گیری قابل مشاهده و قابل حسابرسی باشد و امکان دستکاری یا تغییر نتایج وجود نداشته باشد. فناوری بلاک‌چین با ثبت هر رأی در زنجیره‌ای غیرقابل تغییر و قابل ردیابی، به تحقق این اصل کمک می‌کند (Jafar & Ab Aziz, ۲۰۲۲, p. ۷۷۰۷).

علاوه بر این، فلسفه دموکراسی تأکید دارد که اعتماد عمومی به نظام انتخاباتی باید حفظ شود. استفاده از فناوری‌های امن و شفاف، مانند بلاک‌چین، می‌تواند اعتماد شهروندان را افزایش دهد و مشروعیت نتایج انتخابات را تضمین کند (Shaikh et al., ۲۰۲۵, p. ۲۲۳).در مجموع، مبانی فلسفی انتخابات دیجیتال نشان می‌دهد که فناوری‌های نوین باید نه تنها ابزار فنی باشند، بلکه با اصول اخلاقی و فلسفی دموکراسی هماهنگ شوند تا آزادی، برابری و شفافیت به‌طور واقعی تحقق یابد. این رویکرد فلسفی، پایه و زمینه‌ای برای ایجاد چارچوب‌های حقوقی و فنی ایمن و پاسخگو در سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین فراهم می‌کند (Belen-Saglam et al., ۲۰۲۳, p. ۳۱۰؛ موسوی، ۲۰۲۳، ص. ۵۶).

مبانی فقهی

در فقه اسلامی، حفظ امانت و صحت در نقل و انتقال اطلاعات و اموال از اهمیت بالایی برخوردار است. هرگونه اقدام یا فناوری که منجر به تقلب، دستکاری یا اختلال در حق مردم شود، مغایر با اصول امانت‌داری و عدالت است (موسوی، ۲۰۲۳، ص. ۵۷).با توجه به این اصول، استفاده از فناوری‌هایی که امکان دستکاری داده‌ها و آراء را کاهش می‌دهند، با مبانی فقهی هم‌خوانی دارد. سامانه‌های مبتنی بر بلاک‌چین با ثبت غیرقابل تغییر تراکنش‌ها و شفافیت کامل، می‌توانند امانت رأی‌دهندگان را تضمین کنند و احتمال تقلب یا سوءاستفاده را به حداقل برسانند .فقه اسلامی همچنین بر رعایت عدالت و

مساوات میان افراد تأکید دارد. در انتخابات، این بدان معناست که همه رأی‌دهندگان باید از حقوق برابر برخوردار باشند و هیچ‌کس حق ندارد با استفاده از قدرت یا نفوذ، نتایج رأی‌گیری را تغییر دهد (رضایی، ۲۰۲۴، ص. ۵۸). فناوری بلاک‌چین با ارائه یک سامانه توزیع‌شده و شفاف، امکان رعایت این عدالت و مساوات را فراهم می‌کند و می‌تواند تضمین کند که هیچ رأیی بدون ثبت معتبر باقی نماند.علاوه بر آن، اصول فقهی بر شفافیت و قابلیت بررسی امور تأکید دارند. استفاده از سامانه‌های دیجیتال و بلاک‌چین، با فراهم آوردن قابلیت رهگیری و حسابرسی مستقل، این اصل را تحقق می‌بخشد و باعث افزایش اعتماد عمومی به نظام انتخاباتی می‌شود .

در نتیجه، مبانی فقهی با فناوری بلاک‌چین و سیستم‌های رأی‌گیری الکترونیک همسو هستند، به شرطی که این فناوری‌ها به‌درستی پیاده‌سازی شده و تضمین‌کننده صحت، امانت و عدالت در فرآیند انتخابات باشند. این هم‌راستایی فقهی می‌تواند پایه‌ای برای تدوین چارچوب‌های قانونی و حقوقی سازگار با اصول اسلامی در انتخابات دیجیتال فراهم کند .

مبانی حقوقی

در حقوق عمومی، اصولی نظیر حاکمیت قانون، شفافیت، پاسخ‌گویی و رعایت حقوق شهروندان از ارکان اساسی به‌شمار می‌آید. سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین می‌توانند با ارائه شفافیت در فرآیند رأی‌گیری و امکان حسابرسی مستقل، این اصول را تقویت کنند (Ohize, ۲۰۲۵, p. ۴۶)(موسوی، ۲۰۲۳، ص. ۵۹).اصل حاکمیت قانون به معنای رعایت قوانین و مقررات در تمامی مراحل انتخابات است و جلوگیری از هرگونه دستکاری یا نقض قانون را تضمین می‌کند. فناوری بلاک‌چین با ثبت غیرقابل تغییر آراء و تراکنش‌ها، زمینه را برای رعایت این اصل فراهم می‌آورد و امکان پیگیری قانونی هر تغییر یا خطای احتمالی را ایجاد می‌کند (Hajian Berenjestanaki, ۲۰۲۳, p. ۲۴).اصل پاسخ‌گویی مستلزم این است که مسئولان و ناظران انتخابات بتوانند اقدامات خود را توضیح دهند و در صورت نقض قانون یا سوءمدیریت، پاسخگو باشند. سامانه‌های دیجیتال و بلاک‌چین با قابلیت ثبت و ضبط دقیق تمامی تراکنش‌ها، بستر مناسبی برای افزایش پاسخ‌گویی فراهم می‌کنند (Shaikh et al., ۲۰۲۵, p. ۲۲۳).شفافیت نیز از ارکان مهم حقوقی انتخابات است و مستلزم آن است که فرآیند رأی‌گیری و شمارش آراء برای ناظران و شهروندان قابل مشاهده و قابل بررسی باشد. استفاده از فناوری بلاک‌چین با ایجاد زنجیره‌ای از داده‌های غیرقابل تغییر، شفافیت و قابلیت حسابرسی را بهبود می‌بخشد و اعتماد عمومی به نتایج انتخابات را افزایش می‌دهد .علاوه بر این، مبانی حقوقی تأکید دارند که حفاظت از داده‌ها و حریم خصوصی رأی‌دهندگان الزامی است. استفاده از فناوری‌های امن، رمزنگاری پیشرفته و معماری غیرمتمرکز بلاک‌چین، می‌تواند این حفاظت را تضمین کند و از نقض حقوق شهروندان جلوگیری نماید (Zafar, ۲۰۲۵, p. ۱۳).

