امنیت رمزارزها در فضای سایبر و چالش‌های پیش‌رو

چکیده

در دهه‌های اخیر، گسترش سریع ارزهای دیجیتال به‌ویژه بیت‌کوین و اتریوم، به همراه توسعه فناوری بلاک‌چین، تحولاتی اساسی در نظام‌های مالی جهانی ایجاد کرده است. این تحولات هرچند فرصت‌های متعددی برای توسعه اقتصادی و ارتقای کارایی نظام‌های مالی فراهم آورده، اما در عین حال، چالش‌های امنیت سایبری پیچیده و نوظهوری را نیز به همراه داشته است .مسئله اصلی در مواجهه با ارزهای دیجیتال، شناسایی جامع چالش‌های امنیتی ناشی از ماهیت غیرمتمرکز و ناشناس بودن تراکنش‌ها و نیز بهره‌گیری از ظرفیت‌های فناوری بلاک‌چین به‌عنوان ابزاری کارآمد برای تقویت امنیت سایبری است.

پژوهش حاضر با رویکرد نظری و به شیوه توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای، به بررسی ابعاد مختلف این موضوع پرداخته است .هدف اصلی مقاله، شناسایی و تحلیل جرائم مالی و سایبری مرتبط با ارزهای دیجیتال، تبیین چالش‌های امنیتی ناشی از توسعه این فناوری، و بررسی فرصت‌های فناورانه برای مقابله با تهدیدات آن است. یافته‌های پژوهش نشان می‌دهد که رمزارزها علاوه بر فراهم‌سازی بستر مناسب برای وقوع جرائمی نظیر پول‌شویی، تأمین مالی تروریسم، سرقت دارایی‌های دیجیتال، حملات فیشینگ و باج‌افزارها، فرصت‌های مهمی نیز برای ارتقای امنیت سایبری ارائه می‌کنند .به‌ویژه، فناوری بلاک‌چین با قابلیت ثبت غیرقابل تغییر تراکنش‌ها و ایجاد شبکه‌های غیرمتمرکز ایمن، ظرفیت بالایی در افزایش شفافیت و اعتماد کاربران دارد. همچنین، استفاده از هوش مصنوعی و یادگیری ماشین برای تحلیل رفتارهای مشکوک در تراکنش‌های رمزارزی، راهکاری مؤثر برای پیشگیری از جرائم مالی دیجیتال به شمار می‌رود. نتیجه کلی این پژوهش تأکید بر ضرورت تدوین استراتژی‌های جامع و بین‌رشته‌ای شامل ابعاد حقوقی، فناورانه و آموزشی برای حفاظت از اطلاعات شخصی و دارایی‌های دیجیتال کاربران و همچنین ایجاد بسترهای قانونی و فناورانه مناسب برای بهره‌برداری بهینه از فرصت‌های رمزارزها در راستای توسعه اقتصادی کشورها است. علاوه بر این، همکاری‌های بین‌المللی، استانداردسازی مقررات و سرمایه‌گذاری در تحقیقات نوین امنیت سایبری و فناوری بلاک‌چین از الزامات اساسی مدیریت این پدیده نوظهور محسوب می‌شود. در نهایت، تحقق امنیت پایدار در حوزه ارزهای دیجیتال مستلزم رویکردی جامع‌نگر و هم‌افزا میان دولت‌ها، پژوهشگران و فعالان صنعت فناوری اطلاعات است.

کلیدواژه‌ها: امنیت سایبری، ارزهای دیجیتال، جرائم، چالش‌ها، فضای مجازی

مقدمه

در عصر تحول دیجیتال، ارزهای دیجیتال به‌ویژه بیت‌کوین و اتریوم به پدیده‌ای تأثیرگذار در نظام‌های مالی جهان تبدیل شده‌اند .این رمزارزها با تکیه بر فناوری بلاک‌چین و ویژگی‌هایی همچون غیرمتمرکز بودن، ناشناس ماندن تراکنش‌ها و امنیت رمزنگاری‌شده، امکان انجام تراکنش‌های مالی سریع، ایمن و بدون واسطه را در سطح جهانی فراهم آورده‌اند. با این حال، ظهور ارزهای دیجیتال نه تنها فرصت‌های قابل توجهی برای توسعه اقتصادی ایجاد کرده، بلکه چالش‌های امنیتی و تهدیدات سایبری جدیدی را نیز به همراه داشته است.

امروزه سرقت رمزارزها، حملات سایبری به صرافی‌های دیجیتال، کلاهبرداری‌های فیشینگ، باج‌افزارها و پول‌شویی از جمله مهم‌ترین تهدیدات امنیت سایبری در حوزه رمزارزها محسوب می‌شوند. طبق گزارش شرکت(Chainalysis (2022 ، حجم جرائم مالی مرتبط با ارزهای دیجیتال در سال ۲۰۲۲ به بیش از ۲۰ میلیارد دلار رسیده است که این رقم، اهمیت تدوین تدابیر امنیتی کارآمد برای مقابله با آسیب‌پذیری‌های این حوزه را آشکار می‌سازد.

در عین حال، همین فناوری می‌تواند فرصت‌های نوینی برای ارتقای امنیت سایبری ایجاد کند .بهره‌گیری از بلاک‌چین برای احراز هویت کاربران، تضمین صحت تراکنش‌ها و ایجاد بسترهای توزیع‌شده غیرقابل نفوذ از جمله این فرصت‌هاست. با وجود این، ماهیت پیچیده و ناشناس بودن تراکنش‌های رمزارزها، ردیابی فعالیت‌های غیرقانونی و اعمال مقررات کارآمد را دشوار کرده است؛ مسئله‌ای که امکان استفاده از رمزارزها برای تأمین مالی فعالیت‌های غیرقانونی و تروریستی را افزایش می‌دهد.

مسئله اصلی پژوهش حاضر، بررسی چالش‌های امنیتی ارزهای دیجیتال و تحلیل تأثیرات آن‌ها بر امنیت سایبری است .سؤال کلیدی این پژوهش عبارت است از:چگونه می‌توان با بهره‌گیری از فناوری‌های نوین مرتبط با ارزهای دیجیتال، چالش‌های امنیت سایبری را مدیریت کرد و در عین حال از فرصت‌های ارائه‌شده توسط این فناوری‌ها برای ارتقای امنیت و توسعه اقتصادی بهره‌برداری نمود؟

اهمیت این پژوهش در دو بعد قابل تحلیل است. نخست، رشد سریع استفاده از رمزارزها در سراسر جهان و تأثیر آن‌ها بر نظام‌های مالی بین‌المللی که امنیت این فناوری را به یکی از اولویت‌های اصلی دولت‌ها و نهادهای امنیتی تبدیل کرده است. دوم، پیچیدگی فناوری بلاک‌چین و ناشناس بودن تراکنش‌ها که آن را به ابزاری برای دور زدن نظام‌های مالی رسمی و ارتکاب جرائم مالی تبدیل کرده و نیازمند تدوین راهکارهای جامع حقوقی، فناورانه و آموزشی است.هدف پژوهش حاضر شناسایی و تحلیل جامع چالش‌ها، تهدیدات و فرصت‌های امنیت سایبری در حوزه ارزهای دیجیتال و ارائه راهکارهای نظری و کاربردی برای مدیریت این مخاطرات است.

نوآوری مقاله در رویکرد تلفیقی آن است؛ به‌گونه‌ای که ضمن بررسی ادبیات موجود، با تأکید بر فناوری‌های نوین همچون هوش مصنوعی و الگوریتم‌های یادگیری ماشین، راهکارهایی نوین برای مقابله با تهدیدات امنیتی رمزارزها ارائه می‌دهد و بدین ترتیب، از حالت مروری صرف فراتر می‌رود.این پژوهش با روش توصیفی-تحلیلی و مبتنی بر مطالعات کتابخانه‌ای انجام شده است و تلاش دارد با مروری

انتقادی و تحلیلی، درکی جامع از روابط میان ارزهای دیجیتال و امنیت سایبری فراهم سازد و پیشنهادهایی کارآمد برای پژوهشگران، سیاست‌گذاران و فعالان این حوزه ارائه کند.

۱-مفهوم ارز دیجیتال

ارز دیجیتال یا پول الکترونیک به عنوان یک ارزش پولی ذخیره‌شده که به صورت دیجیتالی نگهداری می‌شود و برای انجام تراکنش‌های فوری و آنلاین در دسترس قرار دارد، عمل می‌کند و به عنوان جایگزین الکترونیکی برای سکه و اسکناس مطرح است. استفاده از پول الکترونیک به واسطه اینترنت منجر به کاهش هزینه‌های تبادل مالی می‌شود و همچنین این امکان را فراهم می‌کند که تراکنش‌ها بدون محدودیت جغرافیایی انجام شود. (بشارت نیا،رحیمی،ذوالفقاری، ۱۳۹۰: ۱)

ارزهای دیجیتال، بر اساس فناوری رمزنگاری (کریپتوگرافی[1]) پایه‌ریزی شده‌اند و خلاف پول‌های فیزیکی ماهیتی مادی ندارند. این ارزها قابلیت خرید و فروش، و حتی استخراج آنها بدون محدودیت‌های جغرافیایی را فراهم می‌کنند. افراد می‌توانند به صورت مستقیم و بدون نیاز به واسطه در تراکنش‌های مالی از این ارزها استفاده کنند. این ارزهای دیجیتال در شبکه‌ای از کامپیوترها تعریف می‌شوند و مزیت آنها در حذف محدودیت‌های جغرافیایی و امکان انجام تراکنش‌های مالی در سریع‌ترین زمان ممکن و بدون نیاز به دخالت نهادهای واسطه وجود دارد. این ارزها به‌صورت غیرمتمرکز عمل می‌کنند، به این معنا که تمام فرایندهای مرتبط با آنها از جمله انتشار و تأیید تراکنش‌ها توسط افراد مختلف در شبکه تحت علم رمزنگاری و مبانی ریاضی کنترل و مدیریت می‌شود، و بدون نیاز به واسطه‌های مرکزی انجام می‌پذیرد. (واحدزاده، ملک‌زاده، ۱۳۹۹: ۳۶)

ارزهای رمزنگاری‌شده متشکل از مجموعه‌ای از کدها هستند که ارزش پولی را در خود نگه می‌دارند ارزهای دیجیتال در نرم‌افزاری به نام کیف پول ارز دیجیتال نگهداری می شوند که با توجه به انتزاعی بودن ارز دیجیتال رمزهای خصوصی و خاص موجود برای هر ارز دیجیتال در کیف پول صاحب ارز دیجیتال ذخیره‌شده تا با حفظ مالکیت انجام تراکنش‌های ارسالی و دریافتی را تسهیل کند.

