

تحلیل تطبیقی مسئولیت کیفری در جرایم سایبری مبتنی بر فناوری بلاکچین

امید قهرمانی^{۱*} سید کیهان اسدی^۲

۱. دانشجوی کارشناسی ارشد حقوق کیفری، دانشگاه آزاد اسلامی واحد سنندج، سنندج، ایران

۲. دانش آموخته حقوق بین الملل، مرکز تحصیلات تکمیلی تهران، تهران، ایران

چکیده

ظهور فناوری بلاکچین و گسترش کاربردهای آن در حوزه‌هایی همچون رمزارزها، قراردادهای هوشمند، سامانه‌های مالی غیرمتمرکز و انتقال داده‌های دیجیتال، تحولات بنیادینی را در ساختارهای اقتصادی و اجتماعی ایجاد کرده است. در کنار فرصت‌های گسترده این فناوری، ویژگی‌هایی مانند ناشناس بودن نسبی کاربران، غیرمتمرکز بودن شبکه، دشواری شناسایی مرتکبان و فرامرز بودن فعالیت‌های مبتنی بر بلاکچین، زمینه ارتکاب اشکال جدیدی از جرایم سایبری را فراهم کرده است. این وضعیت، نظام‌های کیفری سنتی را با چالش‌های جدی در زمینه تعیین عنصر قانونی جرم، انتساب رفتار مجرمانه، شناسایی مرتکب و اعمال ضمانت اجرای کیفری مواجه ساخته است.

پژوهش حاضر با روش توصیفی - تحلیلی و رویکرد تطبیقی، مسئولیت کیفری ناشی از جرایم سایبری مبتنی بر فناوری بلاکچین را در نظام حقوقی ایران و برخی نظام‌های حقوقی پیشرو بررسی می‌کند. هدف اصلی پژوهش، پاسخ به این پرسش است که آیا قواعد سنتی مسئولیت کیفری توانایی پاسخگویی به جرایم ناشی از فناوری‌های غیرمتمرکز را دارند یا نیازمند بازنگری تقنینی هستیم. یافته‌های پژوهش نشان می‌دهد که مهم‌ترین چالش حقوق کیفری در مواجهه با جرایم مبتنی بر بلاکچین، نه فقدان کامل قواعد کیفری، بلکه دشواری تطبیق مفاهیم سنتی مانند مباشرت، معاونت، قصد مجرمانه و صلاحیت کیفری با ساختار غیر متمرکز این فناوری است. بررسی تطبیقی نشان می‌دهد که برخی نظام‌های حقوقی با حرکت به سمت جرم‌انگاری رفتار محور، تنظیم‌گری فناوری محور و توسعه مسئولیت کیفری اشخاص حقوقی و ارائه‌دهندگان خدمات دیجیتال، تلاش کرده‌اند خلأهای موجود را کاهش دهند. در حقوق ایران نیز با وجود ظرفیت‌های موجود در قوانین جرایم رایانه‌ای و مقررات مرتبط، هنوز چارچوب جامع و مستقلی برای مواجهه کیفری با جرایم مبتنی بر بلاکچین وجود ندارد.

در پایان، پژوهش پیشنهاد می‌کند قانون‌گذار ایرانی ضمن حفظ اصول بنیادین حقوق کیفری، به سمت تدوین مقررات اختصاصی درباره مسئولیت کیفری فعالان حوزه بلاکچین، رمزارزها و خدمات غیر متمرکز حرکت کند.

واژگان کلیدی:

بلاک چین، جرایم سایبری، مسئولیت کیفری، رمزارز، حقوق کیفری تطبیقی، جرایم رایانه‌ای.

مقدمه:

تحولات فناوری اطلاعات در دهه‌های اخیر، مفهوم سنتی جرم و مسئولیت کیفری را با تغییرات گسترده‌ای مواجه کرده است. در گذشته، ارتکاب جرم غالباً نیازمند حضور فیزیکی مرتکب، وجود قلمرو مشخص و امکان شناسایی آسان فاعل رفتار مجرمانه بود؛ اما ظهور فضای سایبری این پیش‌فرض‌ها را دگرگون کرد. امروزه بسیاری از جرایم بدون حضور فیزیکی، بدون مرز جغرافیایی و حتی بدون امکان شناسایی مستقیم مرتکب انجام می‌شوند (Wall, ۲۰۱۰; Brenner, ۲۰۰۷). در میان فناوری‌های نوظهور، بلاکچین جایگاه ویژه‌ای دارد. بلاکچین یک فناوری ثبت غیرمتمرکز اطلاعات است که امکان ذخیره و انتقال داده‌ها را بدون نیاز به یک مرجع مرکزی فراهم می‌کند. این فناوری ابتدا با ظهور رمز ارزها شناخته شد، اما به تدریج در حوزه‌هایی مانند قراردادهای هوشمند، امور مالی غیرمتمرکز، مالکیت دیجیتال و مدیریت داده‌ها نیز توسعه یافت (Nakamoto, ۲۰۰۸, ۲۰۱۵).

اگرچه بلاکچین در ذات خود یک فناوری مجرمانه نیست، اما برخی ویژگی‌های آن، مانند دشواری حذف اطلاعات ثبت‌شده، ناشناس بودن نسبی کاربران، استفاده از کیف پول‌های دیجیتال و فعالیت شبکه‌های فرامرزی، فرصت‌هایی برای ارتکاب جرایمی مانند پول‌شویی دیجیتال، کلاهبرداری رمز ارزی، سرقت دارایی‌های دیجیتال، حملات سایبری مبتنی بر قراردادهای هوشمند و تأمین مالی فعالیت‌های غیرقانونی ایجاد کرده است (FATF, ۲۰۲۳; Europol, ۲۰۲۱). این تحولات، نظام عدالت کیفری را با پرسش‌های بنیادینی مواجه ساخته است: چه کسی مسئول رفتار مجرمانه در یک شبکه غیرمتمرکز است؟ آیا توسعه‌دهنده یک قرارداد هوشمند مسئول نتایج مجرمانه آن خواهد بود؟ آیا ارائه‌دهندگان خدمات مرتبط با رمز ارزها باید مسئولیت کیفری داشته باشند؟ آیا قواعد سنتی معاونت و مشارکت کیفری قابلیت اعمال بر ساختارهای غیر متمرکز را دارند؟ این پرسش‌ها در سال‌های اخیر به یکی از مهم‌ترین مباحث حقوق کیفری فناوری تبدیل شده‌اند (Lessig, ۲۰۰۶; Werbach, ۲۰۱۸).

پاسخ به این پرسش‌ها نیازمند مطالعه تطبیقی نظام‌های مختلف حقوقی است؛ زیرا کشورها در مواجهه با فناوری بلاکچین رویکردهای متفاوتی اتخاذ کرده‌اند. برخی کشورها با تمرکز بر تنظیم‌گری مالی و پیشگیری از جرایم، مقررات خاصی وضع کرده‌اند و برخی دیگر با استفاده از ظرفیت قوانین موجود جرایم رایانه‌ای تلاش کرده‌اند خلأهای قانونی را پوشش دهند (FATF, ۲۰۲۱; UNODC, ۲۰۲۴).

۱. بیان مسئله

حقوق کیفری سنتی بر مفاهیمی همچون رفتار انسانی مشخص، رابطه سببیت روشن، عنصر روانی قابل اثبات و امکان انتساب جرم به شخص معین استوار است. با این حال، فناوری بلاکچین بسیاری از این مفاهیم را با چالش مواجه کرده است. در ساختارهای متمرکز، معمولاً شناسایی مسئول جرم امکان‌پذیرتر است؛ زیرا یک سازمان، مدیر یا ارائه‌دهنده خدمت مشخص وجود دارد. اما در شبکه‌های غیرمتمرکز بلاکچینی، تصمیم‌ها ممکن است توسط هزاران کاربر، الگوریتم‌ها یا قراردادهای هوشمند اتخاذ شوند.

