ارزیابی چالش‌های رمزارزهای بومی

مرجان بحرالعلوم*[1] و زهرا فردوسی[2]

[1]عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات، پژوهشکده امنیت، تهران، ایران
bahrololum@itrc.ac.ir

[2]فارغ التحصیل دکترای کد ورمز از دانشگاه صنعتی امیرکبیر، تهران، ایران
ferdosi@aut.ac.ir

چکیده

امروزه فضای رمزارزها در سامانه‌های پرداخت جهانی به‌عنوان راه‌کاری به جهت استقلال از بانک‌داری سنتی و خارج‌شدن از سیطره بانک‌ها و سیاست‌های پولی دولت‌ها و عدم امکان تقلب در تراکنش‌های بانکی و جعل آن مطرح شده است. از طرفی رشد روزافزون رمزارزها در دنیای دیجیتال، امکان بروز برخی چالش‌ها را در سطوح مختلف پیاده‌سازی و استفاده موجب خواهد شد؛ ازاین‌رو در این مقاله سعی شده است با رویکردی کمی و کیفی به ارائه تصویری جامع از بررسی‌های انجام‌شده در شناسایی موانع و چالش‌های این حوزه پرداخته شود. این تصویر جامع در برگیرندهٔ تحلیل سه‌جانبهٔ چالش‌ها براساس ویژگی‌های فناورانه، محیطی و حاکمیتی است؛ همچنین، در این مقاله با تحلیل داده‌های تجربی از کشورهای مختلف در به‌کارگیری رمزارزها و نیز با شناخت جامع از نظام اقتصادی، اجتماعی و سیاسی کشور ایران، موانع و چالش‌های رمزارز ملی ارائه می‌شود تا با هدف‌گذاری و رویکردی ملی، اهمیت به‌کارگیری آن در سطح کلان مورد مطالعه بیشتر قرارگیرد.

واژگان کلیدی: تحلیل فناورانه، تحلیل محیطی و حاکمیتی، رمزارز، زنجیره‌بلوکی، چالش.

۱- مقدمه

در تمدن‌های اولیه بشری (شش‌هزار سال قبل از میلاد)، به‌طورمعمول از تبادلات کالا به کالا برای رفع نیازهای خود استفاده می‌کردند؛ به این صورت که افراد کالایی را در قبال کالای دیگر با یکدیگر تعویض می‌کردند. در چهارهزار سال بعد نیز افراد هر منطقه نوع یا انواعی از کالای فیزیکی را برای تبادلاتشان انتخاب کردند و آن را مبدأ تبادلات خود قرار دادند. هزار سال قبل از میلاد مردم فلزات و نقره را به‌عنوان پول جهانی قرار دادند که در تمام جهان قابل استفاده باشد و همه آن را به رسمیت بشناسند. پول کاغذی در قرن دوازدهم میلادی با پدیدارشدن بانک‌ها، چاپ شد و ارزهای فیات با پشتوانه طلا و نقره به‌وجود آمدند، یعنی برای چاپ ارز باید به همان اندازه طلا یا نقره در ذخایر بانک مرکزی وجود داشته باشد. سال ۱۹۸۰ میلادی یکی از کاربردهای اینترنت، بانک‌داری برخط به‌وجود آمد. در سال ۲۰۰۱ شرکت پی‌پال به‌طوررسمی سرویسی را ارائه داد که کاربران می‌توانستند پرداخت‌های برخط خود را در سراسر جهان انجام دهند. سال ۲۰۰۸ نخستین پول دیجیتالی غیرمتمرکز معروف به بیت‌کوین[1] (نخستین رمزارز[2]) جهت تمرکززدایی و حفظ ارزش پول و دارایی مردم معرفی شد [۱-۲].

رمزارز پدیده به‌نسبه نوظهوری است که درحدود یک دهه قبل به‌عنوان وسیله‌ای برای جایگزینی پول و ارز توسط فعالان حوزه فناوری ابداع شد. رمزارز نوعی پول دیجیتالی است که در بستر اینترنت و به‌صورت رمزنگاری‌شده (با استفاده از کلید خصوصی و عمومی) برای انتقال سکه استفاده می‌شود [۲]. با به‌کارگیری رمزارزها، پرداخت و دریافت پول در فضای مجازی تسهیل و تبادلات به‌صورت امن انجام می‌شود. ماهیت بنیادی بیش‌تر رمزارزها یکسان است و بر بستر زنجیره بلوکی[3] راه‌اندازی می‌شوند [۳-۶]. زنجیره بلوکی یک دفتر حساب یا پایگاه داده امن، توزیع‌شده و سراسری برای ذخیرهٔ فعالیت‌های شبکه است. ایده اصلی زنجیره بلوکی قراردادن تعداد زیادی چشم ناظر در شبکه است که بتوانند هر اتفاقی در شبکه را ثبت و ضبط کنند و یک نسخه از

[1] Bitcoin
[2] Cryptocurrency
[3] Blockchain

* نویسندهٔ عهده‌دار مکاتبات

اتفاقات شبکه را در اختیار تمام اعضای شبکه قرار دهند، همچنین با ایجاد یک سیاست انگیزشی در زنجیره بلوکی که می‌تواند حتی غیرمالی نیز باشد، افراد به رفتار درست‌کارانه در شبکه تشویق می‌شوند [۴].