بنابراین، مبانی حقوقی با فناوری بلاک‌چین همسو هستند و این فناوری می‌تواند با فراهم آوردن شفافیت، پاسخ‌گویی، حاکمیت قانون و حفاظت از حقوق رأی‌دهندگان، زمینه برگزاری انتخابات الکترونیک امن و مشروع را فراهم کند. این رویکرد حقوقی، پایه‌ای محکم برای تدوین مقررات و چارچوب قانونی توسعه سامانه‌های رأی‌گیری دیجیتال به‌شمار می‌آید (Kusi, ۲۰۲۵, p. ۴).

مبانی اقتصادی

از منظر اقتصادی، استفاده از فناوری‌های نوین مانند سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین می‌تواند هزینه‌های اجرایی انتخابات را کاهش دهد. کاهش هزینه‌ها شامل کاهش نیاز به نیروی انسانی زیاد برای شمارش دستی آراء، کاهش چاپ و توزیع برگه‌های رأی و صرفه‌جویی در زمان و منابع مالی است(Hald, K., & Tamm, A. ۲۰۲۳) علاوه بر کاهش

هزینه‌ها، این فناوری‌ها می‌توانند کارایی فرآیند رأی‌گیری را افزایش دهند. به دلیلسرعت بالای پردازش تراکنش‌ها، شمارش آراء در زمان کوتاه انجام می‌شود و امکان اعلام نتایج سریع و دقیق فراهم می‌شود (Wang, B. ,۲۰۲۴)این افزایش کارایی موجب افزایش اعتماد عمومی و مشارکت رأی‌دهندگان می گردد، زیرا شهروندان اطمینان دارند که آراء آن‌ها به صورت امن و بدون دستکاری شمارش می‌شوند .

استفاده از بلاک‌چین همچنین می‌تواند منجر به کاهش خطاهای انسانی و کاهش هزینه‌های ناشی از رسیدگی به شکایات و اختلافات انتخاباتی شود. به این ترتیب، سرمایه‌گذاری اولیه در فناوری‌های امن و شفاف، در بلندمدت صرفه‌جویی اقتصادی و افزایش مشروعیت انتخابات را به دنبال خواهد داشت (Shaikh et al., ۲۰۲۵).مبانی اقتصادی نشان می‌دهند که پیاده‌سازی سامانه‌های دیجیتال و بلاک‌چین در انتخابات نه تنها به کاهش هزینه‌ها و افزایش کارایی کمک می کند، بلکه با تقویت مشارکت عمومی و اعتماد شهروندان، اثرات مثبتی بر پایداری و مشروعیت نظام سیاسی خواهد داشت (Belen-Saglam et al., ۲۰۲۳).

نظریه‌های حقوقی مرتبط

۱. نظریه حاکمیت قانون

بر اساس نظریه حاکمیت قانون، تمامی اقدامات دولت و نهادهای اجرایی باید بر اساس قوانین مصوب و با رعایت حقوق شهروندان انجام شود. این نظریه تأکید دارد که هیچ‌کس بالاتر از قانون نیست و همه اشخاص و نهادها موظف به رعایت آن هستند (Zafar, ۲۰۲۵, ص. ۱۴؛ موسوی، ۲۰۲۳، ص. ۶۳).در زمینه انتخابات الکترونیک، نظریه حاکمیت قانون ایجاب می‌کند که سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین با قوانین ملی، از جمله قانون انتخابات و قانون جرائم رایانه‌ای، و همچنین با استانداردهای بین‌المللی حقوق بشر و حفاظت داده‌ها هم‌خوانی داشته باشند (Ohize, ۲۰۲۵, ص. ۴۷). رعایت این هماهنگی قانونی باعث تضمین مشروعیت نتایج انتخابات، شفافیت فرآیند رأی‌گیری و حفاظت از حقوق رأی‌دهندگان می‌شود (Hajian Berenjestanaki, ۲۰۲۳).علاوه بر آن، حاکمیت قانون شامل الزام ناظران و مسئولان انتخابات به پاسخ‌گویی در برابر اقدامات خود است. سامانه‌های بلاک‌چین با قابلیت ثبت و ضبط تراکنش‌های غیرقابل تغییر، زمینه‌ای فراهم می‌کنند که در صورت بروز هرگونه تخلف یا سوءمدیریت، امکان بررسی و پیگرد قانونی وجود داشته باشد .

بنابراین، نظریه حاکمیت قانون نه تنها چارچوب قانونی برای طراحی و اجرای سامانه‌های رأی‌گیری الکترونیک فراهم می‌کند، بلکه با ایجاد سازوکارهای نظارتی و حفاظت از حقوق رأی‌دهندگان، موجب تقویت مشروعیت و اعتماد عمومی به فرآیند انتخابات می‌شود (Belen-Saglam et al., ۲۰۲۳).

۲. نظریه شفافیت

نظریه شفافیت بر لزوم شفافیت در تمامی فرآیندهای دولتی و تصمیم‌گیری‌های اجرایی تأکید دارد و بیان می‌کند که دسترسی عمومی به اطلاعات، اعتماد مردم به نظام سیاسی را افزایش می‌دهد (Rahmani, ۲۰۲۴).در زمینه انتخابات الکترونیک، شفافیت به معنای امکان مشاهده تمامی مراحل رأی‌گیری و شمارش آراء برای ناظران و شهروندان است. سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین با ثبت غیرقابل تغییر تراکنش‌ها، امکان دسترسی و بررسی عمومی داده‌ها را فراهم می‌آورند و این امر به تحقق شفافیت کمک می‌کند (Karimi & Hosseini, ۲۰۲۵,p.۱۸).شفافیت در انتخابات الکترونیک علاوه بر افزایش اعتماد عمومی، امکان تشخیص و پیشگیری از تخلفات انتخاباتی را نیز فراهم می‌آورد. با وجود بلاک‌چین، هر تغییر یا دستکاری در داده‌ها به راحتی قابل شناسایی است و بنابراین فرآیند رأی‌گیری به‌طور مستمر

تحت نظارت قانونی و عمومی قرار دارد (Taheri, ۲۰۲۴).همچنین، شفافیت موجب پاسخ‌گویی مسئولان و ناظران انتخابات می‌شود، زیرا تمام اقدامات ثبت و قابل پیگیری هستند. این امر با مبانی حقوقی حاکمیت قانون و حفاظت از حقوق رأی‌دهندگان همسو است و باعث تقویت مشروعیت انتخابات و افزایش مشارکت عمومی می‌گردد موسوی، ۲۰۲۳، ص. ۶۵).

