استفاده از فناوری بلاک‌چین در راستای پیشگیری، کنترل جرایم پولی و بانکی؛ مطالعه موردی جرایم پول‌شویی، اختلاس و کلاهبرداری اینترنتی

دکتر محمدرضا یزدانیان، عضو هیئت‌علمی دانشگاه، معاون قضایی و حقوقی سازمان قضایی نیروهای مسلح
مهدی خلیلی، دانشجوی کارشناسی ارشد حقوق جزا و جرم‌شناسی

چکیده

فناوری بلاک‌چین به‌عنوان یکی از نوآوری‌های انقلابی در حوزه فناوری اطلاعات و اقتصاد دیجیتال، پتانسیل بالایی برای ایجاد تحول در ساختارهای مالی و قضایی کشورها دارد. این فناوری، با تکیه بر ویژگی‌هایی همچون شفافیت، عدم تمرکز، تغییرناپذیری اطلاعات و قابلیت رهگیری دقیق تراکنش‌ها، ظرفیت مناسبی برای شناسایی، کنترل و پیشگیری از انواع جرایم مالی از جمله اختلاس، پول‌شویی، جعل اسناد و کلاهبرداری بانکی فراهم می‌کند. این پژوهش با روش تحلیلی-توصیفی و با بهره‌گیری از منابع معتبر بین‌المللی، به بررسی جایگاه بلاک‌چین در تقویت سازوکارهای مقابله با جرایم مالی پرداخته است. یافته‌ها نشان می‌دهد که این فناوری می‌تواند نه‌تنها فرآیندهای نظارتی بانک‌ها و نهادهای مالی را بهبود بخشد، بلکه به‌طور خاص ابزار مؤثری در اختیار پلیس اقتصادی و پلیس فضای تولید و تبادل اطلاعات (فتا) قرار دهد تا فرآیند کشف، مستندسازی و پیگیری جرایم مالی با سرعت و دقت بیشتری انجام شود. یکی از مزیت‌های مهم بلاک‌چین، فراهم کردن امکان اجرای خودکار تعهدات مالی از طریق قراردادهای هوشمند است. این قراردادها که به‌صورت برنامه‌ریزی‌شده و بدون دخالت انسانی عمل می‌کنند، می‌توانند بخش زیادی از تخلفات ناشی از اجرای ناقص یا مغرضانه تعهدات مالی را حذف کنند. همچنین، به دلیل ثبت غیرقابل تغییر اطلاعات در دفاتر کل توزیع‌شده، امکان جعل، حذف یا دستکاری داده‌ها تقریباً از بین می‌رود. از منظر نهادهای انتظامی و قضایی، بلاک‌چین ابزار نوینی برای ارتقای شفافیت اطلاعات، رصد لحظه‌ای تراکنش‌ها و ایجاد بستری ایمن برای تعاملات مالی به شمار می‌رود. این فناوری می‌تواند نقش پلیس را از حالت صرفاً واکنشی به نقشی فعال و پیشگیرانه ارتقا دهد و مسیر را برای تشکیل پرونده‌های دقیق و قابل استناد در مقابله با فساد مالی هموار کند. با وجود این مزایا، اجرای گسترده بلاک‌چین در نظام بانکی و قضایی ایران با چالش‌هایی نظیر نبود زیرساخت قانونی، هزینه‌های پیاده‌سازی و مقاومت سازمانی در برابر تغییر روبه‌روست. با این حال، تقویت همکاری میان نهادهای قانون‌گذار، نهادهای اجرایی و پلیس، می‌تواند زمینه‌ساز گسترش استفاده از بلاک‌چین و تحقق اهداف بلندمدت در راستای افزایش امنیت مالی، ارتقای اعتماد عمومی و کاهش پایدار جرایم مالی شود.

واژگان کلیدی: بلاک‌چین، زنجیره‌های بلوکی، جرایم پولی و بانکی، حقوق بانکی

درآمد

در سال‌های اخیر، فناوری بلاک‌چین به‌عنوان یکی از نوآوری‌های بنیادین در حوزه اقتصاد دیجیتال و فناوری اطلاعات، جایگاه ویژه‌ای در نظام‌های مالی و نظارتی جهان پیدا کرده است. این فناوری که مبتنی بر ثبت غیرمتمرکز، تغییرناپذیر و شفاف داده‌هاست، امکان ذخیره‌سازی تراکنش‌های مالی به شکلی امن، قابل رهگیری و عاری از دستکاری را فراهم می‌آورد. در جهانی که پیچیدگی‌های اقتصادی، گسترش فناوری‌های نوین مالی و ظهور ابزارهای دیجیتالی جدید بستری مناسب برای رشد جرایم پولی و بانکی فراهم کرده‌اند، بهره‌گیری از ظرفیت‌های فناورانه برای مقابله با این جرایم، ضرورتی اجتناب‌ناپذیر به نظر می‌رسد. در این میان، پلیس به‌عنوان نهاد مسئول در پیشگیری و کشف جرم، می‌تواند با استفاده از فناوری بلاک‌چین، گام‌های مؤثرتری در جهت مقابله با فساد مالی، پول‌شویی، اختلاس، کلاهبرداری و سایر جرایم بانکی بردارد.

نقش پلیس در ساختار امنیت اقتصادی کشور، تنها محدود به واکنش پس از وقوع جرم نیست، بلکه در دنیای امروز نیازمند بازتعریف در قالب نقش پیشگیرانه، فناورمحور و تحلیل‌محور است. با استفاده از فناوری بلاک‌چین، پلیس می‌تواند به اطلاعات دقیق و غیرقابل دستکاری در مورد تراکنش‌های مالی دسترسی داشته باشد، اطلاعاتی که به‌صورت دائمی در دفترکل‌های دیجیتال ذخیره می‌شوند و به‌واسطه ساختار شبکه‌ای این فناوری، امکان تغییر یا پنهان‌سازی آنها وجود ندارد. این قابلیت باعث می‌شود مسیر حرکت وجوه مشکوک یا منابع مالی غیرقانونی از مبدأ تا مقصد قابل رهگیری بوده و زمینه سوءاستفاده مجرمان از خلأهای نظارتی تا حد زیادی از میان برداشته شود. در بسیاری از کشورها، بهره‌گیری از این ابزار فناورانه به پلیس کمک کرده است تا فرآیندهای کشف جرم را نه‌تنها سریع‌تر و دقیق‌تر، بلکه با پشتوانه‌ای مستند و مورد قبول دستگاه قضایی پیش ببرد.

ویژگی‌هایی مانند تمرکززدایی، شفافیت و تغییرناپذیری بلاک‌چین، بستر مناسبی برای استقرار نظارت‌های مالی پیشرفته ایجاد می‌کنند که پلیس می‌تواند با اتکا به آنها به‌جای صرفاً پیگیری پس از جرم، در فرآیندهای پیشگیری، تحلیل ریسک و کنترل هوشمند ورود کند. برای مثال، شناسایی تراکنش‌های مشکوک در مراحل اولیه، پیش از آنکه به شکل یک تخلف بزرگ یا شبکه‌ای درآیند، می‌تواند به‌واسطه تحلیل داده‌های بلاک‌چینی انجام شود. این تحلیل‌ها، با بهره‌گیری از الگوریتم‌های یادگیری ماشین و هوش مصنوعی، قابلیت تشخیص الگوهای تکرارشونده یا غیرعادی را دارند که در شرایط سنتی به‌سادگی قابل ردیابی نبودند. به این ترتیب، پلیس می‌تواند با تکیه بر اطلاعات ثبت‌شده در بستر بلاک‌چین، به تحلیل رفتارهای مالی پرداخته و هشدارهای به‌موقع برای جلوگیری از وقوع جرم صادر کند.

از سوی دیگر، ابزارهایی مانند قراردادهای هوشمند، یکی دیگر از مزایای قابل توجه بلاک‌چین برای نهادهای انتظامی محسوب می‌شوند. این قراردادها مجموعه‌ای از دستورات برنامه‌ریزی‌شده هستند که در صورت تحقق شرایط مشخص، به‌صورت خودکار اجرا می‌شوند. در حوزه مقابله با جرایم مالی، پلیس می‌تواند از این ابزار برای اطمینان از اجرای دقیق مقررات بانکی و مالی استفاده کند. برای نمونه، در صورتی که فعالیت یک حساب بانکی از

الگوهای مجاز تخطی کند، قرارداد هوشمند می‌تواند به‌طور خودکار اقدامات کنترلی مانند مسدودسازی حساب، ارسال هشدار به پلیس یا اطلاع‌رسانی به نهادهای نظارتی را فعال کند. این ویژگی باعث افزایش کارآمدی در اجرای قوانین و کاهش بار اداری و بروکراتیک بر سیستم‌های امنیتی می‌شود.

با وجود این ظرفیت‌ها، بهره‌گیری عملی و فراگیر پلیس از فناوری بلاک‌چین نیازمند زیرساخت‌های فنی، حقوقی و آموزشی گسترده‌ای است. تربیت نیروی انسانی متخصص در حوزه تحلیل داده‌های بلاک‌چین، توسعه بسترهای بومی برای ثبت و نظارت بر تراکنش‌های مالی، ایجاد هماهنگی‌های بین‌نهادی میان پلیس، بانک مرکزی و دیگر نهادهای قضایی و اقتصادی و همچنین تدوین قوانین و دستورالعمل‌های دقیق در خصوص حریم خصوصی، مالکیت داده‌ها و تبادل اطلاعات، از جمله اقداماتی است که باید به‌طور جدی مدنظر قرار گیرد. تنها در چنین بستری است که پلیس می‌تواند از بلاک‌چین نه‌تنها به‌عنوان یک فناوری، بلکه به‌عنوان یک رویکرد تحول‌آفرین در ساختار نظارتی خود بهره‌برداری کند.

در نهایت، باید اذعان داشت که استفاده از فناوری بلاک‌چین می‌تواند ساختار نظارتی و امنیتی کشور را در حوزه اقتصادی دگرگون سازد و پلیس را از یک نهاد واکنش‌محور به نهادی تحلیل‌گر، پیشگیرانه و فناورانه ارتقاء دهد. این تحول، نه‌تنها زمینه‌ساز کاهش جرایم پولی و بانکی خواهد بود، بلکه با ایجاد شفافیت ساختاری در نظام مالی، اعتماد عمومی به سیستم‌های بانکی و قضایی را نیز افزایش خواهد داد. امید است با نگاه هوشمندانه سیاست‌گذاران به ظرفیت‌های بلاک‌چین و فراهم‌سازی زیرساخت‌های لازم برای بهره‌برداری پلیس از این فناوری، شاهد بهبود چشمگیر در امنیت اقتصادی و کاهش معنادار تخلفات مالی در کشور باشیم.