حیات یک رمزارز به درست‌کاری بیشینه اعضای موجود در زنجیره بلوکی وابسته است. در واقع از زنجیره بلوکی به‌عنوان دموکراسی در دنیای دیجیتال یاد می‌شود، زیرا هر تصمیم و یا تغییری در شبکه در صورتی محقق می‌شود که بیشینه شبکه با آن موافق باشند؛ بنابراین یک نهاد متمرکز برای آینده و اتفاقات درون شبکه تصمیم‌گیری نمی‌کند. همه چیز به‌صورت شفاف در اختیار اعضای شبکه قرار می‌گیرد تا نسبت به آن اعلام نظر می‌کنند؛ سپس شبکه مطابق نظر بیشینه اعضای شبکه ادامه پیدا خواهد کرد. از این رو هرچه در یک زنجیره بلوکی مشارکت افراد افزایش یابد، احتمال تخلف در آن کاهش پیدا می‌کند. بنابراین توسعه‌دهندگان زنجیره بلوکی، به‌دنبال فرآیندها و سیاست‌های تشویقی هستند که مشارکت بیشینه‌ای را به همراه داشته باشد [۴].

دلایل زیادی در استقبال افراد برای استفاده از رمزارزها وجود دارد که می‌توان به موارد کلی شامل جلوگیری از تورم، مقابله با بحران‌های اقتصادی، قابل بهره‌برداری برای شهروندان با نداشتن حساب بانکی، عدم محدودیت در برداشت از حساب‌ها، متضررنشدن از نرخ تبدیل پول‌ها به یکدیگر، عدم نیاز به اعتماد به نهاد خاص اشاره کرد و همچنین دسترسی آسان و همیشگی، آزادی در پرداخت و دسترسی بین‌المللی، داشتن سرعت بالا در نقل و انتقالات بین‌المللی، نبود نهاد نظارتی بر معاملات شخصی، عدم امکان تقلب در تراکنش‌های بانکی و جعل رمزارزها، استفاده از رمزنگاری قوی برای محافظت از تهدید و تغییر اطلاعات، سهولت‌بخشیدن تراکنش‌های بین‌المللی از دیگر مزایای رمزارزها است [۴-۷].

۲- بررسی کشورهای مختلف در مورد رمزارزها

با توجه به ویژگی پدیدهٔ رمزارزها در سطح بین‌المللی، اتفاق‌نظری بین سیاست‌گذاران پولی درخصوص شیوه مقررات‌گذاری برای آن‌ها وجود ندارد. شاید یکی از دلایل این عدم اتفاق نظر، ذات رمزارزها باشد که بر مبنای عدم کنترل طراحی شده است. برخی از کشورها به داشتن پتانسیل رمزارزها برای پول‌شویی و تغذیه مالی تروریسم اعتقاد دارند. کشورها سیاست‌های مختلفی در قبال رمزارزها دارند و استانداردهای متفاوتی را اعمال می‌کنند [۸]. در هر صورت مقررات بین‌المللی در این‌خصوص از آزادی کامل برخوردار نیستند به‌عنوان مثال کشورهایی چون ژاپن به‌طور کامل آزادند و کشورهایی مانند چین با محدودیت کامل در استفاده مواجه هستند. البته می‌توان گفت در همه کشورها سیاست‌ها در حال تغییر و اصلاح است. سیاست برخی کشورها در قبال رمزارزها در ادامه توضیح داده خواهد شد.

ژاپن

دولت ژاپن رمزارزها را به‌عنوان پول قانونی پذیرفته است و صرافی‌های رمزارز را نیز به شرطی که در آژانس خدمات مالی (FSA)[1] این کشور ثبت شوند و مجوز بگیرند، قانونی می‌شمارد. این دولت توانسته با ثبت صرافی‌ها و ارسال بخشنامه‌های مالی به آن‌ها از بروز پول‌شویی و کلاه‌برداری جلوگیری کند. آژانس FSA برای ارتقای صرافی‌ها و ارائه یک محیط امن برای معاملات رمزارزها پنج ملاحظه قانونی را برای تأیید ثبت صرافی‌ها قرار داده است [۹]. این ملاحظات مربوط به حفظ امنیت رمزارزها و جلوگیری از انجام سرقت‌های بزرگ به‌وسیله هک‌کردن است. برای مثال، عدم وجود این ملاحظات موجب هک‌شدن صرافی‌ای به‌نام CoinCheck[2] شد [۱۰]. این ملاحظات عبارتند از:

- آژانس خدمات مالی (FSA)، صرافی‌ها را از لحاظ مدیریت سامانه بررسی می‌کند؛ این که رمزارزها در رایانه‌هایی که متصل به اینترنت هستند نگه‌داری نشوند و برای مبادلات مالی چند رمز تعیین کنند.
- صرافی‌ها از لحاظ اقدام علیه پول‌شویی بررسی می‌شوند که در صورت تراکنش‌های با مبالغ بالا ابتدا فرد تأیید هویت شود.
- معاملات رمزارزهایی که ردیابی آن‌ها با پیچیدگی همراه است، ممنوع اعلام شده است. از نمونه‌های آن می‌توان به سه کوین مونرو، Dash و Zcash اشاره کرد که در فهرست سیاه قرار گرفته‌اند.
- بررسی موجودی حساب مشتریان، توسط صرافی‌ها در صورت تخلف به‌سرعت تشخیص داده شود.
- سهام‌داران از بخش مدیریت صرافی‌ها منفک شوند تا کارفرمایان قادر به دست‌کاری سامانه به‌نفع خود نباشند.

چین

ممنوعیت استفاده از رمزارزها برای مردم در چین به‌طور

[1] Financial Supervisory Agency

[۲] صرافی CoinCheck یکی از بزرگترین صرافی‌های رمزارز به‌حساب می‌رفت. این صرافی در ماه ژانویه ۲۰۱۸ هک شد و بیش از ۵۳۰ میلیون دلار رمزارز NEM به‌سرقت رفت.

