*فصلنامه مطالعات راهبردی فضای سایبر*
*سال دوم، شماره چهارم، پائیز ۱۴۰۱*
*مقاله چهارم از صفحات ۱۲۴-۹۷*

# تهدیدهای رمز ارزها بر امنیت اقتصادی و ارائه راهکارهای مقابله با آن

محمد بابک[۱]، امیر مسعود سعادتمند[۲]، محمدرضا مرادی[۳]

تاریخ دریافت: ۱۴۰۰/۱۱/۳۰ تاریخ پذیرش: ۱۴۰۱/۰۴/۳۰

## چکیده

امروزه امنیت مفهومی گسترده و پیچیده پیداکرده است. هرچند درگذشته، امنیت نظامی و یا سیاسی دارای بیشترین اهمیت بود، لیکن اکنون امنیت اقتصادی نیز در اولویت بالایی قرارگرفته و رصد تهدیدهای اقتصادی، از مباحث راهبردی هر حاکمیتی شده است. با گسترش فضای سایبر در همه حوزه‌ها ازجمله اقتصاد، رمز ارزها شکل گرفتند و شناخت درست تهدیدها و فرصت‌های آن، اولین قدم در راستای اخذ راهبرد صحیح حکمرانان در قبال این پدیده جدید مالی و سایبری است چراکه ویژگی‌های خاص رمز ارزها، آن‌ها را به‌عنوان پول آینده اقتصاد جهانی مطرح ساخته است و در کشور ما نیز لزوم پرداختن به آن حس شده اما هنوز قانون خاصی برای آن تدوین‌نشده؛ بنابراین هدف این تحقیق، شناخت درست تهدیدهای رمز ارزها و تأثیر آن بر امنیت اقتصادی کشور و ارائه راهکارهای صحیح در قبال آن است.

این تحقیق ازنظر هدف کاربردی، متدولوژی آن کیفی، روش تحقیق داده بنیاد، ابزار گردآوری اسناد و مصاحبه و درنهایت شیوه تحلیل، کدگذاری سه‌گانه داده بنیاد می‌باشد. بر اساس نتایج حاصله تعداد ۲۵ کد منحصربه‌فرد، شش مفهوم و دو مقوله استخراج گردید و در دو مرحله نیز این کدها به تائید خبرگان رسید و به کمک نرم‌افزار مکس‌کیودا نمایش داده شد. تهدیدها به دو بخش ملی (مشکلات امنیتی، مشکلات اقتصاد کلان و فقدان رگولاتوری) و حوزه بین‌المللی (مشکلات نظری و دانشی، جرائم مالی و مشکلات حفظ سرمایه) تقسیم شدند و بهترین راهکارها نیز، شروع به‌موقع جهت شناخت وضعیت رمز ارزها (استخراج، خریدوفروش و کیف پول‌ها) و ورود قانون‌گذار برای منظم کردن (رگلاتوری) قبل از تبدیل‌شدن به یک بحران اجتماعی – اقتصادی است.

کلیدواژه‌ها: رمز ارز، امنیت اقتصادی، اقتصاد دیجیتال.

۱. دانش‌آموخته مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول)MohammadBabkk@gmail.com
۲. دانش‌آموخته مقطع دکتری دانشگاه عالی دفاع ملی ph.amirSaadatmand@gmail.com
۳. دانش‌آموخته مقطع دکتری دانشگاه عالی دفاع ملی MohamadRezaMoradii@gmail.com

**مقدمه**

ارزش امنیت در هر مجموعهٔ اجتماعی و برای هر ملتی، با چیز دیگری قابل مقایسه نیست و هر جامعه‌ای در برای تحقق اهداف خود نیاز به امنیت دارد. به‌عبارت دیگر، نهادها و سازمان‌های جامعه باید در محیطی آرام و امن، بدون دغدغه خاطر و عوامل مزاحم، اهداف جامعه را تحقق بخشند. نقش مدیریت در این زمینه اهمیت بسزایی دارد؛ زیرا می‌تواند با برنامه‌ریزی‌ها، سازمان‌دهی‌ها و هماهنگی‌ها و نظارت‌ها و البته قانون‌گذاری درست و به‌موقع، در ایجاد این امنیت نقش مهمی بر عهده داشته باشد. نهادهای یک جامعه اگر از این امنیت بی‌بهره باشند، در جهت تحقق اهداف خود ناخواسته با مشکلات بی‌شماری روبرو می‌گردند که آثار زیان‌بخش و جبران‌ناپذیری برای جامعه در بر خواهد داشت (حق نویس، شاهین، ۱۳۹٦: ۲).

اهداف امنیت ملی را می‌توان حفظ نظام جمهوری اسلامی، برخوردار از قدرت بازدارندگی، برقراری عدالت اجتماعی، رفع تبعیض و تأمین رفاه عمومی، حفظ و تحکیم انسجام ملی، ثبات سیاسی و نظم و آرامش عمومی، حفظ تمامیت ارضی، سرمایه‌های ملی و زیرساخت‌های حیاتی کشور و نهایتاً دوری از تهدیدها است ضمن اینکه رصد کردن مسائل بین‌المللی و حوادث بین‌المللی و خبرهای بین‌المللی موجب می‌شود که ما بدانیم تهدیدها چیست (بیانات رهبری ۱۳۹٤/٦/۲۵)؛ بنابراین شناخت مسائل محیط پیرامونی در تمام حوزه‌ها ازجمله فضای سایبر، می‌تواند در ارتقای امنیت ملی مفید و مؤثر باشد.

امنیت ملی دارای ابعاد زیادی است ابعادی مانند امنیت فرهنگی، امنیت سیاسی، امنیت اقتصادی امنیت اجتماعی، امنیت قضایی، امنیت نظامی و انتظامی، امنیت اخلاقی و روانی، امنیت فکری و معنوی، امنیت علمی و فناوری و امنیت زیست‌محیطی. در بین این مؤلفه‌ها مسلماً امنیت اقتصادی از اهمیت بالایی برخوردار است. امنیت اقتصادی باید به‌گونه‌ای باشد که کار اقتصادی، حرکت اقتصادی، تلاش اقتصادی، رونق اقتصادی و سازندگی اقتصادی، از هر نوع، امکان‌پذیر باشد (بیانات رهبری ۱۳۷۸/٦/۱۰).

ازنظر رابرت ماندل امنیت اقتصادی عبارت است از: «میزان حفظ و ارتقای شیوه زندگی مردم یک جامعه از طریق تأمین کالاها و خدمات، وهم از مجرای عملکرد داخلی و هم حضور در بازارهای بین‌المللی.» باری بوزان نیز از امنیت اقتصادی سخن رانده و در سه سطح فردی، گروه‌ها و طبقات به این موضوع می‌پردازد اما در نگرش اسلامی، علاوه بر تعاریفی که از امنیت اقتصادی مطرح گردید در ساده‌ترین تعاریف، امنیت مزبور به این معنا است که مردم در اموالشان امنیت داشته باشند و دولت با مدارا و رعایت عدل و انصاف و با توجه به دیگر اخلاق پسندیده اسلامی، از آنان مالیات و زکات اخذ نماید.

در شرایط امروز جهان لزوم درک و شناخت بهتر و عمیق‌تر تحولات دنیای فناوری و اتخاذ سیاست‌های هماهنگ و مؤثر جهت مشارکت فعال در جامعه فناوری‌های نوین به‌عنوان گزینه‌ای راهبردی فراروی سیاست‌گذاران و برنامه‌ریزان کشور مطرح است. این فناوری‌ها به‌عنوان موتور محرک توسعه در جوامع پیشرفته برای افزایش دانایی و نوآوری نقش مهمی ایفا می‌کند و باعث تحولاتی بنیادی در ارکان اقتصادی، اجتماعی و فرهنگی کشورها می‌شود.

یکی از این فناوری‌های نوین که مستقیماً در اقتصاد آینده جهان تأثیرگذار خواهد بود، استفاده از فناوری زنجیره بلوک یا بلاک چین است. بلاک چین، دفتر کلی است که اطلاعات ثبت‌شده روی آن، میان تمام افرادی که به آن متصل می‌شوند، به اشتراک گذاشته می‌شود و کاربردهای زیادی چون مالی و بانکی، رمز ارزها، قرارداد هوشمند، اینترنت اشیا، خدمات شهری، انتخابات، بهداشت و درمان و زنجیره تأمین دارد. فناوری بلاک چین فضایی را برای ما فراهم کرده است که ما می‌توانیم در این فضا مبادلات را ساماندهی کنیم و ابزارهای متعددی خلق کنیم که قابلیت مبادله با هر کالای دیگری را دارند بدون اینکه تأیید بانک مرکزی روی آن باشد و یا اصلاً نیازی به تأیید آن باشد (رنجبر فلاح، محمدرضا، ۱۳۹۷).

روند رو به رشد بهره‌گیری از رمز ارزها بر پایهٔ فناوری زنجیره بلوک به محدوده جغرافیایی خاصی تعلق نداشته و می‌توان گفت که ارزهای رمزینه و فناوری زنجیره بلوک جدیدترین نوآوری‌هایی هستند که در قالب یک بازار مهیج

دیجیتالی، باعث شده‌اند افراد در سرتاسر دنیا هرروز به دنبال یادگیری مفاهیم آن و بهره‌مندی از آن باشند (صالحان، علیرضا و امید الهی، ۱۳۹۷). تلاش زیاد فعالان قانون‌گذار در سرتاسر دنیا برای قانون‌گذاری و نظم‌بخشی بر مقوله رمز ارزها خود گواه بر این مدعاست که آینده اقتصاد کشورها و درنتیجه آینده امینت اقتصادی کشورها به توسعه قانون‌مند پدیده‌های اقتصادی من‌جمله رمز ارزها وابسته است، این وادی بسیار پیچیده و جدید، عزمی راسخ می‌خواهد تا بتوان بر آن چیره شد.