۱-تعریف بلاک چین و بیان ویژگی‌های آن

بلاک‌چین یکی از فناوری‌های نوینی است که در سال‌های اخیر تأثیر عمیقی بر حوزه‌های مالی، بانکی و امنیتی گذاشته است. این فناوری که در ابتدا به‌عنوان زیرساخت بیت‌کوین معرفی شد، اکنون به عنوان یک سیستم ثبت اطلاعات غیرمتمرکز در بسیاری از زمینه‌ها، از جمله مبارزه با جرایم مالی و بانکی، مورد استفاده قرار می‌گیرد (Werbach, ۲۰۱۸: ۴۵). بلاک‌چین یک دفتر کل توزیع‌شده است که تمامی تراکنش‌ها را به صورت شفاف، تغییرناپذیر و رمزنگاری‌شده ذخیره می‌کند. در این فناوری، اطلاعات در بلوک‌هایی قرار می‌گیرند که به‌طور زنجیره‌ای به یکدیگر متصل شده‌اند. این ساختار موجب می‌شود که تغییر یا حذف اطلاعات ثبت‌شده تقریباً غیرممکن باشد، زیرا هر بلوک حاوی هش رمزنگاری‌شده‌ای است که به بلوک قبلی متصل است (Tapscott & Tapscott, ۲۰۱۶: ۷۸). این ویژگی نه‌تنها باعث افزایش امنیت داده‌ها می‌شود، بلکه امکان پیگیری و شفافیت در تراکنش‌ها را نیز فراهم می‌کند.

یکی از مهم‌ترین ویژگی‌های بلاک‌چین، شفافیت آن است. برخلاف سیستم‌های سنتی بانکی که اطلاعات تراکنش‌ها در اختیار نهادهای محدودی قرار دارد، بلاک‌چین امکان مشاهده تمامی تراکنش‌ها را برای عموم فراهم می‌کند. این شفافیت موجب کاهش امکان تقلب، پول‌شویی و سایر جرایم مالی می‌شود، زیرا هر تراکنش به‌صورت دائمی در شبکه ثبت و قابل رهگیری است (Mougayar, ۲۰۱۶: ۱۱۲). علاوه بر این، غیرمتمرکز بودن بلاک‌چین از کنترل و دستکاری داده‌ها توسط یک نهاد یا فرد خاص جلوگیری می‌کند و این امر اعتماد عمومی را نسبت به صحت اطلاعات مالی افزایش می‌دهد.

ویژگی دیگر بلاک‌چین، امنیت بالای آن است. تراکنش‌های ثبت‌شده در بلاک‌چین از طریق الگوریتم‌های رمزنگاری پیشرفته محافظت می‌شوند. این امر موجب می‌شود که هکرها و مجرمان سایبری نتوانند به‌راحتی به داده‌های کاربران دسترسی پیدا کنند یا آنها را تغییر دهند. در واقع، برای تغییر یک تراکنش، لازم است که تمامی بلوک‌های بعدی آن نیز تغییر یابند که این امر در عمل بسیار دشوار و تقریباً غیرممکن است (Antonopoulos, ۲۰۱۷: ۱۵۶).این ویژگی بلاک‌چین را به ابزاری مؤثر برای پیشگیری از حملات سایبری و تقلب‌های بانکی تبدیل کرده است. علاوه بر این، استفاده از قراردادهای هوشمند در بلاک‌چین، روند اجرای توافقات مالی را بهبود می‌بخشد. قراردادهای هوشمند، کدهای برنامه‌نویسی خوداجرایی هستند که بدون نیاز به واسطه‌ها، تعهدات قراردادی را اجرا می‌کنند. این قابلیت باعث کاهش هزینه‌های اجرایی، افزایش سرعت تراکنش‌ها و حذف ریسک‌های مربوط به عدم رعایت تعهدات می‌شود (Werbach, ۲۰۱۸: ۹۵). در نتیجه، بسیاری از سازمان‌ها و مؤسسات مالی به دنبال بهره‌گیری از بلاک‌چین برای ایجاد سیستم‌های مالی شفاف‌تر و کارآمدتر هستند.

از جنبه کاربردی، بلاک‌چین در مبارزه با جرایم پولی و بانکی نقش مهمی ایفا می‌کند. به عنوان مثال، در مبارزه با پول‌شویی، بلاک‌چین می‌تواند تمامی تراکنش‌های مشکوک را به‌صورت خودکار شناسایی و ثبت کند. از آنجایی که هر تراکنش یک ردپای دیجیتالی ایجاد می‌کند، امکان ردیابی جریان‌های مالی غیرقانونی تسهیل می‌شود (Tapscott & Tapscott, ۲۰۱۶: ۱۳۴).این ویژگی موجب می‌شود که مجرمان نتوانند سرمایه‌های غیرقانونی را از طریق روش‌های سنتی به حساب‌های رسمی منتقل کنند.

۲- ویژگی‌های بلاک‌چین و ارتباط آن با پیشگیری و سرکوب جرایم پولی و بانکی

فناوری بلاک‌چین به‌عنوان ابزاری نوین و پیشرفته در ذخیره‌سازی و انتقال ایمن اطلاعات، فرصت‌های بی‌سابقه‌ای را در اختیار نیروهای پلیس و نهادهای امنیتی قرار داده تا با بهره‌گیری از ویژگی‌هایی همچون شفافیت، امنیت، تغییرناپذیری و غیرمتمرکز بودن، به‌طور مؤثرتری به شناسایی و پیشگیری از جرایم فضای مجازی بپردازند. این فناوری با فراهم‌سازی زیرساختی شفاف و قابل ردیابی، به پلیس این امکان را می‌دهد تا رد فعالیت‌های مشکوک مالی را در محیط‌های دیجیتال به‌راحتی دنبال کند و با سرعت بیشتری واکنش نشان دهد (Casey & Vigna, ۲۰۱۸: ۱۱۲).

یکی از شاخص‌ترین ظرفیت‌های بلاک‌چین برای پلیس، شفافیت بالا در ثبت تراکنش‌ها است. برخلاف سیستم‌های سنتی که اطلاعات مالی تنها در اختیار نهادهای محدودی قرار دارد، بلاک‌چین یک دفتر کل توزیع‌شده است که همه تراکنش‌ها را به‌صورت عمومی ثبت می‌کند. این شفافیت موجب می‌شود نیروهای پلیس بتوانند به داده‌های دقیق و بدون واسطه دسترسی پیدا کنند و با تحلیل آنها، شبکه‌های پول‌شویی، کلاهبرداری دیجیتال و سایر جرایم سازمان‌یافته سایبری را شناسایی کنند (Zohar, ۲۰۱۵: ۸۷).

تغییرناپذیری داده‌ها در بلاک‌چین نیز نقش تعیین‌کننده‌ای در جمع‌آوری و ارائه شواهد معتبر برای پرونده‌های کیفری ایفا می‌کند. هنگامی‌که اطلاعات یک تراکنش وارد زنجیره بلوک‌ها شود، دستکاری آن بدون جلب مشارکت گسترده کل شبکه عملاً ناممکن است. این ویژگی، پلیس را قادر می‌سازد تا به مدارک دیجیتالی با قابلیت استناد بالا دست یابد، بدون آنکه نگران جعل یا حذف آنها توسط مجرمان باشد (Chuen, ۲۰۱۵: ۱۵۳). از سوی دیگر، امنیت رمزنگاری‌شده بلاک‌چین، سطح حفاظت اطلاعات را تا حد زیادی افزایش می‌دهد. این ویژگی باعث می‌شود پلیس بتواند در بستر امن‌تری به بررسی داده‌ها بپردازد و در عین حال از نفوذ و نشت اطلاعات محرمانه جلوگیری کند؛ همچنین از آنجایی‌که داده‌ها در بلاک‌چین به‌صورت غیرمتمرکز نگهداری می‌شوند، امکان نفوذ موفق به کل سامانه به‌شدت کاهش می‌یابد (Goodell & Aste, ۲۰۲۰: ۱۸۴).

در بعد غیرمتمرکز بودن شبکه بلاک‌چین، پلیس می‌تواند با استفاده از داده‌هایی که از منابع مختلف و بدون وابستگی به یک مرکز واحد جمع‌آوری می‌شود، تحلیل دقیق‌تر و سریع‌تری از الگوهای مجرمانه به دست آورد. این امر، به‌ویژه در پرونده‌های پیچیده‌ای مانند جرایم سازمان‌یافته یا حملات فیشینگ بین‌المللی، می‌تواند بسیار مؤثر باشد (Casey & Vigna, ۲۰۱۸: ۲۱۱).

همچنین، قراردادهای هوشمند، ابزارهای خودکار و شفاف هستند که در صورت تحقق شروط از پیش تعیین‌شده، اجرا می‌شوند. پلیس می‌تواند از این ابزارها برای طراحی سیستم‌هایی بهره ببرد که از قبل، احتمال وقوع برخی تخلفات مانند کلاهبرداری مالی یا دستکاری در معاملات دیجیتال را به صفر می‌رسانند. این قراردادها در فرایند احراز هویت دیجیتال نیز مفید واقع شده و مسیر شناسایی مجرمان سایبری را هموارتر می‌سازد (Chuen, ۲۰۱۵: ۱۹۶). در نهایت، بلاک‌چین با تسهیل و تسریع دسترسی به داده‌های دقیق تراکنش‌ها، امکان تحلیل کلان‌داده و کشف الگوهای مجرمانه را برای نهادهای نظارتی و پلیسی فراهم می‌سازد. این توانایی در کاهش هزینه‌ها، بهبود سرعت عملکرد و اثربخشی مداخلات پلیسی نقش چشم‌گیری دارد و مسیر را برای یک همکاری نزدیک‌تر میان نهادهای انتظامی و فناوری‌های نوین هموار می‌کند.(Goodell & Aste, ۲۰۲۰: ۲۷۵)

۳- جرایم پولی و بانکی و دشواری‌های تعقیب کیفری آن

جرایم پولی و بانکی شامل مجموعه‌ای از تخلفات مالی است که با هدف کسب سود غیرقانونی، تقلب، پول‌شویی و سوءاستفاده از سیستم‌های مالی انجام می‌شوند. این جرایم می‌توانند شامل کلاهبرداری بانکی، سرقت هویت، جعل اسناد مالی، اختلاس، فرار مالیاتی و تأمین مالی فعالیت‌های غیرقانونی باشند. با گسترش فناوری‌های مالی و دیجیتالی، روش‌های ارتکاب این جرایم نیز پیچیده‌تر شده‌اند و مقابله با آنها نیازمند رویکردهای نظارتی و فناورانه پیشرفته‌تری است (Catalini & Gans, ۲۰۱۷: ۴۵).