سخت‌گیرانه‌ای انجام می‌شود؛ به‌طوری که تبادلات بیت‌کوین در این کشور پهناور، تنها حدود یک‌درصد از معاملات کل بیت‌کوین را در سراسر دنیا شامل می‌شود. به‌عبارتی، Renminbi (پول رسمی چین) در حدود کمتر از یک درصد معاملات مربوط به بیت‌کوین مورد استفاده قرار گرفته است. برای رسیدن به این هدف دولت چین با فشار و تبلیغ زیاد و برداشتن حمایت خود از قانون خرید و فروش و انجام معاملات در زمینه رمزارزها و همچنین صدور ممنوعیت سفر برای سران بزرگ‌ترین صرافی‌های این کشور به نام‌های Huobi و OKCoin توانست به هدف ممنوعیت استفاده از رمزارزها برسد؛ اما چین یکی از پیشروترین کشورهای دنیا در به‌کارگیری گسترده رمزارز بومی است و با هدف مشارکت بیشتر در تنظیم چارچوب اقتصاد جهانی استفاده آزمایشی از رمزارز بومی و ملی را در مناطق مختلف آغاز کرده است. رمزارز یادشده در چین با عنوان یوان دیجیتال و یا (RMB) شناخته می شود. این رمزارز یکی از عناصر سازنده حرکت چین به سمت وضعیت نوینی در "بازار جهانی" و مشارکت بیشتر در تنظیم چارچوب اقتصاد جهانی است. این رمزارز مزایایی دارد: ۱- امنیت پرداخت‌ها را برای مشترکان به‌دنبال خواهد داشت. ۲- لازم نیست کاربران در موقع پرداخت به اینترنت متصل باشند، همچنین برای دسترسی به وجوه خود به حساب های بانکی احتیاج ندارند؛ لذا شمار زیادی از کاربران این رمزارز بی آن‌که حساب بانکی داشته باشند می‌توانند از این رمزارز بهره بگیرند و این می‌تواند هزینه‌ها را برای آنان کاهش دهد که برای اقشار آسیب‌پذیرتر جامعه بسیار مورد مهمی است. همچین استفاده از رمزارز باعث جلوگیری از فعالیت‌های غیرقانونی از جمله پول‌شویی، جعل پول، تأمین مالی غیرقانونی و فرارهای مالیاتی می‌شود که درواقع فناوری زنجیره بلوکی این امکان را فراهم می‌کند؛ افزون بر این هزینه چاپ اسکناس نیز به‌تدریج کاهش خواهد یافت. رمزارز دیجیتال چینی برخلاف سایر رمزارزها توسط دولت مرکزی حمایت می‌شود، اما دیگر رمزارزهای دیجیتالی جهان چنین پشتوانه‌ای ندارند. این رمزارز جدید به نوعی یک یوان دیجیتال به‌شمار می‌رود و علاوه‌بر مصارف داخلی، احتمال این نیز می‌رود که کشورهای بسیاری آن را به‌عنوان وسیله مبادله قبول کنند که این امر برای چین بسیار خوشایند خواهد بود. تحقق طرح یک کمربند-یک راه و احیای جاده ابریشم که بیش از شصت کشور جهان را زیر چتر اقتصادی چین گرد می‌آورد، بستر لازم برای بین‌المللی‌شدن رمزارز دیجیتال چین را فراهم خواهد کرد. ایران، چین و روسیه، هر کدام به دلایلی خواهان پایان‌دادن به سلطه دلار و یا دست‌کم کاهش وابستگی اقتصاد خود به آن هستند؛ زیرا می‌دانند حذف دلار از سبد ذخیره ارزی این کشورها، به‌ویژه اقتصادهای بزرگ و مطرحی مانند روسیه و چین می‌تواند به‌شدت اقتصاد آمریکا را تحت فشار قرار دهد. استفاده از رمزارزها کمک شایانی به تحقق این امر خواهد کرد؛ اما رمزارزهای موجود در بازار برای آنها چالش برانگیز است؛ ازاین‌رو اقدام چین برای توسعه رمزارز ملی می‌تواند این چالش‌ها را کمتر کند. چین مدعی است که رمزارز ملی آن می‌تواند دست آمریکا را از مداخله در روابط چین و ایران کوتاه کند. گفتنی است که بدون شک بدون توان و قدرت اقتصادی بالا این امر مشکل خواهد بود؛ اما در صورت تحقق اهداف «طرح یک کمربند یک راه» و نقش آفرینی فعال ایران با توجه به موقعیت و جایگاه مهم و استراتژیکی که در این طرح دارد و همچنین ترمیم اقتصاد کشور و افزایش و بهبود شاخص‌های کلان اقتصادی، زمینه تحدید و تضعیف دلار، امری دست نیافتنی نخواهد بود. روابط میان کشورهایی که در طرح یادشده قرار دارند، بخش اعظم نیازهای تجاری این کشورها را برآورده می‌سازد، بدون این‌که حضور و سایه دلارآمریکا را احساس کنند [۱۱].