به‌طورقطع، مردم برای حفظ دارایی‌های خود و یا سود بیشتر، به سمت رمز ارزها خواهند رفت و سیاست‌گذاری به‌موقع باعث کاهش خطرات منافع عامه و نظارت بیشتر حاکمیت می‌شود و همچنین عدم خط‌مشی گذاری می‌تواند نارضایتی‌های عمومی به همراه آورده که زمینه‌ساز بحران‌های اقتصادی و سپس سیاسی و درنهایت منجر به بحران‌های امنیتی گردد. از دغدغه‌های گسترش این رمز ارزها می‌توان به پول‌شویی، تأمین مالی تروریسم، خریدوفروش قاچاق و فرار مالیاتی اشاره کرد.

امروزه جمهوری اسلامی ایران جزء کشورهایی است که بیشترین حملات تروریستی سایبری به زیرساخت‌های مالی، هسته‌ای و نظامی خود را متحمل می‌شود. به ثمر نشستن هرکدام از این حملات می‌تواند نتایج فاجعه باری برای امنیت و سلامت کشور و ملت به همراه داشته باشد؛ بنابراین بایستی هم امنیت فضای سایبر در کشور را ارتقاء و هم بتوانیم با تقویت مکانیسم‌های امنیتی در بعضی موارد حتی مقابله‌به‌مثل نماییم (مقدسی و همت، ۱۳۹۷).

لزوم برنامه‌ریزی و مقابله با تهدیدهای سایبری به‌عنوان یکی از مهم‌ترین تهدیدها و آسیب‌ها با توجه به اقدامات تخریبی علیه آن نظیر استاکس نت واضح و روشن است؛ بنابراین با اتخاذ یک روش و برنامه‌ریزی مناسب می‌توان این روند را معکوس نمود و مهم‌ترین کار ویژه امنیتی یک نظام، یعنی تبدیل تهدیدها به فرصت‌ها را صورت داد (موسوی، ۱۳۹۸).

در آینده نزدیک، در کشور ما نیز، مردم برای حفظ دارایی‌های خود و یا سود بیشتر، به سمت رمز ارزها خواهند رفت؛ بنابراین وجود یک سیاست‌گذاری منسجم در قبال آن‌ها

باعث کاهش خطرات منافع عامه و نظارت بیشتر حاکمیت می‌شود و همچنین عدم توجه به آن می‌تواند نارضایتی‌های عمومی را به همراه آورد بنابراین اکنون که شرکت‌هایی همچون تلگرام با انتشار رمز ارز گرام، امنیت اقتصادی و نهایتاً امنیت ملی کشورها را هدف قرار داده‌اند باید به‌قدری زیرکانه عمل کنیم که از این فناوری برای کاهش مشکلات و محدودیت‌های اقتصادی کشور استفاده کرده و از تهدیدهای بالقوه آن در امان باشیم؛ بنابراین ورود حاکمیت به فناوری بلاک چین و شناخت فرصت‌ها و تهدیدهای آن می‌تواند نقطه عطفی در برون‌رفت جامعه از برخی مشکلات اقتصادی مانند تحریم‌ها گردد تا با ارائه چارچوبی برای سیاست‌گذاری رمز ارزها، خطرات در کمین نشسته اشاره‌شده را کاهش داده و کشور را در مسیر اقتصاد مقاوم، درون‌زا و برون‌نگر هدایت کند و با هجوم ناگهانی مردم به بازار جذاب رمز ارزها از ورشکستگی بانک‌ها و مؤسسات مالی که خود زمینه‌ساز بحران‌های امنیتی است جلوگیری نماید؛ بنابراین سؤال این تحقیق به این صورت تبیین می‌شود که «تهدیدهای رمز ارزها چه تأثیری می‌تواند بر امنیت اقتصادی کشور داشته باشد و راهکارهای پیشنهادی برای مقابله با هر تهدید چیست؟»؛ بنابراین علی‌رغم فرصت‌های زیادی که برای رمز ارزها متصور است اما پرداختن به بخش تهدیدهای هر پدیده جزء لاینفک امنیت به‌حساب می‌آید و اکنون زمان طلایی برای پرداختن همه‌جانبه به رمز ارزها و زیرشاخه‌های آن می‌باشد تا اشتباهاتی که سال‌های گذشته در مواجهه با شبکه‌های اجتماعی و پیام‌رسان‌ها انجام شد، در رویارویی با رمز ارزها تکرار نشود.

## مبانی نظری تحقیق و ادبیات تحقیق

### امنیت

امنیت ازنظر لغوی به معنی، ایمن بودن، ایمن شدن و در امان بودن می‌باشد (تهامی، ١٣٩٤). ریشه لغوی امنیت از زبان عربی گرفته و در زبان فارسی متداول شده است و تقریباً با مفهوم یکسانی مورداستفاده فارسی‌زبانان قرار می‌گیرد. امنیت از کلمه امن می‌آید که واژه‌های آرامش یافتن، بیمناک نبودن و نترسیدن را متبلور می‌سازد و در مفهوم مصدری از

«الامن» به‌عنوان دستیابی به اطمینان و آرامش پس از رهایی از ترس نام‌برده می‌شود. بری بوزان امنیت را رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل یکپارچگی کارکردی در مقابل نیروی تغییردهنده تعریف می‌کند (بوزان[۱]۱۹۹۱).

**امنیت ملی و ویژگی‌های آن**

امنیت ملّی یک کشور در درجهٔ اوّل به معنای تأمین شرایطی است که کشور را از تعرض دیگران به استقلال سیاسی، ارزش‌های فرهنگی و رفاه اقتصادی دورنگه دارد (بیانات رهبری ۱۳۷۳/٤/۲۹). بنابراین می‌توان دو بعد اساسی برای امنیت ملی هر کشوری قائل شد: یکی، بعد سلبی که دلالت بر رفع و تقلیل تهدیدهای موجود دارد و دیگری، بعد ایجابی که حکایت از ارتقاء و بهینه‌سازی وضعیت زیست‌بوم جوامع در عرصه‌های مختلف سیاسی اجتماعی، اقتصادی، نظامی و دارد (افتخاری و خیراتی به نقل از کریمیمله، ۱۳۸۳) در مورد خصوصیات و ویژگی‌های امنیت ملی نیز به‌طور عمده بر روی سه ویژگی تحول‌پذیری، نسبی بودن و ذهنی بودن مفهوم امنیت ملی تأکید شده است. در مورد ویژگی اول، یعنی تحول‌پذیری مفهوم امنیت ملی باید گفت به دلیل نیاز حکومت به تعریف مشخصی از امنیت ملی، صاحب‌نظران کوشیده‌اند به این مهم دست یابند، اما تاکنون هیچ‌یک از آنان تعریف جامعی از این مفهوم ارائه نداده‌اند. در مورد ویژگی دوم یعنی نسبی بودن نیز باید افزود که ادعای دست‌یابی به امنیت مطلق، قابل‌تصور نیست .کشوری که ممکن است ازلحاظ نظامی و اقتصادی دچار ناامنی نباشد، تهدیدهایی با ماهیت فرهنگی و اجتماعی، امنیت آن را در معرض خطر قرار دهد. جنبه دیگر نسبی بودن امنیت، توانایی‌های نسبی دولت‌ها برای مقابله با تهدیدهاست (خلیلی پور رکن‌آبادی، علی و یاسر نورعلی وند، ۱۳۹۱). ویژگی آخر یعنی ذهنی بودن امنیت به برداشت‌ها از احساس امنیت یا عدم امنیت

۱ Buzan

مربوط می‌شود و ممکن است افراد و گروه‌های مختلف نسبت به آن نظر واحـدی نداشـته باشند.

**تهدید**

کلیهٔ عوامل و پدیده‌هایی که معمولاً در خارج از محیط موردمطالعه وجود دارد را شامل می‌شود مانند قابلیت‌ها و توانمندی‌ها، نیات و اقدامات حریف، رقیـب یـا دشـمن بـالقوه و بالفعل که می‌تواننـد مجموعـه را بـه مخـاطره انداختـه و از رسـیدن بـه اهـداف مـوردنظر جلوگیری نموده یا انجام موفقیت‌آمیز مأموریت را با اختلال مواجه نمایند.

## ارز دیجیتال[1] ارز مجازی[2] و رمز ارزها[3]

ارزهای دیجیتال، ارزهایی هستند که به‌صورت الکترونیکی ذخیـره و منتقـل مـی‌شـوند. هرگونه پولی که بر مبنای صفر و یک باشد در این تعریف می‌گنجد. مثلاً پول‌هـای موجـود در حساب بانکی بازنمایی کننده پول واقعی هستند که جایی نگهداری می‌شوند، در تعریف ارز دیجیتالی جای می‌گیرند (ونگر ٢٠١٤). بیت کوین‌ها هم چون مبنای صفر و یک دارنـد ارز دیجیتالی هستند درنتیجه ازنظر حقوقی عبارت «ارز دیجیتالی» یک عبارت موسع اسـت (مرکز پژوهش‌های مجلس شورای اسـلامی، ١٣٩٧). ارزهـای مجـازی گونـه‌ای از ارزهـای دیجیتالی به شمار می‌آیند، اما هرگونه ارز دیجیتالی ارز مجازی بـه شـمار نمـی‌رود (وگنـر، ٢٠١٤). رمز ارزهایی مانند بیت کوین نیز گونه‌ای از ارزهای مجازی هستند که برای امنیـت خود از رمزگذاری استفاده می‌شوند اما همه ارزهای مجازی رمز ارز نیستند.