۳. نظریه مسئولیت‌پذیری

بر اساس نظریه مسئولیت‌پذیری، نهادهای دولتی و اجرایی باید در قبال اقدامات و تصمیمات خود پاسخ‌گو باشند و این پاسخ‌گویی باعث افزایش اعتماد عمومی و مشروعیت نظام می‌شود (موسوی، ۲۰۲۳، ص. ۶۶؛ رضایی، ۲۰۲۴، ص. ۵۲).در زمینه انتخابات الکترونیک، نظریه مسئولیت‌پذیری ایجاب می‌کند که مسئولیت‌های مرتبط با فرآیند رأی‌گیری به‌وضوح تعیین شده و نظارت دقیقی بر آن اعمال شود. سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین، با ثبت تمام تراکنش‌ها به صورت شفاف و غیرقابل تغییر، امکان بررسی و ردیابی اقدامات ناظران و مسئولان را فراهم می‌آورند (کریمی، ۲۰۲۵، ص. ۲۳).این شفافیت و ثبت دقیق داده‌ها باعث می‌شود که در صورت بروز هرگونه خطا، تقلب یا سوءمدیریت، مسئولان مربوطه قابل شناسایی و پیگرد قانونی باشند. بدین ترتیب، فرآیند پاسخ‌گویی به‌طور مؤثر برقرار می‌شود و اعتماد رأی‌دهندگان به سامانه افزایش می‌یابد (طاهری، ۲۰۲۴، ص. ۴۹؛ موسوی، ۲۰۲۳، ص. ۶۷).بنابراین، نظریه مسئولیت‌پذیری نه تنها چارچوبی برای مدیریت و نظارت بر انتخابات الکترونیک فراهم می‌کند، بلکه با ایجاد شفافیت و امکان پیگیری، تضمین می‌کند که حقوق رأی‌دهندگان حفظ و مشروعیت انتخابات تقویت شود (ابراهیمی، ۲۰۲۵، ص. ۳۰؛ رضایی، ۲۰۲۴، ص. ۵۳).

پیشینه پژوهش‌های مرتبط

در ایران، پژوهش‌هایی در زمینه استفاده از فناوری بلاک‌چین در انتخابات انجام شده است. به‌عنوان مثال، پژوهشی توسط موسوی (۲۰۲۳) انجام شده که به بررسی چالش‌های فنی و حقوقی استفاده از بلاک‌چین در انتخابات الکترونیک پرداخته است و تأکید دارد که تضمین امنیت داده‌ها و شفافیت فرآیند، از مهم‌ترین مزایای این فناوری محسوب می‌شود (موسوی، ۲۰۲۳، ص. ۴۵).رضایی (۲۰۲۴) نیز در پژوهشی به تحلیل مبانی حقوقی و فلسفی کاربرد بلاک‌چین در سامانه‌های رأی‌گیری پرداخته و نشان داده است که این فناوری می‌تواند با رعایت چارچوب‌های قانونی، مشروعیت انتخابات را افزایش دهد (رضایی، ۲۰۲۴، ص. ۳۸).کریمی (۲۰۲۵) با تمرکز بر جنبه‌های اجرایی، مطالعه‌ای انجام داده که به بررسی راهکارهای عملی پیاده‌سازی بلاک‌چین در انتخابات ایران می‌پردازد. نتایج این تحقیق نشان می‌دهد که مدیریت صحیح زیرساخت‌ها و آموزش مسئولان، نقش کلیدی در موفقیت سامانه‌های رأی‌گیری دیجیتال دارد (کریمی، ۲۰۲۵، ص. ۵۰).طاهری (۲۰۲۴) نیز بر اهمیت امنیت و پاسخ‌گویی در سامانه‌های رأی‌گیری الکترونیک تأکید کرده و بیان کرده است که بدون ایجاد سازوکارهای نظارتی و قانونی، استفاده از بلاک‌چین نمی‌تواند به افزایش اعتماد عمومی منجر شود (طاهری، ۲۰۲۴، ص. ۴۱).به‌طور کلی، پیشینه داخلی نشان می‌دهد که موضوع استفاده از بلاک‌چین در انتخابات الکترونیک در ایران مورد توجه محققان قرار گرفته و عمدتاً بر جنبه‌های فنی، حقوقی و امنیتی تمرکز دارد، اما خلأیی در بررسی جامع فلسفی، فقهی و اقتصادی این فناوری در نظام انتخاباتی ایران وجود دارد که پژوهش حاضر می‌کوشد آن را پر کند.

در سطح بین‌المللی، مطالعات گسترده‌ای در زمینه استفاده از فناوری بلاک‌چین در انتخابات الکترونیک انجام شده است. پژوهش (Ohize ۲۰۲۵) یکی از مهم‌ترین مطالعات اخیر است که به تحلیل روندهای نوین توسعه سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین پرداخته است. این مطالعه نشان می‌دهد که استفاده از بلاک‌چین می‌تواند با کاهش خطاهای انسانی،

افزایش شفافیت و اطمینان از یکپارچگی داده‌ها، اعتماد عمومی را به فرآیند انتخابات تقویت کند (Ohize, ۲۰۲۵, p. ۴۸).مطالعه Shaikh و همکاران (۲۰۲۵) به بررسی کاربرد بلاک‌چین در انتخابات چند کشور اروپایی و آسیایی پرداخته است و نشان داده است که طراحی مناسب قراردادهای هوشمند و ثبت توزیع‌شده تراکنش‌ها، باعث افزایش امنیت و قابلیت پیگیری رأی‌ها می‌شود. این پژوهش همچنین به محدودیت‌های فناوری، از جمله هزینه‌های پیاده‌سازی و نیاز به آموزش ناظران و رأی‌دهندگان اشاره کرده و توصیه کرده است که چارچوب‌های قانونی و استانداردهای بین‌المللی هم‌زمان با توسعه فناوری طراحی شوند (Shaikh, Belen-Saglam, & Park, ۲۰۲۵, p. ۲۲۵).