یکی از مهم‌ترین چالش‌ها در پیشگیری و سرکوب جرایم پولی و بانکی، پیچیدگی روزافزون روش‌های مورد استفاده توسط مجرمان است. مجرمان مالی از تکنیک‌های پیشرفته‌ای مانند پول‌شویی چندلایه‌ای، استفاده از شرکت‌های صوری و بهره‌گیری از ارزهای دیجیتال برای پنهان کردن ردپای مالی خود استفاده می‌کنند. به دلیل افزایش حجم تراکنش‌های مالی جهانی و گسترش بازارهای غیرمتمرکز، شناسایی و پیگیری این جرایم برای نهادهای نظارتی دشوارتر شده است (Yeoh, ۲۰۱۷: ۲۰۲).

نظارت بر سیستم‌های مالی نیازمند همکاری میان نهادهای دولتی، بانک‌ها و سازمان‌های بین‌المللی است؛ اما یکی از موانع اصلی در این زمینه، تفاوت‌های قانونی و نظارتی میان کشورهاست. برخی از کشورها قوانین سختگیرانه‌ای برای مقابله با جرایم بانکی دارند، در حالی که برخی دیگر به دلیل ضعف سیستم‌های نظارتی، به پناهگاهی برای مجرمان مالی تبدیل شده‌اند. این تفاوت‌های قانونی موجب می‌شود که مجرمان بتوانند با انتقال سرمایه‌های خود به حوزه‌های قضایی با نظارت ضعیف‌تر، از مجازات فرار کنند (Peters & Panayi, ۲۰۱۶: ۵۸۰). از دیگر دشواری‌های پیشگیری از جرایم مالی، تأثیرگذاری محدود روش‌های سنتی در کشف و مهار این جرایم است. بسیاری از بانک‌ها و مؤسسات مالی هنوز از سیستم‌های نظارتی قدیمی استفاده می‌کنند که توانایی تحلیل و تشخیص سریع تراکنش‌های غیرقانونی را ندارند. پیشرفت‌های هوش مصنوعی و داده‌کاوی می‌توانند به بهبود این فرآیند کمک کنند، اما توسعه و پیاده‌سازی این فناوری‌ها به زمان و سرمایه‌گذاری قابل توجهی نیاز دارد (Gandal et al. ۲۰۱۸: ۹۲).

جرایم پولی و بانکی علاوه بر خسارات مالی، پیامدهای اجتماعی و اقتصادی گسترده‌ای نیز دارند. این جرایم می‌توانند موجب کاهش اعتماد عمومی به نظام بانکی، افزایش هزینه‌های نظارتی و کاهش سرمایه‌گذاری‌های اقتصادی شوند. همچنین، تأمین مالی فعالیت‌های غیرقانونی مانند قاچاق مواد مخدر و تأمین مالی تروریسم از طریق پول‌شویی، تهدیدی جدی برای امنیت جهانی محسوب می‌شود. به همین دلیل، کشورهای مختلف به دنبال تقویت همکاری‌های بین‌المللی و تدوین قوانین سختگیرانه‌تر برای مقابله با این تهدیدات هستند (Yeoh, ۲۰۱۷: ۲۰۹). با توجه به پیچیدگی و پویایی جرایم پولی و بانکی، استفاده از فناوری‌های نوین مانند بلاک‌چین برای کنترل و پیشگیری از این جرایم ضروری به نظر می‌رسد. این فناوری با ویژگی‌هایی مانند شفافیت، غیرمتمرکز بودن، تغییرناپذیری داده‌ها و امنیت بالا، امکان نظارت دقیق‌تر و جلوگیری از تخلفات مالی را فراهم می‌کند. با وجود

چالش‌های قانونی و فنی، بلاک‌چین می‌تواند به‌عنوان ابزاری کارآمد برای بهبود نظارت مالی و کاهش تخلفات در سیستم بانکی مورد استفاده قرار گیرد (Catalini & Gans, ۲۰۱۷: ۵۷).

۴- تطبیق استفاده از بلاک چین بر وضعیت تعقیب و سرکوب تعدادی از جرایم پولی و بانکی

در ادامه، به بررسی نقش فناوری بلاک‌چین در تعقیب، پیشگیری و سرکوب برخی از مهم‌ترین جرایم بانکی و پولی می‌پردازیم. این فناوری با ایجاد یک سیستم ثبت غیرقابل تغییر، امکان رهگیری دقیق تراکنش‌ها را فراهم کرده و به کاهش جرایمی مانند پول‌شویی، تأمین مالی تروریسم، تقلب مالی و فرار مالیاتی کمک می‌کند. همچنین، ویژگی شفافیت و غیرمتمرکز بودن بلاک‌چین، نظارت نهادهای مالی و قضایی را تسهیل کرده و مانع از دستکاری و سوءاستفاده از اطلاعات مالی می‌شود.

۴-۱-کلاهبرداری اینترنتی

کلاهبرداری اینترنتی یکی از مهم‌ترین جرایم مالی در دنیای مدرن است که با توسعه فناوری‌های دیجیتال و افزایش استفاده از اینترنت به شکل گسترده‌ای رشد کرده است. در ارتباط با کلاهبرداری اینترنتی توجه به این نکته ضروری است که کلاهبرداری اینترنتی به جرایمی اطلاق می‌شود که ذات آنها مبتنی بر بهره‌گیری از بستر شبکه جهانی اینترنت و فناوری‌های مرتبط با آن برای فریب اشخاص و تحصیل مال غیر به صورت غیرقانونی است؛ به بیان دیگر، اینترنت در این نوع جرم، ابزار اصلی ارتکاب بزه محسوب می‌شود. در مقابل، کلاهبرداری در بستر اینترنت ناظر بر هر نوع رفتار متقلبانه‌ای است که شروع فرآیند آن در فضای مجازی صورت می‌پذیرد، اما الزامی به استفاده مستمر از اینترنت در تمامی مراحل وقوع جرم وجود ندارد؛ به عبارت دیگر، بستر اولیه ارتکاب این نوع کلاهبرداری فضای آنلاین است، اما عملیات مجرمانه می‌تواند در محیط فیزیکی نیز تکمیل گردد. کلاهبرداری اینترنتی بر اساس ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به معنای تحصیل مال یا منفعت از طریق اعمال متقلبانه‌ای نظیر وارد کردن، تغییر، محو یا متوقف کردن داده‌ها در سامانه‌های رایانه‌ای یا مخابراتی تعریف شده و برای آن مجازات حبس و جزای نقدی مقرر گردیده است. در مقابل، کلاهبرداری در بستر اینترنت مشمول ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ می‌باشد که ناظر بر هر نوع عملیات متقلبانه‌ای است که به قصد فریب اشخاص و تحصیل مال غیر انجام می‌گیرد، حتی اگر شروع آن در فضای مجازی باشد؛ لذا در این نوع کلاهبرداری، اینترنت صرفاً به‌عنوان ابزار مقدماتی ایفای نقش می‌کند و تمامی مراحل جرم لزوماً وابسته به فضای سایبری نیست.

یکی از ویژگی‌های مهم کلاهبرداری اینترنتی، عدم نیاز به حضور فیزیکی مجرم در محل وقوع جرم است. این امر باعث می‌شود که شناسایی و تعقیب مجرمان دشوارتر شده و فرآیندهای قضایی و پلیسی با پیچیدگی‌های بیشتری مواجه شوند. مجرمان اینترنتی می‌توانند از نقاط مختلف جهان، بدون نیاز به تماس مستقیم با قربانی، عملیات خود

را انجام دهند و از این طریق ناشناس باقی بمانند (میرمحمدصادقی، ۱۳۹۷: ۱۷۸). علاوه بر این، سرعت بالای انجام تراکنش‌ها در فضای دیجیتال باعث می‌شود که قربانیان معمولاً پس از وقوع جرم متوجه آن شوند و در بسیاری از موارد، بازیابی وجوه سرقت‌شده دشوار یا غیرممکن باشد.

از دیگر ویژگی‌های این جرم، امکان مقیاس‌پذیری و تکرارپذیری بالای آن است. در حالی که در کلاهبرداری‌های سنتی، مجرمان محدود به تعداد مشخصی از قربانیان هستند، در کلاهبرداری اینترنتی امکان هدف قرار دادن هزاران یا حتی میلیون‌ها نفر به‌صورت هم‌زمان وجود دارد. برای مثال، در روش فیشینگ، مجرمان می‌توانند با ارسال ایمیل‌های جعلی به میلیون‌ها کاربر، اطلاعات ورود به حساب‌های بانکی آنها را سرقت کنند. این مقیاس‌پذیری، کلاهبرداری اینترنتی را به یکی از سودآورترین روش‌های جرم در دنیای امروز تبدیل کرده است (Adrian & Mancini-Griffoli, ۲۰۱۹: ۴۲).

یکی دیگر از جنبه‌های مهم کلاهبرداری اینترنتی، استفاده از فناوری‌های نوین برای پنهان کردن ردپای مالی و دیجیتال است. مجرمان از ارزهای دیجیتال مانند بیت‌کوین و سایر رمزارزها برای جابه‌جایی پول‌های سرقت‌شده استفاده می‌کنند که به دلیل ماهیت غیرمتمرکز و ناشناس بودن این ارزها، ردیابی آنها دشوار است. همچنین، استفاده از شبکه‌های رمزگذاری‌شده و نرم‌افزارهای تغییر هویت دیجیتال، امکان شناسایی مجرمان را برای نهادهای امنیتی پیچیده‌تر کرده است (Trautman, ۲۰۱۶: ۹۱۲).

در کنار این چالش‌ها، نهادهای نظارتی و بانک‌های مرکزی در تلاش هستند تا با وضع مقررات جدید و توسعه فناوری‌های مقابله‌ای، از وقوع این جرایم جلوگیری کنند. به‌عنوان مثال، بسیاری از بانک‌ها و مؤسسات مالی از سیستم‌های احراز هویت چندعاملی و الگوریتم‌های یادگیری ماشین برای شناسایی تراکنش‌های مشکوک و فعالیت‌های غیرمعمول استفاده می‌کنند. همچنین، بانک‌های مرکزی و سازمان‌های بین‌المللی مانند کمیته نظارت بر بانکداری بازل توصیه‌هایی برای کاهش خطرات ناشی از فناوری‌های مالی و توسعه سیستم‌های امنیتی قوی‌تر ارائه کرده‌اند (Basel Committee on Banking Supervision, ۲۰۱۸: ۵۸).