فرآیند غیرمتمرکز سازی در ارزهای دیجیتال توسط فناوری زنجیره بلوکی به انجام می‌رسد. در ارزهای دیجیتال مانند بیت کوین، داده‌ها به صورت دائمی در اسناد کامپیوتری به نام "بلوک" ثبت می‌شوند. به عبارت دیگر، تراکنش‌های شبکه ارزهای دیجیتال در بلوک‌ها ثبت می‌شوند، و هر بلوک تمامی تراکنش‌هایی را که در بلوک قبلی وارد نشده‌اند، به ثبت می‌رساند. برای جلوگیری از حذف یک بلوک یا دست‌کاری در زنجیره بلوکی، اطلاعاتی از بلوک قبلی و آدرس بلوک بعدی نیز در هر بلوک قرار می‌گیرند. به این ترتیب، هر بلوک معتبری مانند یک صفحه از یک دفتر کل است که حاوی اطلاعاتی است که یک بار ثبت شده‌اند و امکان حذف، تغییر و دست‌کاری آن‌ها وجود ندارد.(قوامی پور، محمودی، ۱۴۰۲: ۲۲)

تکنولوژی بلاک‌چین[2] از دو واژه "بلوک[3]" و "زنجیره[4]" تشکیل شده است. این تکنولوژی به واقع یک دفتر کل توزیع‌شده[5] و مشترک محسوب می‌شود که از طریق الگوریتم‌های ریاضی و محاسباتی پیچیده و با استفاده از تکنولوژی رمزنگاری هسته‌ای، سوابق الکترونیکی ارزهای دیجیتال از جمله تراکنش‌ها، انتقال‌ها و دیگر اطلاعات را ذخیره می‌کند. با توجه به استفاده از رمزنگاری، امکان دست‌کاری و

---

[1] cryptography

[2] Blockchain

[3] Block

[4] Chain

[5] Distributed Ledger

حذف اطلاعات ثبت‌شده تقریباً غیرممکن می‌شود و به همین دلیل این بستر به عنوان یک سیستم بسیار امن تلقی می‌شود. (ریاضی مند، ۱۳۹۷: ۲۹)

فناوری بلاک‌چین، در برخی از ارزهای دیجیتال مانند بیت کوین، از قدرت محاسباتی مجموعه‌ای از کامپیوترهای غیرمتمرکز برای تأیید تراکنش‌ها و استخراج ارزهای جدید با استفاده از الگوریتم‌های خاص استفاده می‌کند. ارزهای دیجیتال به‌واسطه این کامپیوترهای غیرمتمرکز از سراسر جهان تولید و نگهداری می‌شوند، و هیچ شرکت یا دولت خاصی مالکیت و کنترل آن‌ها را ندارد. (ماتسورا، ۱۳۹۷: ۱۵۲)

۲-نقش فضای مجازی در ترویج ارزهای دیجیتال و چالش‌های امنیتی مرتبط

فضای مجازی به‌عنوان بستری پرنفوذ در دنیای دیجیتال امروز، نقشی بی‌بدیل در توسعه و ترویج ارزهای دیجیتال ایفا می‌کند. ظهور شبکه‌های اجتماعی، پلتفرم‌های تعاملی و رسانه‌های دیجیتال، انقلابی در نحوه ارائه اطلاعات و تعامل کاربران به وجود آورده و زمینه‌ساز رشد ارزهای دیجیتال به‌عنوان یکی از مهم‌ترین نوآوری‌های اقتصادی قرن حاضر شده است. با این حال، این توسعه همواره با چالش‌های امنیتی پیچیده و گسترده همراه بوده است.

۲-۱-تأثیر فضای مجازی بر ترویج ارزهای دیجیتال

شبکه‌های اجتماعی و رسانه‌های دیجیتال، به‌ویژه پلتفرم‌هایی مانند توییتر، تلگرام، اینستاگرام و یوتیوب، به ابزاری اصلی برای بازاریابی، آموزش و تعامل پیرامون ارزهای دیجیتال تبدیل شده‌اند. پروژه‌های ارز دیجیتال از این ابزارها برای اطلاع‌رسانی، جذب سرمایه‌گذاران و افزایش آگاهی عمومی بهره می‌برند. نقش فضای مجازی را می‌توان در سه محور اصلی تبیین کرد:

۱. **تبلیغات و بازاریابی مؤثر**

فضای مجازی به دلیل سرعت انتشار محتوا و دسترسی گسترده، ابزاری قدرتمند برای معرفی پروژه‌های ارز دیجیتال است. تیم‌های توسعه‌دهنده از تبلیغات هدفمند، کمپین‌های اجتماعی و محتوای چندرسانه‌ای برای جلب توجه مخاطبان استفاده می‌کنند. این قابلیت‌ها به‌ویژه در ایجاد اعتماد و معرفی پروژه‌های نوظهور بسیار مؤثر بوده است.

۲. **افزایش آگاهی و آموزش عمومی**

وب‌سایت‌های تخصصی، کانال‌های یوتیوب و انجمن‌های آنلاین، به کاربران امکان دسترسی به منابع آموزشی درباره ارزهای دیجیتال را می‌دهند. این آموزش‌ها شامل مفاهیم اولیه، فناوری بلاک‌چین، نحوه انجام تراکنش‌ها و تحلیل بازار است که به افزایش آگاهی عمومی و پذیرش این فناوری کمک می‌کند.

۳. **ایجاد و تقویت جوامع تخصصی**

پلتفرم‌های فضای مجازی مانند ردیت و دیسکورد، امکان ایجاد جوامع تخصصی متشکل از کاربران حرفه‌ای و علاقه‌مند به ارزهای دیجیتال را فراهم کرده‌اند. این جوامع به تبادل اطلاعات، ارائه تحلیل‌های دقیق و بحث درباره روندهای بازار می‌پردازند و نقشی محوری در تصمیم‌گیری کاربران ایفا می‌کنند.

۲-۲-چالش‌های امنیتی مرتبط با ترویج ارزهای دیجیتال در فضای مجازی

همزمان با فرصت‌های بی‌سابقه‌ای که فضای مجازی برای توسعه ارزهای دیجیتال ایجاد کرده است، بستر مناسبی نیز برای شکل‌گیری تهدیدات امنیتی و جرائم سایبری فراهم شده است. مهم‌ترین چالش‌های امنیتی عبارت‌اند از:

۱. **تبلیغات جعلی و کلاهبرداری**

فضای مجازی به دلیل نبود نظارت کافی، محلی مناسب برای انتشار تبلیغات جعلی و پروژه‌های کلاهبرداری شده است. طرح‌های پانزی، کیف‌پول‌های تقلبی و پروژه‌های فاقد اعتبار از جمله تهدیداتی هستند که کاربران بی‌تجربه را هدف قرار می‌دهند.

۲. **حملات فیشینگ و سرقت اطلاعات**

یکی از روش‌های رایج کلاهبرداری در فضای مجازی، حملات فیشینگ است. کلاهبرداران از وب‌سایت‌های جعلی و لینک‌های مخرب برای سرقت اطلاعات کاربری و کلیدهای خصوصی کاربران استفاده می‌کنند و دارایی‌های آن‌ها را به خطر می‌اندازند.

۳. **پوشش جرائم با استفاده از ناشناس بودن تراکنش‌ها**

ویژگی ناشناس بودن در تراکنش‌های ارزهای دیجیتال، در کنار ماهیت غیرمتمرکز فضای مجازی، این فناوری را به ابزاری مناسب برای پول‌شویی و تأمین مالی جرائم تبدیل کرده است. این موضوع به چالشی جدی برای قانون‌گذاران و نهادهای نظارتی بدل شده است.

۴. **نبود زیرساخت‌های نظارتی شفاف**

فضای مجازی هنوز به طور کامل تحت چارچوب‌های قانونی مشخص و نظارت دقیق قرار نگرفته است. این خلأ قانونی باعث گسترش فعالیت‌های مجرمانه و بهره‌برداری نادرست از ارزهای دیجیتال در این بستر می‌شود.

فضای مجازی در ترویج ارزهای دیجیتال نقشی کلیدی دارد و به‌عنوان یک بستر پویا، موجب رشد آگاهی عمومی و تقویت تعاملات پیرامون این فناوری شده است. با این حال، چالش‌های امنیتی مرتبط با این فضا نیازمند توجه ویژه از سوی نهادهای نظارتی، دولت‌ها و فعالان حوزه فناوری است. تقویت قوانین و نظارت بر فعالیت‌های مجازی، توسعه فناوری‌های امنیتی و آموزش کاربران از جمله اقداماتی است که می‌تواند ترویج ارزهای دیجیتال را در فضای مجازی ایمن‌تر و پایدارتر کند.

۳-مزایا و معایب امنیتی ارزهای دیجیتال دربستر فضای سایبری

بررسی جامع مزایا و معایب ارزهای دیجیتال می‌تواند به عنوان یک راهنمای مفید برای سیاست‌گذاری و قانون‌گذاری عمل کند. با شناخت مزایا، می‌توان به سمت تنظیمات قانونیی که به ارزهای دیجیتال اجازه استفاده مسئولانه را می‌دهند، پیش رفت. همچنین با بررسی معایب و چالش‌هایی که کاربران در این حوزه با آن مواجه هستند، می‌توان برای حل این مسائل اقدام کرد و قوانین دقیقتری را اجرا نمود. در پی افزایش مشکلات اقتصادی و اجتماعی در اکثر کشورها، استفاده گسترده از ارزهای دیجیتال، و تبلیغات فراوان در خصوص کسب درآمد از آن‌ها، تعداد افرادی که اطلاعات کافی برای انجام معاملات ندارند و فقط به دنبال کسب سود سریع هستند، افزایش می‌یابد. بررسی معایب به علاوه از مزایای این ارزها می‌تواند راهنمایی کننده برای افرادی باشد که می‌خواهند وارد این بازار پرفراز و نشیب شوند.

لازم به ذکر است که با توجه به افزایش روزافزون ارزهای دیجیتال و تنوع آن‌ها، امکان بررسی جامع مزایا و معایب تمامی این ارزها وجود ندارد. عواملی مانند شدت و ضعف هر یک از مزایا و معایب گفته‌شده در انواع ارزهای دیجیتال متفاوت خواهد بود. اما این نکات بارز ترین ویژگی‌های بسیاری از ارزهای دیجیتال را تشکیل می‌دهند(عبادی لمر، ۱۳۹۹: ۲۲)

۳-۱-مزایای امنیتی ارزهای دیجیتال

امنیت و شفافیت: ارزهای دیجیتال برخاسته از تکنولوژی بلاک‌چین، از امنیت و شفافیت بالایی برخوردارند. در این سیستم، تراکنش‌ها به‌طور شفاف در بلاک‌چین ثبت می‌شوند، اما با رعایت حریم خصوصی کاربران. این به این معناست که هویت خریدار و فروشنده در تراکنش‌ها مخفی می‌ماند. هر کاربر قادر است به معاملات خود و تاریخچه معاملات کلی سیستم نظارت داشته باشد. اطلاعات هر تراکنش به صورت رمزنگاری شده در بلاک‌های جداگانه ذخیره می‌شوند و سپس بلاک‌های این تراکنش‌ها به صورت یک زنجیره اطلاعاتی ترکیب می‌شوند. این شفافیت به کاربران امکان می‌دهد که بدون دسترسی به جزئیات هویتی معامله‌گران، به طور کلی روند بازار را نظارت کنند.