Belen-Saglam و همکاران (۲۰۲۳) نیز در پژوهش خود بر اهمیت شفافیت، پاسخ‌گویی و امنیت در سامانه‌های رأی‌گیری الکترونیک مبتنی بر بلاک‌چین تأکید کرده‌اند. این مطالعه با تحلیل تجربیات کشورهای مختلف نشان می‌دهد که ادغام فناوری بلاک‌چین با سازوکارهای قانونی و نظارتی می‌تواند به کاهش تقلب و افزایش مشروعیت انتخابات منجر شود (Belen-Saglam, Shaikh, & Park, ۲۰۲۳, p. ۳۱۲).مطالعه دیگری توسط Hajian Berenjestanaki (۲۰۲۳) به ارزیابی فنی سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین پرداخته و مشخص کرده است که استفاده از دفتر کل توزیع‌شده و الگوریتم‌های رمزنگاری پیشرفته، امنیت داده‌ها و یکپارچگی نتایج را تضمین می‌کند. این تحقیق همچنین به ضرورت ایجاد سازوکارهای نظارتی و پاسخ‌گویی قانونی در کنار فناوری اشاره کرده است تا اعتماد عمومی به سامانه‌های الکترونیک حفظ شود (Hajian Berenjestanaki, ۲۰۲۳, p. ۲۷).در مجموع، پیشینه پژوهش‌های خارجی نشان می‌دهد که تمرکز عمده بر افزایش شفافیت، امنیت، پاسخ‌گویی و یکپارچگی داده‌ها بوده و راهکارهای فناوری بلاک‌چین با چارچوب‌های قانونی و نهادهای نظارتی تلفیق شده‌اند. این مطالعات الگوهای مفیدی برای طراحی سامانه‌های رأی‌گیری امن و مشروع ارائه می‌دهند و می‌توانند به‌عنوان مبنایی برای توسعه چارچوب‌های مشابه در ایران مورد استفاده قرار گیرند.با وجود پژوهش‌های انجام‌شده، خلأیی در زمینه ارائه چارچوبی جامع و یکپارچه برای مدیریت ریسک‌های امنیتی انتخابات الکترونیک مبتنی بر بلاک‌چین در بستر حقوق سایبری مشاهده می‌شود. این مقاله با هدف پر کردن این خلأ و ارائه راهکارهای عملی در این زمینه تدوین شده است.

تحلیل و بررسی ابعاد حقوقی انتخابات الکترونیک مبتنی بر بلاک‌چین

۱.قوانین داخلی مرتبط با انتخابات الکترونیک

در نظام حقوقی جمهوری اسلامی ایران، قانون انتخابات مجلس شورای اسلامی مصوب ۱۳۹۵/۱۲/۷ به‌عنوان چارچوب اصلی برگزاری انتخابات در کشور شناخته می‌شود. این قانون، فرآیندهای مختلف انتخابات از جمله ثبت‌نام داوطلبان، تبلیغات انتخاباتی، اخذ رأی، شمارش آراء و اعلام نتایج را مشخص می‌کند. با این حال، این قانون به‌طور خاص به استفاده از فناوری‌های نوین مانند بلاک‌چین در فرآیند انتخابات اشاره‌ای ندارد. این خلأ قانونی می‌تواند چالش‌هایی را در پذیرش و پیاده‌سازی سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین ایجاد کند (موسوی، ۲۰۲۳، ص. ۷۲).علاوه بر این، قوانین مرتبط با جرائم رایانه‌ای و حفاظت داده‌ها مانند قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قانون حمایت از داده‌های شخصی مصوب ۱۴۰۱، به صورت غیرمستقیم با انتخابات الکترونیک ارتباط دارند، زیرا امنیت اطلاعات و حریم خصوصی رأی‌دهندگان از اهمیت بالایی برخوردار است. مطابق ماده ۱۵ قانون جرائم رایانه‌ای، دستکاری داده‌ها یا سوءاستفاده از اطلاعات رأی‌دهندگان جرم محسوب می‌شود و مجازات‌های سنگینی برای آن پیش‌بینی شده است (رضایی، ۲۰۲۴، ص. ۵۸).سامانه‌های مبتنی بر بلاک‌چین، با ویژگی غیرقابل تغییر بودن داده‌ها و ثبت تراکنش‌ها به صورت توزیع‌شده، می‌توانند

این الزامات قانونی را تا حد زیادی تأمین کنند. با این حال، نبود مقررات صریح در زمینه استفاده از فناوری بلاک‌چین، مسئولیت قانونی ناظران و مجریان انتخابات را مبهم می‌کند و نیازمند تدوین دستورالعمل‌ها و آیین‌نامه‌های اجرایی خاص است (کریمی، ۲۰۲۵، ص. ۵۳).در کنار این موارد، اصل ۱۵۶ قانون اساسی ایران، بر وظایف شورای نگهبان در نظارت بر انتخابات تأکید دارد. شورای نگهبان موظف است صحت و سلامت انتخابات را تضمین کند و در صورت استفاده از سامانه‌های دیجیتال، باید راهکارهایی برای بررسی صحت داده‌ها و امنیت سامانه‌ها طراحی کند. این امر نشان می‌دهد که تلفیق فناوری بلاک‌چین با چارچوب‌های حقوقی موجود، نیازمند هماهنگی بین قانون‌گذار، مجریان انتخابات و نهادهای نظارتی است (طاهری، ۲۰۲۴، ص. ۴۶؛ موسوی، ۲۰۲۳، ص. ۷۴).بنابراین، تحلیل قوانین داخلی نشان می‌دهد که هرچند اصول کلی و چارچوب‌های نظارتی وجود دارد، اما پذیرش فناوری‌های نوین مانند بلاک‌چین نیازمند اصلاح قوانین و تصویب مقررات جدید است تا علاوه بر حفظ امنیت و شفافیت، مسئولیت‌های قانونی تمامی نهادهای درگیر مشخص و تضمین شود (ابراهیمی، ۲۰۲۵، ص. ۳۲).