کانادا

طبق اعلام بانک مرکزی در کانادا، مردم این کشور در سال جاری تمایل بیشتری برای خرید و استفاده از رمزارزها نشان داده‌اند. هدف اصلی آنان سرمایه‌گذاری، خرید کالا و خدمات اینترنتی است. بیت‌کوین محبوب‌ترین رمزارز در بین جوانان این کشور به‌شمار می‌رود؛ بنابراین بانک مرکزی کانادا به‌تازگی به‌منظور بررسی دقیق فرصت‌ها و تهدیدهای رمزارزها، کار مطالعه و تجزیه و تحلیل رمزارزها را به‌طور خاص بر بیت‌کوین شروع کرده است [۱۲].

آمریکا

در گذشته آمریکا در تمامی ایالت‌های خود بیت‌کوین و دیگر رمزارزها را ممنوع کرده بود؛ ولی درحال حاضر حدود دوهزار دستگاه ATM برای مبادلات بیت‌کوین در سراسر آمریکا وجود دارد و به‌طور موازی جلساتی درخصوص بررسی تمامی جوانب رمزارزها توسط مؤسسات مالی به‌خصوص موسسه NASDAQ[1] (یکی از بزرگ‌ترین بازار بورس سهام در آمریکا) انجام می‌شود. همچنین کمیسیون بورس و اوراق بهادار آمریکا (SEC)[2] قوانین پیشنهادی خود را برای ICOها اعلام کرده است. در این بیانیه تمام استارتاپ‌ها که قصد فروش توکن‌های خود را

[1] National Association of Securities Dealers
[2] Securities and *Exchange Commissio*

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

دارند، باید توکن خود را در SEC ثبت کرده و تمام اطلاعات لازم را در اختیار این نهاد قرار دهند [۱۴-۱۳].

کشورهای آفریقایی

طبق گزارشی که بانک‌داری آفریقایی Ecobank در اول آگوست ۲۰۱۸ منتشر کرده، کشورهای دارای نقشه‌راه مقرارت برای رمزارزها در این قاره را به پنج بخش طبقه‌بندی کرده است.

(جدول-۱): موضع کشورهای مختلف قاره آفریقا [۱۵]

۱	استفاده از رمزارزها غیرقانونی و ممنوع است.
۲	موضع مخالف نسبت به رمزارزها دارند ولی با رویکردی نظارتی دائم بر وضعیت پیش‌رو
۳	موضع تحقیقاتی در مورد رمزارزها همراه با هشدار را پیش گرفته‌اند.
۴	موضع کاملاً مطلوب و قابل قبول اما بدون تدوین قانون کامل و مشخص
۵	رمزارزها در این کشورها پذیرفته شده و به صورت قانون تنظیم شده است.

(شکل-۱): موضع کشورهای واقع در قاره آفریقا [۱۵]

هیچ یک از کشورهای قاره آفریقا در دسته پنجم قرار ندارند؛ ولی کشورهای تونس، سنگال و سوازیلند موضع به‌طورکامل مطلوب و قابل قبول اما بدون تدوین قانون کامل و مشخص را در پیش گرفته‌اند.

کشورهای عضو گروه بیست

گروه G20 یک مجمع بین‌المللی اقتصاد متشکل از وزرای اقتصاد و دارایی و مسئولان بانک‌های مرکزی بیست اقتصاد مطرح دنیاست. گروه بیست متشکل از قدرتمندترین کشورهای جهان است که در مجموع ۸۵ درصد اقتصاد جهان را در اختیار دارند. در گروه G20 گروهی به‌نام FSB[1] وجود دارند که نظارت بر نظام مالی جهانی را به‌عهده دارند. این گروه بر این باور است که رمزارزها خطر جدی برای ثبات مالی جهانی به‌وجود نمی‌آورند، اما باید نظارت هوشمندانه‌ای بر آن‌ها داشت.

این گروه، چارچوب جدیدی برای نظارت بر رمزارزها ارائه داده است [۱۶]. این چارچوب با همکاری کمیسیون پرداخت‌ها و زیرساخت‌های بازار (CPMI)[2] به‌وجود آمده است [۱۷]. کمیسیون CPMI از نمایندگان بانک مرکزی کشورهای G10[3] تشکیل شده است. این کمیسیون معیارهایی را ارائه می‌دهد که FSB از آن‌ها برای نظارت در بازارهای دارایی دیجیتالی استفاده خواهد کرد.

این چارچوب شامل معیارهای ریسک است که خطرات پیش‌رو را با استفاده از اطلاعات و منابع موجود مشخص می‌کند.

علاوه‌بر FSB، سازمان بین‌المللی کمیسیون بورس اوراق بهادار (IOSCO)[4] نقش نظارتی را بر رمزارزها به‌عهده دارد. این سازمان یک سامانه مشاوره برای عرضه اولیه پول با نام ICO Consultation Network راه‌اندازی کرده تا خطرات و چالش‌های سرمایه‌گذاری در ICOها مشخص و بررسی شود.