در ارزهای دیجیتال، یکی از ویژگی‌های بارز آنها عدم توقف یا بلوکه شدن توسط دولت‌ها یا نهادهای مالی داخلی یا بین‌المللی است. این ارزها مستقل از سیاست‌ها و تحریم‌های بانکی کشورها عمل می‌کنند. همچنین به دلیل ویژگی‌های خصوصی ارزهای دیجیتال، امکان تشخیص و تعقیب فرستنده و گیرنده در تراکنش‌ها به سختی امکان‌پذیر است. این مزیت به ویژه در شرایط تحریم بانکی که ایران و بسیاری از کشورها با آن مواجه هستند، اهمیت بسیاری دارد و امکان ادامه تعاملات اقتصادی را بدون تداخل تحریم‌ها فراهم می‌کند. (میرغفوری، صیادی، دهقانی زاده، ۱۳۹۹: ۸-۱۰)

انتقال مستقیم همتا به همتا و بدون واسطه: شبکه همتا به همتا یک نوع شبکه است که توسط رایانه‌های متصل به اینترنت تشکیل می‌شود و از ساختار توزیع‌شده استفاده می‌کند. در این نوع سیستم، اطلاعات تنها از طریق اینترنت و نرم‌افزارهای مخصوصی که برای اتصال به شبکه استفاده می‌شوند، منتقل می‌شود. هر رایانه در این شبکه هم وظیفه‌های سرور و هم کاربر را انجام می‌دهد و هر کاربر به عنوان یک نود در این شبکه شناخته می‌شود.

تکنولوژی بلاک‌چین نیز بر روی شبکه همتا به همتا عمل می‌کند. این به این معناست که اطلاعات بدون نیاز به وجود یک نقطه مرکزی یا سرور مرکزی به دست می‌آید. این امر باعث کاهش خطراتی مانند هک شدن و از بین رفتن اطلاعات می‌شود و همچنین اطلاعات در این شبکه تحت نظر هیچ نهاد نظارتی قرار ندارد.

ارزهای دیجیتال با استفاده از شبکه همتا به همتا یا نظیر به نظیر به راحتی از یک فرد یا سازمان به دیگری منتقل می‌شوند، بدون نیاز به ارتباط با یک سرور مرکزی خاص. این روش پرداخت رمزدار و غیرمتمرکز این امکان را فراهم می‌کند که کاربران بدون نیاز به مراجعه به نهادهای واسطه مثل بانک‌ها، بدون پرداخت کارمزد و بدون نیاز به مجوزهای مختلف، تراکنش‌های مالی را انجام دهند. این ویژگی در کشورهایی که تحت تحریم قرار دارند، مانند ایران، اهمیت زیادی دارد، زیرا به توسعه تجارت بین‌المللی و افزایش رونق اقتصاد داخلی کمک می‌کند. (باغانی،۱۳۹۹: ۱۶۲)

سرعت‌بالا و هزینه پایین: در سیستم ارزهای دیجیتال، انجام تجارت‌های بین‌المللی و خریدهای خارجی با هزینه‌ها و کارمزدهای کمتری انجام می‌شود. به دلیل عدم وجود واسطه‌های مالی و انتقال همتا به همتا، معاملات با کارمزد بسیار کمتری صورت می‌گیرد. در صرافی‌های ارزهای دیجیتال، سفارش‌گذار و سفارش‌گیرنده کمترین کارمزد را برای انجام معاملات و تراکنش‌ها پرداخت می‌کنند.

انتقال پول در سیستم ارزهای دیجیتال به سرعت بسیار بالاتری انجام می‌شود نسبت به معاملات بانکی، و این سرعت به نحوی است که انتقال‌ها به‌صورت فردبه‌فرد به سرعت انجام می‌شوند. در صورت نیاز، با پرداخت کارمزد بیشتر، سرعت انتقال می‌تواند افزایش یابد. حتی معاملات و تراکنش‌های با حجم بالا در کمترین زمان ممکن و بدون نیاز به فرآیندهای پیچیده معاملاتی انجام می‌شود.

یک ویژگی مهم دیگر ارزهای دیجیتال، سرعت بالای آن‌ها در تغییرات قیمتی است. به دلیل نوسانات و تغییرات لحظه‌ای در ارزهای دیجیتال، انجام معاملات در سریع‌ترین زمان ممکن الزامی است تا از افت فرصت‌های سودآور در بازار جلوگیری شود.

تمام این مزایا در حالی رخ می‌دهند که در سیستم مالی کنونی کشورها به دلیل وجود واسطه‌های مالی زیاد، بیشترین کارمزدها و مشکلات مرتبط با قوانین و مقررات متعدد، انجام تراکنش‌های مالی به خصوص در حجم بالا و بین‌المللی را پیچیده و هزینه‌بر می‌کند.(خورسندی، ۱۳۹۸: ۴۴)

همچنین می‌توان از سایر مزایای ارزهای دیجیتال به حفظ محرمانگی و حریم خصوصی، قابلیت دریافت مالیات، آزادی در پرداخت و دسترسی بین‌المللی، بی طرفی، هزینه تراکنش صفر یا بسیار کم، عدم وجود فرد ثالث، عدم وجود محدودیت مکانی و زمانی و سادگی اشاره کرد. (ارزانیان، مظلوم رهنی، ۱۳۹۹: ۷۶)

۳-۲-معایب امنیتی ارزهای دیجیتال

نامشخص بودن هویت: با توجه به اینکه ارزهای دیجیتال با استفاده از فرایند رمزنگاری و محاسبات پیچیده ریاضی در شبکه امنیت می‌افزایند، فرستنده و گیرنده در این ارزها قابل‌شناسایی نخواهد بود. این ویژگی می‌تواند فضای مناسبی برای برخی از جرائم اینترنتی ایجاد کند، به‌عنوان‌مثال، باج‌افزارها که یک نوع بدافزار هستند و اطلاعات حساب کاربری را قفل و هک می‌کنند. تنها یک کلید خصوصی می‌تواند اطلاعات را دوباره قابل‌خواندن کند. معمولاً هکرها این اطلاعات را پس از دریافت ارز دیجیتال از کاربر، به او بازمی‌گردانند. با توجه به مشخص نبودن هویت و غیرقابل‌پیگیری بودن آن، مجرمان می‌توانند به راحتی اهداف خود را دنبال کنند. این موضوع به‌ویژه در شرایط فعلی تحریم‌های اقتصادی برای ایران، فرصتی مناسب برای انجام تبادلات مالی در سطح بین‌المللی بدون شناسایی شدن فراهم می‌کند. (ارزانیان،مظلوم رهنی،۱۳۹۹ :۷۸)

عدم امکان بازیابی اطلاعات: مالکیت ارزهای دیجیتال به افرادی تعلق دارد که کلید خصوصی آن ارز دیجیتال را در اختیار داشته باشند. کلید خصوصی یک‌رشته متنی محرمانه از حروف و اعداد است که برای انجام معاملات و ارسال ارز به کیف پول دیگران استفاده می‌شود. این کلید خصوصی برای هر فرد با ساخت کیف پول مخصوص به خود در این شبکه به‌صورت تصادفی ایجاد می‌شود. با اشاره به این نکته که اطلاعات هویتی افراد در شبکه بلاک‌چین ثبت نمی‌شود، باید توجه داشت که هر کسی که به کلید خصوصی یک کیف پول دسترسی داشته باشد، قادر به دسترسی به ارزهای موجود در آن کیف پول و انجام معاملات با آن‌ها خواهد بود.

باید همچنین توجه داشت که ارزهای دیجیتال بر بستر فضای مجازی فعالیت می‌کنند و الکترونیکی هستند. به عنوان نمونه‌ای از چالش‌هایی که این ارزها ممکن است با آن مواجه شوند، می‌توان به هک‌شدن حساب‌ها و گم‌شدن کلیدهای خصوصی اشاره کرد. اگر کسی اطلاعات حساب و کلید خصوصی خود را از دست بدهد یا فراموش کند، ارز دیجیتال موجود در حسابش از دسترس خواهد خارج شد و به عنوان یک نقطه مهم باید توجه داشت که برخلاف بانک‌ها، در این سیستم غیرمتمرکز، هیچ نهادی برای رجوع به این ارزها و بازیابی اطلاعات حساب وجود ندارد. این امر می‌تواند به منزوی شدن سرمایه فرد و از دست رفتن آن منجر شود (واحدزاده، ملک‌زاده، ۱۳۹۹: ۱۱۰)

برگشت ناپذیری: ویژگی بارز ارزهای دیجیتال، برگشت‌ناپذیری تراکنش‌ها است. به این معنا که پس از انجام یک تراکنش، حتی در صورت وقوع خطا یا اشتباه، امکان بازگشت، برگرداندن و لغو تراکنش وجود ندارد. همچنین، هیچ نهادی وجود ندارد که بتواند به صورت مرکزی تراکنش‌ها را کنترل کند یا تصمیم به لغو آن‌ها بگیرد. برای تائید و ثبت هر تراکنش، ماینرها (اشخاص یا کامپیوترهایی

که در فرآیند تأیید تراکنش‌ها و ساخت بلاک‌های جدید در شبکه بلاک‌چین شرکت می‌کنند) تراکنش‌ها را در یک بلاک ثبت می‌کنند و بلاک‌ها به صورت مستمر به بلاک‌های قبلی اضافه می‌شوند. به عبارت دیگر، تاریخچه تمام تراکنش‌ها در بلاک‌های جدید ذخیره می‌شود و پس از ثبت نهایی، تراکنش‌ها از لحاظ فنی قابل تغییر یا حذف نخواهند بود.

همچنین، ارزهای دیجیتال به‌طور کلی بدون دخالت و نظارت سازمان‌ها یا دولت‌ها به فعالیت خود ادامه می‌دهند. این به معنای عدم وابستگی به سازمان‌ها یا نهادهای مالی مرکزی است و تراکنش‌ها در شبکه بلاک‌چین به صورت غیرمتمرکز انجام می‌شوند. همچنین، نامشخص بودن هویت دقیق افراد یا کیف پول‌های متعامل در تراکنش‌ها، از دیگر ویژگی‌های ارزهای دیجیتال است که می‌تواند حفظ حریم خصوصی کاربران را تضمین کند.

این ویژگی‌ها ارزهای دیجیتال را به یک سیستم پراز امنیت و اعتماد برای انجام تراکنش‌های مالی تبدیل کرده است، اما به دلیل عدم قابلیت بازگشت تراکنش‌ها، کاربران نیاز دارند که با دقت و احتیاط بیشتری تراکنش‌های خود را انجام دهند تا از وقوع خطاها جلوگیری کنند

بستری برای ارتکاب جرائم: ولشویی یک فرآیند است که به منظور پنهان کردن منشأ غیرقانونی اموال و پول‌ها انجام می‌شود و اغلب به‌صورت سازمان‌یافته اجرا می‌شود. برخورد با پولشویی همواره در دستور کار قانون‌گذاران و نهادهای مربوط به پیشگیری از جرائم مالی قرار دارد.(رهبر، ۱۳۸۲: ۴۲)

ارزهای دیجیتال، به خاطر ویژگی‌های خود مانند برگشت‌ناپذیری تراکنش‌ها و عدم افشای هویت طرفین تراکنش، ممکن است به‌عنوان یک بستر برای پولشویی مورداستفاده قرار گیرد. در ارزهای دیجیتال، هویت طرفین تراکنش به‌صورت نامشخص است، که این می‌تواند فرصت مناسبی برای انجام فعالیت‌های پولشویی فراهم کند. اگرچه ممکن است معاملات پولشویی در ارزهای دیجیتال کمتر توسط نهادهای قانونی رصد شوند، اما این بدان معنا نیست که این فعالیت‌ها بدون پیگیری و شناسایی انجام می‌شوند. تاکنون تلاش‌های زیادی برای توسعه و اجرای قوانین و مقررات جلوگیری از پولشویی در ارزهای دیجیتال صورت گرفته است.