فناوری بلاک‌چین به عنوان یکی از نوآوری‌های تحول‌آفرین در حوزه امنیت سایبری و مالی، می‌تواند نقش مؤثری در جلوگیری از جرم کلاهبرداری اینترنتی ایفا کند. بلاک‌چین با ویژگی‌هایی همچون تغییرناپذیری داده‌ها، شفافیت، امنیت رمزنگاری‌شده و غیرمتمرکز بودن، بستری مطمئن برای جلوگیری از دستکاری اطلاعات و فعالیت‌های مجرمانه در فضای دیجیتال فراهم می‌کند (Cachin, ۲۰۱۶: ۷).

یکی از مهم‌ترین ویژگی‌های بلاک‌چین که به پیشگیری از کلاهبرداری اینترنتی کمک می‌کند، تغییرناپذیری داده‌ها است. به دلیل ساختار زنجیره‌ای و رمزنگاری‌شده بلاک‌چین، هر تراکنش که در شبکه ثبت شود، قابل حذف یا تغییر نیست. این ویژگی باعث می‌شود که کلاهبرداران نتوانند سوابق تراکنش‌ها را دستکاری کرده یا هویت‌های جعلی

برای سرقت اطلاعات مالی ایجاد کنند (Deloitte, ۲۰۲۰: ۱۵)؛ برای مثال، در حوزه تجارت الکترونیکی، اگر از بلاک‌چین برای ثبت سفارشات و پرداخت‌ها استفاده شود، مشتریان و فروشندگان می‌توانند به‌راحتی از صحت تراکنش‌ها اطمینان حاصل کنند و خطر کلاهبرداری‌های ناشی از پرداخت‌های جعلی کاهش یابد.

شفافیت یکی دیگر از عوامل مهمی است که بلاک‌چین را به ابزاری کارآمد در جلوگیری از کلاهبرداری اینترنتی تبدیل می‌کند. در این فناوری، تمامی تراکنش‌ها در یک دفتر کل عمومی ثبت می‌شوند که همه کاربران می‌توانند به آن دسترسی داشته باشند. این شفافیت موجب کاهش فعالیت‌های مجرمانه، مانند جعل هویت یا تقلب در پرداخت‌های آنلاین، می‌شود؛ برای مثال در صنعت بانکداری، بلاک‌چین می‌تواند برای تأیید هویت کاربران و جلوگیری از ثبت‌نام‌های جعلی یا سرقت اطلاعات هویتی مورد استفاده قرار گیرد.(Böhme et al. ۲۰۱۵: ۲۲۵)

افزون بر این، امنیت رمزنگاری‌شده بلاک‌چین، سطح حفاظت از داده‌ها را به میزان قابل توجهی افزایش می‌دهد. در روش‌های سنتی، اطلاعات مالی کاربران در پایگاه‌های داده متمرکز ذخیره می‌شود که در معرض حملات هکری قرار دارد؛ اما در بلاک‌چین، داده‌ها در یک شبکه گسترده از نودها توزیع شده‌اند و هر تغییر در اطلاعات نیازمند تأیید تمام اعضای شبکه است. این مکانیزم موجب کاهش حملات سایبری و جلوگیری از دسترسی غیرمجاز به اطلاعات مالی کاربران می‌شود (Zohar, ۲۰۱۵: ۱۱۰). به عنوان مثال، در سیستم‌های پرداخت دیجیتال مبتنی بر بلاک‌چین، مانند بیت‌کوین، امکان تقلب در پرداخت یا سرقت اطلاعات کارت‌های اعتباری به شدت کاهش می‌یابد.

علاوه بر ویژگی‌های امنیتی، بلاک‌چین با استفاده از قراردادهای هوشمند نیز می‌تواند از وقوع کلاهبرداری‌های اینترنتی جلوگیری کند. قراردادهای هوشمند کدهای خوداجرایی هستند که شرایط توافق بین طرفین را بدون نیاز به واسطه‌های مالی اجرا می‌کنند. این فناوری در صنایعی مانند بیمه و بازارهای آنلاین، احتمال تقلب و سوءاستفاده را کاهش می‌دهد؛ برای مثال در یک پلتفرم تجارت آنلاین که از قراردادهای هوشمند استفاده می‌کند، پرداخت تنها زمانی انجام می‌شود که کالا به دست خریدار برسد و شرایط قرارداد به طور کامل رعایت شود، بنابراین خطر کلاهبرداری فروشندگان کاهش می‌یابد (Schrepel, ۲۰۱۹: ۱۴۰).

نمونه‌های واقعی نشان می‌دهند که استفاده از بلاک‌چین می‌تواند تأثیر چشمگیری در کاهش جرایم اینترنتی داشته باشد. به عنوان مثال، برخی بانک‌های بین‌المللی مانند جی‌پی مورگان و HSBC از بلاک‌چین برای رهگیری تراکنش‌های مالی و تأیید هویت مشتریان استفاده می‌کنند که منجر به کاهش چشمگیر در تقلب‌های بانکی شده است (Deloitte, ۲۰۲۰: ۲۲) ؛ همچنین برخی شرکت‌های تجارت الکترونیکی مانند آمازون و علی‌بابا به دنبال راهکارهای مبتنی بر بلاک‌چین برای جلوگیری از فروش کالاهای تقلبی و محافظت از اطلاعات مشتریان هستند.

۲-۴-پول‌شویی

جرم پول‌شویی یکی از جرایم پیچیده و مهم مالی و اقتصادی است که با هدف پنهان‌سازی منابع غیرقانونی درآمدها از طریق فرآیندهای قانونی انجام می‌شود. پول‌شویی به عنوان عملی در جهت مشروعیت‌بخشی به درآمدهای به دست آمده از فعالیت‌های غیرقانونی تعریف می‌شود. این فعالیت‌ها ممکن است شامل قاچاق مواد مخدر، رشوه‌خواری، فساد مالی، کلاهبرداری یا هر نوع جرم اقتصادی دیگری باشد. هدف اصلی پول‌شویی این است که پول‌های حاصل از این فعالیت‌ها به نظر برسد که از منابع مشروع و قانونی به دست آمده‌اند، به گونه‌ای که در سیستم اقتصادی قانونی قابل استفاده و قابل انتقال شوند (گلدوزیان، ۱۳۹۹: ۸۵).

برای تحقق جرم پول‌شویی در حقوق ایران، سه شرط اصلی لازم است: اول، وجود عواید و درآمدهای حاصل از ارتکاب جرم مقدم یا همان جرم منشاء؛ مانند قاچاق، اختلاس، کلاهبرداری و غیره؛ دوم، انجام اقدامات به منظور تطهیر این اموال، از جمله تبدیل، انتقال، تملک، استفاده، نگهداری یا مخفی کردن منشأ غیرقانونی آنها؛ و سوم، قصد فریب نهادهای نظارتی یا قانونی به‌منظور مشروع جلوه دادن منابع این اموال و پنهان کردن منشاء مجرمانه آنها. جرم پول‌شویی به‌طور صریح در قانون مبارزه با پول‌شویی مصوب ۱۳۸۶ و اصلاحیه ۱۳۹۷ در مواد مختلف، به‌ویژه ماده ۲، تعریف و جرم‌انگاری شده است. علاوه بر این، ماده ۷ قانون مجازات اسلامی (مصوب ۱۳۹۲) نیز به جرایم سازمان‌یافته و فراملی اشاره دارد که پول‌شویی به‌عنوان یکی از مصادیق این جرایم، مشمول آن می‌شود و تحت تعقیب و مجازات قرار می‌گیرد. همچنین، در فصل سی‌ام قانون مجازات اسلامی، تحت عنوان «جرایم علیه اموال و مالکیت»، برخی از رفتارهایی که می‌تواند با جرم پول‌شویی مرتبط باشد (مانند تحصیل مال از طریق نامشروع) مطرح شده است؛ بنابراین جرم پول‌شویی در کنار قانون خاص خود، در دیگر قوانین کیفری ایران نیز مورد توجه و شمول قرار دارد.

ماهیت جرم پول‌شویی به این دلیل پیچیده است که این جرم با استفاده از راهکارهای مالی و تکنیکی انجام می‌شود که می‌تواند تأثیرات گسترده‌ای بر سیستم‌های مالی و اقتصادی جهان داشته باشد. فرآیند پول‌شویی به طور معمول در سه مرحله اصلی صورت می‌گیرد: نخست، جمع‌آوری و نگهداری وجوه غیرقانونی، دوم، تبدیل این وجوه به شکلی که از نظر ظاهری مشروع به نظر برسد؛ مانند انتقال به حساب‌های مختلف یا خرید دارایی‌های مختلف و در نهایت، ادغام این منابع به چرخه اقتصادی قانونی؛ به طور مثال فردی که از راه قاچاق مواد مخدر درآمد کسب کرده، می‌تواند این درآمدها را به شرکت‌های مختلف وارد کند یا از طریق خرید و فروش ملک، این وجوه را به صورت قانونی درآورد (زراعت، ۱۳۸۶: ۱۱۲).

ویژگی‌های جرم پول‌شویی از آن جهت مهم است که این نوع جرم معمولاً در پشت پرده قرار دارد و به راحتی قابل شناسایی نیست. یکی از ویژگی‌های این جرم، استفاده از پیچیدگی‌های مالی و سیستم‌های مختلف است که موجب می‌شود تا شناسایی و اثبات جرم بسیار دشوار باشد؛ برای مثال با استفاده از فناوری‌های نوین مالی همچون بلاک چین، ممکن است این روند پیچیده‌تر شود. در حالی که بلاک چین مزایای زیادی در زمینه شفافیت و امنیت مالی

دارد، در برخی موارد ممکن است به عنوان ابزاری برای پول‌شویی به کار رود(Trautman, ۲۰۱۶: ۹۱۴)؛ همچنین استفاده از ارزهای دیجیتال نیز به افزایش چالش‌های مبارزه با پول‌شویی کمک کرده است. به طور خاص، ارزهای دیجیتال مانند بیت‌کوین می‌توانند این فرایند را تسهیل کنند؛ زیرا این ارزها ویژگی‌هایی مانند ناشناسی و عدم شفافیت در تراکنش‌ها دارند که می‌تواند استفاده از آنها برای پول‌شویی را آسان‌تر کند (Adrian & Mancini-Griffoli, ۲۰۱۹: ۸).