برای مثال، در یک حمله سایبری مبتنی بر قرارداد هوشمند، مشخص نیست مسئولیت کیفری متوجه چه شخصی است:

- برنامه‌نویس قرارداد هوشمند؟
- فردی که از آسیب‌پذیری آن سوءاستفاده کرده است؟
- مدیران پلتفرم؟
- کاربران شبکه؟

• یا هیچ شخص معینی؟

این ابهام، اصل شخصی بودن مسئولیت کیفری را با چالش مواجه می کند. در حقوق ایران نیز اگرچه قانون جرایم رایانه ای و برخی مقررات مرتبط ظرفیت هایی برای مقابله با رفتارهای مجرمانه دیجیتال ایجاد کرده اند، اما این قوانین عمدتاً برای فضای سایبری سنتی طراحی شده اند و پاسخ روشنی برای ویژگی های خاص فناوری بلاکچین ارائه نمی کنند. بنابراین مسئله اصلی پژوهش حاضر این است که: آیا نظام های حقوق کیفری موجود، توانایی انتساب مسئولیت کیفری در جرایم مبتنی بر فناوری بلاکچین را دارند یا باید الگوهای جدیدی برای مسئولیت کیفری دیجیتال طراحی شود؟

۲. اهمیت و ضرورت تحقیق

اهمیت این پژوهش از چند جهت قابل بررسی است: نخست، گسترش سریع فناوری بلاکچین موجب شده است که حقوق کیفری ناگزیر از مواجهه با پدیده ای جدید شود که با ساختارهای سنتی جرم تفاوت اساسی دارد. دوم، نبود چارچوب روشن مسئولیت کیفری می تواند موجب ایجاد خلأ قانونی و کاهش قدرت نظام عدالت کیفری در مقابله با جرایم نوظهور شود. سوم، مطالعه تطبیقی تجربه کشورهای مختلف می تواند راهکارهایی برای اصلاح نظام حقوقی ایران ارائه دهد. چهارم، این موضوع علاوه بر جنبه حقوقی، دارای ابعاد اقتصادی، امنیتی و اجتماعی نیز هست؛ زیرا بسیاری از فعالیت های مالی آینده ممکن است بر بستر فناوری های غیرمتمرکز انجام شود.

۳. اهداف تحقیق

هدف اصلی:

تحلیل تطبیقی مبانی و چالش های مسئولیت کیفری در جرایم سایبری مبتنی بر فناوری بلاکچین. اهداف فرعی:

۱. بررسی قابلیت اعمال قواعد سنتی مسئولیت کیفری بر جرایم بلاکچینی.
۲. تحلیل جایگاه عنصر مادی و معنوی جرم در فضای غیرمتمرکز.
۳. بررسی رویکرد نظام های حقوقی منتخب در مواجهه با جرایم مبتنی بر بلاکچین.
۴. ارائه پیشنهاد های تقنینی برای حقوق کیفری ایران.

۴. سؤالات تحقیق

سؤال اصلی:

مسئولیت کیفری ناشی از جرایم سایبری مبتنی بر فناوری بلاکچین در نظام های حقوقی مختلف چگونه تعیین می شود؟ سؤالات فرعی:

۱. مهم ترین چالش های انتساب جرم در فناوری بلاکچین چیست؟
۲. آیا قواعد سنتی مشارکت و معاونت کیفری پاسخگوی جرایم غیر متمرکز هستند؟
۳. حقوق ایران چه ظرفیت هایی برای مقابله با این جرایم دارد؟

۴. چه الگویی از تجربه نظام‌های حقوقی دیگر می‌تواند برای ایران مفید باشد؟

۵. روش تحقیق

این پژوهش از نظر هدف، کاربردی و از نظر روش، توصیفی - تحلیلی است. روش گردآوری اطلاعات، کتابخانه‌ای و اسنادی بوده و منابع شامل قوانین داخلی، اسناد بین‌المللی، مقررات کشورهای منتخب، کتاب‌ها و مقالات علمی مرتبط است. روش تحلیل نیز تطبیقی است؛ به این معنا که ابتدا وضعیت حقوق ایران بررسی شده و سپس با رویکردهای منتخب در نظام‌های حقوقی پیشرو مقایسه خواهد شد.

۶. پیشینه تحقیق

با گسترش فناوری بلاکچین و توسعه کاربردهای آن در حوزه‌های مالی، تجاری و خدمات دیجیتال، پژوهش‌های متعددی به بررسی ابعاد حقوقی و کیفری این فناوری پرداخته‌اند. بررسی ادبیات موجود نشان می‌دهد که مطالعات انجام‌شده را می‌توان در دو دسته کلی شامل پژوهش‌های خارجی و پژوهش‌های داخلی طبقه‌بندی کرد.

الف) پژوهش‌های خارجی

یکی از نخستین آثار بنیادین در این حوزه، مقاله ساتوشی ناکاموتو (۲۰۰۸) است که با معرفی بیت‌کوین، ساختار فنی بلاکچین را به‌عنوان یک سامانه پرداخت همتا به همتا بدون نیاز به نهاد مرکزی تبیین کرد. هرچند این اثر ماهیت فنی دارد، اما زمینه‌ساز شکل‌گیری مباحث حقوقی و کیفری مرتبط با فناوری بلاکچین شد.

ملانی سوان (۲۰۱۵) در کتاب Blockchain: Blueprint for a New Economy، ضمن تشریح کاربردهای گسترده بلاکچین، به آثار حقوقی قراردادهای هوشمند، سازمان‌های غیرمتمرکز و چالش‌های ناشی از حذف واسطه‌ها اشاره می‌کند و معتقد است که نظام‌های حقوقی برای مواجهه با این فناوری نیازمند بازنگری هستند.

کوین ورباخ (۲۰۱۸) در کتاب The Blockchain and the New Architecture of Trust، بلاک چین را معماری جدیدی برای ایجاد اعتماد در فضای دیجیتال معرفی می‌کند. وی ضمن بررسی ابعاد اقتصادی و حقوقی این فناوری، بیان می‌کند که مسئولیت اشخاص در شبکه‌های غیرمتمرکز با الگوهای سنتی مسئولیت حقوقی و کیفری تفاوت اساسی دارد.

در پژوهشی که واترز (۲۰۲۳) با عنوان When Criminals Abuse the Blockchain انجام داده است، مسئله صلاحیت کیفری و تعقیب مرتکبان جرایم در شبکه‌های غیرمتمرکز بررسی شده است. نتایج تحقیق نشان می‌دهد که ویژگی فرامرزی بلاکچین و نبود نهاد مرکزی، اعمال قواعد سنتی صلاحیت کیفری را با دشواری‌های جدی مواجه ساخته و ضرورت تدوین قواعد جدید را آشکار می‌کند.

همچنین گزارش گروه ویژه اقدام مالی (FATF، ۲۰۲۱) با تمرکز بر دارایی‌های مجازی و ارائه‌دهندگان خدمات مرتبط با رمز ارزها، مخاطرات پول‌شویی، تأمین مالی تروریسم و سایر جرایم مالی را بررسی کرده و بر لزوم ایجاد نظام‌های نظارتی مؤثر، احراز هویت کاربران و همکاری‌های بین‌المللی تأکید کرده است.

در مطالعه‌ای جدید، مانولانگ و همکاران (۲۰۲۵) به بررسی نقش فناوری بلاکچین در تحول مسئولیت کیفری اشخاص حقوقی پرداخته‌اند. نتایج این پژوهش نشان می‌دهد که ویژگی‌های شفافیت، تغییرناپذیری و قراردادهای هوشمند می‌تواند هم ابزار ارتقای پاسخگویی باشد و هم چالش‌های تازه‌ای درباره انتساب مسئولیت کیفری ایجاد کند.