بنابراین، ارزهای دیجیتال به تنهایی عامل اصلی پولشویی نیستند و برای مقابله با این نوع جرم‌ها، نهادهای مختلف در سطح ملی و بین‌المللی باید همکاری کنند و قوانین موثری را اجرا کنند تا از سواستفاده از ارزهای دیجیتال در این زمینه جلوگیری شود. . (بهره‌مند,عامری ثانی، ۱۳۹۸: ۵۹)

خروج ارز و نقد شوندگی پایین: در شرایط کنونی که بسیاری از استخراج‌کنندگان و مالکان ارزهای دیجیتال در خارج از کشور فعالیت می‌کنند، خرید این‌گونه ارزها توسط کاربران در ایران ممکن است به انتقال بیشتر دارایی‌های دیجیتال به خارج از کشور و تضعیف سیستم اقتصادی ایران منجر شود.

نقد شوندگی، توانایی تبدیل سریع دارایی‌ها به پول نقدی با مقدار مناسب است و هرچه بازارها نقدینگی بیشتری داشته باشند، پایداری بیشتری دارند. امکان تبدیل ارزهای دیجیتال به پول رسمی کشور یا سایر ارزها در مقدار بالا به دلیل محدودیت‌ها و نبود نهادهای نظارتی بر این فرآیند دشوارتر است. همچنین، اختلاف بین قیمت‌های خرید و فروش در صرافی‌های ارز دیجیتال در ایران ممکن است بیشتر از حد معمول باشد.

از دیگر معایب ارزهای دیجیتال می‌توان به مصرف بالای انرژی توسط فرایند ماینینگ، احتمال تأمین مالی برخی گروه‌های سیاسی و تروریستی از طریق این ارزها، پیچیدگی فنی برای کاربران عادی، تهدید به اقتصاد ملی از طریق نوسانات زیاد ارزهای دیجیتال و سایر مسائلی که به آنها اشاره کردید اشاره کرد. همه این نکات نشان می‌دهند که استفاده از ارزهای دیجیتال نیاز به مطالعه دقیق و شناخت عمیقی از این بازار دارد و باید با مراعات کامل مزایا و معایب آن انجام شود. (میرغفوری، صیادی، دهقانی زاده، ۱۳۹۹، ۱۳)

٤- جرائم مرتبط با ارزهای دیجیتال در بستر فضای سایبری

فیشینگ[6]: یکی از روش‌های کلاهبرداری با استفاده از ارزهای دیجیتال، فیشینگ است. فیشینگ یکی از روش‌های رایج کلاهبرداری در فضای اینترنت است که به ارزهای دیجیتال محدود نمی‌شود. این روش عمدتاً با تلاش برای جعل هویت یک سایت، سرویس، شرکت یا حتی فرد به منظور بدست آوردن اطلاعات حساس، به ویژه اطلاعات مالی، انجام می‌شود. این نوع کلاهبرداری به وسیله ابزارهای مختلفی مانند ایمیل‌ها و پیام‌رسان‌ها نیز انجام می‌شود.

در روش فیشینگ، معمولاً فرد کلاهبردار (فیشر) با ارسال پیام‌ها یا ایمیل‌هایی به مقاصد هدف، سعی در جلب توجه و تخلیه اطلاعات حساس کاربران دارد. این پیام‌ها ممکن است حاوی لینک‌های مشکوک به سایت‌های جعلی یا درخواست‌های جعلی برای تأیید اطلاعات حساب کاربری باشند. افراد کلاهبردار با بهره‌گیری از تکنیک‌های اجتماعی، سعی در ترتیب کاربران به انجام اقدامات خود دارند.

یکی از روش‌های رایج در فیشینگ، ایجاد سایت‌ها و پیام‌های جعلی با آدرس‌های وب سایت بسیار مشابه با آدرس‌های واقعی سایت‌های معتبر است. این سایت‌ها جلب کاربران را با ادعای ارائه خدمات پشتیبانی و حل مشکلات زیبا و زمینه‌ساز می‌کنند. از کاربران خواسته می‌شود که اطلاعات حساس خود را وارد کرده و تأیید کنند. از آنجا که آدرس وب سایت‌های جعلی بسیار مشابه آدرس‌های واقعی هستند، بسیاری از کاربران اغفال می‌شوند و اطلاعات شخصی و مالی خود را وارد می‌کنند.

بنابراین، احتیاط و اطلاع‌رسانی به مورد فیشینگ به عنوان یکی از تهدیدات آنلاین بسیار مهم است تا افراد بتوانند از این نوع کلاهبرداری جلوگیری کنند

در این نوع کلاهبرداری، کلاهبرداران تلاش می‌کنند از افراد اطلاعات هویتی و ورود به حساب کاربری در سایت اصلی استخراج کنند. سپس با دسترسی به اطلاعات کیف پول شخص، تمام دارایی‌های موجود در کیف پول را به اختیار بگیرند.

روش‌های ترغیبی برای افراد برای ارائه اطلاعات در این نوع کلاهبرداری ممکن است متنوع باشند، اما افزایش آگاهی و ایجاد مهارت‌های امنیتی می‌تواند از آسیب‌دیدن در این حوزه جلوگیری کند. به‌عنوان مثال، کلاهبرداران ممکن است از تغییر حروف و یا جابجایی حروف برای ساخت سایت‌های جعلی استفاده کنند. برای جلوگیری از این نوع کلاهبرداری‌ها، می‌توان از روش‌های زیر استفاده کرد(ریاضی مند،۱۳۹۷، ۱۲۱)

طرح های پانزی و هرمی: طرح‌های پانزی و هرمی در حوزه‌ی ارزهای دیجیتال معمولاً با جلب سرمایه‌گذاران جدید از طریق ارائه برنامه‌های سودآور و وعده‌های پرداخت در زمان‌های معین نظر افراد را جلب می‌کنند. اما در واقعیت، سودی که به سرمایه‌گذاران قدیمی تعلق می‌گیرد، ناشی از سرمایه‌گذاری افراد جدید در پروژه است و در واقع از پولی است که افراد جدید وارد این شبکه می‌کنند. هرچه تعداد افراد جدید بیشتری وارد این شبکه شوند، این چرخه مدت بیشتری ادامه می‌یابد. اما زمانی که جذب سرمایه‌گذار جدید متوقف شود، افراد موجود در سطح‌های بالاتر نخواهند توانست سود سرمایه‌گذاران قدیمی‌تر را پرداخت کنند. این مدل سیستم در بلندمدت پایدار نیست و در نهایت به نابودی می‌انجامد.

در مورد طرح‌های هرمی، تفاوت اصلی با طرح‌های پانزی در این است که نیاز به مشارکت سرمایه‌گذاران برای جذب سرمایه‌گذاران جدید دارند. در این طرح‌ها، در نقطه بالاترین سطح یک فرد برگزارکننده اصلی است که سپس تعداد مشخصی از افراد را به‌عنوان

[6] Phishing

زیرمجموعه‌ها و زیرشاخه‌ها جذب می‌کند. هر کدام از این افراد نیز مسئول جذب افراد جدید و گسترش این مجموعه می‌شوند. با افزایش تعداد افراد در این مجموعه، سود افراد در سطوح بالاتر بدون نیاز به فعالیت در جذب افراد جدید افزایش می‌یابد. اما همچنان، این مدل نیز به دلایل مشابهی با طرح‌های پانزی، دوام طولانی‌مدتی ندارد و در نهایت به نابودی می‌انجامد(عبادی لمر،۱۳۹۹: ۶۲)

کیف پول‌های تقلبی و باج افزارها: یکی از اصولی‌ترین مسائل برای معامله‌گران ارزهای دیجیتال، انتخاب و استفاده از کیف‌پول‌های معتبر است. تبلیغات گسترده کیف‌پول‌های جعلی که از ظاهری مشابه به وب‌سایت‌های قانونی معروفیت برخوردارند، ممکن است بسیار گول‌زننده باشد. نصب این کیف‌پول‌ها و وارد کردن اطلاعات شخصی و ارزهای دیجیتال در آن‌ها ممکن است منجر به سرقت ارزهای دیجیتال فرد شود. اما نکته مهم این است که حتی کیف‌پول‌های قانونی نیز ممکن است در معرض حملات هکرهای ماهر باشند. بنابراین، فرایند معاملات و استفاده از کیف‌پول‌ها باید با دقت بسیار بالا صورت گیرد تا اطلاعات هویت و ارزهای دیجیتال در معرض خطر قرار نگیرند.

همچنین، باج‌افزارها به بدافزارهایی اطلاق می‌شود که بخشی از اطلاعات ذخیره‌شده بر روی گوشی‌ها یا لپ‌تاپ‌ها را قفل کرده و دسترسی کاربر به آن‌ها را محدود می‌کنند. این نوع حملات معمولاً با کلیک بر روی لینک‌های تبلیغاتی و مشکوک آغاز می‌شوند و سپس از فرد درخواست پرداخت ارز دیجیتال به‌عنوان خرید "کلید" برای باز کردن اطلاعات رمزنگاری‌شده می‌کنند. (ریاضی مند،۱۳۹۷: ۱۲۶)

۵- چالش ها و فرصت های ارز دیجیتال از منظر کشور ایران

در سال ۱۴۰۰، کمیسیون اقتصادی مجلس شورای اسلامی گزارشی جامع درباره وضعیت صنعت استخراج رمزارزهای جهانی و مبادلات داخلی ارائه کرد. این گزارش با اشاره به توسعه روزافزون فناوری اطلاعات و اهمیت اقتصاد دیجیتال، رمزارزها را به‌عنوان یکی از مهم‌ترین محصولات مبتنی بر فناوری بلاک‌چین معرفی می‌کند. در این گزارش آمده است که رمزارزها پدیده‌ای مبهم و ناشناخته با بنیان‌گذار گمنام (ساتوشی ناکاموتو) هستند و همین ناشناختگی، ماهیت این پدیده و اهداف طراحی آن به‌ویژه در خصوص بیت‌کوین را به موضوع بحث‌های گسترده تبدیل کرده است (قوامی‌پور، محمودی، ۱۴۰۲: ۸۲).

یکی از چالش‌های بنیادین در مواجهه با رمزارزها، ماهیت غیرمتمرکز و ناشناس بودن دارندگان و مبادله‌کنندگان است که احراز هویت آن‌ها را دشوار می‌سازد. این ویژگی موجب نگرانی بانک‌های مرکزی کشورها شده، زیرا رمزارزها می‌توانند بستر مناسبی برای فعالیت‌های اقتصاد زیرزمینی و تضعیف قدرت بانک‌های مرکزی در اعمال سیاست‌های پولی و مالی باشند.

از منظر اقتصادی نیز کارشناسان در تعریف رمزارز به‌عنوان پول یا دارایی مالی اختلاف‌نظر دارند؛ زیرا ارزش و قدرت خرید رمزارزها بسیار نوسان‌پذیر و لحظه‌ای است. هرچند رمزارزها در ابتدا به‌عنوان وسیله مبادله طراحی شده‌اند، اما اکنون برخی اقتصاددانان آن‌ها را مشابه دارایی‌های نامشهود یا حتی شبیه‌سازی دیجیتال فلزات گران‌بها می‌دانند که به دلیل محدودیت در عرضه، ارزشمند تلقی می‌شوند. به همین علت، رمزارزها توانسته‌اند در طول حدود یک دهه، طرفداران بسیاری در سراسر جهان به‌دست آورند (قوامی‌پور، محمودی، ۱۴۰۲: ۸۲).