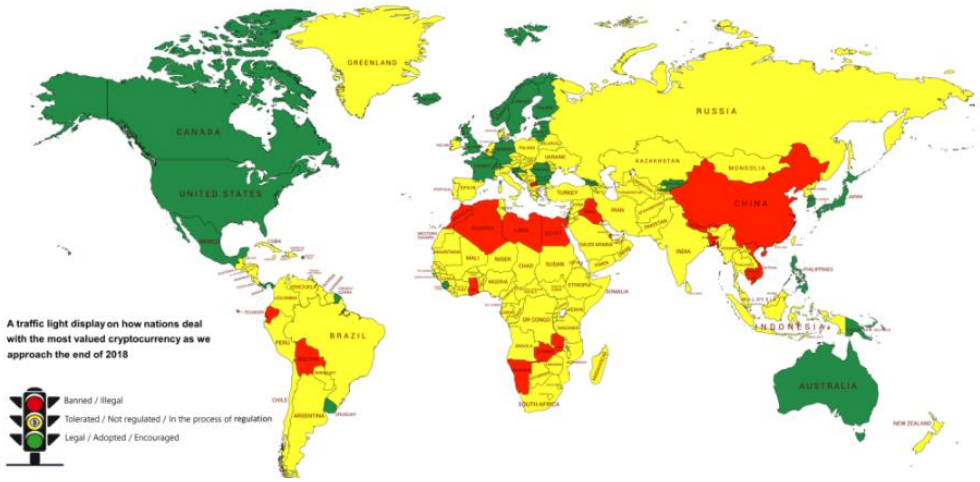
کمیته نظارت بانک‌داری (BCBS)[5] که توسط نمایندگان G10 تشکیل‌شده‌اند، بر روی تأثیرات رمزارزها بر بانک‌ها چه به‌طور مستقیم و چه غیرمستقیم در حال بررسی است.

سازمان FATF[6] برای بررسی وضعیت قوانین پول‌شویی در بازارهای مختلف مالی در سرتاسر جهان توسط گروه G7 تشکیل شد. این سازمان روند پول‌شویی را در دنیا بررسی کرده و در سطح ملی و بین‌المللی بر نحوه اجرای قوانین و فعالیت‌های مالی کشورها نظارت دارد و استانداردهایی برای مبارزه با پول‌شویی طراحی می‌کند. این کار به‌منظور بررسی مخاطرات سرمایه‌گذاری در بازارهای مالی جهان برای این کشورها انجام می‌پذیرد. در کنفرانسی که در فرانسه اواخر فوریه ۲۰۱۸ برگزار شد،

[1] Financial Stability Board
[2] Committee on Payments and Market Infrastructures
[3] کشورهای گروه ۱۰ یا G10 مشتمل از اعضای صندوق بین‌المللی پول (بلژیک، کانادا، فرانسه، ایتالیا، ژاپن، هلند، بریتانیا، آلمان، سوئد و آمریکا) است که این کشورها قبول کردند تا منابع صندوق بین‌المللی پول را تأمین کنند.
[4] International Organization of Securities Commissions
[5] Basel Committee on *Banking* Supervision
[6] Financial Action Task Force

کشورهای عضو که نگران ریسک‌های پول‌شویی در تراکنش‌های رمزارزها بودند، خواستار بررسی و ارائه سازوکارهای لازم توسط این سازمان شدند [۱۸].

در شکل (۲)، نمایی کلی بر اساس میزان پذیرش رمزارزها در کشورهای مختلف نشان داده شده است، کشورهایی چون چین و اندونزی سیاست سخت‌گیرانه‌ای نسبت به رمزارزها از خود نشان می‌دهند.



(شکل-۲): میزان سختی پذیرش رمزارزها در کشورهای مختلف [۳۳]

گزارشی در ۲۶ مارس ۲۰۱۸ [۱۸] منتشر شده که در آن به شش سؤال مطرح درخصوص رمزارز برای کشورها پاسخ داده شده است، این سؤالات عبارتند از:

۱- تبادلات رمزارزها در این کشور ممنوع است و یا به‌صورت قانونی درآمده و یا در هاله‌ای از ابهام (خاکستری) است؟

۲- فعالیت ICOها ممنوع است، یا به‌صورت قانونی درآمده و یا در هاله‌ای از ابهام (خاکستری) است؟

۳- آیا پرداخت با رمزارزها ممنوع است؟ (✗ ممنوع نیست، ✓ ممنوع است)

۴- آیا تبدیل ارزهای دیجیتالی به پول فیات ممنوع است؟ (✗ ممنوع نیست، ✓ ممنوع است)

۵- آیا برنامه‌ای برای افزایش مقررات رمزارزها وجود دارد؟ (✗ وجود ندارد، ✓ وجود دارد)

۶- آیا سازمان تنظیم و مقررات محلی کشور یادشده در مورد سرمایه‌گذاری در مورد رمزارزها هشدار داده است؟ (✗ هشدار نداده است، ✓ هشدار داده است)

(جدول ۲-الف): موضع قاره آسیا در مورد رمزارزها [۱۸]

	مبادله رمزارزها	فعالیت ICOها	ممنوعیت پرداخت رمزارزی	ممنوعیت تبدیل رمزارز به پول فیات	برنامه‌ریزی برای افزایش مقررات رمزارزی	هشدار جهت سرمایه‌گذاری رمزارزها
ژاپن	قانونی	خاکستری	✗	✗	✗	✗
هنگ‌کنگ	خاکستری	خاکستری	✗	✗	✗	✓
تایوان	خاکستری	قانونی	✗	✗	✗	✓
سنگاپور	خاکستری	خاکستری	✗	✗	✗	✓
فیلیپین	قانونی	خاکستری	✗	✗	✓	✓
تایلند	خاکستری	خاکستری	✗	✗	✓	✓
هند	خاکستری	خاکستری	✗	✗	✓	✓
کره‌جنوبی	خاکستری	ممنوع	✗	✗	✓	✓
اندونزی	خاکستری	خاکستری	✓	✓	✓	✓
چین	ممنوع	ممنوع	✓	✓	✓	✓
استرالیا	خاکستری	خاکستری	✗	✗	✓	✓

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

(جدول ۲-ب): موضع قاره آمریکا در مورد رمزارزها [۱۸]