در راستای مقابله با پول‌شویی، بسیاری از کشورها و نهادهای بین‌المللی قوانینی را برای شناسایی و متوقف کردن این جرم وضع کرده‌اند. کمیته نظارت بر بانکداری بیسل (۲۰۱۸) بر لزوم نظارت بر تراکنش‌های مالی و فعالیت‌های بانکی تأکید دارد تا از هرگونه فعالیت مشکوک و مربوط به پول‌شویی جلوگیری شود؛ همچنین شفافیت بیشتر در استفاده از سیستم‌های دیجیتال و بلاک‌چین می‌تواند راه‌حل‌هایی برای مقابله با این پدیده ارائه دهد. از آنجایی که بلاک‌چین به کاربران این امکان را می‌دهد که تمامی تراکنش‌ها را به صورت عمومی و غیرقابل تغییر ثبت کنند، این ویژگی می‌تواند در شفافیت و جلوگیری از پول‌شویی مؤثر باشد (Cachin, ۲۰۱۶: ۲۷).

با وجود این، مهم است که فناوری‌هایی همچون بلاک‌چین و ارزهای دیجیتال به درستی و با نظارت مناسب به کار گرفته شوند، زیرا اگر کنترل‌های لازم در این زمینه‌ها اعمال نشود، ممکن است به ابزاری برای تقویت جرایم مالی تبدیل شوند. گزارش‌های مختلف نشان می‌دهند که بلاک چین و ارزهای دیجیتال می‌توانند به عنوان یک ریسک امنیتی در برابر تلاش‌ها برای مقابله با پول‌شویی مطرح شوند (Deloitte, ۲۰۲۰: ۱۱).

درنتیجه، پول‌شویی یک جرم جهانی و پیچیده است که نه‌تنها به اقتصاد کشورها آسیب می‌زند، بلکه امنیت مالی جهانی را نیز تهدید می‌کند. این جرم با استفاده از روش‌های پیچیده مالی و تکنولوژی‌های نوین در تلاش است تا درآمدهای حاصل از فعالیت‌های غیرقانونی را در جریان‌های مالی مشروع وارد کند. این تهدید نیازمند نظارت مستمر و اتخاذ تدابیر قانونی مناسب در سطح ملی و بین‌المللی است تا از گسترش آن جلوگیری شود (میرمحمدصادقی، ۱۳۹۷: ۹۷).

یکی از ویژگی‌های کلیدی بلاک‌چین، قابلیت ثبت غیرقابل تغییر اطلاعات در یک دفتر کل عمومی است. این ویژگی باعث می‌شود که تمام تراکنش‌ها به صورت دائمی و شفاف در سیستم ثبت شوند. در واقع، هر تراکنش در بلاک چین به صورت یک «بلوک» در زنجیره‌ای از بلوک‌ها ذخیره می‌شود که پس از تأیید توسط شبکه، امکان تغییر یا حذف آن وجود ندارد (Atzori, ۲۰۱۷: ۴۸). این ویژگی می‌تواند به مبارزه با پول‌شویی کمک کند، زیرا باعث می‌شود که هیچ فردی نتواند اطلاعات مربوط به تراکنش‌ها را پنهان کرده یا تغییر دهد؛ برای مثال درصورتی‌که پول‌های حاصل از جرم به صورت غیرقانونی وارد سیستم مالی شوند، می‌توان با استفاده از بلاک چین تراکنش‌ها را پیگیری کرده و رد آنها را پیدا کرد (تذهیبی،۱۳۹۱: ۲۷).

یکی دیگر از مزایای مهم بلاک‌چین در جلوگیری از پول‌شویی، غیرمتمرکز بودن این فناوری است. در سیستم‌های سنتی مالی، تراکنش‌ها و اطلاعات معمولاً از طریق بانک‌ها و مؤسسات مالی مرکزی مدیریت می‌شوند. این امر می‌تواند برای پنهان‌سازی فعالیت‌های غیرقانونی مانند پول‌شویی فرصتی مناسب فراهم کند؛ اما بلاک‌چین به دلیل ساختار غیرمتمرکز خود، این امکان را از بین می‌برد .(De Filippi & Wright, ۲۰۱۸: ۱۰۵). در سیستم بلاک‌چین، هیچ نهاد واحدی کنترل تمام داده‌ها و تراکنش‌ها را ندارد و این تراکنش‌ها توسط شبکه‌ای از نودها (گره‌ها) تأیید و ثبت می‌شوند. به همین دلیل، ردیابی و نظارت بر تراکنش‌ها و جلوگیری از فعالیت‌های مشکوک دشوارتر از سیستم‌های متمرکز است (خواجوی،۱۳۹۹: ۳۴).

علاوه بر این، بلاک‌چین می‌تواند با استفاده از قراردادهای هوشمند (Smart Contracts) به بهبود کنترل‌ها در سیستم‌های مالی کمک کند. قراردادهای هوشمند کدهایی هستند که به طور خودکار و بدون نیاز به واسطه، شرایط توافقات را بر اساس قواعد از پیش تعیین شده اجرا می‌کنند. این قراردادها می‌توانند در بلاک چین برای اطمینان از شفافیت و تطابق تراکنش‌ها با قوانین ضد پول‌شویی طراحی شوند. برای مثال، اگر یک تراکنش در حال انجام باشد که به نظر مشکوک می‌آید، قرارداد هوشمند می‌تواند به طور خودکار آن را متوقف کرده و گزارشات لازم را به مقامات مربوطه ارسال کند (Cong & He, ۲۰۱۹: ۱۷۶۵). این ویژگی می‌تواند باعث کاهش ریسک‌های پول‌شویی و تقویت سیستم‌های نظارتی شود.

همچنین، بلاک‌چین با فراهم کردن شفافیت بیشتر در مسیر حرکت پول، نظارت مؤثری را بر تراکنش‌های مالی ایجاد می‌کند. تراکنش‌ها در بلاک چین به طور عمومی قابل مشاهده هستند و هر فردی می‌تواند اطلاعات مربوط به این تراکنش‌ها را بررسی کند. این ویژگی می‌تواند به مقامات و نهادهای نظارتی کمک کند تا به راحتی تراکنش‌های مشکوک و غیرقانونی را شناسایی کرده و آنها را پیگیری کنند. به این ترتیب، افراد یا سازمان‌هایی که قصد انجام پول‌شویی دارند، با خطر شناسایی سریع‌تر مواجه می‌شوند (Zyskind, Nathan & Pentland, ۲۰۱۵:۱۸۲).

علاوه بر این، با استفاده از بلاک‌چین، می‌توان از تکنولوژی‌هایی مانند شناسایی دیجیتالی و احراز هویت بیومتریک برای تأیید هویت کاربران استفاده کرد. این اقدامات می‌تواند به جلوگیری از استفاده نادرست از سیستم‌های مالی توسط افراد غیرمجاز کمک کند. درواقع، بلاک‌چین به عنوان یک فناوری می‌تواند به اطمینان از اینکه تنها افراد و نهادهای معتبر قادر به انجام تراکنش‌ها هستند، کمک کند .(Hendrickson & Luther, ۲۰۲۰: ۱۵۷) با اعمال چنین تدابیری، جلوگیری از پول‌شویی و دیگر فعالیت‌های مالی غیرقانونی تسهیل می‌شود.

در نهایت، یکی دیگر از مزایای بلاک‌چین در مبارزه با پول‌شویی، امکان ادغام با سیستم‌های نظارتی و قوانین ضد پول‌شویی موجود است. بسیاری از کشورها و نهادهای بین‌المللی، مانند گروه ویژه اقدام مالی (FATF)، استانداردهایی را برای مبارزه با پول‌شویی و تأمین مالی تروریسم وضع کرده‌اند. بلاک‌چین با ویژگی‌های خود می‌تواند به راحتی این استانداردها را در سیستم‌های مالی اجرا کند و از بروز تخلفات جلوگیری کند ,Gikay).

(۴۴ :۲۰۱۸در واقع، بلاک چین به‌عنوان یک ابزار نظارتی می‌تواند مقامات را در شناسایی و مقابله با فعالیت‌های مالی غیرقانونی یاری کند.

درنتیجه، بلاک‌چین به عنوان یک فناوری مبتنی بر شفافیت، غیرمتمرکز بودن و امنیت می‌تواند ابزاری مؤثر در پیشگیری و کنترل جرم پول‌شویی باشد. این فناوری می‌تواند با ویژگی‌های خود، شفافیت مالی را افزایش داده، ردیابی و نظارت بر تراکنش‌ها را تسهیل کرده و از بروز تقلب و فعالیت‌های غیرقانونی جلوگیری کند؛ بنابراین استفاده از بلاک‌چین در مبارزه با پول‌شویی می‌تواند به‌طور چشمگیری به بهبود سیستم‌های مالی جهانی کمک کند و سطح امنیت و اعتماد عمومی را افزایش دهد.

۴-۳- اختلاس

اختلاس یکی از جرایم مهم مالی و اقتصادی محسوب می‌شود که معمولاً در سازمان‌ها، نهادهای دولتی و مؤسسات مالی رخ می‌دهد. این جرم به طور کلی به معنای تصرف غیرقانونی و سوءاستفاده از وجوه، اموال یا دارایی‌هایی (برداشت و تصاحب) است که فرد به طور قانونی به آنها دسترسی دارد؛ اما از آنها برای منافع شخصی خود بهره می‌برد؛ به عبارت دیگر، فرد مرتکب اختلاس کسی است که به دلیل موقعیت شغلی خود، به دارایی‌های یک سازمان یا نهاد دسترسی دارد و بدون مجوز قانونی، از این منابع برای خود استفاده می‌کند. این جرم معمولاً در دستگاه‌های دولتی، بانک‌ها، شرکت‌های خصوصی و مؤسسات مالی رخ می‌دهد و می‌تواند تأثیرات منفی گسترده‌ای بر اقتصاد و اعتماد عمومی بگذارد (رهبر، ۱۳۹۸: ۱۲۵).

برای تحقق جرم اختلاس در حقوق ایران، وجود چند شرط اساسی لازم است: اول، مرتکب باید کارمند یا مستخدم رسمی یا غیررسمی دولت، نهادها و سازمان‌های عمومی، یا شرکت‌ها و مؤسسات وابسته به دولت باشد؛ دوم، اموال یا وجوهی که موضوع جرم قرار می‌گیرد باید به‌موجب وظایف شغلی در اختیار مرتکب قرار گرفته باشد؛ و سوم، مرتکب این اموال را به نفع خود یا دیگری برداشت یا تصاحب کند. جرم اختلاس به‌صراحت در ماده ۵ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ جرم‌انگاری شده است که بر اساس آن، کارمندان دولت و وابستگان به آنها در صورت برداشت غیرقانونی وجوه یا اموالی که به آنها سپرده شده، به مجازات حبس و جزای نقدی و انفصال از خدمت محکوم می‌شوند. علاوه بر این، ماده ۶ قانون مذکور شرایط تشدید مجازات در صورت اختلاس مبالغ کلان یا تکرار جرم را پیش‌بینی کرده است (صادقی، ۱۴۰۱: ۲۹).