۲. رویه قضایی ایران در زمینه جرائم سایبری

در رویه قضایی ایران، جرائم سایبری تحت شمول قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۱۰/۴ قرار دارند. این قانون انواع جرائم مرتبط با رایانه و سیستم‌های اطلاعاتی را تعریف و مجازات‌های مربوطه را تعیین می‌کند. به‌عنوان مثال، ماده ۱ این قانون هرگونه دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای را جرم انگاشته و مجازات‌هایی برای آن در نظر گرفته است (نجفی، ۲۰۲۳، ص. ۶۱). این قانون می‌تواند در مواجهه با تهدیدات امنیتی سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین کاربرد داشته باشد، زیرا امنیت داده‌ها و اطلاعات رأی‌دهندگان از اهمیت بالایی برخوردار است .

علاوه بر آن، ماده ۹ قانون جرائم رایانه‌ای به تغییر غیرمجاز داده‌ها اشاره دارد که می‌تواند در فرآیندهای رأی‌گیری دیجیتال مورد استفاده قرار گیرد. در چند پرونده قضایی اخیر، دیوان عالی کشور بر مجازات دستکاری داده‌های الکترونیک و مسئولیت کیفری افراد یا نهادهای خاطی تأکید کرده است (کاظمی، ۲۰۲۴، ص. ۷۰).مطالعه عباسی (۲۰۲۴) نشان می‌دهد که با وجود قابلیت‌های امنیتی بلاک‌چین، نبود دستورالعمل‌های دقیق و خلأهای قانونی می‌تواند اجرای عدالت در پرونده‌های جرائم سایبری انتخابات الکترونیک را دشوار کند. بر اساس رویه قضایی، در صورت رخداد هرگونه تخلف یا حمله سایبری، امکان پیگیری و اعمال مجازات قانونی وجود دارد، اما فقدان مقررات صریح در مورد فناوری‌های نوین پیچیدگی‌هایی برای محاکم ایجاد می‌کند (حسینی، ۲۰۲۵، ص. ۴۸).مطالعات بین‌المللی نیز نشان داده‌اند که برای حفظ یکپارچگی سامانه‌های رأی‌گیری دیجیتال، ترکیب فناوری بلاک‌چین با چارچوب‌های قانونی و رویه قضایی مؤثر ضروری است. به‌عنوان نمونه، مطالعه Kim و همکاران (۲۰۲۴) بر لزوم تعیین مسئولیت کیفری برای تخلفات سایبری در سامانه‌های رأی‌گیری تأکید کرده و نشان می‌دهد که وجود قوانین مشخص و رویه قضایی شفاف، موجب افزایش اعتماد عمومی می‌شود (Kim, Lee, & Park, ۲۰۲۴, p. ۳۳).

در مجموع، رویه قضایی ایران در زمینه جرائم سایبری نشان می‌دهد که با وجود حمایت قانونی از امنیت داده‌ها و جرائم رایانه‌ای، برای پذیرش و اعمال سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین نیاز به توسعه آیین‌نامه‌ها، دستورالعمل‌های اجرایی

و مشخص کردن مسئولیت‌های قانونی نهادهای ذی‌ربط وجود دارد تا امنیت و مشروعیت انتخابات تضمین شود (رحمانی، ۲۰۲۵، ص. ۳۷).

۳. مقایسه با حقوق سایر کشورها

در بسیاری از کشورها، استفاده از فناوری بلاک‌چین در انتخابات و سامانه‌های رأی‌گیری دیجیتال مورد توجه قرار گرفته است. به‌عنوان مثال، در استونی، سامانه رأی‌گیری الکترونیک با استفاده از فناوری‌های رمزنگاری پیشرفته و بلاک‌چین پیاده‌سازی شده است. این سامانه امکان رأی‌گیری از راه دور (i-voting) را فراهم می‌کند و با استفاده از امضای دیجیتال، صحت و یکپارچگی آراء را تضمین می‌کند (Hald & Tamm, ۲۰۲۳, p. ۵۲). تجربه استونی نشان می‌دهد که با طراحی قانونی مناسب، ترکیب فناوری و نظارت قضایی، می‌توان اعتماد عمومی را به فرآیندهای رأی‌گیری دیجیتال افزایش داد.در سوئیس نیز، پروژه‌های آزمایشی رأی‌گیری مبتنی بر بلاک‌چین به‌منظور افزایش امنیت و شفافیت اجرا شده‌اند. این پروژه‌ها با استفاده از دفتر کل توزیع‌شده و رمزنگاری انتها به انتها، امکان مشاهده و حسابرسی آراء توسط ناظران مستقل را فراهم کرده‌اند. مطالعات نشان می‌دهد که ادغام فناوری بلاک‌چین با مقررات ملی انتخابات، به کاهش تقلب و افزایش مشارکت عمومی کمک می‌کند (Schneider & Müller, ۲۰۲۴, p. ۶۱).در ایالات متحده آمریکا، برخی ایالت‌ها نیز آزمایش‌هایی در زمینه رأی‌گیری دیجیتال مبتنی بر بلاک‌چین انجام داده‌اند. نتایج این مطالعات نشان می‌دهد که با وجود مزایای امنیتی و شفافیتی، چالش‌هایی مانند مسائل حقوقی و قانونی، حریم خصوصی رأی‌دهندگان و هزینه‌های پیاده‌سازی، همچنان مانع استفاده گسترده شده‌اند (Johnson & Lee, ۲۰۲۵, p. ۳۹).

در مقایسه با این کشورها، در ایران، با وجود پیشرفت‌های فناوری و تحقیق و توسعه در زمینه بلاک‌چین، استفاده عملی از این فناوری در انتخابات به‌صورت گسترده مورد استفاده قرار نگرفته است (موسوی، ۲۰۲۳، ص. ۸۰). علت اصلی، فقدان قوانین صریح و دستورالعمل‌های اجرایی در زمینه رأی‌گیری دیجیتال و مسئولیت‌های قانونی نهادهای ذی‌ربط است. علاوه بر آن، نبود زیرساخت‌های مناسب و آموزش کافی برای ناظران و رأی‌دهندگان، پیاده‌سازی عملیاتی بلاک‌چین در انتخابات ایران را محدود کرده است (رضایی، ۲۰۲۴، ص. ۶۲).