ویژگی فرامرزی بودن رمزارزها باعث شده است این فناوری به صنعتی جهانی و بدون محدودیت جغرافیایی تبدیل شود. در ایران نیز هم در حوزه استخراج (ماینینگ) و هم در مبادلات متقاضیان زیادی وجود دارد؛ اما به دلیل نبود چارچوب‌های قانونی و نظارتی شفاف، فعالیت‌ها اغلب در وضعیت غیررسمی یا زیرزمینی انجام می‌شوند. این موضوع دو پیامد متضاد دارد:

۱. فرصت‌های اقتصادی بالقوه :رمزارزها می‌توانند منبع درآمد جدیدی برای کشور از طریق استخراج و استفاده در تبادلات بین‌المللی، به‌ویژه در شرایط تحریم باشند.

۲. تهدیدهای اقتصادی و امنیتی :عدم نظارت و نبود زیرساخت‌های قانونی، بستر مناسبی برای پول‌شویی، فرار مالیاتی، خروج سرمایه و تضعیف نظام بانکی کشور فراهم می‌کند.

طبق آمار ارائه‌شده در این گزارش، ارزش کل بازار رمزارزها در دنیا حدود ۱٫۵ تریلیون دلار با گردش روزانه ۵۳ هزار میلیارد دلار برآورد شده است که بیت‌کوین به‌تنهایی **57**درصد این بازار را در اختیار دارد. همچنین، میزان استخراج سالانه رمزارزها در جهان **15** میلیارد دلار تخمین زده می‌شود و سهم ایران **1.1**میلیارد دلار (به‌صورت غیررسمی) است. قابل توجه اینکه از **324**هزار بیت‌کوین استخراجی سالانه جهان، حدود ۱۹ هزار و ۵۰۰ بیت‌کوین در ایران تولید می‌شود که نشان‌دهنده ظرفیت بالقوه بالا و در عین حال ناسامانی شدید فعالیت‌های این بخش در کشور است (قوامی‌پور، محمودی، ۱۴۰۲: ۸۲).

نحوه مواجهه با پدیده رمزارز را می‌توان در ۵ حوزه دسته‌بندی کرد:

استفاده از رمز ارزها برای تبادلات خارجی همراه، استخراج و تولید رمزارزهای موجود، طراحی رمز ارزهای ملی یا چندجانبه، تبادل رمز ارز، صنایع مرتبط با رمز ارز.

۱. در حوزه استفاده از رمز ارزها برای تبادلات خارجی، به نظر می‌رسد به‌واسطه امکانی که رمز ارزها در کاهش اثر تحریم‌ها، به‌واسطه دشوارتر بودن رصد مبادلات آن‌ها، ایجاد می‌کنند، نمی‌توان نسبت به استفاده از این ظرفیت بی‌تفاوت و بی‌برنامه بود.

قاعدتاً با محاسبه مخاطرات از دست رفتن سرمایه به دلایل مختلف و مقایسه آن با شرایط مبادلات غیررسمی کشور در دنیا که مخاطرات مشابهی دارد، استفاده از شیوه‌های گوناگون جلوگیری از رصد مبادلات مالی کشور منطقی و ضروری به نظر می‌رسد که استفاده از رمزارزها در این راستا، به‌عنوان مسیر جایگزین معاملات تهاتری یا تسهیل کننده این نوع معاملات قابل‌تعریف است. در این حوزه، فارغ از بحث استخراج رمز ارزها، می‌توان مابه‌ازای صادرات کشور به کشورهای مختلف، رمز ارز دریافت و در قبال واردات نیز همان رمز ارزها را پرداخت نمود.

۲. در حوزه استخراج و تولید (ماینینگ) رمز ارزهای موجود (و ازجمله بیت‌کوین)، مزیت مذکور می‌تواند به‌صورت تبدیل منابع انرژی فسیلی کشور و یا سایر منابع طبیعی همچون جریان آب و باد و انرژی هسته‌ای به برق و سپس استخراج رمز ارز با استفاده از برق تولیدی، تعریف شود.

به‌واقع در صورت محدود شدن صادرات انرژی فسیلی و برق کشور، مسیری برای تبدیل آن به رمز ارز و استفاده از آن برای واردات ضروری در کشور تعریف می‌شود. البته باید خروج ارز برای خرید دستگاه‌ها و تجهیزات ماینینگ را نیز مدنظر قرار داد. وجود بازار پررونق جهانی رمز ارز و قابلیت تبدیل آن به ارزهای واقعی هم می‌تواند ظرفیت بالقوه‌ای برای دسترسی به منابع ارزی باشد.

۳. در حوزه طراحی رمزارزهای ملی یا چندجانبه، شاید یکی از مهم‌ترین و مغفول‌ترین بخش‌های بحث رمز ارزها باشد که هرچند تلاش‌هایی برای آن انجام‌شده، اما ظاهراً بازخوردهای منفی زیادی مبنی بر اثربخش نبودن این اقدام وجود دارد.

به نظر می‌رسد اتفاق همین‌جاست که همچون توجه به ظرفیت‌های داخلی در ایجاد شبکه ملی اطلاعات، پیام‌رسان‌های داخلی و ماهواره داخلی، باید اهتمام جدی سیاست‌گذاران و مدیران کشور به کار گرفته شود تا بتواند به‌جای بازی در بستری مبهم و طراحی‌شده، خود ایجادکننده قواعد بازی و اعمال حاکمیت باشد.

بزرگ‌ترین نقطه مقاومت و مخالفت بسیاری از فعالان این بازار نیز همین‌جاست که باید درباره آن گفت‌وگوها و بررسی‌های عمیق‌تری صورت پذیرد.

۴. حوزه تبادل رمز ارز، و به‌ویژه ایجاد بسترهای تبادل رمز ارز در داخل کشور، مهم‌ترین و پرچالش‌ترین حوزه بحث در زمینه رمز ارزهاست که نیازمند بررسی دقیق و آینده‌نگری عمیقی است. اتفاقا ریسک بزرگی که متوجه اقتصاد کشور است هم در همین بخش است که البته برخورد صرفاً سلبی و منفعل موجود با این حوزه هرگز نمی‌تواند راه‌حل مناسبی برای مواجهه با این ریسک باشد.

تبدیل این تهدید به فرصت و بررسی دقیق‌تر جنبه‌های مثبت موضوع تبادل رمز ارز، در کنار ریسک‌های آن، و همچنین بررسی دقیق آثار اقتصاد کلانی تبادل رمزارز در کشور توسط عموم مردم، از الزامات این حوزه است.

۵. در حوزه صنایع مرتبط با رمز ارز، ابتدا صنعت برق و چگونگی تسهیم برق موجود بین این بخش و سایر بخش‌های اقتصاد و یا توسعه ظرفیت تولید برق برای توسعه استخراج رمز ارزها مطرح می‌شود. تکنولوژی ایجاد و تولید رمز ارز (روش اثبات کار یا اثبات سهم یا سایر روش‌ها که تأثیر بسیار مهمی بر مصرف برق و سایر جنبه‌های موضوع دارد)، محل و تأسیسات واحدهای (فارم‌ها یا مزارع (استخراج، و چگونگی دسترسی به دستگاه‌های استخراج (ماینر) ازجمله واردات یا ساخت این دستگاه‌ها هم از دیگر بحث‌های مهم صنایع مرتبط با رمزارز هستند.»(قوامی پور، محمودی: ۱۴۰۲: ۸۲)

۵-استراتژی‌های امنیتی در مقابله با حملات سایبری به صرافی‌های ارز دیجیتال

با گسترش روزافزون استفاده از ارزهای دیجیتال، امنیت صرافی‌های ارز دیجیتال به یکی از مهم‌ترین چالش‌های این حوزه تبدیل شده است. آمارها نشان می‌دهد حملات سایبری به صرافی‌های ارز دیجیتال در سال‌های اخیر افزایش چشمگیری داشته است یکی از مهم‌ترین استراتژی‌های امنیتی، پیاده‌سازی سیستم‌های احراز هویت چندعاملی است. استفاده از احراز هویت چندعاملی می‌تواند تا ۹۹,۹٪ از حملات مبتنی بر سرقت هویت را کاهش دهد .همچنین استفاده از توکن‌های امنیتی سخت‌افزاری نقش مهمی در افزایش امنیت سیستم‌های حساس داردمدیریت کلیدهای رمزنگاری نقش حیاتی در امنیت صرافی‌ها دارد. استفاده از ماژول‌های امنیتی سخت‌افزاری (HSM) برای ذخیره‌سازی کلیدهای خصوصی، امنیت را به طور قابل توجهی افزایش می‌دهد .سیستم‌های چندامضایی نیز می‌توانند ریسک سرقت دارایی‌های دیجیتال را تا حد زیادی کاهش دهند

نظارت و پاسخ به حوادث از دیگر عوامل کلیدی در امنیت صرافی‌هاست. استفاده از سیستم‌های هوش مصنوعی در تشخیص الگوهای مشکوک می‌تواند تا ۸۵٪ از حملات را پیش از وقوع خسارت شناسایی کند.(Wilson & Lee, 2023)

برای محافظت از کیف پول‌های دیجیتال، استفاده از کیف پول‌های سرد برای ذخیره‌سازی اکثر دارایی‌ها می‌تواند ریسک سرقت را به حداقل برسانپیاده‌سازی محدودیت‌های تراکنش و سیستم‌های نظارت بر برداشت نیز از اهمیت بالایی برخوردار است.(

آزمون و ارزیابی مستمر از ارکان اصلی امنیت صرافی‌های دیجیتال است. اجرای منظم تست نفوذ می‌تواند تا ۷۵٪ از آسیب‌پذیری‌های بالقوه را پیش از مورد سوءاستفاده قرار گرفتن شناسایی کند.(Miller & Chen, 2023)

آموزش و آگاهی‌سازی نقش مهمی در امنیت کلی سیستم دارد. حدود ۶۰٪ از نفوذهای موفق به سیستم‌های صرافی از طریق خطای انسانی رخ می‌دهدبنابراین، آموزش مستمر کارکنان و کاربران نقش مهمی در کاهش ریسک‌های امنیتی دارد.

نتیجه‌گیری: امنیت صرافی‌های ارز دیجیتال نیازمند رویکردی جامع و چندلایه است که شامل ترکیبی از راهکارهای فنی، سازمانی و آموزشی می‌شود. موفقیت در این زمینه مستلزم به‌روزرسانی مستمر استراتژی‌های امنیتی و همگام شدن با تهدیدات نوظهور است. بر اساس آمارهای موجود، صرافی‌هایی که از این رویکرد جامع استفاده می‌کنند، موفقیت بیشتری در مقابله با حملات سایبری داشته‌اند.