اختلاس دارای ویژگی‌هایی است که آن را از سایر جرایم مالی متمایز می‌کند. یکی از مهم‌ترین ویژگی‌های آن، این است که مرتکب جرم، خود فردی است که به طور قانونی به منابع مالی یا اموال دسترسی دارد، اما از این موقعیت سوءاستفاده می‌کند. این جرم معمولاً در قالب برداشت‌های غیرمجاز، جعل اسناد مالی، دستکاری در حساب‌های بانکی و استفاده شخصی از دارایی‌های سازمانی اتفاق می‌افتد (Iansiti & Lakhani, ۲۰۱۷: ۱۲۱). یکی دیگر از

ویژگی‌های اختلاس، مخفیانه بودن آن است. افراد مرتکب این جرم اغلب تلاش می‌کنند که فعالیت‌های خود را از دید نهادهای نظارتی و مسئولان پنهان کنند. آنها ممکن است از روش‌هایی مانند ثبت اسناد جعلی، انتقال وجوه به حساب‌های واسطه یا ایجاد حساب‌های ساختگی برای پنهان کردن عملیات خود استفاده کنند. این امر باعث می‌شود که کشف و شناسایی جرم اختلاس زمان‌بر و دشوار باشد (Lee, ۲۰۱۹: ۸۷).

همچنین، اختلاس معمولاً یک جرم تدریجی است، به این معنا که مجرم به جای اینکه یکباره مبلغ زیادی را برداشت کند، در طول زمان و به صورت مداوم، مبالغ کوچکی را تصاحب می‌کند تا کمتر مورد توجه قرار گیرد. این روش باعث می‌شود که نهادهای نظارتی دیرتر متوجه جرم شوند و فرد مدت بیشتری به اختلاس ادامه دهد (Houben & Snyers, ۲۰۱۸: ۳۹).

دلایل متعددی برای بروز این جرم وجود دارد که برخی به ساختارهای مدیریتی و نظارتی مرتبط هستند و برخی دیگر به عوامل فردی و اجتماعی بازمی‌گردند. یکی از مهم‌ترین عواملی که زمینه را برای اختلاس فراهم می‌کند، عدم شفافیت در ساختارهای مالی و مدیریتی است. نبود شفافیت در سازمان‌ها باعث می‌شود که اطلاعات مالی به‌طور دقیق ثبت و گزارش نشود، در نتیجه، امکان سوءاستفاده از منابع مالی افزایش می‌یابد. هنگامی که اطلاعات مالی به‌صورت عمومی و منظم در دسترس نهادهای نظارتی، حسابرسان و حتی کارکنان یک سازمان قرار نگیرد، فرصت برای افرادی که قصد سوءاستفاده دارند، بیشتر خواهد شد. برای مثال، در بسیاری از کشورها، اختلاس‌های کلان به دلیل عدم شفافیت در تخصیص بودجه‌های دولتی یا قراردادهای بزرگ رخ داده است (Houben & Snyers, ۲۰۱۸: ۴۱).

شفافیت مالی یکی از مهم‌ترین ابزارهای پیشگیری از جرایم اقتصادی، از جمله اختلاس، محسوب می‌شود. زمانی که یک سازمان یا نهاد دولتی موظف باشد تمام تراکنش‌های مالی خود را به‌طور دقیق ثبت کند و گزارش‌های مالی را به‌طور منظم منتشر نماید، احتمال وقوع فساد مالی کاهش می‌یابد. متأسفانه در بسیاری از موارد، اطلاعات مالی تنها در اختیار گروه محدودی از مدیران قرار دارد و سایر بخش‌های سازمان، ازجمله نهادهای نظارتی، دسترسی کافی به آن ندارند. این وضعیت باعث می‌شود که برخی مدیران یا کارمندان فرصت سوءاستفاده از منابع مالی را داشته باشند. عدم شفافیت همچنین موجب می‌شود که کشف موارد اختلاس به تأخیر بیفتد و هنگامی که جرم افشا می‌شود، بخش زیادی از اموال اختلاس‌شده از بین رفته یا به حساب‌های خارجی منتقل شده باشد (Lee, ۲۰۱۹: ۹۴).

یکی دیگر از دلایل اصلی بروز اختلاس، نبود سیستم‌های گزارش‌دهی و حمایت از افشاگران است. در بسیاری از موارد، کارمندان یک سازمان از وقوع تخلفات مالی آگاه هستند، اما به دلیل ترس از انتقام‌جویی، از گزارش دادن این جرایم خودداری می‌کنند (کیانی زاده، ۱۳۹۴: ۶۵). عدم وجود سازوکارهای حمایتی برای افشاگران، مانند حفاظت از هویت آنها یا ارائه مشوق‌های قانونی، باعث می‌شود که تخلفات مالی بدون افشا باقی بمانند. اگر در یک سازمان،

کارمندان بتوانند تخلفات را به‌صورت ناشناس و بدون ترس از عواقب منفی گزارش دهند، احتمال کشف زودهنگام جرایم مالی مانند اختلاس افزایش می‌یابد. کشورهای پیشرفته با ایجاد سامانه‌های محرمانه گزارش‌دهی و تصویب قوانین حمایتی برای افشاگران، توانسته‌اند میزان فساد و اختلاس را به میزان قابل توجهی کاهش دهند (Iansiti & Lakhani, ۲۰۱۷: ۱۲۵).

علاوه بر این عوامل، ضعف در نظارت و کنترل داخلی نیز در افزایش موارد اختلاس مؤثر است. نبود سازوکارهای نظارتی دقیق، باعث می‌شود که بسیاری از تخلفات مالی در مراحل اولیه شناسایی نشوند. همچنین، فساد اداری و روابط ناسالم درون سازمان‌ها می‌تواند موجب شود که متخلفان با حمایت برخی مدیران یا مقام‌های بالادستی از پیگرد قانونی مصون بمانند. فشارهای اقتصادی و مشکلات مالی افراد نیز می‌تواند انگیزه‌ای برای ارتکاب اختلاس باشد، به‌ویژه در شرایطی که کارمندان احساس کنند که حقوق و مزایای آنها برای تأمین نیازهای زندگی کافی نیست (Morabito, ۲۰۱۷: ۶۲).

در مجموع، اختلاس نتیجه ترکیبی از ضعف‌های نظارتی، نبود شفافیت، عدم حمایت از افشاگران و سایر عوامل ساختاری و فردی است. اگرچه برخی از این عوامل ممکن است در کوتاه‌مدت تغییر نکنند، اما با بهبود شفافیت مالی و ایجاد سیستم‌های گزارش‌دهی محرمانه، می‌توان میزان وقوع این جرم را کاهش داد. برای مبارزه مؤثر با اختلاس، دولت‌ها و سازمان‌ها باید اقدامات جدی در جهت اصلاح ساختارهای مالی، تقویت نهادهای نظارتی و حمایت از گزارش‌دهندگان فساد انجام دهند (غلامی، ۱۳۹۹: ۲۱۱).

فناوری بلاک‌چین به عنوان یک سیستم ثبت غیرمتمرکز و شفاف، توانایی بالقوه‌ای برای کاهش جرایمی مانند اختلاس دارد. این فناوری می‌تواند با رفع عواملی که منجر به بروز اختلاس می‌شوند، به ایجاد یک سیستم مالی شفاف و غیرقابل تغییر کمک کند. در ادامه بررسی می‌کنیم که چگونه بلاک‌چین می‌تواند بر این عوامل اثر بگذارد و در نهایت، احتمال وقوع اختلاس را کاهش دهد. یکی از مهم‌ترین عوامل بروز اختلاس، عدم شفافیت در مدیریت مالی و نظارت بر تراکنش‌ها است. بلاک‌چین با ایجاد یک دفتر کل توزیع‌شده که تمامی تراکنش‌ها را به‌صورت عمومی و دائمی ثبت می‌کند، به شفافیت بیشتر در امور مالی کمک می‌کند. به دلیل ماهیت غیرقابل تغییر بلاک‌چین، هیچ نهادی نمی‌تواند به‌صورت یک‌جانبه داده‌های مالی را تغییر دهد یا حذف کند. این ویژگی باعث می‌شود که تمامی تراکنش‌های مالی به‌طور دقیق ثبت شده و به راحتی قابل ردیابی باشند (Swan, ۲۰۱۵: ۴۵). در یک سیستم مبتنی بر بلاک چین، مقامات نظارتی، حسابرسان و حتی عموم مردم می‌توانند اطلاعات مالی را مشاهده کرده و هرگونه تخلف احتمالی را شناسایی کنند. این سطح از شفافیت، فرصت‌های اختلاس را به میزان قابل توجهی کاهش می‌دهد.

عامل مهم دیگری که موجب گسترش اختلاس می‌شود، نبود سیستم‌های گزارش‌دهی و حمایت از افشاگران است. در سیستم‌های سنتی، افرادی که قصد افشای تخلفات مالی را دارند، معمولاً با خطرات زیادی مواجه‌اند، از جمله از

دست دادن شغل یا تهدیدات شخصی؛ اما بلاک‌چین می‌تواند با فراهم کردن یک بستر امن و ناشناس برای گزارش‌دهی تخلفات، این مشکل را حل کند. به‌عنوان مثال، با استفاده از قراردادهای هوشمند و سیستم‌های رمزگذاری شده، افراد می‌توانند بدون افشای هویت خود، موارد مشکوک را گزارش دهند (Allen, ۲۰۱۹: ۳۲۰). این موضوع موجب می‌شود که فساد مالی در مراحل اولیه کشف شده و امکان وقوع اختلاس‌های گسترده کاهش یابد.

علاوه بر این، بلاک‌چین با حذف واسطه‌ها و افزایش کارایی نظارت مالی، نقش مهمی در کاهش فساد و اختلاس ایفا می‌کند. در سیستم‌های مالی سنتی، وجود واسطه‌های متعدد مانند بانک‌ها و نهادهای مالی، امکان دست‌کاری و سوءاستفاده از منابع مالی را فراهم می‌کند؛ اما با استفاده از بلاک‌چین، تراکنش‌های مالی به‌طور مستقیم بین طرفین انجام شده و در یک بستر شفاف ثبت می‌شوند. این امر نه تنها هزینه‌های مالی را کاهش می‌دهد، بلکه ریسک وقوع جرایمی مانند اختلاس را نیز کم می‌کند (Möser & Böhme, ۲۰۱۷: ۴۲).