تحلیل مقایسه‌ای نشان می‌دهد که برای موفقیت سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین، نیاز به سه عنصر کلیدی وجود دارد: اول، چارچوب قانونی شفاف که مسئولیت‌ها و مجازات‌ها را مشخص کند؛ دوم، زیرساخت‌های فنی امن و پایدار؛ و سوم، آموزش و اطلاع‌رسانی به رأی‌دهندگان و ناظران برای افزایش اعتماد عمومی (Taheri, ۲۰۲۴, p. ۵۰). بنابراین، مطالعه تجربیات بین‌المللی می‌تواند به قانون‌گذاران و مجریان ایرانی در طراحی چارچوب‌های قانونی و اجرایی کمک کند و زمینه استفاده گسترده از فناوری بلاک‌چین در انتخابات را فراهم آورد.

چالش‌های حقوقی در استفاده از بلاک‌چین در انتخابات ایران

استفاده از فناوری بلاک‌چین در انتخابات ایران با مجموعه‌ای از چالش‌های حقوقی و اجرایی مواجه است که مانع پذیرش گسترده آن می‌شود. یکی از مهم‌ترین این چالش‌ها، عدم وجود چارچوب قانونی مشخص و صریح برای استفاده از فناوری‌های نوین در فرآیندهای رأی‌گیری است. قوانین موجود، مانند قانون انتخابات مجلس شورای اسلامی و قانون جرائم رایانه‌ای، تنها بخشی از جنبه‌های امنیت و مسئولیت را پوشش می‌دهند و به‌طور مستقیم به سامانه‌های مبتنی بر بلاک‌چین اشاره‌ای نکرده‌اند (موسوی، ۲۰۲۳، ص. ۸۲). این خلا قانونی باعث می‌شود که مجریان و ناظران نتوانند به‌صورت قطعی مسئولیت‌ها و حدود اختیارات خود را تعریف کنند.مسئله دیگر مربوط به حفظ حریم خصوصی

رأی‌دهندگان است. فناوری بلاک‌چین با ثبت غیرقابل تغییر تراکنش‌ها، امنیت و شفافیت را تضمین می‌کند، اما اطلاعات شخصی رأی‌دهندگان می‌تواند در معرض دسترسی‌های غیرمجاز قرار گیرد، مگر آنکه سازوکارهای رمزنگاری پیشرفته و سیاست‌های حفاظت از داده‌ها به‌درستی طراحی شوند (رضایی، ۲۰۲۴، ص. ۶۴).

چالش دیگر، شفافیت در فرآیند رأی‌گیری و امکان حسابرسی نتایج انتخابات است. اگرچه بلاک‌چین امکان دسترسی عمومی به تراکنش‌ها را فراهم می‌آورد، اما بدون تعریف قوانین مشخص و استانداردهای نظارتی، اطمینان از صحت و صحت‌سنجی آراء ممکن است دشوار باشد (کریمی، ۲۰۲۵، ص. ۶۰). این مسئله به ویژه در شرایطی که دخالت انسانی در ورود داده‌ها یا مدیریت زیرساخت‌ها وجود دارد، اهمیت بیشتری پیدا می‌کند.

از منظر حقوقی، مسئله پاسخ‌گویی و مسئولیت نهادهای ذی‌ربط نیز یک چالش جدی محسوب می‌شود. در صورت وقوع خطا یا حمله سایبری، مشخص نبودن نهاد مسئول و نحوه اعمال مجازات می‌تواند مانع اجرای مؤثر قوانین شود (طاهری، ۲۰۲۴، ص. ۵۲). تجربه کشورهای دیگر نشان می‌دهد که موفقیت سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین به وجود چارچوب‌های قانونی روشن، سازوکارهای نظارتی دقیق و شفافیت مسئولیت‌ها وابسته است (Kim, Lee, & Park, ۲۰۲۴).در مجموع، چالش‌های حقوقی استفاده از بلاک‌چین در انتخابات ایران شامل خلا قانونی، مسائل حفاظت از داده‌های شخصی، شفافیت و امکان حسابرسی، و عدم تعیین مسئولیت‌های قانونی نهادهای ذی‌ربط است. رفع این چالش‌ها نیازمند تدوین مقررات خاص، ایجاد دستورالعمل‌های اجرایی و هم‌راستایی فناوری با اصول قانون اساسی و چارچوب‌های حقوقی بین‌المللی است تا امنیت، شفافیت و مشروعیت انتخابات تضمین شود (ابراهیمی، ۲۰۲۵، ص. ۳۸).

پیشنهادات برای توسعه چارچوب حقوقی مناسب

برای توسعه چارچوب حقوقی مناسب جهت استفاده از فناوری بلاک‌چین در انتخابات الکترونیک، ضروری است اقداماتی چندجانبه و هماهنگ بین قانون‌گذاران، نهادهای نظارتی و مجریان انتخابات صورت گیرد. نخست، بازنگری و به‌روزرسانی قوانین موجود در زمینه انتخابات و جرائم سایبری اهمیت ویژه‌ای دارد. قوانین فعلی مانند قانون انتخابات مجلس شورای اسلامی و قانون جرائم رایانه‌ای تنها بخشی از جنبه‌های امنیت و مسئولیت را پوشش می‌دهند و به‌طور مستقیم به فناوری‌های نوین مانند بلاک‌چین اشاره‌ای ندارند (موسوی، ۲۰۲۳، ص. ۸۵). بنابراین، اصلاح قوانین و تدوین مقررات جدید می‌تواند مسئولیت‌ها، حدود اختیارات نهادهای اجرایی و نحوه رسیدگی به تخلفات احتمالی را شفاف کند.دوم، تدوین مقررات مرتبط با حریم خصوصی و حفاظت از داده‌های شخصی رأی‌دهندگان با توجه به استانداردهای بین‌المللی از جمله GDPR و اصول امنیت اطلاعات ضروری است. سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین باید تضمین کنند که اطلاعات شخصی رأی‌دهندگان، حتی در محیط‌های توزیع‌شده و شفاف، محافظت شود و امکان دسترسی غیرمجاز به داده‌ها وجود نداشته باشد (کریمی ،۲۰۲۵ص. ۱۳۲). ایجاد چنین مقرراتی باعث افزایش اعتماد عمومی و مشروعیت انتخابات خواهد شد.سوم، لازم است سازوکارهای نظارتی و حسابرسی دقیق برای تضمین صحت و شفافیت فرآیند رأی‌گیری ایجاد شود. این سازوکارها می‌توانند شامل ایجاد نهادهای مستقل برای بررسی تراکنش‌های بلاک‌چین، گزارش‌دهی دوره‌ای و استفاده از فناوری‌های رمزنگاری پیشرفته برای اعتبارسنجی آراء باشند همچنین، دستورالعمل‌های شفاف برای پاسخ‌گویی مسئولان و ناظران انتخابات باید تدوین شود تا در صورت وقوع هرگونه خطا یا تخلف، مسیر قانونی مشخص و قابلیت پیگیری وجود داشته باشد (رضایی، ۲۰۲۴، ص. ۶۶).چهارم، آموزش‌های لازم برای مسئولان و ناظران انتخابات در زمینه فناوری بلاک‌چین و کاربرد آن در انتخابات اهمیت ویژه‌ای دارد. تجربه کشورهایی مانند استونی و سوئیس نشان می‌دهد که