	مبادله رمزارزها	فعالیت ICOها	ممنوعیت پرداخت رمزارزی	ممنوعیت تبدیل رمزارز به پول فیات	برنامه‌ریزی برای افزایش مقررات رمزارزی	هشدار جهت سرمایه‌گذاری رمزارزها
آمریکا	خاکستری	قانونی	×	×	×	✓
کانادا	خاکستری	قانونی	×	×	×	✓
برزیل	خاکستری	خاکستری	×	×	×	✓

(جدول ۲ -ج): موضع قاره اروپا در مورد رمزارزها [۱۸]

	مبادله رمزارزها	فعالیت ICOها	ممنوعیت پرداخت رمزارزی	ممنوعیت تبدیل رمزارز به پول فیات	برنامه‌ریزی برای افزایش مقررات رمزارزی	هشدار جهت سرمایه‌گذاری رمزارزها
انگلیس	خاکستری	خاکستری	×	×	×	✓
فرانسه	خاکستری	خاکستری	×	×	✓	✓
آلمان	خاکستری	خاکستری	×	×	×	✓
روسیه	خاکستری	خاکستری	×	×	✓	✓

(جدول ۲-د): موضع قاره آفریقا در مورد رمزارزها[۱۸]

	مبادله رمزارزها	فعالیت ICOها	ممنوعیت پرداخت رمزارزی	ممنوعیت تبدیل رمزارز به پول فیات	برنامه‌ریزی برای افزایش مقررات رمزارزی	هشدار جهت سرمایه‌گذاری رمزارزها
نیجریه	خاکستری	خاکستری	×	×	✓	✓
آفریقای جنوبی	خاکستری	خاکستری	×	×	✓	✓
زیمباوه	خاکستری	خاکستری	✓	×	×	✓
کنیا	خاکستری	خاکستری	×	×	×	✓

۳- چالش‌های رمزارزها

مهم‌ترین بحث در برخورد با هر پدیده‌ی نوظهوری، شناخت چالش‌های ناشی از آن در فرآیند سیاست‌گذاری مواجه به آن است. با توجه به مزیت‌های فناوری زنجیره بلوکی و بزرگ‌ترین محصول آن یعنی رمزارزها که امکان آزادی در پرداخت و دسترسی بین‌المللی را با پایین‌آوردن هزینه عملیاتی و بالابردن سرعت در انتقالات بین‌المللی و فرامرزی فراهم کرده است، می‌توان گفت بهره‌گیری از رمزارزها منجر به عدم وابستگی هر کشور به سیاست‌های دولت‌ها شده، کاهش قدرت تحریم‌های دلاری آمریکا علیه اقتصاد جهان، تسهیل در پیمان‌های پولی دو یا چند جانبه، ایجاد موقعیت جذب و افزایش سرمایه‌گذاری‌های خارجی در جهانی‌شدن کسب‌وکارهای داخلی و بهبود صادرات در هر کشور خواهد شد. ازاین‌رو با فراگیرشدن رمزارزها و مزیت‌های منحصربه‌فردی که در اختیار استفاده‌کنندگان قرار می‌دهد، لازم است، روش‌های تجزیه و تحلیل متفاوتی را که برای شناسایی چالش‌های حوزهٔ رمزارزها وجود دارد، را مورد بررسی قرار داد [۲۸-۲۰]. در این مقاله با توجه به ترکیب سه‌گانه عوامل براساس جنبه‌های فناورانه، محیطی و حاکمیتی، چالش‌های مطرح در حوزه رمزارزها مورد بررسی قرار گرفته است و کلیه چالش‌ها در تصویری جامع معرفی می‌شوند. با توجه به ویژگی‌های رمزارزها و خدمات مناسبی که به ارمغان می‌آورند، شناسایی چالش‌ها در سطح رمزارز ملی از دیگر مواردی است که در این مقاله به آن پرداخته می‌شود و همانند چالش‌های رمزارزها سعی شده در تصویری جامع سطوح مختلف آن ارائه شود.

۳-۱- چالش‌های رمزارزهای عمومی

ین دسته از چالش‌ها مرتبط با ذات و ماهیت رمزارزهای عمومی است و در رمزارز ملی نیز می‌تواند کم و بیش وجود داشته باشد. جنبه فناورانه از چهار بعد امنیت داده،

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

پردازش داده، ذخیره‌سازی و استخراج بررسی شده است که به شرح ذیل به آن‌ها اشاره می‌شود (شکل ۵).

۳-۱-۱- امنیت داده

برای ایجاد محرمانگی و نیز حفظ حریم خصوصی به‌ترتیب در هر تبادل و تراکنش یک رمزارز از تابع‌های چکیده‌سازی و نیز کلیدهای خصوصی و عمومی استفاده می‌شود که کلیدها براساس الگوریتم‌های رمزنگاری کلید عمومی مبتنی بر خم بیضوی تولید می‌شوند. با ظهور رایانه‌های کوانتومی در سال ۱۹۹۴ اثبات شد که سامانه‌های رمزنگاری مبتنی بر نظریه اعداد از قبیل RSA و الجمال و نیز خم بیضوی توسط رایانه‌های کوانتومی شکسته می‌شوند [۲۹]. ازاین‌رو رایانه‌های کوانتومی باعث ایجاد اختلال در رمزنگاری‌های به‌کاررفته در مدیریت کلید زنجیره بلوکی و نیز رمزارز خواهند شد و به‌عنوان یک چالش و تهدید مطرح است. این مسأله در رمزارزهای ملی بیشتر مشاهده خواهد شد؛ زیرا کشورهای متخاصم با به‌کارگیری تمام قدرت محاسباتی خود با هدف ایجاد اختلال در شبکه رمزارز ملی اقدام به حمله می‌کنند.