همچنین، استفاده از قراردادهای هوشمند در بلاک‌چین می‌تواند از سوءاستفاده‌های مالی جلوگیری کند. قراردادهای هوشمند مجموعه‌ای از کدهای دیجیتالی هستند که به‌طور خودکار اجرا می‌شوند و تنها در صورت رعایت شرایط خاص، پرداخت‌ها را انجام می‌دهند. این موضوع به‌ویژه در مدیریت بودجه‌های دولتی و پرداخت‌های کلان مالی اهمیت دارد، زیرا دیگر امکان پرداخت‌های غیرقانونی یا تغییر در قراردادهای مالی وجود نخواهد داشت (Chuen, Guo, & Wang, ۲۰۱۷: ۲۵)

در کنار این موارد، نظارت بین‌المللی بر تراکنش‌های مالی نیز از طریق بلاک‌چین تقویت می‌شود. بسیاری از پرونده‌های اختلاس شامل جابه‌جایی پول به حساب‌های خارجی و فرار مالیاتی هستند؛ اما با استفاده از بلاک‌چین، نهادهای نظارتی می‌توانند تراکنش‌های مالی را به‌طور دقیق ردیابی کرده و مانع از جابه‌جایی غیرقانونی سرمایه‌ها شوند. مطالعات نشان داده‌اند که در کشورهایی که بلاک چین برای نظارت بر تراکنش‌های مالی مورد استفاده قرار گرفته، میزان جرایم اقتصادی به میزان قابل توجهی کاهش یافته است (Hileman & Rauchs, ۲۰۱۷: ۵۰).

در نهایت، بلاک‌چین می‌تواند با ایجاد استانداردهای جدید برای نظارت مالی و شفافیت اقتصادی، یک تغییر بنیادین در مقابله با جرایم مالی مانند اختلاس ایجاد کند. بسیاری از سازمان‌های بین‌المللی، از جمله سازمان همکاری و توسعه اقتصاد (OECD)، تأکید دارند که فناوری‌های نوین مانند بلاک‌چین می‌توانند در جلوگیری از تخلفات مالی و بهبود سیستم‌های نظارتی نقش کلیدی ایفا کنند (OECD, ۲۰۲۰: ۷۷). این فناوری با از بین بردن نقاط ضعف سیستم‌های سنتی، می‌تواند گام مهمی در جهت کاهش فساد مالی و افزایش اعتماد عمومی به نظام‌های اقتصادی باشد.

بنابراین، بلاک‌چین از طریق شفاف‌سازی تراکنش‌های مالی، ایجاد بسترهای امن برای گزارش‌دهی تخلفات، کاهش وابستگی به واسطه‌ها، استفاده از قراردادهای هوشمند و افزایش نظارت بین‌المللی، می‌تواند به‌طور مؤثری در پیشگیری از اختلاس نقش ایفا کند. هرچند پیاده‌سازی این فناوری نیازمند همکاری دولت‌ها و نهادهای نظارتی است، اما پتانسیل آن برای کاهش فساد مالی غیرقابل انکار است.

برآمد

فناوری بلاک‌چین می‌تواند با ایجاد شفافیت، افزایش امنیت اطلاعات و ارتقای کارایی سامانه‌ها، نقش مؤثری در توانمندسازی پلیس و نظام قضایی ایران برای مقابله با جرایم مالی، پولی و سایبری ایفا کند. این فناوری، ابزاری نوین در اختیار نیروهای انتظامی قرار می‌دهد تا با استفاده از ثبت غیرقابل تغییر داده‌ها، شناسایی دقیق‌تر جرایم سازمان‌یافته و تحلیل ردپای دیجیتال مجرمان، فرایند کشف و پیگیری جرایم را به شکل مؤثری ارتقا دهند. در نظام قضایی، استفاده از بلاک‌چین برای ثبت اسناد و مدارک به صورت غیرقابل تغییر، می‌تواند مانع از جعل، تغییر یا حذف مستندات شود. این امر کمک شایانی به پلیس در زمینه جمع‌آوری شواهد قابل استناد و تسریع روند تحقیقات کیفری می‌کند. همچنین، بهره‌گیری از قراردادهای هوشمند در رسیدگی‌های قضایی، می‌تواند فرآیندهای حقوقی را شفاف و قابل پیگیری کرده و از بروز فساد یا دخالت‌های غیرقانونی در روند دادرسی جلوگیری کند.

در حوزه بانکی و مالی نیز بلاک‌چین ابزار قدرتمندی برای مقابله با تخلفات اقتصادی در اختیار پلیس قرار می‌دهد. شناسایی مسیرهای انتقال غیرقانونی وجوه، ردگیری معاملات مشکوک و افشای زنجیره‌های پول‌شویی با بهره‌گیری از دفترکل‌های توزیع‌شده و شفاف بلاک‌چین، با دقت بسیار بیشتری قابل انجام است. این اطلاعات می‌توانند مبنای تشکیل پرونده‌های کیفری و پیگرد مجرمان اقتصادی قرار گیرند. از منظر امنیت سایبری، پلیس می‌تواند با اتکا به ساختار رمزنگاری‌شده بلاک‌چین، از حملات سایبری به سامانه‌های بانکی و نشت اطلاعات جلوگیری کرده و بستر امن‌تری برای تعاملات دیجیتال فراهم آورد. کاهش نیاز به واسطه‌ها و تمرکززدایی از سیستم‌ها نیز احتمال نفوذ و سوءاستفاده داخلی را به‌طور چشمگیری کاهش می‌دهد. با وجود این ظرفیت‌ها، تحقق کامل این اهداف مستلزم ایجاد زیرساخت‌های فنی، حقوقی و قانونی مناسب و همچنین همکاری مستمر میان پلیس، قوه قضاییه و نهادهای دولتی و بانکی است. با این حال، ورود هدفمند به حوزه بلاک‌چین می‌تواند آغاز تحولی بنیادین در فرآیندهای پیشگیری، کشف و رسیدگی به جرایم مالی و سایبری در ایران باشد؛ تحولی که نیروهای انتظامی و ضابطان قضایی در خط مقدم آن قرار دارند.

فناوری بلاک‌چین، نه تنها می‌تواند عملکرد نظام قضایی و بانکی کشور را ارتقاء بخشد، بلکه به‌عنوان ابزاری راهبردی، ظرفیت‌های پلیس را در مبارزه با جرایم اقتصادی، اداری و سایبری گسترش می‌دهد. پلیس فتا و پلیس اقتصادی با به‌کارگیری سامانه‌های مبتنی بر بلاک‌چین، می‌توانند در پیشگیری، شناسایی و پیگیری جرایم عملکرد دقیق‌تر، شفاف‌تر و سریع‌تری داشته باشند. تحقق این هدف نیازمند همکاری میان قوه قضاییه، بانک مرکزی،

نهادهای امنیتی و مراکز علمی برای طراحی و استقرار زیرساخت‌های بلاک‌چین در سیستم‌های عملیاتی کشور است. نهایتاً می‌توان به نتایج زیر به عنوان دستاوردهای پژوهشی مقاله حاضر اشاره نمود.

۱. بهره‌گیری از بلاک‌چین در نظام قضایی با محوریت پلیس

نظام قضایی ایران سالانه با انبوهی از پرونده‌های مربوط به جرایم اقتصادی، فساد اداری، جعل اسناد و کتمان اطلاعات مواجه است. بسیاری از این پرونده‌ها نیازمند مستندات دقیق، غیرقابل تغییر و قابل‌ردیابی هستند که بتوانند در فرآیند کشف جرم و اثبات آن مؤثر واقع شوند. پلیس، به‌عنوان ضابط قضایی، می‌تواند با استفاده از بلاک‌چین، مأموریت‌های خود را با دقت و شفافیت بیشتری انجام دهد.

یکی از دغدغه‌های مهم پلیس در بررسی پرونده‌های مالی، وجود مدارک جعلی یا سوابق دست‌کاری‌شده است. با استفاده از بلاک‌چین، اسناد و مدارک حقوقی و مالی می‌توانند به‌صورت رمزنگاری‌شده در یک سامانه غیرمتمرکز ذخیره شوند، به‌گونه‌ای که امکان حذف یا ویرایش آنها وجود نداشته باشد. این ویژگی می‌تواند صحت و اعتبار مدارک جمع‌آوری‌شده توسط پلیس را افزایش دهد و فرآیند استنادپذیری در دادگاه را ساده‌تر و قاطع‌تر کند.

در برخی پرونده‌ها، فقدان شفافیت در روند دادرسی و اجرای احکام زمینه‌ساز فساد و تبانی می‌شود. پلیس می‌تواند با استناد به تراکنش‌ها و اطلاعات ثبت‌شده در بستر بلاک‌چین، روند رسیدگی به جرایم را دقیق‌تر مستندسازی کند و حتی در مراحل رسیدگی، ابزار کنترلی در اختیار نهادهای نظارتی قرار دهد. ثبت عمومی آرای صادرشده یا مراحل بررسی پرونده‌ها، نظارت مردمی و رسانه‌ای را نیز تسهیل می‌کند.

قراردادهای هوشمند (Smart Contracts) در بستر بلاک‌چین می‌توانند ابزار مهمی برای جلوگیری از نقض تعهدات مالی باشند. پلیس می‌تواند از این قراردادها برای پیگیری دعاوی مرتبط با وام، تعهدات پرداخت، بیمه و حتی معاملات ملکی استفاده کند. این قراردادها به‌صورت خودکار اجرا می‌شوند و می‌توانند به‌عنوان سند معتبر در تحقیقات پلیسی و قضایی استفاده شوند.

۲. استفاده از بلاک‌چین در نظام بانکی با رویکرد پلیس اقتصادی

نظام بانکی ایران، با چالش‌هایی نظیر پول‌شویی، انتقال غیرقانونی سرمایه، فساد در اعطای تسهیلات و حملات سایبری مواجه است. پلیس اقتصادی، برای رصد و پیشگیری از این جرایم، نیازمند دسترسی به داده‌های دقیق، آنی و قابل‌ردیابی است. بلاک‌چین می‌تواند دسترسی به این نوع اطلاعات را بدون نیاز به واسطه و با شفافیت بالا در اختیار پلیس قرار دهد.