از سوی دیگر، پژوهش آرنونه، اسپیره و بیوونا (۲۰۲۵) که به صورت مرور نظام‌مند ادبیات انجام شده است، نشان می‌دهد مهم‌ترین چارچوب مرتبط با بلاک چین شامل پول شویی، کلاهبرداری، اخاذی، باج‌افزارها و سوءاستفاده از دارایی‌های رمزنگاری شده است. نویسندگان همچنین تأکید می‌کنند که هنوز خلأهای قابل توجهی در زمینه مسئولیت کیفری بازیگران شبکه‌های غیرمتمرکز وجود دارد.

(ب) پژوهش‌های داخلی

در ایران نیز همزمان با گسترش استفاده از رمز ارزها، پژوهش‌های متعددی درباره ابعاد حقوقی بلاکچین انجام شده است. بخش قابل توجهی از این مطالعات بر وضعیت حقوقی رمز ارزها، امکان قانون‌گذاری، ماهیت قراردادهای هوشمند و چالش‌های ناشی از جرایم سایبری متمرکز بوده‌اند. برخی پژوهشگران نیز مسئولیت کیفری صرافی‌های رمز ارزی، پول شویی با استفاده از دارایی‌های دیجیتال و نقش فناوری بلاکچین در ارتکاب جرایم اقتصادی را بررسی کرده‌اند.

با وجود این، بررسی ادبیات داخلی نشان می‌دهد که اغلب پژوهش‌ها ماهیتی توصیفی داشته و بیشتر بر جنبه‌های مالی یا فنی فناوری بلاکچین تمرکز کرده‌اند. مطالعات اندکی به طور مستقل به موضوع مسئولیت کیفری در شبکه‌های غیرمتمرکز، مسئولیت توسعه‌دهندگان قراردادهای هوشمند، اعتبار قواعد سنتی مشارکت و معاونت در جرایم مبتنی بر بلاکچین و مطالعه تطبیقی نظام‌های حقوقی پرداخته‌اند. از این رو، همچنان خلأ پژوهشی قابل توجهی در زمینه تحلیل تطبیقی مسئولیت کیفری بازیگران مختلف اکوسیستم بلاکچین، به ویژه در حقوق ایران، وجود دارد.

۲-

مبانی نظری فناوری بلاکچین و چالش‌های حقوق کیفری سنتی

۲-۱.

تحولات فناورانه همواره حقوق را با پرسش‌های جدیدی مواجه ساخته‌اند. حقوق کیفری به عنوان یکی از حوزه‌هایی که بیشترین ارتباط را با رفتارهای انسانی و ضمانت اجرای آنها دارد، بیش از سایر شاخه‌های حقوقی نیازمند سازگاری با تغییرات اجتماعی و تکنولوژیک است.

ظهور اینترنت، فضای سایبری و سپس فناوری‌های غیرمتمرکز، مفهوم سنتی جرم را از حالت کلاسیک آن خارج کرده است. در ساختارهای سنتی، جرم معمولاً دارای سه ویژگی اصلی بود: وجود مرتکب مشخص، محل وقوع قابل تعیین و امکان اعمال صلاحیت کیفری توسط یک دولت معین. اما در محیط‌های دیجیتال، این ویژگی‌ها به تدریج تضعیف شده‌اند.

فناوری بلاکچین نقطه اوج این تحول محسوب می‌شود؛ زیرا برای نخستین بار امکان انجام تراکنش‌ها و اجرای دستورات دیجیتال بدون وجود یک نهاد مرکزی فراهم شده است. این ویژگی، اگرچه موجب نوآوری اقتصادی و فنی شده، اما همزمان چالش‌های عمیقی برای حقوق کیفری ایجاد کرده است.

۲-۲. مفهوم و ماهیت فناوری بلاکچین

بلاکچین نوعی دفتر کل توزیع شده دیجیتال است که اطلاعات در آن در قالب مجموعه‌ای از بلوک‌های به هم پیوسته ذخیره می‌شود. هر بلوک دارای اطلاعاتی است که پس از ثبت در شبکه، تغییر یا حذف آن بسیار دشوار خواهد بود.

برخلاف پایگاه‌های داده سنتی که تحت کنترل یک سازمان مرکزی قرار دارند، در بلاکچین اطلاعات میان تعداد زیادی از کاربران شبکه توزیع می‌شود. این ویژگی سبب می‌شود که کنترل و مدیریت سیستم به جای یک شخص یا نهاد، میان اعضای شبکه تقسیم شود.

به طور کلی، سه ویژگی اساسی بلاکچین عبارت‌اند از:

الف) غیرمتمرکز بودن

در سیستم‌های سنتی، یک مرکز کنترل‌کننده وجود دارد؛ برای مثال بانک‌ها، مؤسسات مالی یا شرکت‌های ارائه‌دهنده خدمات اینترنتی.

اما در بلاکچین، تصمیم‌گیری و اعتبارسنجی تراکنش‌ها توسط مجموعه‌ای از مشارکت‌کنندگان شبکه انجام می‌شود. این ویژگی اگرچه امنیت و استقلال سیستم را افزایش می‌دهد، اما از منظر کیفی موجب دشواری تعیین مسئولیت می‌شود.

ب) تغییرناپذیری اطلاعات

یکی از مهم‌ترین ویژگی‌های بلاکچین، ثبت دائمی اطلاعات است.

پس از ثبت داده در زنجیره، اصلاح یا حذف آن بسیار دشوار خواهد بود. این ویژگی در حوزه‌های مشروع مانند ثبت قراردادهای یا انتقال دارایی‌ها مفید است، اما در حوزه کیفری می‌تواند مشکلاتی ایجاد کند؛ زیرا اطلاعات مجرمانه نیز ممکن است برای مدت طولانی در شبکه باقی بماند.

ج) ناشناس بودن نسبی کاربران

در بسیاری از شبکه‌های بلاکچینی، کاربران با نشانی‌های دیجیتال فعالیت می‌کنند و الزاماً هویت واقعی آنان آشکار نیست. البته برخلاف تصور عمومی، بلاکچین کاملاً ناشناس نیست؛ زیرا تراکنش‌ها قابل مشاهده هستند، اما ارتباط میان نشانی دیجیتال و هویت واقعی فرد ممکن است دشوار باشد.

این ویژگی، فرایند کشف جرم و تعقیب کیفری را پیچیده می‌کند.

۲-۳. انواع جرایم سایبری مبتنی بر فناوری بلاکچین

فناوری بلاکچین خود جرم نیست، اما می‌تواند بستر ارتکاب برخی جرایم قرار گیرد. مهم‌ترین این جرایم عبارت‌اند از:

۲-۳-۱. کلاهبرداری‌های رمز ارزی

یکی از شایع‌ترین جرایم مرتبط با بلاکچین، ایجاد طرح‌های فریبکارانه برای جذب سرمایه یا انتقال غیرقانونی دارایی‌های دیجیتال است.

نمونه‌هایی از این رفتارها عبارت‌اند از:

- عرضه اولیه جعلی رمز ارزها؛
- ایجاد پروژه‌های ساختگی؛
- وعده سودهای غیرواقعی؛
- سرقت کلیدهای خصوصی کاربران.

در این موارد، چالش اصلی حقوق کیفری، شناسایی مرتکب و اثبات قصد مجرمانه است.

۲-۳-۲. پول‌شویی مبتنی بر رمز ارز

یکی از نگرانی‌های مهم نظام‌های کیفری، استفاده از رمز ارزها برای پنهان‌سازی منشأ دارایی‌های نامشروع است.

ویژگی‌هایی مانند سرعت انتقال، امکان فعالیت فرامرزی و استفاده از ابزارهای افزایش‌دهنده ناشناسی، می‌تواند فرآیند پول‌شویی را تسهیل کند.