**تأثیر تهدیدهای سایبری بر امنیت ملی**

بسیاری از کارشناسان و تحلیل گران حوزه امنیت، بر این باورند که پایان یـافتن دوران جنگ سرد نه‌تنها منجر به امن‌تر شدن جهان نشده است، بلکه به‌وجود آمـدن چـالش‌هـای

1. Digitall Currency
2. Virtual Currency
3. Cryptocurrency

امنیتی غیرنظامی جدیدی همچون تخریب محیط‌زیست، کاهش رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی‌تری نسبت به گذشته مواجه ساخته است. تحلیل گران بر این باورند که اهمیت این مسائل جدید نه‌تنها بازاندیشی درتهدیدهای امنیتی، بلکه تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد (خلیلی پور رکن‌آبادی و نورعلی وند.۱۳۹۱).

درعین‌حال، انتقادی که بر ادبیات موجود امنیت وارد است این است که اغلب این متون به تهدیدهای سایبر به‌عنوان یکی از همین چالش‌های امنیتی جدید که در این زمینه بسیار هم پراهمیت به‌نظر می‌رسد، توجه اندکی داشته‌اند. همان‌طور که در بخش‌های پیشین اشاره شد، آنچه در مورد این تهدیدهای جدید قابل‌توجه است، این است که ویروس‌ها، کرم‌ها، هکرها و حملات اینترنتی، امروزه واقعیت مسلم و روزمره هستند. حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به‌عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی که ایالات‌متحده آمریکا اعلام کرده است که این حملات را به‌عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد از طرف دیگر، بحث و گفتگو درباره این تهدیدات متأثر از انقلاب مداوم اطلاعات و رسوخ آن به تمام جنبه‌های زندگی بشر امروز است؛ بنابراین، در بخش پیش رو، ابتدا به انقلاب اطلاعات و تأثیر شگرفی که بر روی قدرت و منابع آن خواهد داشت پرداخته و سپس از این رهگذر، تهدیدهای سایبری وابسته به آن و تأثیری که می‌تواند بر امنیت ملی داشته باشد، موردبررسی قرار خواهد گرفت (خلیلی پور رکن‌آبادی و نورعلی وند، ۱۳۹۱).

پیش از سال ۲۰۱۷ و اوایل آن، بیت کوین بیش از ۹۰ درصد از سهم بازار رمز ارزها را تشکیل می‌داده و بارونق چشمگیر این بازار در سال ۲۰۱۷ و ورود رمز ارزهای جدید، این سهم کاهش‌یافته و به حدود ۵۰ درصد رسیده است. سهم رمز ارزهای دیگر به‌مرور افزایش‌یافته و تا حدودی تسلط کامل بیت کوین را بر این بازار کاهش داده است (نوری، ۱۳۹۷) اما با توجه به سیل خروشان خرید بیت کوین در ایران و عطش بسیار مردم و به‌ویژه جوانان نیاز به بررسی دقیق فرصت‌ها و تهدیدهای بیت کوین در ایران به‌شدت

احساس می‌شد، در این مقاله با نگاه به حفظ امنیت ملی کشورمان تهدیدات بالقوه رمز ارزها را بررسی می‌نماییم. توجه ویژه به رمز ارزها آنجا لزوم دوچندان پیدا می‌کند که آمار رجوع مردم به‌ویژه جوانان برای خرید رمز ارزها و یا استخراج آن‌ها را در بازار می‌بینیم، شاید مهم‌ترین فرصت، شروع به‌موقع جهت شناخت وضعیت میدان ورود قانون‌گذار برای امور رگلاتوری باشد.

## نیروهای مسلح و رمز ارزها

قدر مسلم در کشور ما با توجه قانونی نبودن رمز ارزها (البته فعلاً) هنوز هیچ‌گونه فعالیتی از ورود نیروهای مسلح به این حوزه مشاهده نشده است اگرچه در مراکز تحقیقاتی و آموزشی به این امر پرداخته‌شده است لیکن ارتش برخی کشورها همچون آمریکا و روسیه سرمایه‌گذاری‌های زیادی در خصوص بلاک چین و رمز ارز انجام داده‌اند که نشان می‌دهد نیروهای مسلح هر کشور هم می‌توانند همچون سایر بخش‌ها از فرصت‌های رمز ارزها استفاده کرده و یا در معرض تهدیدهای آن قرار گیرند.

### پیشینه‌شناسی

از زمان استخراج اولین بیت کوین در سال ۲۰۰۹، اندر مزایا و معایب و همچنین فرصت‌ها و تهدیدهای رمز ارزها سخنان بسیاری گفته‌شده و تحقیقات زیادی انجام‌شده است.

در تحقیقی که مرکز پژوهش‌های مجلس شورای اسلامی در سال ۱۳۹۷ با موضوع ارز مجازی: قانون‌گذاری در کشورهای مختلف و پیشنهادها برای ایران انجام داده، تهدیدهای آن را غیاب یک ساختار حکمرانی تاب آور و قابل‌اتکا، نوسانات بالای ارزهای مجازی و قابلیت خلق حباب‌های سفته‌بازی و غیاب نظارت‌های تنظیم مقرراتی سنتی، پادمان‌ها و حقوق حفاظتی مناسب، عدم قطعیت حقوقی پیرامون کاربردهای جدید دفاتر کل توزیع‌شده، مصرف بالای انرژی، تأثیر بر سیاست‌های پولی، قابلیت کاربرد در تراکنش‌ها بازارهای سیاه، پول‌شویی، تأمین مالی تروریسم و فرار و تقلب مالیاتی عنوان نموده است.

علی‌اصغر دهقانی در مقاله بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا در سال ۱۳۹۷ به این نتیجه رسیده‌اند که یکی از این سازوکارها که در دوران جنگ سرد و برای سال‌ها، منطق استراتژیک جنگ سرد را به طرزی موفقیت‌آمیز شکل داده بود، بازدارندگی است. باوجود موفقیت این سازوکار در عرصه‌های سنتی، فهم بازدارندگی در فضای سایبر مشکل است؛ چراکه ذهن ما با ادبیات جنگ سرد، مبنی بر بازدارندگی به‌مثابه تهدید به‌تلافی یک حمله هسته‌ای با استفاده از ابزارهای هسته‌ای، شکل‌گرفته است. مقایسه وضعیت کنونی با بازدارندگی جنگ سرد اشتباه است. جلوگیری از آسیب در فضای سایبر، سازوکارهای پیچیده‌ای مانند تهدید به‌تلافی، انکار، گرفتار کردن و هنجارها را می‌طلبد.

حاجی ملا میرزایی در پول مجازی اذعان داشته که پول مجازی، ترکیبی از فنّاوری‌های رمزنگاری، ذخیره‌سازی داده، سامانه‌های توزیع‌شده و محاسبات ریاضی است که پیش‌بینی می‌شود در آینده‌ای نه‌چندان دور، جایگزین پول‌های اعتباری فعلی شود و ابعاد فنی و ماهیت‌شناسی رمز ارزها، بررسی تجارب دیگر کشورها، بررسی قوانین و مقررات و احکام فقهی ناظر بر آن‌ها و شناخت فرصت‌ها و تهدیدهایی که پول مجازی در پی دارد و سیاست‌هایی که در قبال آن‌ها می‌توان رفتار کرد را تبیین نموده است (۱۳۹۸: ۸۹).

بابایی و شریف‌زاده در پژوهشی با موضوع بررسی فواید و مضرات رمز ارزها و تأثیر آن‌ها در پول‌شویی به این نتیجه رسیده‌اند که قانون‌گذاری نباید از دستیابی رمز ارزها به پتانسیل مثبت آن‌ها جلوگیری کند. در طرف دیگر، قانون‌گذاری باید از تبدیل‌شدن رمز ارزها به هدفی برای فعالیت مجرمانه جلوگیری کند (۱۳۹۹).

در تحقیقی که مجمع تشخیص مصلحت نظام در سال ۱۳۹۸ با عنوان پدیده رمز ارز، مخاطرات، فرصت‌ها و نحوه سیاست‌گذاری انجام‌شده است تهدیدهای فضای رمز ارزها را این‌گونه برشمرده‌اند: هجوم مردم به بازار جذاب رمز ارزها و امکان بروز بحران در مؤسسات مالی؛ کیف پول‌های الکترونیکی، صرافی‌ها و سکه‌های بدون مجوز؛ هژمونی مالکان رمز ارزها و امکان حمله به اقتصاد ایران؛ امکان اعمال تحریم‌های جدید توسط

کنگره ایالات‌متحده به بهانه استفاده از رمز ارزها؛ به‌کارگیری رمز ارزها توسط گروه‌های تروریستی؛ خلق انبوه سکه توسط نهادهای مالی و شرکت‌های فناوری؛ ریزش شدید بازار رمز ارزها و ایجاد نارضایتی عمومی.

شاهین حق نویس در تحقیقی با عنوان کنکاشی در تهدیدات و فرصت‌های رمز ارزها از دیدگاه امنیت ملی، اذعان داشته که شناخت درست تهدیدات و فرصت‌های رمز ارزها اولین قدم در راستای اخذ راهبرد صحیح در قبال این پدیده جدید مالی و سایبری است. در این مقاله با نگاه به حفظ امنیت ملی کشور، ابتدا فرصت‌ها و سپس تهدیدات بالقوه رمز ارزها را بررسی نموده است. توجه ویژه به رمز ارزها آنجا لزوم دوچندان پیدا می‌کند که آمار رجوع مردم به‌ویژه جوانان برای خرید رمز ارزها و یا استخراج آن‌ها را در بازار می‌بینیم، شاید مهم‌ترین فرصت، شروع به‌موقع جهت شناخت وضعیت میدان و ورود قانون‌گذار برای امور رگولاتوری باشد. در این تحقیق به مباحث امنیت ملی اشارهٔ چندانی نشده و فقط به‌صورت کلی به فرصت‌ها و تهدیدهای رمز ارزها پرداخته است (حق نویس، ١٣٩٦).