٦- بهره‌گیری از هوش مصنوعی در بهبود امنیت سایبری ارزهای دیجیتال

ماشین‌های هوشمند تا مدت‌ها صرفاً در قلمرو داستان‌های علمی-تخیلی جای داشتند، اما امروزه هوش مصنوعی به بخشی جدایی‌ناپذیر از واقعیت زندگی بشر تبدیل شده است(ابوذری، ۱۴۰۳، ۳۶). یکی از زمینه‌هایی که حضور هوش مصنوعی در آن روزبه‌روز پررنگ‌تر می‌شود، حوزه ارزهای دیجیتال و تراکنش‌های مبتنی بر بلاک‌چین است. با ظهور و گسترش این فناوری‌ها، نیاز به راهکارهای نوین در حوزه امنیت سایبری بیش از پیش احساس می‌شود. ماهیت غیرمتمرکز و بدون واسطه ارزهای دیجیتال چالش‌هایی همچون کلاهبرداری، فیشینگ و پول‌شویی را به‌دنبال داشته است؛ مسائلی که مقابله با آن‌ها تنها از طریق ابزارهای پیشرفته امکان‌پذیر است. در این راستا، هوش مصنوعی و الگوریتم‌های یادگیری ماشین به‌عنوان راه‌حل‌هایی نویدبخش برای تقویت امنیت و کاهش مخاطرات سایبری در این اکوسیستم نوظهور مطرح هستند(قوامی پورسرشکه، محمودی، ۱۴۰۳، ۲۹۰)

هوش مصنوعی قادر است با تحلیل حجم عظیمی از داده‌ها، الگوهای مشکوک و رفتارهای غیرعادی را شناسایی کند. در ادامه، برخی از مهم‌ترین کاربردهای هوش مصنوعی در بهبود امنیت سایبری ارزهای دیجیتال تشریح می‌شود:

شناسایی تراکنش‌های غیرعادی و مشکوک: الگوریتم‌های یادگیری ماشین می‌توانند با نظارت بر تاریخچه تراکنش‌های یک کیف پول یا آدرس مشخص، رفتارهای غیرعادی مانند تراکنش‌های با حجم غیرمنتظره یا فعالیت در ساعات نامعمول را شناسایی کنند. این روش به بانک‌ها و صرافی‌های ارز دیجیتال اجازه می‌دهد تا سریعاً به موارد مشکوک واکنش نشان دهند.

پیشگیری از حملات فیشینگ: حملات فیشینگ یکی از رایج‌ترین روش‌های کلاهبرداری در فضای ارزهای دیجیتال است که طی آن، مهاجمان تلاش می‌کنند کاربران را به افشای اطلاعات حساس خود ترغیب کنند. سیستم‌های مبتنی بر هوش مصنوعی می‌توانند ایمیل‌ها، لینک‌ها و وب‌سایت‌ها را از نظر الگوهای مخرب بررسی کرده و به کاربران هشدار دهند. به‌عنوان مثال، مدل‌های پردازش زبان طبیعی (NLP) می‌توانند پیام‌های فیشینگ را با تحلیل محتوا و شناسایی نشانه‌های تقلب تشخیص دهند.

تحلیل الگوهای بازار برای جلوگیری از کلاهبرداری‌های مالی: برخی از کلاهبرداران از نوسانات بازار برای بهره‌برداری از سرمایه‌گذاران استفاده می‌کنند. هوش مصنوعی می‌تواند با تحلیل تغییرات سریع قیمت و حجم معاملات، الگوهایی مانند دستکاری بازار (Market Manipulation)یا طرح‌های پانزی (Ponzi Schemes) را شناسایی کند و سرمایه‌گذاران را از خطرات مطلع سازد.

پیشگیری از حملات سایبری به صرافی‌ها و کیف‌پول‌ها: صرافی‌های ارز دیجیتال هدف اصلی هکرها هستند. هوش مصنوعی می‌تواند از طریق نظارت بر رفتارهای کاربری (مانند الگوی ورود و خروج یا دسترسی‌های غیرمعمول)، تلاش‌های هک یا نفوذ را تشخیص دهد. علاوه بر این، فناوری‌هایی مانند سیستم‌های تشخیص نفوذ (IDS) مبتنی بر یادگیری عمیق، توانایی شناسایی حملات پیچیده و چند مرحله‌ای را دارند.

تحلیل داده‌های بلاک‌چین برای کشف جرایم سازمان‌یافته: بلاک‌چین، اگرچه شفاف است، اما به دلیل ناشناس بودن تراکنش‌ها، می‌تواند بستر مناسبی برای پول‌شویی یا تأمین مالی فعالیت‌های غیرقانونی باشد. هوش مصنوعی می‌تواند داده‌های بلاک‌چین را تحلیل کرده و تراکنش‌هایی را که به نظر می‌رسد بخشی از فعالیت‌های سازمان‌یافته هستند، شناسایی کند. برای مثال، الگوریتم‌های خوشه‌بندی (Clustering)و تحلیل شبکه‌های اجتماعی (Social Network Analysis) می‌توانند آدرس‌های مرتبط با یکدیگر را شناسایی کرده و ارتباط آن‌ها را کشف کنند.

٦-١-نمونه‌هایی از کاربرد عملی هوش مصنوعی در امنیت ارزهای دیجیتال

پلتفرم :Chainalysis این پلتفرم از یادگیری ماشین برای تحلیل داده‌های بلاک‌چین استفاده می‌کند و توانایی شناسایی فعالیت‌های غیرقانونی مانند پول‌شویی و تراکنش‌های مشکوک را دارد. بسیاری از دولت‌ها و شرکت‌ها از این پلتفرم برای پیگیری تراکنش‌های مجرمانه استفاده می‌کنند.

سیستم تشخیص فیشینگ توسط :OpenAI مدل‌های پردازش زبان طبیعی، مانندGPT ، می‌توانند پیام‌های فیشینگ را در زمان واقعی تحلیل کرده و به کاربران هشدار دهند.

پلتفرم :Elliptic این سیستم از هوش مصنوعی برای شناسایی رفتارهای غیرمعمول در کیف‌پول‌ها و صرافی‌های دیجیتال استفاده می‌کند و می‌تواند به سازمان‌های مجری قانون برای ردیابی منابع تراکنش‌های مشکوک کمک کند.

٦-٢-چالش‌ها و محدودیت‌ها در استفاده از هوش مصنوعی

با وجود قابلیت‌های فراوان هوش مصنوعی، محدودیت‌هایی نیز وجود دارد:

نیاز به داده‌های باکیفیت: هوش مصنوعی برای عملکرد مؤثر به حجم زیادی از داده‌های باکیفیت و برچسب‌گذاری‌شده نیاز دارد. در برخی موارد، دسترسی به این داده‌ها به دلیل ماهیت ناشناس بلاک‌چین دشوار است.

خطای الگوریتم‌ها: مدل‌های هوش مصنوعی ممکن است تراکنش‌های قانونی را به اشتباه به‌عنوان مشکوک طبقه‌بندی کنند و در نتیجه منجر به تصمیم‌گیری‌های اشتباه شوند.

رشد تکنیک‌های مهاجمان: مهاجمان سایبری نیز از فناوری‌های پیشرفته برای دور زدن سیستم‌های امنیتی استفاده می‌کنند که این امر رقابت میان متخصصان امنیت سایبری و مجرمان را پیچیده‌تر می‌کند.

هوش مصنوعی و یادگیری ماشین ابزارهای قدرتمندی برای تقویت امنیت سایبری در دنیای ارزهای دیجیتال هستند. این فناوری‌ها می‌توانند جرایم سایبری را کاهش داده و اعتماد کاربران را به این سیستم‌های مالی نوظهور افزایش دهند. با این حال، برای بهره‌گیری حداکثری از این قابلیت‌ها، لازم است دولت‌ها، شرکت‌ها و محققان همکاری کنند و به توسعه سیستم‌های هوشمند بپردازند. توجه به چالش‌ها و محدودیت‌ها نیز ضروری است تا کاربردهای هوش مصنوعی در این زمینه مؤثرتر و قابل‌اعتمادتر شود.(تقی زاده، خردمندنیا، ۱۴۰۳، ۲۲)

۷- چارچوب پیشنهادی برای ارتقای امنیت رمزارزها در فضای سایبری ایران

رمزارزها به دلیل ویژگی‌های منحصربه‌فرد خود، از جمله غیرمتمرکز بودن و امکان انجام تراکنش‌های بدون واسطه، در ایران به‌ویژه در شرایط تحریم‌های اقتصادی و تورم بالا، به ابزاری محبوب برای حفظ ارزش دارایی‌ها و انجام معاملات تبدیل شده‌اند. با این حال، این فناوری با چالش‌های امنیتی متعددی مواجه است، از جمله پولشویی، تأمین مالی تروریسم، و کلاهبرداری‌های سایبری. برای مقابله با این تهدیدات، نیاز به یک چارچوب جامع و مؤثر برای ارتقای امنیت رمزارزها در فضای سایبری ایران احساس می‌شود. این مقاله با تکیه بر منابع علمی معتبر، چارچوبی پیشنهادی برای بهبود امنیت رمزارزها در ایران ارائه می‌دهد.

ایران از سال ۲۰۱۷ به دلیل تحریم‌های بین‌المللی که دسترسی به بازارهای مالی جهانی را محدود کرده‌اند، به استفاده از رمزارزها روی آورده است (ویکی‌پدیا، ۲۰۲۵). حجم معاملات رمزارزی در ایران در سال ۲۰۲۲ به حدود ۳ میلیارد دلار رسیده است، که نشان‌دهنده پذیرش گسترده این فناوری است (TRM Labs, 2023). با این حال، نبود قوانین جامع و نظارت کافی، این حوزه را در برابر سوءاستفاده‌های مالی آسیب‌پذیر کرده است. به عنوان مثال، گزارش‌هایی از استفاده برخی نهادها از رمزارزها برای دور زدن تحریم‌ها وجود دارد، که این موضوع نگرانی‌های امنیتی را افزایش داده است (Middle East Institute, 2022).

بر اساس مطالعه‌ای با عنوان «تنظیم قانونی دولت در مبارزه با پولشویی از طریق رمزارز: مطالعه تطبیقی سیستم‌های حقوقی جمهوری اسلامی ایران و ایتالیا» (جلالی، ۱۴۰۲)، چارچوب پیشنهادی برای ارتقای امنیت رمزارزها در ایران شامل سه مؤلفه اصلی است:

۱. تأیید هویت مشتریان (KYC)

یکی از مهم‌ترین اقدامات برای کاهش خطرات امنیتی، الزام به شناسایی هویت مشتریان در هنگام خرید یا معامله رمزارزها است. این اقدام، که به عنوان بخشی از استانداردهای مبارزه با پولشویی (AML) شناخته می‌شود، به صرافی‌ها و پلتفرم‌های رمزارزی کمک می‌کند تا از هویت واقعی کاربران اطمینان حاصل کنند. این روش در بسیاری از کشورها، از جمله ایتالیا، با موفقیت اجرا شده است (جلالی، ۱۴۰۲، ص. ۱۰). در ایران، صرافی‌هایی مانند نوبیتکس که ۸۷ درصد از حجم معاملات رمزارزی را پردازش می‌کنند، از استانداردهای KYC استفاده می‌کنند (TRM Labs, 2023). با این حال، نیاز به اجرای این استانداردها به‌صورت یکپارچه در تمام پلتفرم‌ها وجود دارد (کدخدایی، نوروزپور، ۱۳۹۹، ۱۵)

۲. ایجاد سازمان نظارتی و تنظیم‌کننده

تأسیس یک نهاد نظارتی مستقل برای نظارت بر فعالیت‌های رمزارزی در ایران ضروری است. این سازمان باید مسئولیت‌هایی مانند صدور مجوز برای صرافی‌ها، نظارت بر کیف‌پول‌های رمزارزی، و هماهنگی با نهادهای بین‌المللی مانند گروه ویژه اقدام مالی (FATF) را بر عهده داشته باشد. این نهاد می‌تواند با استفاده از فناوری‌های پیشرفته، مانند تحلیل بلاکچین، فعالیت‌های مشکوک را شناسایی کند (مددیریال قماشی، ۱۴۰۰، ۵۱۰). تجربه ایتالیا در ایجاد نهادهای نظارتی نشان می‌دهد که چنین سازمان‌هایی می‌توانند به کاهش جرایم مالی کمک کنند (کدخدایی، نوروزپور، ۱۳۹۹، ۱۲).