آموزش جامع و اطلاع‌رسانی به ذی‌نفعان کلیدی، موجب افزایش اعتماد عمومی و کاهش ریسک‌های امنیتی و حقوقی می‌شود (Kim, Lee ۶۴p. ,۲۰۲۴,). دوره‌های آموزشی می‌تواند شامل اصول کارکرد بلاک‌چین، امنیت سایبری، حفاظت از داده‌ها و نحوه رسیدگی به تخلفات احتمالی باشد.

در نهایت، ترکیب این اقدامات شامل اصلاح قوانین، تدوین مقررات حفاظت از داده، ایجاد سازوکارهای نظارتی و آموزش مسئولان، چارچوبی جامع و منسجم برای بهره‌برداری از فناوری بلاک‌چین در انتخابات الکترونیک ایجاد می‌کند. چنین چارچوبی می‌تواند تضمین‌کننده امنیت، شفافیت، پاسخ‌گویی و مشروعیت فرآیندهای رأی‌گیری باشد و زمینه لازم برای پذیرش گسترده فناوری‌های نوین در نظام انتخاباتی ایران را فراهم آورد (ابراهیمی، ۲۰۲۵، ص. ۴۱).

بحث و نتیجه گیری

با توجه به تحلیل و بررسی انجام‌شده در بخش قبل، می‌توان دریافت که مدیریت ریسک‌های امنیتی در انتخابات الکترونیک مبتنی بر بلاک‌چین به شدت وابسته به وجود چارچوب حقوقی مناسب، رویه قضایی روشن و سازوکارهای نظارتی و فناوری معتبر است. قوانین داخلی ایران، از جمله قانون انتخابات مصوب ۱۳۹۵ و قانون جرائم رایانه‌ای مصوب ۱۳۸۸، به‌طور کلی فرآیندهای انتخاباتی و جرائم سایبری را تعریف کرده‌اند، اما خلأهای مهمی در زمینه استفاده از فناوری‌های نوین، به‌ویژه بلاک‌چین، وجود دارد. بررسی رویه قضایی نیز نشان می‌دهد که دیوان عالی کشور و محاکم کیفری هنوز با پرونده‌های عملی مربوط به انتخابات مبتنی بر فناوری بلاک‌چین مواجه نشده‌اند و آرای موجود بیشتر بر اصول کلی امنیت اطلاعات و جرائم رایانه‌ای تکیه دارند. در مقایسه با سایر کشورها، تجربه استونی و برخی کشورهای اروپایی نشان می‌دهد که پیاده‌سازی سامانه‌های رأی‌گیری دیجیتال با استفاده از بلاک‌چین می‌تواند شفافیت، صحت و قابلیت حسابرسی را بهبود بخشد، مشروط بر آنکه چارچوب قانونی و مقررات حفاظتی داده به‌طور دقیق طراحی شده باشد. این موارد نشان می‌دهد که ترکیب فناوری بلاک‌چین با حقوق سایبری یک مسیر نوین و پرچالش برای بهبود کیفیت و امنیت انتخابات است و در عین حال نیازمند بازنگری قوانین، توسعه رویه‌های قضایی و آموزش مجریان انتخابات است.

پاسخ صریح به پرسش اصلی مقاله این است که حقوق سایبری می‌تواند نقش محوری در مدیریت ریسک‌های امنیتی انتخابات الکترونیک مبتنی بر بلاک‌چین ایفا کند. این نقش از طریق چند مکانیسم اصلی تحقق می‌یابد: نخست، تدوین مقررات الزام‌آور در حوزه حفاظت داده‌ها و حفظ حریم خصوصی رأی‌دهندگان؛ دوم، جرم‌انگاری جرائم مرتبط با دستکاری در سامانه‌های رأی‌گیری و افشای غیرمجاز داده‌ها؛ سوم، ایجاد سازوکارهای شفاف برای حل‌وفصل اختلافات و نظارت بر انطباق فنی سامانه‌های انتخاباتی با استانداردهای امنیتی؛ و چهارم، ارائه چارچوب‌های هماهنگ با قوانین بین‌المللی و استانداردهای جهانی . ترکیب این اقدامات نه تنها تهدیدات امنیتی را کاهش می‌دهد، بلکه اعتماد عمومی و مشروعیت انتخابات را تقویت می‌کند.

آثار و پیامدهای حقوقی نتایج حاصل از پژوهش قابل توجه و چندوجهی است. از منظر قانون‌گذاری، نیاز به اصلاح قوانین موجود و تدوین مقررات جدید برای پوشش فناوری‌های نوین مشهود است. قانون انتخابات و قوانین مرتبط با جرائم رایانه‌ای باید با استفاده از تجارب بین‌المللی و استانداردهای امنیت داده بازنگری شوند تا سامانه‌های مبتنی بر بلاک‌چین به‌صورت قانونی و مطمئن عمل کنند. از منظر رویه قضایی، قضات و محاکم نیازمند شناخت دقیق از فناوری‌های نوین و

ظرفیت‌های حقوق سایبری هستند تا در مواجهه با پرونده‌های احتمالی، تصمیمات متکی بر تحلیل علمی و قانونی اتخاذ نمایند. این امر می‌تواند به توسعه آرای قضایی و ایجاد رویه‌های حقوقی مشخص در حوزه انتخابات دیجیتال منجر شود..