کیان ولی (٢٠١٦) در پایان‌نامه خود ضمن برشمردن خطرات فراگیری پول‌های رمزنگاری‌شده ازجمله پول‌شویی، فرار مالیاتی، جرائم اینترنتی و سایبری در خریدوفروش کالاهای غیرمجاز، اثبات کرده‌اند که با گسترش این پول‌ها راه تخلفات فوق هموارتر و آسان‌تر شده است. شواهد این پژوهش نشان می‌دهد که پول‌های رمزنگاری‌شده، به‌خصوص در گسترش و تسهیل جرائم سایبری نقش مؤثری ایفا کرده است (کیان ولی ٢٠١٦،٥).

جان‌پرور و حیدری (١٣٩٠) در مطالعه‌ای با بررسی تعداد بیش از ٣٠ مقالهٔ داخلی و خارجی با عنوان آسیب‌شناسی فضای سایبر بر امنیت اجتماعی با تأکید بر شناخت آسیب‌ها و چالش‌هایی که فضای سایبر بر امنیت اجتماعی کشورمان ایجاد نموده، پیشنهادهایی در جهت افزایش توانایی مقابله با آسیب‌های ناشی از فضای مذکور ارائه نموده است. کورکی نژاد (١٣٩٤) در پایان‌نامه کارشناسی ارشد خود در دانشگاه تهران با عنوان تروریسم

سایبری (دهشت افکنی در فضای سایبر) و راهکارهای افـزایش امنیـت سـایبر در ایـران بـا تأکید بر عملکرد دولت ایالات‌متحده آمریکا با بررسی تأثیرات تهدیدهای سـایبری بـر روی فرد و بخش‌های دولتی و خصوصی مؤکـداً بـر قـانون ارتقـاء آمـوزش امنیـت سـایبری در سطوح ملی و انجام انواع مختلف پژوهش‌های حقوقی در این زمینه تأکیـد و اصـرار داشـته است.

نور محمد (۱۳۹۰) در مطالعه‌ای با عنوان جنگ نرم، فضـای سـایبر و امنیـت جمهـوری اسلامی ایران به این نتیجه رسیده که جنگ نرم سایبری یکی از مهم‌ترین جلوه‌هـای تهدیـد آفرین امنیت ملی جمهوری اسلامی ایران است. صادقی و نادری (۱۳۹٤) در تحقیقی دیگـر با موضوع تحلیل ابعاد امنیت دولت در ایران قرن ۲۱، در فصلنامهٔ دولت پژوهی، با اشاره به محورهای اساسی مکتب کپنهاگ (مطرح‌شدن امنیت به‌عنـوان مفهـومی بینـا ذهنـی، دولـت به‌عنوان مرجع امنیت، موسع بودن امنیت و ابعاد پنج‌گانه آن) امنیت ملی را بـه‌عنـوان مرکـز ثقل امنیت قلمداد نموده‌اند.

سانچز (۲۰۱۸) در مقاله‌ای با عنوان نقش بانک مرکزی در ارزهای دیجیتـال، تـأثیر یـک ارز دیجیتالی صادرشده توسط بانک مرکزی را بر نرخ بهره، سطح فعالیت اقتصـادی و رفـاه را بررسی می‌کند. نتایج این مقاله حاکی از این امر اسـت کـه اگـر خانوارهـا و بنگـاه‌هـای اقتصادی ارز دیجیتال را نگهداری و استفاده نمایند، معرفی یک ارز دیجیتالی توسـط بانـک مرکزی یک نوآوری بالقوه تاریخی در سیاست پولی کشورها است. مقـدار قابـل‌تـوجهی از چنین ارز، تغییر قابل‌توجهی در نقدینگی کل کشور و نوع دارایی‌هایی کـه مبادلـه مـی‌شـود ایجاد می‌کند (سانچز ۲۰۱۸،٦).

نوری و نواب پور (۱۳۹۷) در پژوهشی با موضوع چالش‌ها و فرصت‌های رمزینه ارزهـا در اقتصاد ایران با رویکرد تنظیم‌گری، به بیان انـواع ارز مجـازی پرداختـه و پـس از تبیـین سازوکار پول مجازی (بیت کوین)، چالش‌ها و ریسک‌هـای ارزهـای مجـازی را ارائـه داده است (نوری و نواب پور، ۱۳۹۷).

تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن دیگر مقاله‌ای است که محمدرضا موسوی و همکاران آن تقریر داشته و در آن عنوان داشته‌اند که: جهانی‌شدن که یکی از ابزارهای آن، فن‌آوری‌های سایبری می‌باشد، هم یک فرصت و هم یک تهدید به‌شمار می‌رود تروریسم سایبری باهدف نابودسازی ساختارهای اساسی یک کشور ازجمله این تهدیدات (علیه امنیت ملی) می‌باشد.

بررسی فقهی پول مجازی، ماهیت شناسی پول مجازی و تحلیل فقهی پدیده پول، بر پایه نظریه مال اعتباری بودن پول، احکام شرعی در خصوص پول مجازی را تبیین می‌کند. این مقاله در تحلیل فقهی پول مجازی عناصر کلیدی و اجزای تشکیل‌دهنده پول مجازی شامل (ماهیت و پشتوانه پول، خصوصی بودن، الکترونیکی بودن و ورود پول مجازی به دنیای حقیقی) مورد واکاوی قرار داده است (سلیمانی نژاد و همکاران ١٣٩٦).

هایلمن در مقاله مطالعه پایدار جهانی رمز ارزها که در دانشگاه کمبریج در سال ٢٠١٧ به چاپ رسیده، تهدیدهای آن را ماهیت رمز ارزها، پول یا کالا، ارزش واقعی یک رمز ارز، نوسانات زیاد ارزش، نبود پشتیبانی حقوقی، امکان اثرگذاری منفی بر روی بانک‌ها و سامانهٔ بانکداری موجود، آسیب‌پذیری بسیار بالای ولت‌ها (کیف‌های پول دیجیتال) در برابر هکرها و امکان استفاده گروه‌های تروریستی از رمز ارزها دانسته است.

با بررسی پیشینهٔ پژوهش‌ها در می‌یابیم که در غالب این تحقیق‌ها، فرصت‌ها و تهدیدهای رمز ارزها به‌صورت کلی و همچنین اثر تهدیدهای سایبری بر امنیت ملی بیان‌شده اما به‌طور خاص تأثیر تهدیدهای رمز ارزها بر امنیت ملی کشور موردتوجه واقع نشده است و راهکارهایی نیز برای آن ارائه نشده است.

## روش‌شناسی تحقیق

ازآنجایی‌که هدف این پژوهش، شناخت درست تهدیدهای رمز ارزها و تأثیر آن بر امنیت اقتصادی کشور است، از روش کیفی استفاده‌شده است؛ بر این اساس، نخست به

بررسی تهدیدهای رمز ارزها و ارتباط آن‌ها با امنیت اقتصادی پرداخته شد. سپس، با اجرای مصاحبه و طرح پرسش‌های باز برای اکتشاف و توصیف نگرش مصاحبه‌شوندگان، انبوهی از متغیرها و تهدیدهای حوزه رمز ارز جمع‌آوری شدند و درنهایت، به کمک روش نظریهٔ برخاسته از داده‌ها و طی فرایندی به شیوهٔ کدگذاری باز و محوری، یافته‌های پژوهش دسته‌بندی و تبیین شدند. روش جمع‌آوری داده‌ها نیز روش کتابخانه‌ای در مرحله ادبیات تحقیق، روش گراندد تئوری برای تحلیل داده‌ها (ثبت و ضبط مصاحبه‌ها، مراجعه به اسناد و مقالات بین‌المللی، تجربیات شخصی، استفاده از نرم‌افزارهای مربوطه) و کدگذاری داده‌ها و همچنین آزمون **خبرگان** در مرحله اعتبارسنجی کدگذاری‌ها است. در این پژوهش، با استفاده از روش نمونه‌گیری هدفمند، با ۱۷ نفر از اساتید و خبرگان رمز ارزها و افراد باتجربه و نخبهٔ امنیت ملی و اقتصادی، به‌صورت باز مصاحبه شد؛ بدین ترتیب که نخست طبق شناخت پژوهشگر و با درنظرگرفتن اهداف پژوهش، با خبرگان منتخبی که شایستگی پاسخ به پرسش‌های مطرح‌شده را داشتند، مصاحبه شد. سپس، آن‌ها خبرگان دیگری را معرفی کردند تا نمونه‌گیری ادامه یابد. با توجه به شیوهٔ گردآوری اطلاعات، چنانچه هدف از مصاحبه، اکتشاف و توصیف نگرش‌های مصاحبه‌شونده باشد و نیز با درنظرگرفتن زمان و منابع در دسترس، ۱۰ تا ۱۵ نمونه برای مصاحبه کافی خواهد بود (کوال، ۱۹۹۶: ۲). از مصاحبهٔ یازدهم به بعد، تکرار در داده‌های دریافتی مشاهده شد و در مصاحبهٔ پانزدهم، میزان داده‌های دریافتی از مصاحبه‌شونده‌ها به اشباع رسید؛ اما به دلیل اطمینان از داده‌های دریافتی، انجام مصاحبه تا مصاحبهٔ هفدهم ادامه یافت. در این پژوهش از دو مرحله استفاده شد: مرحلهٔ نخست، روش کدگذاری باز بود. برای مفهوم‌سازی داده‌ها و تحلیل اطلاعات، یکی از روش‌ها استفاده از کدگذاری باز است تا با استفاده از آن بتوان داده‌ها را در مقوله‌های مشخص دسته‌بندی کرد. در مرحلهٔ کدگذاری باز، مفاهیم از عمق داده‌ها به سطح آورده می‌شوند. همچنین، تحلیلگر به نحوهٔ شکل‌دهی مقوله‌ها و ویژگی‌های آن‌ها می‌پردازد (استراس و کوربین ۱۳۸۷: ۱)؛ کدهای به‌دست‌آمده طبق نظر خبرگان تصحیح و سپس تائید شد. در مرحلهٔ بعد، فرایند کدگذاری محوری انجام شد. کدگذاری محوری، فرایند تبدیل