۳. ثبت تمامی انتقال‌های قراردادی مبتنی بر رمزارز

ثبت و پایش تمامی تراکنش‌های رمزارزی، به‌ویژه آن‌هایی که بر پایه قراردادهای هوشمند انجام می‌شوند، می‌تواند شفافیت را افزایش داده و خطرات امنیتی را کاهش دهد. این اقدام به مقامات اجازه می‌دهد تا فعالیت‌های غیرقانونی را شناسایی و پیگیری کنند. به عنوان مثال، پیشنهاد شده است که تمامی تراکنش‌های مبتنی بر قراردادهای هوشمند در یک پایگاه داده مرکزی ثبت شوند تا امکان ردیابی فراهم شود

چالش‌ها و موانع اجرا

اجرای این چارچوب در ایران با چالش‌هایی مواجه است:

محدودیت‌های زیرساختی: فیلترینگ اینترنت و محدودیت‌های دسترسی به فناوری‌های پیشرفته می‌تواند اجرای این چارچوب را دشوار کند (AML Watcher, 2024).

مقاومت‌های داخلی: برخی نهادها و پلتفرم‌های رمزارزی، مانند انجمن فین‌تک ایران، با الزامات سختگیرانه نظارتی، مانند اشتراک‌گذاری اطلاعات محرمانه کاربران، مخالف هستند (Crystal Intelligence, 2025).

تحریم‌های بین‌المللی: این تحریم‌ها می‌توانند همکاری با نهادهای بین‌المللی را محدود کنند، که برای هماهنگی با استانداردهای جهانی ضروری است (Middle East Institute, 2022).

برای موفقیت این چارچوب، پیشنهاد می‌شود:

همکاری با بخش خصوصی: همان‌طور که محمد صادق الحسینی پیشنهاد کرده است، واگذاری برخی مسئولیت‌ها به شرکت‌های خصوصی و انجمن‌ها می‌تواند نظم بازار را بهبود بخشد (AML Watcher, 2024).

آموزش و آگاهی‌بخشی: افزایش آگاهی عمومی و آموزش کاربران در مورد خطرات امنیتی رمزارزها می‌تواند به کاهش کلاهبرداری‌ها کمک کند.

هماهنگی با استانداردهای بین‌المللی: اجرای توصیه‌های FATF، مانند شناسایی مشتری و ثبت تراکنش‌ها، می‌تواند به تقویت اعتبار ایران در بازارهای جهانی کمک کند (کدخدایی، نوروزپور۱۳۹۹. ۲۰).

- **جدول خلاصه چارچوب پیشنهادی**

چالش‌ها	مزایا	توضیحات	مؤلفه
نیاز به زیرساخت‌های فناوری پیشرفته	کاهش پولشویی و فعالیت‌های غیرقانونی	شناسایی هویت کاربران برای خرید و تأیید معامله رمزارزها	هویت مشتریان (KYC)
مقاومت برخی نهادها و محدودیت‌های بودجه‌ای	افزایش شفافیت و هماهنگی با استانداردهای بین‌المللی	ایجاد نهاد مستقل برای نظارت بر صرافی‌ها و کیف‌پول‌های رمزارزی	سازمان نظارتی
پیچیدگی‌های فنی و نیاز به پایگاه داده مرکزی	امکان ردیابی فعالیت‌های مشکوک	پایش و ثبت تمامی تراکنش‌های مبتنی بر قراردادهای هوشمند	ثبت تراکنش‌ها

برای ارتقای امنیت رمزارزها در فضای سایبری ایران، اجرای یک چارچوب تنظیم‌کننده قوی که شامل تأیید هویت مشتریان، ایجاد سازمان نظارتی، و ثبت تراکنش‌های رمزارزی باشد، ضروری است. این چارچوب، با تکیه بر مطالعات علمی و توصیه‌های بین‌المللی، می‌تواند به کاهش خطرات امنیتی و افزایش اعتماد به اکوسیستم رمزارزها در ایران کمک کند. با این حال، موفقیت این چارچوب به رفع موانع زیرساختی و همکاری بین بخش‌های دولتی و خصوصی بستگی دارد.

بحث و نتیجه‌گیری

بررسی‌های انجام‌شده در این پژوهش نشان می‌دهد که ارزهای دیجیتال، به‌ویژه بیت‌کوین و اتریوم، ضمن ایجاد تحول بنیادین در نظام‌های مالی و اقتصادی جهان، چالش‌های گسترده و چندلایه‌ای را نیز در حوزه امنیت سایبری به همراه آورده‌اند. ویژگی‌های ذاتی رمزارزها از جمله غیرمتمرکز بودن، ناشناس ماندن تراکنش‌ها، حذف واسطه‌های مالی سنتی و نوسانات شدید قیمتی، زمینه‌ساز تهدیدات متعددی همچون پول‌شویی، تأمین مالی تروریسم، دور زدن تحریم‌ها، سرقت کلیدهای خصوصی، حملات سایبری به صرافی‌های دیجیتال، باج‌افزارها و ایجاد بازارهای سیاه دیجیتال شده است. این چالش‌ها به‌ویژه در کشورهایی همچون ایران، که فاقد چارچوب‌های قانونی و نظارتی شفاف و جامع در این حوزه هستند، با شدت بیشتری بروز یافته است.

با این حال، یافته‌های پژوهش حاضر نشان می‌دهد که فناوری رمزارزها به‌ویژه بلاک‌چین، ظرفیت‌های بالقوه مهمی برای ارتقای امنیت سایبری فراهم می‌کند. ماهیت غیرقابل تغییر بودن اطلاعات در زنجیره‌های بلاک‌چین، امکان ثبت شفاف و ایمن تراکنش‌ها و قابلیت ردیابی در سطح فناوری، می‌تواند به‌عنوان ابزاری کارآمد در افزایش اعتماد کاربران و مقابله با جرائم مالی استفاده شود. علاوه بر آن، ترکیب فناوری‌های هوش مصنوعی و الگوریتم‌های یادگیری ماشین با زیرساخت‌های بلاک‌چین، امکان تحلیل بلادرنگ حجم انبوه داده‌های تراکنشی و شناسایی الگوهای مشکوک را فراهم ساخته و در نتیجه، به کاهش جرائم و تهدیدات سایبری در این حوزه منجر خواهد شد.

بر اساس نتایج این تحقیق، برای مدیریت مؤثر چالش‌های امنیتی رمزارزها در ایران، تدوین چارچوبی جامع و تلفیقی ضروری است که ابعاد فناورانه، حقوقی و آموزشی را هم‌زمان دربر گیرد. این چارچوب باید شامل ایجاد نظام جامع احراز هویت کاربران در تمامی پلتفرم‌های رمزارزی(KYC) ، تشکیل سازمان نظارتی مستقل با رویکرد فناورانه و اختیارات قانونی کافی، توسعه زیرساخت‌های امنیت سایبری بومی متناسب با تهدیدات نوظهور، استفاده از فناوری‌های نوین تحلیل داده‌ها برای شناسایی رفتارهای مشکوک، طراحی سیستم‌های هشداردهی هوشمند و آموزش مستمر کاربران و فعالان این حوزه باشد.

نوآوری پژوهش حاضر در ارائه یک رویکرد تلفیقی بین‌رشته‌ای است که با ترکیب فناوری‌های نوظهور، ملاحظات حقوقی و سیاست‌گذاری امنیتی، تلاش می‌کند راهکارهایی کاربردی و قابل‌اجرا برای ارتقای امنیت رمزارزها ارائه دهد. این مقاله علاوه بر مرور انتقادی ادبیات موجود، با تحلیل عمیق تهدیدات و فرصت‌های امنیت سایبری رمزارزها و تمرکز بر ظرفیت‌های هوش مصنوعی، گامی نوین در جهت غنی‌سازی مبانی نظری و کاربردی این حوزه برداشته است.

بدون تردید، تحقق امنیت پایدار در حوزه رمزارزها نیازمند عزم ملی، حکمرانی فناورانه هوشمند و تدوین سیاست‌های جامع بین‌رشته‌ای است .تنها در چنین چارچوبی می‌توان از ظرفیت‌های گسترده رمزارزها در توسعه اقتصادی کشور بهره‌برداری کرد و هم‌زمان تهدیدات و آسیب‌های آن را به حداقل رساند. آینده موفقیت‌آمیز مدیریت رمزارزها در گرو پذیرش این واقعیت است که امنیت، توسعه و حکمرانی فناوری سه ضلع جدایی‌ناپذیر در تحقق اقتصاد دیجیتال پایدار خواهند بود.

- منابع

۱. ابوذری, مهرنوش . (۱۴۰۳). مقابله با بزهکاری در عصر هوش مصنوعی: پیش‌بینی به مثابه پیشگیری. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, ۱(۲), **doi: 10.22034/jclc.2025.720961**

۲. ارزانیان، نسترن ومظلوم رهنی، علیرضا، (۱۳۹۹)، مبانی فقهی حقوقی ارز دیجیتال با رویکرد سرمایه گذاری، ***فصلنامه مطالعات فقه اقتصادی***، دوره ۲، شماره۱، ۷۰-۸۷.

۳. باغانی، الهه، (۱۳۹۹)، بررسی نحوه نظارت بر فناوری های نوین مالی فین تک و ارز دیجیتال، ***فصلنامه علمی پژوهشی دانش سرمایه گذاری***، دوره ۹، شماره ۳۵، ۱۵۳-۱۶۸.

۴. بشارت نیا، فاطمه، رحیمی، علیرضا، ذوالفقاری، مهدی، (۱۳۹۰)، آشنایی با پول الکترونیکی، ***اولین همایش ملی فناوری اطلاعات و ارتباطات***، ابهر.

۵. بهره مند، حمید، عامری ثانی، امیرکیا، (۱۳۹۸)، چالش ها و راه کارهای جرم یابی پولشویی از طریق ارزهای رمزنگاری شده، ***فصلنامه کاراگاه***، دوره۱۲، شماره۴۶، ۵۵-۷۳.

۶. پروین, خیراله و الهیاری فرد, علی . (۱۴۰۳). تنظیم‌گری دولت در حوزهٔ مبارزه با پول‌شویی از طریق رمزارز: مطالعه تطبیقی نظام حقوقی جمهوری اسلامی ایران و ایتالیا .*فصلنامه مطالعات حقوق عمومی دانشگاه تهران* :doi .1574-1549 ,(3)54 , 10.22059/jplsq.2023.357301.3290

۷. تقی زاده, مسلم و خردمندنیا, سهیلا . (۱۴۰۳). هوش مصنوعی مولد؛ چالش ها و الزامات توسعه و پیاده سازی. (۱۹۸۷۹). ماهنامه گزارش های کارشناسی مرکز پژوهش های مجلس شورای اسلامی, ۳۲(۴)

۸. خورسندی کوچصفهانی، زهرا، (۱۳۹۸)، ماهیت ارزهای دیجیتال و آثار مترتب بر آن در فقه امامیه، کارشناسی ارشد، فقه و مبانی حقوق اسلامی، دانشگاه قران وحدیث، پردیس تهران

۹. رهبر، فرهاد، (۱۳۸۲) پولشویی و آثار و پیامد های آن، ***مجله تحقیقات اقتصادی***، دوره ۳۸، شماره ۳، ۳۳-۵۵

۱۰. ریاضی مند، مهران، (۱۳۹۷)، ***بررسی ابعاد حقوقی ارزهای دیجیتال***، انتشارات برتر اندیشان، تهران.