در نتیجه، بسیاری از نظام‌های حقوقی تلاش کرده‌اند با اعمال الزامات شناسایی مشتری (KYC) و مبارزه با پول‌شویی (AML)، خطرات موجود را کاهش دهند.

۳-۳-۲. حملات علیه قراردادهای هوشمند

قرارداد هوشمند برنامه‌ای رایانه‌ای است که در صورت تحقق شرایط مشخص، به صورت خودکار اجرا می‌شود. با وجود مزایای فراوان، آسیب‌پذیری‌های برنامه‌نویسی ممکن است موجب خسارت‌های گسترده شود.

در این وضعیت پرسش مهم این است:

اگر یک قرارداد هوشمند دارای نقص امنیتی باشد و خسارت ایجاد کند، مسئولیت کیفری متوجه چه کسی است؟

• برنامه‌نویس؟

• مالک پروژه؟

• استفاده‌کننده؟

• یا هیچ‌کس؟

این مسئله یکی از پیچیده‌ترین چالش‌های حقوق کیفری معاصر است.

۴-۲. چالش مفهوم سنتی «مرتکب جرم» در فضای بلاکچین

یکی از اصول بنیادین حقوق کیفری، اصل شخصی بودن مسئولیت کیفری است. مطابق این اصل، تنها شخصی که رفتار مجرمانه را انجام داده یا در تحقق آن نقش مؤثر داشته است، باید پاسخگو باشد.

اما فناوری بلاکچین ساختارهای جدیدی ایجاد کرده است که تعیین مرتکب را دشوار می‌کند.

برای مثال، در یک سازمان خودگردان غیرمتمرکز (DAO)، تصمیم‌ها ممکن است توسط هزاران دارنده توکن اتخاذ شود.

در چنین وضعیتی، آیا می‌توان همه مشارکت‌کنندگان را مسئول دانست؟

یا باید مسئولیت را متوجه توسعه‌دهندگان اولیه کرد؟

پاسخ به این پرسش‌ها نیازمند بازنگری در مفاهیم سنتی مسئولیت کیفری است.

۵-۲. چالش عنصر مادی جرم در فناوری بلاکچین

عنصر مادی جرم معمولاً شامل رفتار خارجی قابل انتساب به مرتکب است.

اما در فضای بلاکچین، رفتار مجرمانه ممکن است:

• توسط کد رایانه‌ای اجرا شود؛

• در چند کشور مختلف انجام گیرد؛

• توسط چندین عامل انسانی و غیرانسانی شکل گیرد.

بنابراین، رابطه میان رفتار و نتیجه مجرمانه دیگر مانند جرایم سنتی روشن نیست.

۶-۲. چالش عنصر معنوی جرم

اثبات قصد مجرمانه یکی از دشوارترین مسائل در جرایم بلاکچینی است.

برای مثال، اگر شخصی یک نرم‌افزار غیرمتمرکز طراحی کند و بعدها دیگران از آن برای فعالیت مجرمانه استفاده کنند، آیا قصد

مجرمانه او قابل اثبات است؟

در حقوق کیفری، صرف امکان سوءاستفاده از یک فناوری، برای تحقق مسئولیت کیفری کافی نیست؛ بلکه باید علم و اراده مرتکب نسبت به نتیجه مجرمانه اثبات شود.

۷-۲. ضرورت شکل‌گیری رویکرد جدید در حقوق کیفری
 بررسی ویژگی‌های بلاکچین نشان می‌دهد که اعمال صرف قواعد سنتی حقوق کیفری ممکن است با محدودیت‌هایی مواجه شود.
 از این رو، نظام‌های حقوقی باید میان دو هدف تعادل ایجاد کنند:
 نخست، جلوگیری از استفاده مجرمانه از فناوری‌های نوین؛
 دوم، جلوگیری از توسعه بی‌ضابطه مسئولیت کیفری و نقض اصل قانونی بودن جرم و مجازات.
 راهکار مطلوب، جرم‌انگاری گسترده و مبهم نیست؛ بلکه ایجاد مقررات دقیق و مبتنی بر رفتارهای مشخص است.
 فناوری بلاکچین با ایجاد ساختارهای غیر متمرکز، مفاهیم بنیادین حقوق کیفری مانند مرتکب جرم، رابطه سببیت، عنصر مادی و عنصر معنوی را با چالش مواجه کرده است.
 ویژگی‌هایی مانند توزیع‌شدگی، ناشناس بودن نسبی و فرامرزی بودن فعالیت‌ها، موجب شده است که روش‌های سنتی تعقیب کیفری کارآمدی سابق را نداشته باشند.
 بنابراین، بررسی تطبیقی راهکارهای نظام‌های حقوقی مختلف برای تعیین مسئولیت کیفری در این حوزه، ضرورت اساسی دارد.

۳:

تحلیل تطبیقی مسئولیت کیفری جرایم سایبری مبتنی بر بلاکچین در حقوق ایران، اتحادیه اروپا و ایالات متحده

۳-۱.

فناوری بلاکچین به دلیل ویژگی‌های خاص خود، مرزهای سنتی میان قلمروهای حقوقی را تغییر داده است. در گذشته، تعیین مسئولیت کیفری عمدتاً بر پایه وجود یک مرتکب مشخص، رفتار مادی قابل شناسایی و ارتباط مستقیم میان فعل و نتیجه انجام می‌شد؛ اما در محیط‌های غیرمتمرکز، این عناصر با پیچیدگی‌های جدیدی مواجه شده‌اند.
 نظام‌های حقوقی مختلف، بسته به مبانی حقوقی، سیاست جنایی و میزان توسعه فناوری، رویکردهای متفاوتی نسبت به این پدیده اتخاذ کرده‌اند. برخی کشورها تلاش کرده‌اند با توسعه قوانین موجود، پاسخ کیفری ارائه دهند و برخی دیگر به سمت ایجاد چارچوب‌های خاص برای دارایی‌های دیجیتال و خدمات مبتنی بر بلاکچین حرکت کرده‌اند.
 در این فصل، وضعیت حقوق ایران با دو رویکرد مهم در حقوق تطبیقی، یعنی اتحادیه اروپا و ایالات متحده آمریکا، مقایسه می‌شود تا نقاط قوت، ضعف و امکان استفاده از تجربه‌های تطبیقی برای نظام حقوقی ایران مشخص شود.

۲-۳. مسئولیت کیفری جرایم بلاکچینی در حقوق ایران

۱-۲-۳. وضعیت تقنینی موجود

در حقوق ایران، مقررات مستقلی که به‌طور جامع مسئولیت کیفری ناشی از فناوری بلاکچین را تنظیم کند، وجود ندارد. با این حال، برخی قوانین موجود قابلیت اعمال بر بخشی از رفتارهای مجرمانه مرتبط با این فناوری را دارند.
 مهم‌ترین مقررات قابل استناد عبارت‌اند از:

• قانون جرایم رایانه‌ای؛

• قانون مجازات اسلامی؛

• مقررات مربوط به مبارزه با پول‌شویی؛

• مقررات ناظر بر فعالیت‌های اقتصادی و مالی.

قانون جرایم رایانه‌ای با جرم‌انگاری رفتارهایی مانند دسترسی غیرمجاز، تخریب داده‌ها، سرقت داده‌های رایانه‌ای و کلاهبرداری رایانه‌ای، چارچوب اولیه‌ای برای مقابله با جرایم دیجیتال ایجاد کرده است.

با این حال، این قانون در زمانی تصویب شد که فناوری‌هایی مانند بلاکچین، قراردادهای هوشمند و سازمان‌های غیرمتمرکز هنوز توسعه کنونی را نداشتند.

۳-۲-۲. چالش انتساب مسئولیت کیفری در حقوق ایران

یکی از مهم‌ترین مسائل در حقوق ایران، تعیین شخص مسئول در ساختارهای غیرمتمرکز است.