مفاهیم به مؤلفه‌ها است. برای این کار، نظریه‌پرداز مفهومی از مجموعه مفاهیم مرحلهٔ کدگذاری باز را به‌عنوان مقوله انتخاب می‌کند و طی فرایندی سایر مفاهیم هم‌معنا را به آن مرتبط می‌کند. این کدگذاری بدین دلیل محوری قلمداد می‌شود که حول محور یک مقولهٔ پژوهش انجام می‌شود. برای تجزیه‌وتحلیل و کدبندی مصاحبه‌ها از نرم‌افزار کیفی مکس‌کیودا نسخهٔ ۱۲ بهره گرفته شد. برای بررسی روایی، یافته‌های پژوهش به مشارکت‌کنندگان ارائه شدند؛ آن‌ها متن نظریه را مطالعه کردند و نظرگاه‌های آن‌ها اعمال شد. در پایان، این پژوهش توسط اساتید مطالعه و بازبینی شد و مواردی برای اصلاح یا تغییر نظریهٔ نهایی بیان شد. پایایی داده‌ها از طریق نشان دادن مسیر تصمیم‌های پژوهشگران و همچنین، قرار دادن تمامی داده‌های خام، کدها، مقوله‌ها، فرایند مطالعه، هدف و سؤال، در اختیار اساتید قرار گرفتند و با حسابرسی دقیق صاحب‌نظران، درستی تمام گام‌های پژوهش تأیید شد. برای محاسبهٔ پایایی باز آزمون، معمولاً از میان مصاحبه‌های انجام‌گرفته، چند مصاحبه برای نمونه انتخاب می‌شوند. هریک از مصاحبه‌ها در فاصلهٔ زمانی کوتاه و مشخصی دو بار کدگذاری می‌شوند. سپس، کدهای مشخص‌شده با یکدیگر مقایسه می‌شوند. این روش برای ارزیابی ثبات کدگذاری پژوهشگر به کار می‌رود و برای این کار سه مصاحبه انتخاب و در بازه زمانی یک‌ماهه دو بار کدگذاری شد و درصد توافق درون موضوعی ۰/۷۹ به دست آمد که قابل‌قبول است.

## تجزیه‌وتحلیل یافته‌ها

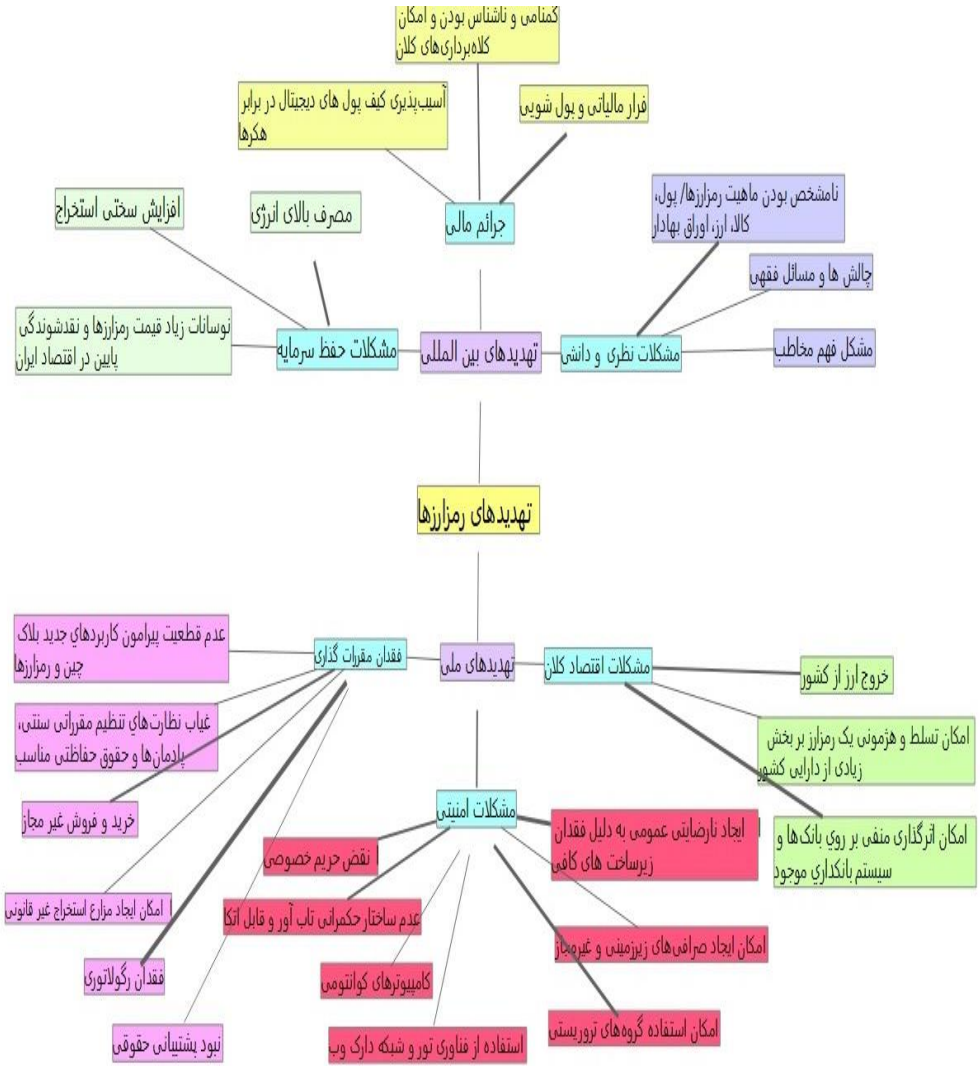
فضای سایبری و فناوری‌های وابسته به آن، یکی از مهم‌ترین منابع قدرت در هزاره سوم هستند. ویژگی‌های فضای سایبری همچون قیمت پایین ورود، گمنامی، آسیب‌پذیری و نامتقارن بودن، پدیده انتشار قدرت را به وجود آورده است، بدین معنی که اگر تاکنون دولت‌ها بازی قدرت را تنها میان خود تقسیم کرده بودند، ازاین‌پس باید آن را با بازیگران دیگری همچون شرکت‌های خصوصی، گروه‌های سازمان‌یافته تروریستی و جنایی و افراد تقسیم نمایند، اگرچه هنوز این دولت‌ها هستند که در این عرصه نقش مهمی را بازی

می‌کنند. به‌تبع، این پدیده امنیت ملی دولت‌ها را از تأثیرگذاری خود بی‌نصیب نخواهد گذاشت. این تأثیرگذاری را از چند جهت می‌توان مورد ارزیابی قرارداد. نخست، مفهوم امنیت است. دیگر نمی‌توان امنیت ملی را همانند گذشته در ارتباط با مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد، بلکه امروزه، خطر افت کیفیت زندگی شهروندان نیز نوعی تهدید برای امنیت ملی محسوب می‌شود. دوم، از میان رفتن بعد جغرافیایی در تهدیدهای سایبری است. درگذشته تهدیدهای نظامی از محل جغرافیایی خاصی برخوردار بودند. درنتیجه، مقابله با آن دست‌کم از جهت شناسایی کار چندان دشواری نبود. سوم، گستردگی آسیب‌پذیری‌های ناشی از تهدیدهای سایبری است. این تهدیدها پراکنده، چندبعدی و چند سویه‌اند و چون در ارتباط با شبکه‌های ارتباطی و زیرساخت‌های حساس می‌باشند، سطح آسیب‌رسانی آن‌ها بسیار بالاست چهارم، این تهدیدها را صرفاً با شیوه‌های سنتی همانند به‌کارگیری ارتش و نیروی پلیسی نمی‌توان مهار کرد و برای مقابله با آن‌ها تلاش دولت‌ها به‌تنهایی کافی نیست و همکاری مؤثر و دوجانبه دولت‌ها و بخش خصوصی را که دارای منافع مشترکی در برخورد با این‌گونه تهدیدها هستند، می‌طلبد. پنجم، همان‌گونه که از نکته قبلی برمی‌آید، تهدیدهای سایبری صرفاً متوجه دولت‌ها نیست، بلکه افراد و شرکت‌ها نیز از آسیب‌های این تهدیدها بی‌نصیب نخواهند بود. ششم، چون امنیت در عصر اطلاعات صرفاً دولت‌محور نیست؛ بنابراین رویکردهای مختلف نظری در روابط بین‌الملل که به‌طور عمده بر مبنای دولت‌محوری به ساختاربندی نظریات خود پرداخته‌اند، یا به‌راحتی از کنار این تهدیدها گذشته‌اند و یا در تحلیل‌های خود با سردرگمی مواجه شده‌اند.

تهدیدهای رمز ارزها به‌عنوان یک پدیده چندوجهی (سایبری، مالی و اقتصادی، صنعتی و فنی) درهم تنیدگی زیادی باهم دارند لیکن در این تحقیق سعی شده بهترین دسته‌بندی برای آن‌ها نمایش داده شود که مهم‌ترین این تهدیدها به‌قرار زیر است.

همان‌طور که در شکل شماره ۱ مشاهده می‌شود تعداد ۲۵ تهدید (کدهای باز) به همراه ٦ مؤلفه (کدهای محوری) در مورد تهدیدهای رمز ارزها بر امنیت اقتصادی از مصاحبه‌ها و

مطالعات مربوطه، کدگذاری شده و خروجی آن به کمک نرم‌افزار مکس‌کیودا ۱۲ بـه شـکل زیر نمایش داده می‌شود.