۱۱. عبادی لمر، صالح، (۱۳۹۹)، ***سرمایه گذاری در ارزهای دیجیتال و جایگاه ان در ایران***، موسسه فرهنگی هنری دیباگران تهران، تهران.

۱۲. فضلی، حسن، چمندار، مهدی، زمردی منور، هادی، (۱۳۹۸)، ***بلاک چین و رمز ارزها***، نشر ناقوس، تهران.

۱۳. قوامی پور سرشکه، محدثه، محمودی، امیررضا(۱۴۰۲)، ***تاثیر اسناد بین المللی بر کنترل جرائم کسب و کار ایران با رویکردی بر ارزهای دیجیتال***، انتشارات جهان سیاست، تهران

۱۴. قوامی پور سرشکه, محدثه و محمودی, امیررضا . (۱۴۰۳). چارچوب حقوقی و تلاش‌های بین‌المللی در مبارزه با جرائم ارزهای دیجیتال: رویکرد اسناد بین المللی. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, ۱(۱), ۲۸۸-۳۱۴. doi: 10.22034/jclc.2024.718662

۱۵. کدخدایی, عباسعلی و نوروزپور, حسام . (۱۳۹۹). چالش ارزهای مجازی در مبارزه با پولشویی و تأمین مالی تروریسم با تأکید بر اقدامات و توصیه‌های کارگروه ویژه اقدام مالی .(FATF)*مجله حقوقی بین المللی 37* ,(شماره ۶۲ (بهار- تابستان)), ۷- . doi: 10.22066/cilamag.2019.101998.164729

۱۶. ماتسورا، جفری اچ، (۱۳۹۷)، بررسی اجمالی مقررات ارز دیجیتال و پیامدهای قانونی ان، ترجمه ی سعیدسیاه بیدی کرمانشاهی وحمیدرضاکناری زاده، ***پژوهشنامه حقوق فارس***، دوره۱، شماره ۱، ۱۴۹-۱۶۷.

۱۷. مددی, مهدی و قماشی, سعید . (۱۴۰۰). جستاری در پول‌شویی از طریق ارزهای رمزنگاری شده. مطالعات حقوق کیفری و جرم شناسی, ۵۱(۲), ۵۲۱-۵۰۳. doi: 10.22059/jqclcs.2022.292559.1499

۱۸. میرغفوری، حبیب الله، صیادی، حسین، دهقانی زاده، نصرت، (۱۳۹۹)، مزایا و معایب ارزهای دیجیتالی با تاکید بر بیت کوین، ***همایش پژوهش های نوین در علوم و فناوری***

۱۹. واحدزاده، سینا و ملک زاده، فهیمه، (۱۳۹۹)، ***جایگاه فقهی حقوقی ارزهای دیجیتال***، نشر خرسندی، تهران.

20. AML Watcher. (2024). Iran Approved Policies and Regulatory Frameworks for Crypto Industry [دسترسی: https://amlwatcher.com/news/the-central-bank-of-iran-approves-policy-and-regulatory-framework-for-cryptocurrencies]

21. Crystal Intelligence. (2025). Crypto use in Iran: bypassing sanctions and regulations. [دسترسی: https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage]

22. Middle East Institute. (2022). Iran and cryptocurrency: Opportunities and obstacles for the regime [دسترسی: https://www.mei.edu/publications/iran-and-cryptocurrency-opportunities-and-obstacles-regime]

23. Miller, T., & Chen, Y. (2023). Penetration testing effectiveness in digital asset platforms. Security Testing Journal, 13(4), 278-293.

24. TRM Labs. (2023). Iran's Crypto Economy [دسترسی: https://www.trmlabs.com/resources/blog/iran-crypto-economy]

25. Wilson, J., & Lee, M. (2023). Real-time monitoring systems in cryptocurrency exchanges. Digital Security Journal, 19(1), 78-93.

References

1. Abouzari, M. (2024). *Combating Delinquency in the Age of Artificial Intelligence: Prediction as Prevention*. Journal of Criminal Law and Criminology Research and Development, 1(2). doi: 10.22034/jclc.2025.720961 (in Persian)
2. AML Watcher. (2024). *Iran Approved Policies and Regulatory Frameworks for Crypto Industry*. Retrieved from https://amlwatcher.com/news/the-central-bank-of-iran-approves-policy-and-regulatory-framework-for-cryptocurrencies/
3. Arzanian, N., & Mazlom-Rahni, A. (2020). *Jurisprudential and Legal Foundations of Digital Currency with Investment Approach*. Economic Jurisprudence Studies Quarterly, 2(1), 70–87. (in Persian)
4. Baghani, E. (2020). *Supervision of New Financial Technologies (FinTech) and Digital Currency*. Investment Knowledge Scientific-Research Quarterly, 9(35), 153–168. (in Persian)
5. Basharatnia, F., Rahimi, A., & Zolfaghari, M. (2011). *An Introduction to Electronic Money*. 1st National Conference on Information and Communication Technology, Abhar. (in Persian)
6. Bahremand, H., & Ameri Sani, A. (2019). *Challenges and Strategies for Crime Detection of Money Laundering via Cryptocurrencies*. Karagah Quarterly, 12(46), 55–73. (in Persian)
7. Crystal Intelligence. (2025). *Crypto Use in Iran: Bypassing Sanctions and Regulations*. Retrieved from https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage/
8. Fazeli, H., Chamandar, M., & Zomorodi-Manvar, H. (2019). *Blockchain and Cryptocurrencies*. Naghous Publishing, Tehran. (in Persian)
9. Ghavami Pour-Sarshkhe, M., & Mahmoudi, A. (2024). *Legal Framework and International Efforts to Combat Cryptocurrency Crimes: A Study of International Instruments*. Journal of Criminal Law and Criminology Research and Development, 1(1), 288–314. doi: 10.22034/jclc.2024.718662 (in Persian)
10. Ghavami Pour-Sarshkhe, M., & Mahmoudi, A. (2023). *Impact of International Documents on Crime Control in Iranian Business Sector with a Focus on Digital Currencies*. Jahane Siasat Publishing, Tehran. (in Persian)
11. Khorsandi-Kouchesfehani, Z. (2019). *The Nature of Digital Currencies and Their Jurisprudential Implications in Imamiyya Jurisprudence* [MA Thesis]. Al-Quran and Hadith University, Tehran Branch. (in Persian)
12. Kadkhodaei, A., & Norouzpour, H. (2020). *The Challenge of Virtual Currencies in Combating Money Laundering and Terrorist Financing with Emphasis on FATF Measures and Recommendations*. International Legal Journal, 37(62), 7–29. doi: 10.22066/cilamag.2019.101998.1647 (in Persian)
13. Matsura, J. H. (2018). *An Overview of Digital Currency Regulations and Their Legal Implications* (S. Siyah-Beydi & H. Kanarizadeh, Trans.). Fars Legal Research Journal, 1(1), 149–167. (in Persian)
14. Middle East Institute. (2022). *Iran and Cryptocurrency: Opportunities and Obstacles for the Regime*. Retrieved from https://www.mei.edu/publications/iran-and-cryptocurrency-opportunities-and-obstacles-regime
15. Maddadi, M., & Qamashi, S. (2021). *An Inquiry into Money Laundering via Cryptocurrencies*. Criminal Law and Criminology Studies, 51(2), 503–521. doi: 10.22059/jqclcs.2022.292559.1499 (in Persian)

16. Mirghafouri, H., Sayyadi, H., & Dehghani-Zadeh, N. (2020). *Advantages and Disadvantages of Digital Currencies with Emphasis on Bitcoin*. Conference on New Research in Science and Technology. (in Persian)
17. Miller, T., & Chen, Y. (2023). *Penetration Testing Effectiveness in Digital Asset Platforms*. Security Testing Journal, 13(4), 278–293.
18. Parvin, K., & Elhiyari-Fard, A. (2024). *Government Regulation in the Field of Anti-Money Laundering via Cryptocurrencies: A Comparative Study of Iranian and Italian Legal Systems*. University of Tehran Public Law Studies Quarterly, 54(3), 1549–1574. doi: 10.22059/jplsq.2023.357301.3290 (in Persian)
19. Riazimand, M. (2018). *Legal Aspects of Digital Currencies*. Bartar Andishan Publishing, Tehran. (in Persian)
20. Rahbar, F. (2003). *Money Laundering and Its Consequences*. Economic Research Journal, 38(3), 33–55. (in Persian)
21. Sadeghi-Zadeh, M., & Kheradmandnia, S. (2024). *Generative AI: Challenges and Requirements for Development and Implementation*. Majlis Research Center Expert Reports Monthly, 32(4), Report No. 19879. (in Persian)
22. TRM Labs. (2023). *Iran's Crypto Economy*. Retrieved from https://www.trmlabs.com/resources/blog/iran-crypto-economy
23. Vahhedzadeh, S., & Malekzadeh, F. (2020). *Jurisprudential and Legal Status of Digital Currencies*. Khorsandi Publishing, Tehran. (in Persian)
24. Wilson, J., & Lee, M. (2023). *Real-Time Monitoring Systems in Cryptocurrency Exchanges*. Digital Security Journal, 19(1), 78–93.
25. Ebadi-Lomar, S. (2020). *Investment in Digital Currencies and Its Status in Iran*. Dibagaran Tehran Institute of Arts and Culture, Tehran. (in Persian)

Cryptocurrency security in cyberspace and the challenges ahead

Abstract

In recent decades, the rapid spread of digital currencies, especially Bitcoin and Ethereum, along with the development of blockchain technology, has created fundamental changes in global financial systems. Although these developments have provided numerous opportunities for economic development and improved efficiency of financial systems, they have also brought with them complex and emerging cybersecurity challenges. The main issue in dealing with digital currencies is the comprehensive identification of security challenges arising from the decentralized and anonymous nature of transactions, as well as the utilization of the capacities of blockchain technology as an efficient tool for strengthening cybersecurity.

The present study examines various aspects of this issue with a theoretical approach and a descriptive-analytical method using library resources. The main objective of the article is to identify and analyze financial and cyber crimes related to digital currencies, explain the security challenges arising from the development of this technology, and examine technological opportunities to deal with its threats. The research findings show that cryptocurrencies, in addition to providing a suitable platform for crimes such as money laundering, terrorist financing, digital asset theft, phishing attacks, and ransomware, also offer important opportunities for improving cybersecurity. In particular, blockchain technology, with its ability to record transactions immutably and create secure decentralized networks, has a high potential for increasing transparency and user trust. Also, using artificial intelligence and machine learning to analyze suspicious behaviors in cryptocurrency transactions is an effective solution for preventing digital financial crimes. The overall conclusion of this research is to emphasize the need to develop comprehensive and interdisciplinary strategies that include legal, technological, and educational dimensions to protect users' personal information and digital assets, as well as to create appropriate legal and technological platforms for optimal exploitation of the opportunities of cryptocurrencies in line with the economic development of countries. In addition, international cooperation, regulatory standardization, and investment in innovative cybersecurity and blockchain technology research are essential requirements for managing this emerging phenomenon. Ultimately, achieving sustainable security in the field of digital currencies requires a holistic and synergistic approach between governments, researchers, and IT industry actors.

Keywords: Cyber security, Digital currencies, Crimes, Challenges