یکی از مهم‌ترین ویژگی‌های بلاک‌چین، ثبت عمومی و غیرقابل‌تغییر تمامی تراکنش‌هاست. این ویژگی باعث می‌شود که پلیس بتواند مسیر گردش وجوه مشکوک را از ابتدا تا انتها ردیابی کند. در مواردی که مجرمان سعی دارند با استفاده از حساب‌های واسطه پول‌شویی کنند، بلاک‌چین با شفاف‌سازی زنجیره تراکنش‌ها، الگوهای مشکوک را برای تیم‌های تحلیلگر پلیس قابل‌شناسایی می‌سازد.

حملات سایبری به سامانه‌های بانکی در سال‌های اخیر، منجر به سرقت اطلاعات حساب‌ها و ایجاد تراکنش‌های غیرمجاز شده است. استفاده از بلاک‌چین در معماری داده‌های بانکی، به دلیل رمزنگاری قوی و تمرکززدایی، سطح نفوذپذیری را کاهش می‌دهد و دسترسی غیرمجاز به داده‌ها را تقریباً غیرممکن می‌کند. این امر به پلیس فتا امکان می‌دهد تا از وقوع جرایم جلوگیری کند و در صورت وقوع، مسیر نفوذ را با دقت بیشتری تحلیل کند.

اعطای وام‌های کلان بدون تضمین کافی یکی از منابع فساد در نظام بانکی ایران است. پلیس اقتصادی می‌تواند با نظارت بر سامانه‌های مبتنی بر بلاک‌چین، تمام مراحل درخواست، تصویب، تضمین و بازپرداخت وام‌ها را رصد کند. در این سامانه‌ها، هر اقدام و امضا ثبت و غیرقابل‌انکار است؛ بنابراین پیگیری جرایم در این زمینه بسیار ساده‌تر خواهد بود.

بلاک‌چین با کاهش نقش واسطه‌ها در فرآیندهای بانکی، امکان پردازش آنی تراکنش‌ها را فراهم می‌کند. پلیس می‌تواند با دسترسی هم‌زمان به اطلاعات، پیش از وقوع جرم یا پول‌شویی، هشدارهای لازم را دریافت کند و واکنش سریع‌تری نشان دهد.

فهرست منابع

الف) منابع فارسی

۱- تذهیبی، فریده، **پیامدهای پول‌شویی و راهبردهای کنترلی با رویکرد به اسناد بین‌المللی**، در مجموعه سخنرانی‌ها و مقالات همایش بین‌المللی مبارزه با پول‌شویی، چاپ اول، تهران: نشر وفاق، ۱۳۹۱

۲- خواجوی، ملیحه، رضایی، ابراهیم و خداویسی، حسن، **برآورد پول‌های کثیف و بررسی پیامدهای آن در اقتصاد ایران: رهیافت آزمون کرانه‌ها**، فصلنامه اقتصاد مقداری، دوره ۷، شماره ۴، ۱۳۹۹

۳- رهبر، فرهاد و میرزاوند، فضل‌الله، **پول‌شویی و روش‌های مقابله با آن**، تهران: انتشارات و چاپ دانشگاه تهران، ۱۳۹۸

۴- زراعت، عباس، **جرایم علیه اموال**، تهران: انتشارات فکرسازان، چاپ سوم، ۱۳۹۶

۵- صادقی، بهروز، گوگردچیان، احمد و شهبازی، نجفعلی، **تحلیل تجربی آثار پول‌شویی بر رشد اقتصادی، مخارج دولت و نابرابری درآمدی در ایران**، پژوهش‌های راهبردی نظم و امنیت اجتماعی، شماره ۱، چاپ اول، ۱۴۰۱

۶- غلامی، علی و پروبخش، محمدعلی، **مبارزه با پول‌شویی در قوانین ایران و اسناد بین‌المللی**، فصلنامه علمی-تخصصی مقالات اقتصاد اسلامی، سال چهارم، شماره ۱، ۱۳۹۹

۷- گلدوزیان، ایرج، **حقوق جزای اختصاصی**، تهران: انتشارات جهاد دانشگاهی، چاپ اول، ۱۳۹۹

۸- کیانی‌زاده، حسین و بکی حسکویی، مرتضی، **بررسی زمینه‌های پول‌شویی و تأثیرات آن بر رشد اقتصادی در ایران**، نشریه پژوهشی دانشگاه امام صادق (ع)، شماره ۲۷، ۱۳۹۴

۹- میرمحمدصادقی، حسین، **حقوق جزای اختصاصی (جرایم علیه اشخاص)**، تهران: انتشارات میزان، چاپ بیست و یکم، ۱۳۹۴

ب) کتاب‌های انگلیسی

۱۰- Antonopoulos, A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media. ۲۰۱۷

۱۱- Casey, M. J. & Vigna, P. The Truth Machine: The Blockchain and the Future of Everything. St. Martin's Press. ۲۰۱۸

۱۲- Chuen, D. L. K. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press. ۲۰۱۵

۱۳- Davidson, S. De Filippi, P. & Potts, J. Economics of Blockchain. Edward Elgar Publishing. ۲۰۱۸

۱۴- Goodell, G. & Aste, T. Financial Crime Prevention with Blockchain: A Regulatory Perspective. Routledge. ۲۰۲۰

۱۵- Lee, D. K. C. Handbook of Blockchain, Digital Finance, and Inclusion, Volume ۲. Academic Press. ۲۰۱۹

۱۶- Mougayar, W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley. ۲۰۱۶

۱۷- Morabito, V. Business Innovation through Blockchain: The Case of Financial Services. Springer. ۲۰۱۷

۱۸- Nakamoto, SBitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: https://bitcoin.org/bitcoin.pdf. ۲۰۰۸

۱۹- Swan, M. Blockchain: Blueprint for a New Economy. O'Reilly Media. ۲۰۱۵

۲۰- Tapscott, D. & Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio Penguin. ۲۰۱۶

۲۱- Werbach, K. The Blockchain and the New Architecture of Trust. MIT Press. ۲۰۱۸

۲۲- Zohar, A. Bitcoin: The Digital Currency of the Future. Elsevier. ۲۰۱۵

ج) مقالات انگلیسی

۲۳- Adrian, T. & Mancini-Griffoli, T. The Rise of Digital Money and the Role of Central Banks. IMF Working Paper. ۲۰۱۹

۲۴- Allen, D. W. The Economic Impact of Blockchain Technology. Journal of Business Ethics, ۱۶۲(۲), ۳۱۱-۳۲۹. ۲۰۱۹

۲۵- Atzori, M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Journal of Governance and Regulation, ۶(۱), ۴۵-۶۲. ۲۰۱۷

۲۶- Basel Committee on Banking Supervision. Implications of Fintech Developments for Banks and Bank Supervisors. Bank for International Settlements Report. ۲۰۱۸

۲۷- Böhme, R. Christin, N. Edelman, B. & Moore, T. Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, ۲۱۳-۲۳۸. ۲۰۱۵

٢٨- Cachin, C. Architecture of the Hyperledger Blockchain Fabric. IBM Research Report. ٢٠١٦

٢٩- Catalini, C. & Gans, J. S. Some Simple Economics of the Blockchain. NBER Working Paper No. ٢٢٩٥٢. ٢٠١٧

٣٠- Chuen, D. L. K. Guo, L. & Wang, Y. Cryptocurrency: A New Investment Opportunity? Journal of Alternative Investments, ٢٠(٣), ١٦-٤٠. ٢٠١٧

٣١- Cong, L. W. & He, Z. Blockchain Disruption and Smart Contracts. Review of Financial Studies, ٣٢(٥), ١٧٥٤-١٧٩٧. ٢٠١٩

٣٢- Deloitte. The Impact of Blockchain on Financial Crime. Deloitte Research Report. ٢٠٢٠

٣٣- De Filippi, P. & Wright, A. Blockchain and the Law: The Rule of Code. Harvard University Press. ٢٠١٨

٣٤- Eyal, I. Blockchain Technology: Transforming Financial Services? Communications of the ACM, ٦٠(٩), ٢٩-٣١. ٢٠١٧

٣٥- Gandal, N. Hamrick, J. T. Moore, T. & Oberman, T. Price Manipulation in the Bitcoin Ecosystem. Journal of Monetary Economics, ٩٥, ٨٦-١٠٢. ٢٠١٨

٣٦- Gikay, A. A. Regulating Decentralized Cryptocurrencies under Payment Services Law: Lessons from European Union Law. Journal of Law, Technology & Policy, ٢٠١٨(١), ٣٣-٦٤. ٢٠١٨

٣٧- Hendrickson, J. R. & Luther, W. J. Banning Bitcoin. Journal of Economic Behavior & Organization, ١٧٢, ١٥٣-١٧٢. ٢٠٢٠

٣٨- Hileman, G. & Rauchs, M. Global Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance. ٢٠١٧

٣٩- Houben, R. & Snyers, A. Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. European Parliament Study. ٢٠١٨

٤٠- Iansiti, M. & Lakhani, K. R. The Truth About Blockchain. Harvard Business Review, ٩٥(١), ١١٨-١٢٧. ٢٠١٧

٤١- Möser, M. & Böhme, R. Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. ACM Conference on Computer and Communications Security, ٣٨-٤٩. ٢٠١٧

٤٢- Narayanan, A. Bonneau, J. Felten, E. Miller, A. & Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press. ٢٠١٦

٤٣- OECD. The Tokenisation of Assets and Potential Implications for Financial Markets. OECD Working Papers on Finance, Insurance and Private Pensions. ٢٠٢٠

٤٤- Peters, G. W. & Panayi, E. Understanding Modern Banking Fraud: The Case of Blockchain Technology. Journal of Financial Crime, ٢٣(٤), ٥٦٧-٥٩٢. ٢٠١٦

٤٥- Schrepel, T. Blockchain Antitrust: The Law and Economics of Trustless Collaboration. Berkeley Technology Law Journal, ٣٤(٢), ١١٢-١٦٠. ٢٠١٩

٤٦- Trautman, L. J. Is Disruptive Blockchain Technology the Future of Financial Services? The Journal of Corporation Law, ٤٢(٤), ٩٠٥-٩٧١. ٢٠١٦

٤٧- Yeoh, P. Regulatory Issues in Blockchain Technology. Journal of Financial Regulation and Compliance, ٢٥(٢), ١٩٦-٢٠٨. ٢٠١٧

٤٨- Zohar, A. Bitcoin: Under the Hood. Communications of the ACM, ٥٨(٩), ٢٠١٥

٤٩- Zyskind, G. Nathan, O. & Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, ٢٠١٥