برای مثال، در یک پروژه رمز ارزی که هزاران کاربر در آن مشارکت دارند، اگر پروژه برای فریب سرمایه‌گذاران طراحی شده باشد، پرسش‌های زیر مطرح می‌شود:

آیا توسعه‌دهندگان مسئول هستند؟

آیا مدیران پلتفرم مسئولیت دارند؟

آیا کاربران شبکه که رأی داده‌اند، شریک جرم محسوب می‌شوند؟

قواعد سنتی شرکت و معاونت در جرم، پاسخ روشنی برای تمام این وضعیت‌ها ارائه نمی‌کنند.

زیرا این قواعد عمدتاً بر مبنای همکاری مستقیم و قابل شناسایی میان اشخاص انسانی طراحی شده‌اند.

۳-۲-۳. امکان اعمال عناوین کیفری سنتی

یکی از رویکردهای ممکن در حقوق ایران، تطبیق رفتارهای بلاکچینی با عناوین کیفری موجود است.

برای نمونه:

الف) کلاهبرداری رایانه‌ای

اگر شخصی با ایجاد یک پروژه جعلی رمز ارزی، افراد را فریب داده و دارایی آنان را منتقل کند، امکان بررسی رفتار وی در قالب کلاهبرداری رایانه‌ای وجود دارد.

اما مشکل اصلی، اثبات عناصر جرم و شناسایی مرتکب در محیط‌های ناشناس است.

ب) پول‌شویی

رمز ارزها می‌توانند وسیله‌ای برای پنهان کردن منشأ غیرقانونی اموال باشند.

در چنین مواردی، مقررات مبارزه با پول‌شویی می‌تواند قابلیت اعمال داشته باشد؛ اما نیازمند سازوکارهای فنی برای ردیابی

تراکنش‌ها و شناسایی مالک واقعی دارایی دیجیتال است.

۳-۳-۳. رویکرد اتحادیه اروپا در قبال جرایم مبتنی بر بلاکچین

۳-۳-۱. حرکت از جرم‌انگاری سنتی به تنظیم‌گری فناوری‌محور

اتحادیه اروپا رویکردی متفاوت نسبت به فناوری‌های نوین اتخاذ کرده است.

این رویکرد بر سه محور اصلی استوار است:

۱. ایجاد شفافیت برای فعالان بازار دیجیتال؛

۲. پیشگیری از سوءاستفاده‌های مالی؛

۳. افزایش قابلیت شناسایی مرتکبان جرایم.

اتحادیه اروپا تلاش کرده است به جای ممنوعیت فناوری، آن را در چارچوب‌های قانونی کنترل کند.

۳-۳-۲. مسئولیت ارائه‌دهندگان خدمات دارایی دیجیتال

یکی از ویژگی‌های مهم رویکرد اروپایی، توجه به نقش واسطه‌های دیجیتال است.

برخلاف ساختارهای کاملاً غیر متمرکز، بسیاری از فعالیت‌های رمز ارزی از طریق صرافی‌ها، کیف پول‌ها و ارائه‌دهندگان خدمات انجام می‌شود.

بنابراین، اتحادیه اروپا تلاش کرده است برای این بازیگران، تعهداتی مانند:

- احراز هویت مشتری؛
 - گزارش فعالیت‌های مشکوک؛
 - همکاری با نهادهای قضایی؛ ایجاد کند.
- این امر باعث می‌شود در صورت وقوع جرم، امکان تعیین مسئولیت حقوقی و کیفری افزایش یابد.
- ۳-۳. چالش DAO و قراردادهای هوشمند در اروپا
- یکی از مسائل حل‌نشده در حقوق اروپا، مسئولیت سازمان‌های خودگردان غیرمتمرکز است. در DAOها، تصمیم‌ها ممکن است توسط مجموعه‌ای از کاربران ناشناس اتخاذ شود. در نتیجه، پرسش اصلی این است:
- آیا DAO می‌تواند دارای شخصیت حقوقی باشد؟
- آیا مشارکت‌کنندگان آن مسئولیت کیفری مشترک دارند؟
- اروپا هنوز پاسخ کاملاً یکسانی برای این مسئله ارائه نکرده است و این موضوع همچنان یکی از چالش‌های مهم حقوق فناوری محسوب می‌شود.
- ۳-۴. رویکرد ایالات متحده آمریکا
- ۳-۴-۱. استفاده از قوانین موجود
- ایالات متحده برخلاف برخی نظام‌های حقوقی، غالباً به جای ایجاد یک قانون کیفری کاملاً جدید، از ظرفیت قوانین موجود استفاده کرده است.
- نهادهای قضایی و نظارتی آمریکا در بسیاری از موارد، رفتارهای مجرمانه مرتبط با رمز ارزها را تحت عناوینی مانند:
- کلاهبرداری؛
 - پول‌شویی؛
 - دستکاری بازار؛
 - نقض قوانین مالی؛ پیگیری کرده‌اند.
- ۳-۴-۲. مسئولیت کیفری مدیران و توسعه‌دهندگان
- یکی از ویژگی‌های مهم رویکرد آمریکایی، تمرکز بر نقش واقعی افراد در طراحی و اداره پروژه‌هاست. صرف توسعه یک فناوری، موجب مسئولیت کیفری نمی‌شود. اما اگر شخصی:
- آگاهانه ابزار فناوری را برای ارتکاب جرم طراحی کند؛
 - از فعالیت مجرمانه سود ببرد؛
 - اطلاعات نادرست به کاربران ارائه دهد؛
- ممکن است با مسئولیت کیفری مواجه شود.
- این رویکرد با اصل شخصی بودن مسئولیت کیفری هماهنگ است.
- ۳-۵. مقایسه تطبیقی سه نظام حقوقی
- موضوع ایران اتحادیه اروپا آمریکا
- قانون اختصاصی بلاکچین محدود در حال توسعه پراکنده اما فعال
- رویکرد اصلی استفاده از قوانین موجود تنظیم‌گری فناوری محور اجرای قوانین موجود
- چالش اصلی فقدان چارچوب جامع مسئولیت DAOها تعارض صلاحیت‌ها

مسئولیت واسطه‌ها محدود گسترده‌تر موردی

حمایت از نوآوری نیازمند توسعه بالا بالا

۳-۶. تحلیل نهایی

مطالعه تطبیقی نشان می‌دهد که هیچ نظام حقوقی تاکنون پاسخ کاملاً جامعی برای مسئولیت کیفری در فضای بلاکچین ارائه نکرده است.

با این حال، تفاوت مهم میان نظام‌ها در شیوه مواجهه با مسئله است:

حقوق ایران بیشتر بر تطبیق فناوری جدید با عناوین کیفری موجود تکیه دارد.

اتحادیه اروپا رویکرد پیشگیرانه و تنظیم‌گرانه اتخاذ کرده است.

ایالات متحده بیشتر بر مسئولیت اشخاصی تمرکز دارد که نقش فعال و آگاهانه در رفتار مجرمانه داشته‌اند.

از این منظر، برای حقوق ایران، ترکیبی از رویکرد آمریکایی در تعیین مسئولیت شخصی و رویکرد اروپایی در تنظیم‌گری می‌تواند الگوی مناسبی باشد.