شکل شماره (۱) کدگذاری‌های تهدیدها و خروجی نرم‌افزار مکس‌کیودا

جدول شماره (۱) نتایج حاصل از کدگذاری تهدیدهای رمز ارزها به همراه راهکارهای مناسب

| ردیف | ابعاد | مؤلفه‌ها (کدهای محوری) | تهدیدها (کدهای باز) | راهکارها |
|---|---|---|---|---|
| ۱ | تهدیدهای ملی | فقدان مقررات گذاری | نبود پشتیبانی حقوقی | ایجاد رمز ارز داخلی با پشتوانه و قابل‌رقابت با نمونه‌های خارجی که سازوکارهای قانونی آن مشخص باشد. |
| ۲ | | | فقدان رگولاتوری | شناخت کارکردها و کاربردهای رمز ارزها<br>ورود نهادهای قانون‌گذار به عرصه رمز ارزها |
| ۳ | | | امکان ایجاد مزارع استخراج غیرقانونی | پایش میزان مصرف برق در هر واحد صنفی<br>ارائه راهکار قانونی جهت ایجاد مزارع استخراج رمز ارز |
| ٤ | | | خریدوفروش غیرمجاز | محدود کردن استفاده کاربران به رمز ارز داخلی باقابلیت اعمال کنترل |
| ٥ | | | غیاب نظارت‌های تنظیم مقرراتی سنتی، پادمان‌ها و حقوق حفاظتی مناسب | ایجاد قوانین و مقررات در همه ابعاد رمز ارزها (خریدوفروش، استخراج، نگهداری)<br>ایجاد یک‌نهاد مرکزی جهت نظارت، ارزیابی و کنترل بازار رمز ارزها |
| ٦ | | | عدم قطعیت پیرامون کاربردهای جدید بلاک چین و رمز ارزها | شناخت کامل ابعاد فنی زنجیره بلوک و رمز ارزها |
| ۷ | | مشکلات امنیتی | ایجاد نارضایتی عمومی به دلیل فقدان زیرساخت‌های کافی برای پشتیبانی از شرایط بحران | توسعهٔ فناوری بلاک چین و ملزومات زیرساختی، محتوایی و امنیتی آن |
| ۸ | | | امکان ایجاد صرافی‌های زیرزمینی و غیرمجاز | ارائه راهکار قانونی جهت اخذ مجوز صرافی‌های مخصوص رمز ارزها |
| ۹ | | | امکان استفاده گروه‌های تروریستی | نیازمند رگولاتوری توسط نهادهای بین‌المللی است<br>استانداردسازی و برقراری محدودیت‌هایی برای نقل و انتقالات |
| ۱۰ | | | استفاده از فناوری تور و شبکه دارک وب | نیازمند رگولاتوری توسط نهادهای بین‌المللی است |
| ۱۱ | | | کامپیوترهای کوانتومی | نیازمند راه‌حل بین‌المللی دارد مثل استفاده از کدهای کوانتومی پرورش نیروی انسانی متخصص و کارآمد |
| ۱۲ | | | عدم ساختار حکمرانی تاب آور و قابل‌اتکا | محدود کردن استفاده کاربران به رمز ارز داخلی باقابلیت اعمال کنترل |
| ۱۳ | | | نقض حریم خصوصی | استفاده از بلاک چین خصوصی جهت تائید تراکنش‌ها |
| ۱٤ | | مشکلات اقتصاد کلان | امکان اثرگذاری منفی بر روی بانک‌ها و سامانهٔ | ورود بانک‌های کشور به مباحث خط‌مشی گذاری، قانون‌گذاری و طراحی و تولید رمز ارز |

| ردیف | ابعاد | مؤلفه‌ها (کدهای محوری) | تهدیدها (کدهای باز) | راهکارها |
|---|---|---|---|---|
| | | | بانکداری موجود | |
| ١٥ | | | امکان تسلط و هژمونی یک رمز ارز بر بخش زیادی از دارایی کشور | بهره‌گیری از طیف مختلف ارزهای رمزینه بیت کوین، اتریوم، یوتا و غیره |
| ١٦ | | | خروج ارز از کشور | نظارت و کنترل دولت بر خروج ارز از کشور همانند کنترل صرافی‌ها و ایجاد رمز ارز توسط یک بانک داخلی |
| ١٧ | تهدیدهای بین‌المللی | مشکلات نظری و دانشی | نامشخص بودن ماهیت رمز ارزها (پول، کالا، ارز، اوراق بهادار و...) | مرکز ملی فضای مجازی به همراه بانک مرکزی و حوزه علمیه کارگروه مشترکی تشکیل داده و ماهیت آن را به دست آورند. |
| ١٨ | | | مشکل فهم مخاطب | آموزش وسیع و گسترده از طریق رسانه‌های اجتماعی و رسانه ملی در خصوص خریدوفروش و نگهداری رمز ارزها و همچنین شرایط استخراج آن، تبیین مزایا و معایب رمز ارزها و افزایش سواد اقتصاد دیجیتال |
| ١٩ | | | چالش‌ها و مسائل فقهی | ایجاد کارگروهی با محوریت علمای اسلام از کشورهای مسلمان جهت بررسی تمام ابعاد فقهی در خصوص خریدوفروش، نگهداری و استخراج رمز ارزها، بررسی و تطبیق قواعد موجود فقه اسلامی با رمز ارزها (قاعده نفی سبیل، قاعده لاضرر، قاعده تلف، قاعده تسعیر و ...). |
| ٢٠ | | جرائم مالی | گمنامی و ناشناس بودن و امکان کلاه‌برداری‌های کلان | ایجاد ساختارهای قانونی جهت خریدوفروش و استخراج رمز ارزها، استفاده از کیف پول‌های دیجیتالی ایمن مثل کیف پول‌های سخت‌افزاری و یا بومی کنترل نقل و انتقالات و تراکنش‌های داخلی |
| ٢١ | | | آسیب‌پذیری کیف پول‌های دیجیتال در برابر هکرها | استفاده از کیف پول‌های دیجیتالی ایمن مثل کیف پول‌های سخت‌افزاری و یا بومی |
| ٢٢ | | | فرار مالیاتی و پول‌شویی | محدود کردن استفاده کاربران به رمز ارز داخلی باقابلیت اعمال کنترل |
| ٢٣ | | مشکلات حفظ سرمایه | نقد شوندگی پایین در اقتصاد ایران و نوسانات زیاد قیمت رمز ارزها | بدون پشتوانه بودن رمز ارز باعث نوسانات شدید می‌شود؛ بنابراین ارائه رمز ارز با پشتوانه (مثل نفت، طلا، ریال و ...) باعث ثبات نسبی قیمت آن می‌گردد مانند ریپل |
| ٢٤ | | | افزایش سختی استخراج | استفاده از رمز ارزهایی که سختی استخراج آن با گذر زمان افزایش نمی‌یابد. |
| ٢٥ | | | مصرف بالای انرژی | توجه به زیرساخت‌های برقی کشور و ایجاد مزارع قانونی استخراج در مکان‌های مناسب و زمان‌های مناسب که به شبکه برقی آسیب وارد نشود |

| ردیف | ابعاد | مؤلفه‌ها (کدهای محوری) | تهدیدها (کدهای باز) | راهکارها |
|---|---|---|---|---|
| | | | | پایش میزان برق مصرفی واحدهای صنفی و کنترل آلودگی محیط‌زیست<br>بهره‌گیری از انرژی‌های پاک در مزارع استخراج |

## نتیجه‌گیری و پیشنهاد

با بررسی دقیق دلایل ممنوعیت، محدودیت و نگرانی استفاده از رمز ارزها می‌توان نتیجه گرفت که تدوین یک راهکار مناسب در راستای استفاده از این نوع ارزها می‌تواند به نفع دولت‌ها و شهروندان و درنتیجه امنیت اقتصادی یک جامعه باشد. این مسئله به‌خصوص در اقتصادهای نوپا همچون اقتصاد ایران که خرید و سرمایه‌گذاری بر روی ارزهای رمزینه مستلزم خروج ارز واقعی از کشور می‌باشد، بسیار حائز اهمیت بوده و بایستی به‌صورتی کاملاً مدون کنترل گردد. فرآیند کنترل بایستی ضمن فراهم نمودن امکان مشارکت افراد علاقه‌مند ورود به بازار ارزهای رمزینه، تهدیدهای موجود را به حداقل رسانده و از آن‌طرف، منافع دولت‌ها را نیز تضمین نماید. به‌عنوان یک نتیجه، بایستی مقررات مناسبی در این راستا تدوین‌شده و نوع مشارکت کاربران و نحوهٔ خریدوفروش ارز رمزینه توسط آن‌ها به‌طور کاملاً شفاف مشخص گردد. با استفاده از یافته‌های پژوهش و همچنین، تجارب و تأملات پژوهشگران مطالعه حاضر دربارهٔ موضوع موردمطالعه، تهدیدهای زیر ممکن است به‌طور مستقیم یا غیرمستقیم، امنیت اقتصادی کشور را با مشکلاتی مواجهه کند:

### نامشخص بودن ماهیت رمز ارزها (پول، کالا، ارز)

طبق تعریف، پول باید سه شرط زیر را داشته باشد: نقش مبادله‌ای، معیار سنجش ارزش، داشتن قابلیت حفظ ارزش با این تعریف، رمز ارزها فعلاً نمی‌توانند این ۳ شرط را داشته باشند؛ بنابراین یا پول خوبی به‌حساب نمی‌آیند یا اصلاً پول نیستند. نقش مبادله‌ای در حال حاضر عملیاتی شده است، اما مقبولیت جهان‌شمولی برای استفاده در زندگی روزمره

را ندارند. همچنین در بحث قابلیت حفظ ارزش، همان‌گونه که دربند نوسان ارز به‌تفصیل به آن خواهیم پرداخت، کم‌وزیاد شدن قیمت آن‌ها مانعی جدی برای همه‌گیرشدن آن‌ها به شمار می‌رود. همین وضعیت باعث شد نشریه اکونومیست بنویسد: تا زمانی که خریداران و فروشندگان بیت کوین به دلار و یورو فکر می‌کنند، بیت کوین پول نمی‌شود (د، سیلوا، ٢٠١٧، ٦).