از دیگر مواردی که در حوزه امنیت رمزارز می‌تواند از چالش‌های مطرح به‌شمار آید و موجب مخاطراتی شود، ویژگی الکترونیکی‌بودن رمزارزها است؛ این ویژگی مخاطراتی نظیر هک‌شدن حساب کاربر و سرقت‌های الکترونیکی را به همراه دارد. به‌عنوان مثال در کیف‌پول Blackwallet با نفوذ از طریق DNS Hijacking مهاجمان توانستند هفت هزار XLM را به‌دست آورند [۳۰]. همچنین علت هک یکی از صرافی‌های ژاپنی مربوط به رمزارز Coincheck، نشت اطلاعات از طریق دریافت بدافزارهای مخرب توسط رایانه کارکنان این صرافی عنوان شده است.

حمله منع سرویس در رمزارزها زمانی اتفاق می‌افتد که شبکه در انتظار تعداد تراکنش زیادی باشد و توانایی پاسخ به آن‌ها را نداشته باشد. همین موضوع باعث می‌شود تراکنش‌ها برای مدت زمانی غیرمعمول و طولانی در انتظار بمانند.

شاید در وهله نخست ایده‌ای که به جلوگیری از این نوع نفوذها به شبکه رمزارز ملی کمک می‌کند، استفاده از «اینترنت ملی» و «شبکه ملی اینترنت» باشد؛ زیرا راه‌اندازی و استفاده از اینترنت ملی برای توسعه شبکه زیرساخت امن و پایدار ملی است. برخلاف تصور عموم، اینترنت ملی هیچ ارتباطی به محدودکردن اینترنت ندارد و تنها نوعی گردش امن اطلاعات در بستر داخلی است. ازاین‌رو جود شبکه ملی اطلاعات، دسترسی امن و پایدار به خدمات ملی را برای کاربران مهیا می‌کند و شرایط را برای بهره‌مندی آن‌ها از پهنای باند بسیار بالایی برای ارتباط و انتقال اطلاعات و نیز بستری برای مسدودکردن خراب‌کاری‌هایِ در حوزهٔ سایبری تا حد زیادی فراهم می‌کند.

۳-۱-۲- پردازش داده

با توجه به بستر زنجیره بلوکی برای رمزارزها تأیید کلیه تراکنش‌های مربوط به یک بلوک، بسته به نوع رمزارز متفاوت است. در رمزارزها برای بررسی صحت و درستی تراکنش‌ها باید چند بلوک صبر کرد. گرچه این زمان برای تراکنش‌های بین‌المللی مناسب، ولی برای تراکنش‌های داخلی بسیار زیاد است؛ ازاین‌رو قدرتمندی و توانایی بالای برخی از استخراج‌کنندگان[1] مخرب، می‌تواند موجب ایجاد اختلال شود؛ زیرا با ایجاد انشعابی نادرست در زنجیره بلوکی یک رمزارز از انجام تراکنش‌های درست جلوگیری کرده و صحت رمزارز که یکی از فاکتورهای مهم امنیتی است، به‌خطر می‌افتد. از طرفی با درنظرگرفتن مبلغ بالایی برای یک سری تراکنش‌ها، استخراج‌کنندگان را برای اولویت‌دادن به آن ترغیب می‌کند؛ ازاین‌رو باعث می‌شود کسی که مبلغ کمی برای ارسال تراکنش خود درنظر گرفته جزو تراکنش‌ها قرار نگیرد.

در نظام‌های بانک‌محور کنونی، اگر مبلغی به اشتباه به دیگری واریز شود، بانک می‌تواند آن وجه را برگرداند؛ ولی به‌دلیل این‌که در رمزارزها هیچ نهاد مسئولی وجود ندارد، این وجه قابل بازگشت نخواهد بود.

۳-۱-۳- ذخیره‌سازی

با توجه به گسترش دنیای دیجیتال، روزانه حجم عظیمی از داده‌ها در دنیا تولید و پیش‌بینی می‌شود این حجم در سال ۲۰۲۰ به ۴۰ZB برسد. با استفاده از زنجیره‌بلوکی، ذخیره‌سازی تراکنش‌ها به‌شیوه‌ای ایمن‌تر انجام خواهد گرفت و با توجه به ساختار رمزنگاری‌شده، یک‌پارچگی بدون هیچ کنترل‌کنندهٔ مرکزی حفظ خواهد شد؛ ولی این ذخیره‌سازی داده با چالش‌هایی همراه است که می‌توان به محدودیت حجم نهایی هر بلوک در برخی رمزارزها اشاره کرد. برای مثال بیت‌کوین فقط قادر به ذخیره 1Mو بیت‌کوین‌کش 8M است که این امر برای ذخیره داده‌های عظیم مناسب نخواهد بود.

[1] Miner

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

با ورود مفهوم اینترنت اشیا، امکان برقراری ارتباط در هر زمان و هر مکان میسر خواهد شد و درنتیجه لازم است، تعداد تراکنش‌ها در هر ثانیه پاسخ‌گوی این موضوع باشد؛ ولی به‌دلیل محدودیت تعداد تراکنش‌ها در ثانیه برای برخی رمزارزها باعث می‌شود نتوان از آن‌ها برای برخی کاربردهای خاص که به تراکنش زیادی نیاز دارند، استفاده کرد. در جدول (۳) تعداد برخی تراکنش‌ها در ثانیه مشخص شده است.