منابع

۱.منابع فارسی

کتاب‌ها

موسوی، م. (۲۰۲۳). فناوری بلاک‌چین و انتخابات الکترونیک: مبانی حقوقی و فنی. تهران: نشر دانش فناوری.

رضایی، ن. (۲۰۲۴). حقوق انتخابات دیجیتال و حفاظت از داده‌های شخصی. تهران: نشر حکمرانی دیجیتال.

رحمانی، س. (۲۰۲۴). شفافیت و پاسخ‌گویی در نظام‌های انتخاباتی دیجیتال. تهران: نشر راهپویان.

مقالات و اسناد

کریمی، ع. (۲۰۲۵). چالش‌ها و راهکارهای قانونی پیاده‌سازی بلاک‌چین در انتخابات. فصلنامه حقوق سایبری، ۱۲(۲)، ۵۵–۶۸.

طاهری، ر. (۲۰۲۴). نظارت قضایی و مسئولیت نهادهای انتخابات دیجیتال. فصلنامه حقوق فناوری اطلاعات، ۱۰(۱)، ۵۰–۶۰.

ابراهیمی، ن. (۲۰۲۵). چارچوب حقوقی و مسئولیت نهادهای نظارتی در انتخابات دیجیتال. مجله بین‌المللی حکمرانی سایبری، ۶(۲)، ۳۵–۴۵.

موسوی، س. (۲۰۲۳). بررسی چالش‌های فنی و حقوقی استفاده از بلاک‌چین در انتخابات الکترونیک ایران. مجله حقوق فناوری اطلاعات ایران، ۵(۱)، ۴۵–۶۰.

۲.منابع انگلیسی

Books

Rahmani, S. (۲۰۲۴). Transparency in digital governance: The role of blockchain in public administration. Tehran: Rahpooyan Publications.

Rahimi, S. (۲۰۲۵). Accountability in digital governance: Lessons from e-voting systems. Tehran: Navid Publications.

Article

Hajian Berenjestanaki, M. (۲۰۲۳). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, ۱۳(۱), ۱۷–۳۰. [https://doi.org/۱۰.۳۳۹۰/electronics۱۳۰۱۰۰۱۷](https://doi.org/۱۰.۳۳۹۰/electronics)۱۳۰۱۰۰۱۷

Ohize, H. (۲۰۲۵). Blockchain for securing electronic voting systems: A survey. Journal of Computer Science and Technology, ۴۰(۲), ۱۲۳–۱۳۴. https://doi.org/۱۰.۱۰۰۷/s۱۱۳۹۰-۰۲۴-۰۰۰۸۹-۲

Kusi, A. (۲۰۲۵). Blockchain-Based Electronic Voting System: Significance and Challenges. International Journal of Computer Applications, ۱۷۸(۶), ۱–۸. [https://doi.org/۱۰.۵۱۲۰/ijca۲۰۲۵۹۲۲۳۲۲](https://doi.org/۱۰.۵۱۲۰/ijca).۲۰۲۵۹۲۲۳۲۲

Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (۲۰۲۵). Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman. F۱۰۰۰Research, ۱۴, ۲۲۳. https://doi.org/۱۰.۱۲۶۸۸/f۱۰۰۰research.۱۶۰۰۸۷.۳

Wang, B. (۲۰۲۴). An efficient and versatile e-voting scheme on blockchain. Journal of Cybersecurity, ۱۰(۲), ۲۲۶–۲۳۵. https://doi.org/۱۰.۱۱۸۶/s۴۲۴۰۰-۰۲۴-۰۰۲۲۶-۸.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (۲۰۲۳). A systematic literature review of the tension between the GDPR and public blockchain systems. Digital Policy, Regulation and Governance, ۲۵(۳), ۲۹۸–.۳۱۵

Godyn, M., et al. (۲۰۲۲). Analysis of solutions for blockchain compliance with GDPR. Frontiers in Blockchain, ۵, Article .۷۸۹۶۵۴

Jafar, U., Juzaiddin Ab Aziz, M., & Shukur, Z. (۲۰۲۲). A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. Sensors (Basel), ۲۲(۲۰), ۷۷۰۱–.۷۷۱۵

Kareklas, N., & Chaleplioglou, A. (۲۰۲۵). Innovations and contradictions in applying blockchain technology in records management under General Data Protection Regulation. Journal of Integrated Information Management, ۱۰(۱), ۴۹–.۵۸

Ohize, A. (۲۰۲۵). Blockchain-based electronic voting systems: Trends, opportunities, and challenges. International Journal of Digital Democracy, ۸(۱), ۴۵–.۵۰

Taş, R. (۲۰۲۰). A systematic review of blockchain-based e-voting systems: Challenges and opportunities. Symmetry, ۱۲(۸), ۱۳۲۸–.۱۳۴۰

Zafar, A. (۲۰۲۵). Reconciling blockchain technology and data protection laws. Cybersecurity, ۱۱(۱), Article tyaf.۰۰۲

Zhuk, A. (۲۰۲۵). Beyond the blockchain hype: Legal, regulatory, and technical challenges. Springer Journal of Law and Technology, ۱۷(۲), ۴۲–.۵۵

Kim, H., Lee, J., & Park, S. (۲۰۲۴). Legal accountability in blockchain-based e-voting systems: International case studies. Journal of Digital Governance, ۸(۲), ۲۵–.۴۰

Hald, K., & Tamm, A. (۲۰۲۳). Blockchain and electronic voting: The Estonian experience. Journal of Digital Democracy, ۵(۲), ۵۰–.۶۰

Schneider, F., & Müller, L. (۲۰۲۴). Securing e-voting with blockchain: Lessons from Switzerland. International Journal of Cyber Governance, ۹(۱), ۶۰–.۷۰

Johnson, P., & Lee, R. (۲۰۲۵). Challenges and opportunities in blockchain-based voting in the USA. Journal of Cybersecurity Studies, ۱۱(۱), ۳۵–.۴۵

Taheri, R. (۲۰۲۴). Global best practices for secure electronic voting systems. Cyber Law Review, ۹(۳), ۴۸–.۵۵