**نوسانات زیاد ارزش**[1]

بالا و پایین رفتن ناگهانی قیمت رمز ارزها یکی از تهدیدهای پیش روی این پدیده است، این نوسانات، جدای از بحث علت و معلولی آن‌ها، لطمه شدیدی به جامعه مخاطب زده است و بسیاری از تاجران و بورس بازان را که می‌توانستند سرمایه‌داران بزرگ رمز ارزها باشند را از ورود به این عرصه محروم کرده است. در حقیقت تا مردم از ثابت ماندن ارزش بیت کوین و دیگر رمز ارزها اطمینان حاصل نکنند، اقبال عمومی به این ارزها زیاد نخواهد بود (هایلمن، ٢٠١٧: ٤٦).

**نبود پشتیبانی حقوقی**

ازآنجایی‌که هیچ سازمان یا ارگان رسمی نمی‌تواند نظارتی بر انتقال پول‌های درون شبکه بلاک چین داشته باشد و عملاً می‌توان در عرض چند ثانیه حجم زیادی از پول را از یک کشور به کشوری دیگر منتقل کرد، یکی از بهترین و سریع‌ترین راه‌های پول‌شویی استفاده از همین ارزهای دیجیتال است، عملاً هیچ منبعی برای استعلام یک تراکنش وجود ندارد و نتیجتاً اعمال قانون نیز بی‌معنی می‌شود. به همین صورت امکان استفاده از رمز ارزها برای پنهان‌سازی اموال و دارایی‌ها در پرونده‌هایی مانند طلاق و... وجود دارد. ازاین‌رو در هنگام مواجهه با انواع جرائم یا کلاه‌برداری‌ها در فضای مجازی وقتی یک پای قضیه رمز ارز باشد، خبری از پشتیبانی حقوقی به معنای آنچه در عرف وجود دارد، در کار نخواهد بود (د، سیلوا، ٢٠١٧: ٧).

---

1. Volatility barrier

**نبود زیرساخت کافی برای پشتیبانی از شرایط بحران**

طبق پروتکل موجود در هر رمز ارز غیرمتمرکز مانند بیت کوین و اتریوم و... در هر ثانیه تعداد تراکنش‌های معینی قابل انجام است، مثلاً در بلاک چین بیت کوین هرروز ۳۰۰ هزار تراکنش قابل انجام است؛ بنابراین همان‌گونه که در ماه آخر سال ۲۰۱۷ شاهد آن بودیم، با افزایش تراکنش‌ها اختلالاتی در شبکه رخ می‌دهد و زمان برای انجام هر تراکنش از سقف مقرر ۱۰ دقیقه بیشتر شد و تائید یک تراکنش، حتی ۳ روز بعد انجام شد؛ بنابراین یکی از تهدیدات پیش روی رمز ارزها همین است. یک رمز ارز غیرمتمرکز باید به‌گونه‌ای طراحی شود که در چنین شرایط بحرانی، به نحوی مدیریت بحران داشته باشد.

**امکان اثرگذاری منفی بر روی بانک‌ها و سامانهٔ بانکداری موجود**

دلالان با رصد بازار رمز ارزها به‌خوبی دریافته‌اند که این بازار پتانسیل سرمایه‌گذاری و سودآوری بالایی را دارد، ازاین‌رو به این عرصه ورود نموده‌اند و سرمایه‌گذاری‌های کلانی نیز داشته‌اند، عده‌ای نیز با راه‌اندازی صندوق‌های سرمایه‌گذاری، با عموم مردمی که به رمز ارزها علاقه دارند اما نگران تهدیداتی مانند هک شدن کیف پول الکترونیکی[1] هستند، وارد قرارداد شدند؛ که این مباحث در مقیاس خرد نیست و رقم‌های قراردادها و متعاقباً تراکنش‌ها بسیار بالاست (جی‌ای او، ۲۰۱۹: ۱۵).

**فقدان رگولاتوری**

بانک مرکزی امریکا[2] اعلام کرده است که هیچ اهرمی برای رگلاتوری یا نظارت بر بیت کوین ندارد، علاوه بر آمریکا، بقیه بانک‌های مرکزی نیز در سرتاسر دنیا به شهروندانشان هشدارهای صریحی مبنی بر خطرات استفاده از بیت کوین و دیگر رمز ارزها به علت

---

۱ Wallet

۲ Federal Reserve Bank

فقدان رگلاتوری داده‌اند (هایلمن، ۲۰۱۷: ٤٢). نبود قانون و مقررات جهت تنظیم‌گری در هر حوزه می‌تواند انواع آسیب‌ها را برای آن به همراه داشته باشد.

**افزایش هزینه‌های تراکنش به علت افزایش سختی استخراج**

با افزایش سختی استخراج، یک دستگاه ماینر باید وقت بیشتری را برای حل معادلات و تائید تراکنش‌ها صرف کند این امر شرایطی را فراهم خواهد آورد که طی آن‌یک دستگاه ماینر دیگر نمی‌تواند منتفع شود چراکه به دلیل افزایش سخت شبکه و هزینه برق مصرفی، دیگر استخراج مقرون‌به‌صرفه نیست و عملاً هزینه استخراج بیشتر می‌شود (د، سیلوا، ۲۰۱۷: ١٤).

**آسیب‌پذیری بسیار بالای کیف پول‌ها[1]**

آسیب‌پذیری کیف پول‌های الکترونیکی و صرافی‌ها امری اجتناب‌ناپذیر است، اصولاً هر نرم‌افزاری قابل هک شدن است غالب کیف پول‌ها چون بر روی بستر وب یا موبایل فعال هستند، همیشه حفره‌هایی برای نفوذ بر روی آن‌ها وجود دارد. صرافی‌ها نیز به همین شکل آسیب‌پذیر هستند و نمونه‌های زیادی از هک و سرقت رمز ارزهای آنان مشاهده می‌شود. در برخی موارد دزدی‌های بزرگی از صاحبان کیف پول رخ‌داده است و یک‌باره چند هزار کیف پول الکترونیکی موجودی‌شان صفر شده است.

**امکان ایجاد صرافی‌های زیرزمینی و غیرمجاز**

می‌توان با شناسایی صرافی‌ها، مشتریان رمز ارزها را شناسایی نمود؛ اما همیشه امکان این هست که یک صرافی غیرقانونی اقدام به فروش بیت کوین یا دیگر رمز ارزها نماید و با تبلیغات در بخش‌های تاریک وب مثل دارک وب به جمع‌آوری مشتریانش بپردازد؛ بنابراین سازمان‌های اطلاعاتی و حتی بدنه بازرسی دولتی همیشه باید گروه‌هایی داشته

---

۱ wallets

باشند که وظیفه آن‌ها شناسایی صرافی‌های غیرمجاز باشد این افراد باید خود را مردم عادی باسواد کامپیوتری کم معرفی کنند؛ که می‌خواهند رمز ارز بخرند، یا رمز ارز خود را بفروشند.

**استفاده از فناوری تور و شبکه دارک وب**

ازآنجایی‌که هر کس در جهان با یک دسترسی به اینترنت می‌تواند به رمز ارزها دسترسی داشته باشد؛ بنابراین لزوم همکاری پلیسی بین کشورهای مختلف جهان امری اجتناب‌ناپذیر است، مانند دستگیری اعضای پروژه سیلک رود یا راه ابریشم[۱] که تجربه موفقی بود، سیلک رود یک بازار سیاه آنلاین بود که به دلیل فروش مواد مخدر و انواع سلاح در دارک وب شهرت بسیاری یافته بود. این وب‌سایت از فناوری تور[۲] استفاده می‌کرد تا بتواند به‌صورت ناشناس به فعالیت خود ادامه دهد.

راهکار پیشنهادی علاوه بر بیان نحوهٔ مشارکت افراد در تبادلات رمز ارزها، مزایای دیگری همانند امکان عرضهٔ یک ارز رمزینهٔ داخلی را نیز فراهم می‌آورد تا به کمک آن پایه‌های امنیت اقتصادی کشور عزیزمان مستحکم گردد. (حق نویس، شاهین، ۱۳۹۶)؛ بنابراین تهدیدهای رمز ارزها در دو بعد ملی و بین‌المللی تقسیم‌بندی شد یعنی بعد ملی بهتر است در داخل کشور سیاست‌گذاری شود و بعد بین‌المللی نیز به کمک سایر کشورها در منطقه و یا جهان سیاست‌گذاری گردند. بنا بر نتایج این تحقیق بعد ملی آن دارای سه مؤلفهٔ مقررات گذاری، امنیتی و اقتصاد کلان بوده و بعد بین‌المللی نیز دارای مؤلفه‌های مشکلات نظری و دانشی، جرائم مالی و مشکلات حفظ سرمایه است و هر مؤلفه نیز چندین تهدید را شامل می‌شود هرچند غالب این تهدیدها چندوجهی بوده و می‌توان آن‌ها را در گروه‌های مختلف دسته‌بندی کرد لیکن طبق نتایج این تحقیق، کدهای به‌دست‌آمده (تهدیدها) در جدول زیر به همراه راهکارهای مناسب جهت کشور ما نشان داده‌شده است.

---

۱ Silk Read

۲ TOR

پدیده رمز ارزها همانند بسیاری از فناوری‌های نوین، هم‌زمان فرصت‌ها و تهدیدهای گوناگونی فراروی ما قرار می‌دهد نگاه منفی بسیاری از دولت‌ها و نهادهای مرکزی نسبت به رمز ارزها و جلوگیری از گسترش طبیعی آن‌ها در اقتصاد، زمان بالای تأیید تراکنش برای مبادلات داخلی، عدم امکان استفاده گسترده از آن‌ها در پرداخت‌های خرد، کارکردهای آن‌ها را موردتردید جدی قرار داده اما می‌توان بیان داشت با پیشرفت فناوری و نیز آشنایی بیشتر مردم، عمق بازار رمز ارزها افزایش‌یافته و باعث کاهش نوسانات آن‌ها و افزایش کاربرد در پرداخت‌های خرد خواهد شد.