جدول شماره ۳-۱. تحلیل تطبیقی مسئولیت کیفری جرایم سایبری مبتنی بر بلاکچین در حقوق ایران، اتحادیه اروپا و ایالات متحده

ایالات متحده	اتحادیه اروپا	ایران
قوانین فدرال، ایالتی و مقررات نهادهای نظارتی	مقررات تخصصی (از جمله MiCA) و قوانین ضد پول‌شویی	فاقد قانون اختصاصی؛ اتکا به قانون جرایم رایانه‌ای و قانون مجازات اسلامی
مسئولیت بر مبنای سوءنیت و نقش مؤثر	مسئولیت بر مبنای نقش و میزان کنترل	ابهام در شبکه‌های غیرمتمرکز
امکان مسئولیت در صورت مشارکت آگاهانه	امکان مسئولیت در صورت نقض مقررات	مقررات اختصاصی ندارد
وابسته به قصد مجرمانه و مشارکت	وابسته به میزان نقش در جرم	تابع قواعد عمومی مشارکت و معاونت
نظارت گسترده FinCEN و DOJ	نظارت هماهنگ AML/KYC	اعمال مقررات عمومی مبارزه با پول‌شویی
تعدد مراجع و پراکندگی قوانین	هماهنگی اجرای مقررات	خلأ تقنینی و دشواری انتساب مسئولیت

جدول ۳-۲. مقایسه مبنای مسئولیت کیفری در جرایم بلاکچینی

ایالات متحده	اتحادیه اروپا	ایران	معیار
تقصیر، سوءنیت و کنترل مؤثر	تقصیر، مدیریت ریسک	تقصیر و سوءنیت	مبنای مسئولیت
اشخاص حقیقی، حقوقی و فعالان بازار	اشخاص حقیقی، حقوقی و ارائه‌دهندگان خدمات	اشخاص حقیقی و حقوقی	شخصیت مسئول
بررسی موردی توسط مراجع قضایی	در حال تنظیم‌گری	فاقد مقررات	وضعیت DAO

جدول ۳-۳. مقایسه رویکرد به قراردادهای هوشمند

ایالات متحده	اتحادیه اروپا	ایران	موضوع
پذیرش تدریجی در برخی ایالت‌ها	در حال قانون‌گذاری	مقررات اختصاصی ندارد	شناسایی قانونی
مسئولیت براساس نقش طرفین	مسئولیت مبتنی بر ریسک	قواعد عمومی قراردادهای	مسئولیت ناشی از اجرا
قابل تعقیب در صورت وقوع جرم	قابل بررسی در قوانین مالی	نامشخص	جایگاه کیفری

جدول ۳-۴. مقایسه مسئولیت صرافی‌های رمزارزی

ایالات متحده	اتحادیه اروپا	ایران	شاخص
الزامی	الزامی	ناقص	نظام مجوزدهی
الزامی	الزامی	محدود	احراز هویت (KYC)
الزامی	الزامی	محدود	گزارش معاملات مشکوک
مقررات اختصاصی	مقررات اختصاصی	قواعد عمومی	ضمانت اجرای کیفری

جدول ۳-۵. مقایسه مبارزه با پول‌شویی در بلاکچین

ایالات متحده	اتحادیه اروپا	ایران	موضوع
توسعه یافته	توسعه یافته	وجود دارد	قوانین AML
گسترده	گسترده	محدود	پوشش رمزارزها
مستمر	مستمر	محدود	نظارت بر تراکنش‌ها

جدول ۳-۶. مقایسه سیاست جنایی

ایالات متحده	اتحادیه اروپا	ایران	معیار
ترکیبی	پیشگیرانه	واکنشی	رویکرد غالب
منعطف	تخصصی	سنتی	قانون‌گذاری
بالا	بالا	پایین	سرعت انطباق با فناوری

جدول ۳-۷. مقایسه چالش‌های حقوقی

ایالات متحده	اتحادیه اروپا	ایران	چالش
متوسط	متوسط	زیاد	انتساب مسئولیت
نسبتاً آسان	نسبتاً آسان	دشوار	شناسایی مرتکب
متوسط	کم	زیاد	خلأ قانونی

جدول ۳-۸. مقایسه نقاط قوت نظام‌های حقوقی

مهم‌ترین نقطه قوت	نظام حقوقی
وجود قواعد عمومی کیفری قابل اعمال	ایران
مقررات تخصصی و هماهنگ	اتحادیه اروپا
رویه قضایی پویا و نظارت مؤثر	ایالات متحده

جدول ۳-۹. مقایسه نقاط ضعف

مهم‌ترین نقطه ضعف	نظام حقوقی
نبود قانون اختصاصی بلاکچین	ایران
تفاوت در اجرای مقررات میان کشورهای عضو	اتحادیه اروپا
تعدد نهادهای نظارتی و پراکندگی مقررات	ایالات متحده

۴ :

چالش‌های آینده و ارائه الگوی پیشنهادی برای نظام مسئولیت کیفری جرایم مبتنی بر بلاکچین در ایران

۴-۱.

تحولات فناوری بلاکچین نشان داده است که حقوق کیفری نمی‌تواند صرفاً با تکیه بر مفاهیم سنتی، پاسخگوی تمام اشکال جدید رفتارهای مجرمانه باشد. ویژگی‌هایی مانند غیرمتمرکز بودن، اجرای خودکار قراردادهای هوشمند، فعالیت فرامرزی و نقش پررنگ الگوریتم‌ها، ساختار کلاسیک مسئولیت کیفری را با پرسش‌های جدیدی مواجه کرده است.

با وجود این، پذیرش تحول فناورانه به معنای کنار گذاشتن اصول بنیادین حقوق کیفری نیست. اصولی مانند قانونی بودن جرم و مجازات، شخصی بودن مسئولیت کیفری، اصل تقصیر و ضرورت احراز رابطه سببیت همچنان باید محور نظام کیفری باقی بمانند. بنابراین، چالش اصلی آن است که چگونه می‌توان میان دو هدف ظاهراً متعارض تعادل ایجاد کرد: نخست؛ حمایت از جامعه در برابر جرایم نوظهور دیجیتال؛

دوم؛ جلوگیری از توسعه بی‌ضابطه مسئولیت کیفری و ایجاد ناامنی حقوقی برای فعالان فناوری.

۴-۲. مهم‌ترین چالش‌های آینده حقوق کیفری در حوزه بلاکچین

۴-۲-۱. چالش ناشناس بودن و شناسایی مرتکب

یکی از مهم‌ترین مشکلات جرایم مبتنی بر بلاکچین، دشواری ارتباط میان هویت دیجیتال و هویت واقعی افراد است. اگرچه تمامی تراکنش‌های بسیاری از شبکه‌های بلاکچینی ثبت می‌شوند، اما این ثبت لزوماً به معنای شناسایی شخص حقیقی پشت تراکنش نیست.

این وضعیت باعث می‌شود مرحله نخست دادرسی کیفری، یعنی کشف جرم و شناسایی مظنون، با مشکلات جدی مواجه شود. در حقوق کیفری سنتی، پلیس و دادگاه معمولاً با یک شخص مشخص مواجه هستند؛ اما در محیط بلاکچین ممکن است تنها با یک نشانی دیجیتال یا مجموعه‌ای از داده‌های رمزنگاری شده روبه‌رو باشند.

۴-۲-۲. چالش صلاحیت کیفری فرامرزی

جرایم مبتنی بر بلاکچین معمولاً محدود به یک کشور نیستند.

برای مثال:

- توسعه‌دهنده یک نرم‌افزار ممکن است در یک کشور باشد؛
- سرورهای مورد استفاده در کشور دیگری قرار داشته باشند؛
- قربانیان در چند کشور مختلف باشند؛
- دارایی دیجیتال در کیف پولی ناشناس نگهداری شود.

در چنین شرایطی، تعیین اینکه کدام کشور صلاحیت رسیدگی کیفری دارد، دشوار خواهد بود. این موضوع نشان می‌دهد که مقابله مؤثر با جرایم بلاکچینی نیازمند همکاری بین‌المللی گسترده‌تر است.

۳-۲-۴. چالش مسئولیت قراردادهای هوشمند

قراردادهای هوشمند یکی از مهم‌ترین نوآوری‌های فناوری بلاکچین هستند. این قراردادها بدون دخالت مستقیم انسان و بر اساس کدهای برنامه‌نویسی اجرا می‌شوند. اما اگر یک قرارداد هوشمند به دلیل نقص برنامه‌نویسی یا طراحی موجب خسارت شود، تعیین مسئولیت کیفری پیچیده خواهد بود.

سه دیدگاه اصلی در این زمینه وجود دارد:

دیدگاه نخست: مسئولیت توسعه‌دهنده

بر اساس این دیدگاه، برنامه‌نویس در صورتی مسئول است که:

- نقص را می‌دانسته؛
- امکان اصلاح آن را داشته؛
- عمداً یا از روی بی‌احتیاطی آن را رها کرده باشد.

دیدگاه دوم: مسئولیت استفاده‌کننده

برخی معتقدند شخصی که از قرارداد هوشمند برای ارتکاب جرم استفاده می‌کند، مسئول اصلی است.

دیدگاه سوم: مسئولیت ترکیبی

بر اساس این دیدگاه، باید نقش هر فرد به صورت جداگانه بررسی شود و مسئولیت بر اساس میزان تأثیر واقعی تعیین گردد.

به نظر می‌رسد دیدگاه سوم با اصول حقوق کیفری سازگارتر است.

۳-۴. ارائه الگوی پیشنهادی مسئولیت کیفری بلاکچین در حقوق ایران

بر اساس مطالعه تطبیقی انجام‌شده، می‌توان الگوی پنج‌مرحله‌ای برای تعیین مسئولیت کیفری پیشنهاد کرد:

مرحله اول: شناسایی نقش واقعی شخص در شبکه

نخست باید مشخص شود فرد مورد نظر چه نقشی داشته است:

- توسعه‌دهنده؛
- مالک پروژه؛
- مدیر پلتفرم؛
- کاربر عادی؛

• ارائه‌دهنده خدمات واسطه‌ای.

صرف ارتباط فنی با یک شبکه بلاکچینی نباید موجب مسئولیت کیفری شود.

مرحله دوم: احراز رفتار مجرمانه مشخص

مسئولیت کیفری باید بر پایه رفتار مشخص شکل گیرد.

برای مثال:

• ایجاد یک طرح کلاهبردانه؛

• دستکاری عمدی اطلاعات؛

• سرقت کلیدهای خصوصی؛

• استفاده آگاهانه از دارایی نامشروع.

وجود فناوری بلاکچین به تنهایی نمی‌تواند عنصر مادی جرم محسوب شود.

مرحله سوم: بررسی عنصر روانی

یکی از مهم‌ترین اصول پیشنهادی این پژوهش، ضرورت احراز علم و اراده مرتکب است.

بنابراین:

طراحی یک فناوری که قابلیت سوءاستفاده دارد، به تنهایی جرم نیست.

اما طراحی ابزاری با هدف ارتکاب جرم یا تسهیل آگاهانه جرم، می‌تواند مسئولیت کیفری ایجاد کند.

مرحله چهارم: تعیین حدود مسئولیت واسطه‌ها

صرافی‌ها، ارائه‌دهندگان کیف پول و سایر خدمات دیجیتال باید دارای مسئولیت متناسب باشند.

این مسئولیت می‌تواند شامل:

• تکالیف نظارتی؛

• گزارش‌دهی فعالیت‌های مشکوک؛

• رعایت استانداردهای امنیتی؛ باشد.

البته نباید مسئولیت کیفری مطلق برای آنان ایجاد شود.

مرحله پنجم: همکاری بین‌المللی کیفری

با توجه به ماهیت فرامرزی بلاکچین، ایجاد سازوکارهای همکاری میان کشورها ضروری است.

بدون همکاری بین‌المللی، حتی بهترین قوانین داخلی نیز ممکن است در اجرای عملی با محدودیت مواجه شوند.

۴-۴. نوآوری‌های پژوهش

این پژوهش دارای چند نوآوری اصلی است:

نخست:

ارائه تحلیل مسئولیت کیفری در بلاکچین بر اساس «نقش واقعی افراد» به جای صرف ارتباط فناورانه.

دوم:

تأکید بر تفاوت میان «استفاده مشروع از فناوری» و «استفاده مجرمانه از فناوری».

سوم:

ارائه مدل ترکیبی از تجربه اتحادیه اروپا و ایالات متحده برای اصلاح حقوق ایران.

چهارم:

پیشنهاد حرکت از جرم‌انگاری صرف به سمت «تنظیم‌گری کیفری هوشمند».

نتیجه‌گیری نهایی:

فناوری بلاکچین یکی از مهم‌ترین دستاوردهای عصر دیجیتال است که در کنار فرصت‌های گسترده اقتصادی و اجتماعی،

چالش‌های جدیدی برای حقوق کیفری ایجاد کرده است.

پژوهش حاضر نشان داد که مهم‌ترین مشکل نظام‌های کیفری در مواجهه با جرایم بلاکچینی، فقدان کامل قانون نیست؛ بلکه دشواری انطباق مفاهیم سنتی مسئولیت کیفری با ساختارهای غیرمتمرکز است. مطالعه تطبیقی حقوق ایران، اتحادیه اروپا و ایالات متحده نشان داد که: نظام حقوقی ایران در حال حاضر بیشتر بر استفاده از قوانین موجود تکیه دارد و فاقد مقررات جامع اختصاصی در این زمینه است. اتحادیه اروپا رویکرد تنظیم‌گرانه و پیشگیرانه را دنبال می‌کند. ایالات متحده بیشتر بر مسئولیت اشخاصی تمرکز دارد که نقش فعال و آگاهانه در ارتکاب جرم دارند. بر این اساس، مناسب‌ترین راهبرد برای حقوق ایران، ایجاد یک نظام ترکیبی است که از یک سو نوآوری فناوری را محدود نکند و از سوی دیگر امکان مقابله مؤثر با سوءاستفاده‌های مجرمانه را فراهم سازد. در نهایت می‌توان گفت که آینده حقوق کیفری در حوزه بلاکچین، نه در حذف فناوری، بلکه در ایجاد تعادل میان توسعه فناوری و حمایت از ارزش‌های اساسی حقوق کیفری خواهد بود.

پیشنهادهای پژوهش

۱. تدوین قانون جامع درباره دارایی‌های دیجیتال و جرایم مرتبط با بلاک چین.
۲. اصلاح قانون جرایم رایانه‌ای با توجه به فناوری‌های غیرمتمرکز.
۳. ایجاد شعب تخصصی قضایی برای رسیدگی به جرایم فناوری‌های نوین.
۴. آموزش تخصصی قضات، ضابطان و کارشناسان درباره بلاک چین.
۵. توسعه همکاری‌های بین‌المللی در زمینه کشف و تعقیب جرایم دیجیتال.
۶. تدوین معیارهای روشن برای مسئولیت کیفری توسعه‌دهندگان و ارائه‌دهندگان خدمات بلاکچینی.

فهرست منابع و ماخذ:

منابع فارسی:

- عبدالحسینی، ش. (۱۳۹۲). مسئولیت کیفری اشخاص حقوقی در پرتو قانون مجازات اسلامی مصوبه جدید (پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد تهران مرکزی).
- رمضانیان سیاهکلودی، ع.، دیانی، ع.، و زرکلام، س. (۱۳۹۹). مسئولیت مدنی واسطه‌های ارائه خدمات اینترنت با تأکید بر نقض مالکیت فکری در فضای سایبر. فصلنامه علمی مطالعات حقوق بشر اسلامی، ۹(۱)، ۲۷۷-۲۹۷.

سعیدی، ب. و کمالی، م. (۱۴۰۳). استخراج و ماینینگ ارز دیجیتال از منظر حقوق کیفری ایران. Contemporary Readings in Law and Social Justice.

عبود الجیزانی، ح. ک.، حیدری، م.، حسین علی، ح. و سعیدی، ی. (۱۴۰۳). مسئولیت کیفری ناشی از جرائم ارتكابی به وسیله ربات‌ها. دانشنامه فقه و حقوق تطبیقی.