وجود ویژگی‌های منحصربه‌فرد آن‌ها همانند آزادی در پرداخت و دسترسی بین‌المللی، هزینه معاملاتی بسیار پایین، سرعت‌بالا در انتقالات بین‌المللی و فرامرزی، عدم خلق پول بی‌رویه در اقتصاد، عدم توانایی دولت‌ها در مصادره و بلوکه کردن، امکان ایجاد توکن[1] و عرضهٔ اولیهٔ سکه[2] امکان بهره‌گیری از قراردادهای هوشمند[3] تسهیل در جهانی‌شدن کسب‌وکارهای داخلی و افزایش سرمایه‌گذاری خارجی، قابلیت تقسیم‌پذیری، عدم امکان جعل رمز ارزها برخلاف پول‌های رایج، انتظار می‌رود باگذشت زمان کارکردهای آن‌ها پررنگ‌تر شود و بتواند یکی از انواع پول‌های آینده اقتصاد جهانی باشد (نوری، ١٣٩٧). لیکن درهرحال، توجه به تهدیدهای اقتصادی رمز ارزها و شناخت راه‌حل‌های ممکن برای ما، می‌تواند چشم‌انداز آینده رمز ارزها را در کشور روشن‌تر کند.

تهدیدهای به‌دست‌آمده در این تحقیق در حوزه امنیت اقتصادی بوده که خود بخش قابل‌توجهی از امنیت ملی کشور را شامل می‌شود. این تهدیدها به دو بخش عمده ملی و بین‌المللی تقسیم‌بندی شدند به این مفهوم که بخش ملی غالباً در داخل کشور قابل‌حل و سیاست‌گذاری است و بخش بین‌المللی بیشتر به کمک سایر کشور قابل‌حل خواهد بود.

---

١ Token

٢ Initial Coin Offering

٣ Smart Contract

در بعد تهدیدهای ملی، مهم‌ترین تهدیدها به علت فقدان قانون و مقررات است چراکه بدون قانون و مقررات، حاکمیت‌ها امکان اثرگذاری کمتری دارند و متخلفان با خاطری آسوده سرمایه‌های مردم را سرقت می‌کنند و با ایجاد نارضایتی عمومی و بحران، اقتصاد کشور و نهایتاً امنیت کشور را به مخاطره می‌اندازند. در بخش اقتصاد کلان نیز برای جلوگیری از خروج ارز و یا تسلط دشمنان بر بازار رمز ارزها می‌توان ضمن کنترل صرافی‌ها، طیف‌های مختلفی از رمز ارزها را گسترش داد و تنها به چند رمز ارز محدود اکتفا نکرد.

در بعد بین‌الملل نیز، آموزش مفاهیم رمز ارز و ایجاد کارگروه‌هایی از جهان اسلام در جهت شناخت ماهیت و مسائل فقهی آن حائز اهمیت است همچنین در خصوص جلوگیری از نفوذ هکرها، استفاده از تجهیزات و برنامه‌های بومی و تأمین کیف پول دیجیتال سخت‌افزاری می‌تواند امنیت سرمایه کاربران را تا حد زیادی تضمین کند. ضمن اینکه حاکمیت نیز در جهت جلوگیری از نوسانات شدید قیمت آن، رمز ارزهایی با پشتوانه (طلا، نفت، ریال و ...) ایجاد کند و دراین‌بین، توجه به صنعت استخراج و استفاده از انرژی‌های پاک و تجدید پذیر نیز می‌تواند در رونق و رقابت سالم بازار رمز ارزها مفید باشد.

رمز ارزها با توجه به نوظهور بودنشان مباحث زیاد و گسترده‌ای دارند و پیشنهاد می‌شود در زیر حوزه‌های آن همچون استخراج، کیف‌های پول دیجیتالی، خریدوفروش و نگهداری آن و همچنین مبانی فقهی رمز ارزها پژوهش‌هایی انجام شود تا با استفاده از نتایج آن‌ها، کشور عزیزمان از ورطه خطرات اقتصادی و اجتماعی آن ایمن شود.

## فهرست منابع و مآخذ

### منبع فارسی


- افتخاری، اصغر و خیراتی، عباس (۱۳۹۸). ***«راهبردهای پسا برجامی آمریکا علیه امنیت ملی جمهوری اسلامی ایران»***. فصلنامهٔ امنیت ملی، سال نهم، شماره ۳۳، پاییز ۱۳۹۸.
- اس، چان. (۲۰۱۷). ***«تحلیل آماری رمز ارزها»***. ژورنال ریسک و مدیریت مالی.

- استراوس، آنسلم و جولیت کوربین (١٣٨٧). ***«اصول روش تحقیق کیفی، نظریه مبنایی، رویه‌ها و شیوه‌ها»***. ترجمهٔ بیوک محمدی، انتشارات پژوهشگاه علوم انسانی و مطالعات فرهنگی. ضمنی، فصلنامهٔ سیاست، ٩٩-١١٢: (٣٨)٤.
- باقری سعید، مرجان (١٣٩٦). ***«ارز دیجیتال، فرصت‌ها و تهدیدهای بالقوه»***. ششمین اجلاس حسابداری، مدیریت مالی و سرمایه‌گذاری.
- «بررسی قانون آلون» (٢٠١٧)، جلد نهم، انتشارات دانشگاه آلون.
- بوزان، بری (١٣٧٨). ***«مردم، دولت‌ها و هراس»***. ترجمهٔ پژوهشکدهٔ مطالعات راهبردی، تهران: پژوهشکدهٔ مطالعات راهبردی.
- ج، چویی (٢٠١٧). ***«رمز ارزها برای تراکنش‌های تجاری بین‌المللی- چشم‌انداز و موانع»***. اجلاس مدرن سازی قوانین تجارت جهانی کمیسیون قوانین تجارت جهانی سازمان ملل وین، ٤ الی ٦ جولای ٢٠١٧.
- جی‌ای او (٢٠١٩). ***«رمز ارزها؛ مقررات نوظهور؛ اجرای قانون و چالش‌های محافظت از مصرف‌کنندگان»***. گزارش کمیته امنیت داخلی و امور دولتی سنای امریکا.
- حاجی ملامیرزایی، حامد (١٣٩٨). ***«پول مجازی»***. تهران: انتشارات راهبردی. دانشگاه عالی دفاع ملی.
- حق نویس، شاهین (١٣٩٧). ***«کنکاشی در تهدیدات و فرصت‌های رمز ارزها از دیدگاه امنیت ملی»***.
- خلیلی پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (١٣٩١). ***«تهدیدات سایبری و تأثیر آن بر امنیت ملی»***. فصلنامهٔ مطالعات راهبردی شماره مسلسل ٥٦. شماره دوم. سال پانزدهم.
- د، سیلوا (٢٠١٧). ***«رمز ارزها: رگلاتوری بین‌المللی و یکپارچه‌سازی رفتارها»***. اجلاس مدرن سازی قوانین تجارت جهانی کمیسیون قوانین تجارت جهانی سازمان ملل وین، ٤ الی ٦ جولای ٢٠١٧.
- دهقانی، علی‌اصغر (١٣٩٧). ***«بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا»***. مجلهٔ رهیافت‌های سیاسی و بین‌المللی.
- رنجبر فلاح، محمدرضا (١٣٩٧). ***«ایجاد پول دیجیتال اکومانی مبتنی بر فناوری زنجیره بلوک بر اساس پیمان چندجانبه پولی منطقه‌ای»***. فصلنامهٔ اقتصاد دفاع، سال سوم، شمارهٔ هفتم، بهار ١٣٩٧، صص ١٠٥-٩٣.

- روزنا، جیمز و دیگران (۱۳۹۰). ***«انقلاب اطلاعات، امنیت و فناوری‌های جدید»***. مترجم علیرضا طیب، تهران: پژوهشکدهٔ مطالعات راهبردی.
- صالحان، علیرضا و امید الهی (۱۳۹۷). ***«بانک ارزهای رمزینه: راهکاری قابل نظارت به‌منظور بهره‌گیری از ارزهای رمزینه در ایران»***.
- گ، هایلمن (۲۰۱۷). ***«مطالعه پایدار جهانی رمز ارزها»***. دانشگاه کمبریج.
- گزارش پنجاهم کمیسیون قوانین تجارت جهانی سازمان ملل (۲۰۱۷)، سازمان ملل.
- مجمع تشخیص مصلحت نظام (معاونت علمی پژوهشی)، (۱۳۹۸)، «پدیده رمز ارز، مخاطرات، فرصت‌ها و نحوه سیاست‌گذاری».
- مقدسی لیچاهی، امیرحسین و همت، حمید (۱۳۹۷). ***«ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه»***. آینده‌پژوهی دفاعی، سال سوم، شماره ۱۰، پائیز ۱۳۹۷.
- موسوی، محمدرضا؛ حیدری، خدیجه و قنبری، علی (۱۳۹۸). ***«تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»***.
- نوری، مهدی (۱۳۹۷). ***«تحلیل ماهیت پولی رمز ارزها در اقتصاد؛ با تأکید بر مقایسه نوسانات رمز ارزهای منتخب با نوسانات یورو- دلار و طلا»***. فصلنامهٔ اقتصاد دفاع. سال سوم، شماره دهم، زمستان ۱۳۹۷، صص ۱۳۰-۱۰۹.
- وزارت امور اقتصادی و دارایی (معاونت امور اقتصادی)، (۱۳۹٦)، «سناریوهای پیش روی اقتصاد جهانی در مواجهه با ارزهای رمز پایه».