میرسعیدی، م. (۱۳۷۷). ارکان مسئولیت کیفری در حقوق ایران و اسلام (پایان نامه کارشناسی ارشد، دانشگاه تربیت مدرس).

بای، حسین علی، و پورقهرمانی، بابک. (۱۳۸۸). بررسی فقهی و حقوقی جرایم رایانه‌ای. قم: پژوهشگاه علوم و فرهنگ اسلامی.

بابایی، جواد. (۱۴۰۴). جرایم رایانه‌ای و آیین دادرسی حاکم بر آن (چاپ نهم). تهران: مرکز مطبوعات و انتشارات قوه قضائیه.

جعفری لنگرودی، محمدجعفر. (۱۴۰۰). ترمینولوژی حقوق (چاپ جدید). تهران: گنج دانش.

خالقی، علی. (۱۴۰۲). آیین دادرسی کیفری (جلد اول). تهران: شهر دانش.

زراعت، عباس. (۱۴۰۱). حقوق جزای عمومی (جلد اول). تهران: ققنوس.

صادقی، حسین میرمحمد. (۱۴۰۱). جرایم علیه اموال و مالکیت (چاپ جدید). تهران: میزان.

صادقی، حسین میرمحمد. (۱۴۰۱). حقوق جزای اختصاصی؛ جرایم علیه امنیت و آسایش عمومی. تهران: میزان.

فتحی‌زاده، امیرهوشنگ، و اسماعیلی عطاآبادی، عقیل. (۱۴۰۱). حقوق بلاکچین: ارزش‌های رمزنگار، عرضه‌های اولیه سکه، قراردادهای

هوشمند، سازمان‌های مستقل غیرمتمرکز و حل‌وفصل اختلافات. تهران: چاپ و نشر بازرگانی.

مظلومان، حسین. (۱۴۰۰). جرایم و مجازات‌های بیت‌کوین و بلاک چین در حقوق ایران. تهران: مهر کلام.

محمدی، ابراهیم. (۱۳۹۹). حقوق فناوری اطلاعات و ارتباطات. تهران: میزان.

میرمحمدصادقی، حسین. (۱۴۰۰). حقوق کیفری اختصاصی. تهران: میزان.

موسی‌زاده، رضا. (۱۴۰۱). حقوق سازمان‌های بین‌المللی. تهران: میزان.

نجفی ابرنآبادی، علی حسین. (۱۳۹۹). بایسته‌های حقوق جزای عمومی. تهران: میزان.

ضیایی بیگدلی، محمدرضا. (۱۴۰۲). حقوق بین‌الملل عمومی. تهران: گنج دانش.

کاتوزیان، ناصر. (۱۳۹۸). مقدمه علم حقوق و مطالعه در نظام حقوقی ایران. تهران: شرکت سهامی انتشار.

قوانین و اسناد حقوقی ایران :

قانون جرایم رایانه‌ای، مصوب ۱۳۸۸، روزنامه رسمی جمهوری اسلامی ایران.

قانون مجازات اسلامی، مصوب ۱۳۹۲، با اصلاحات و الحاقات بعدی.

قانون آیین دادرسی کیفری، مصوب ۱۳۹۲، با اصلاحات بعدی.

قانون مبارزه با پول‌شویی، مصوب ۱۳۸۶، با اصلاحات سال ۱۳۹۷.

قانون تجارت الکترونیکی، مصوب ۱۳۸۲.

قانون مسئولیت مدنی، مصوب ۱۳۳۹.

دستورالعمل‌ها و بخشنامه‌های بانک مرکزی جمهوری اسلامی ایران درباره دارایی‌های رمزنگاری شده

مقالات :

• مقاله «چالش‌های حقوقی ارزش‌های رمزنگاری شده در نظام حقوقی ایران»، فصلنامه تحقیقات حقوقی.

• مقاله «مسئولیت کیفری ناشی از فناوری بلاکچین»، فصلنامه مطالعات حقوق کیفری و جرم‌شناسی.

- مقاله «ابعاد حقوقی قراردادهای هوشمند»، فصلنامه پژوهش‌های حقوق خصوصی.
- مقاله «تحلیل حقوقی جرایم مرتبط با رمزارزها»، مجله تحقیقات حقوقی دانشگاه تهران.
- مقاله «پول‌شویی و ارزهای دیجیتال؛ چالش‌های حقوق کیفری»، فصلنامه حقوق تطبیقی.

• منابع انگلیسی :

- Antonopoulos, A. M. (۲۰۱۷). Mastering Bitcoin: Programming the open blockchain (۲nd ed.). O'Reilly Media.
- De Filippi, P., & Wright, A. (۲۰۱۸). Blockchain and the law: The rule of code. Harvard University Press.
- Hacker, P., & Thomale, C. (۲۰۱۸). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review*, ۱۵(۴), ۶۴۵-۶۹۶.
- Lessig, L. (۲۰۰۶). Code: Version ۲.۰. Basic Books.
- Möser, M., Böhme, R., & Breuker, D. (۲۰۱۳). An inquiry into money laundering tools in the Bitcoin ecosystem.
- Brenner, S. W. (۲۰۱۰). Cybercrime: Criminal Threats from Cyberspace. Praeger.
- Europol. (۲۰۲۳). Internet Organised Crime Threat Assessment (IOCTA) ۲۰۲۳.
- Financial Action Task Force (FATF). (۲۰۲۱). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
- Lessig, L. (۲۰۰۶). Code: Version ۲.۰. Basic Books.
- Nakamoto, S. (۲۰۰۸). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Swan, M. (۲۰۱۵). Blockchain: Blueprint for a New Economy. O'Reilly Media.
- United Nations Office on Drugs and Crime (UNODC). (۲۰۲۴). Global Report on Cybercrime.
- Wall, D. S. (۲۰۰۷). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
- Werbach, K. (۲۰۱۸). The Blockchain and the New Architecture of Trust. MIT Press.

Comparative Analysis of Criminal Liability in Cybercrimes Based on Blockchain Technology

Omid Ghahremani (Corresponding Author)

M.A. Student in Criminal Law, Islamic Azad University, Sanandaj Branch, Sanandaj, Iran

Seyed Keyhan Asadi

Graduate of International Law, Tehran Center for Graduate Studies, Tehran, Iran

Abstract:

The emergence of blockchain technology and its rapid expansion in areas such as cryptocurrencies, smart contracts, decentralized finance, and digital asset management have created significant challenges for traditional criminal law systems. Although blockchain technology provides substantial opportunities for economic and technological development, its specific characteristics, including decentralization, relative anonymity, borderless transactions, and automated execution through smart contracts, have created new forms of cybercrime and complicated the determination of criminal liability.

This article aims to comparatively analyze criminal liability arising from blockchain-based cybercrimes in the legal systems of Iran, the European Union, and the United States. Using a descriptive-analytical and comparative methodology, the study examines the compatibility of traditional criminal law concepts, including *actus reus*, *mens rea*, causation, participation, and criminal attribution, with decentralized digital environments.

The findings indicate that the main challenge in blockchain-related criminal liability is not merely the absence of criminal regulations, but rather the difficulty of applying traditional concepts of liability to decentralized structures. The comparative analysis demonstrates that the European Union has adopted a regulatory and preventive approach, while the United States generally relies on existing criminal laws combined with enforcement mechanisms. In contrast, Iranian criminal law currently lacks a comprehensive framework specifically addressing blockchain-related crimes and mainly relies on general cybercrime and criminal provisions.

The article argues that Iran requires a balanced criminal policy based on technological neutrality, protection of innovation, and effective prevention of criminal misuse of blockchain systems. Therefore, adopting a specialized regulatory framework, clarifying the liability of developers and service providers, and strengthening international cooperation are essential steps toward an efficient criminal justice response.

Keywords:

Blockchain Technology; Cybercrime; Criminal Liability; Cryptocurrency; Comparative Criminal Law; Smart Contracts; Digital Assets.