(جدول-۳): تعداد تراکنش‌ها در ثانیه

رمزارز	تعداد تراکنش‌ها	رمزارز	تعداد تراکنش‌ها
بیت‌کوین	۳ تا ۷	اتریوم	۱۵ تا ۲۰
ریپل	۱۵۰۰تا۵۰۰۰۰	کاردانو	۵ تا ۷
بیت‌کوین‌کش	۶۱	استلار	۱۰۰۰
IOTA	۳	لایت‌کوین	۲۶ تا ۵۶
Monero	۴	NEO	۱۰۰۰
Qtum	۶۰ تا ۷۰	Dash	۴۸
NEM	۱۰۰۰		

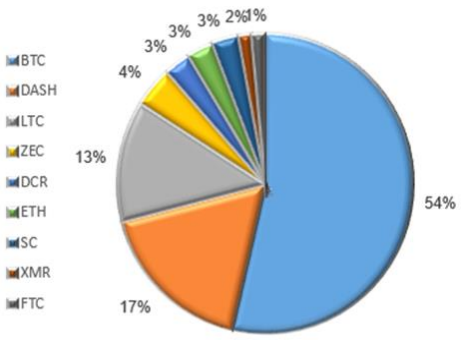
مسأله دیگری که به‌طور کلی در زنجیره‌بلوکی وجود دارد؛ این است که تأیید بلوک‌ها نشان‌دهندهٔ تأیید کامل نیست، بلکه باید چند بلوک برای صحت کامل صبر کرد. گرچه این زمان برای تراکنش‌های بین‌المللی مناسب است، ولی برای تراکنش‌های داخلی بسیار زیاد است. تأیید کلیه تراکنش‌ها بسته به نوع رمزارز متفاوت است.

(جدول-۴): زمان تأیید تراکنش‌ها به دقیقه

رمزارز	زمان تأیید	رمزارز	زمان تأیید
بیت‌کوین	۲۵ تا ۶۰	اتریوم	۲
ریپل	۴ ثانیه	کاردانو	۳ تا ۵
بیت‌کوین‌کش	۶۰	استلار	۲ تا ۵ ثانیه
IOTA	۲	لایت‌کوین	۳۰
Monero	۳۰	NEO	۱۵ تا ۲۰ ثانیه
Qtum	۴ تا ۵	Dash	۴۸
NEM	۱ تا ۲		

۴-۱-۳- استخراج

علمیات استخراج[1] از دیگر حوزه‌هایی است که در رمزارزها باید مورد توجه قرار گیرد. فلسفه زنجیره‌بلوکی، غیرمتمرکزنمودن از یک نهاد خاص است؛ ولی امروزه به دلایل مختلف، تمرکززدایی در این فناوری با چالش روبه‌رو است. استفاده از برنامه مدار یکپارچه خاص (ASIC[2]) تراشه‌ای کامپیوتری است که می‌تواند موجب متمرکزسازی شبکه رمزارز شود. تراشهٔ رایانه‌ای AISC برای انجام کارهایی خاص طراحی شده و در زمینه قدرت پردازش و محاسبات استخراج، دارای کارایی ویژه و بالایی است. از نمونه‌های آن می‌توان به Dragomnit 16T، Antminer S7، Antminer R4 و Avalon 6 اشاره کرد. با توجه به بررسی‌های انجام‌شده در [۳۱] بیش از نیمی از این دستگاه‌ها برای بیت‌کوین و حدود بیست درصد از این دستگاه‌ها برای DASH و مابقی طبق شکل (۳) برای سایر رمزارزها به کار گرفته شده است؛ از این رو بسیاری از طراحی‌های رمزارزها به سمت الگوریتم‌هایی رفته است که کار با حافظه را بالا ببرند تا توان استفاده از دستگاه‌های ASIC کاهش یابد.



(شکل-۳): تعداد رمزارزهایی که دستگاه ASIC برای آن ایجاد شده است [۳۱].

هزینه‌های استخراج برخی از رمزارزها مانند بیت‌کوین، به‌اندازه مصرف برق یک کشور پرمصرف است. پردازش این حجم اطلاعات، هزینه‌های زیادی مانند برق، نیروی انسانی و زیرساخت بر جهان تحمیل می‌کند. پژوهش‌گران، با مقایسهٔ هزینه برق بزرگ‌ترین شرکت‌های الکتریکی جهان Elite Fixtures، ونزوئلا را به‌عنوان ارزان‌ترین کشور و کره‌جنوبی را به‌عنوان پرهزینه‌ترین کشور برای استخراج بیت‌کوین اعلام کرده‌اند. در ونزوئلا برای استخراج یک واحد بیت‌کوین حدود ۵۳۱ دلار و در کره‌جنوبی در حدود ۲۶۱۷۰ دلار نیاز است. به‌طورتقریبی بیش‌تر کشورهایی که در اروپای غربی یا کشورهای جزیره‌ای اقیانوس آرام هستند، جزو کشورهای گران‌قیمت از لحاظ انرژی محسوب می‌شوند. ایران تاحدودی یکی از کشورهایی است که انرژی در آن ارزان است. برای رسیدن به این نتایج، پژوهش‌گران علاوه‌بر هزینه برق کشورها، مصرف برق دستگاه‌های استخراج را از جمله AntMiner S9، AntMiner S7 و Avalon 6 مورد مطالعه قرار داده‌اند.

[1] Mining
[2] Application-Specific Integrated Circuit

(جدول-۵): استخراج یک واحد بیت‌کوین

کره‌جنوبی	**۲۶۱۷۰**	سوئیس	۷۴۹۴	روسیه	۴۶۷۵
بحرین	۱۶۷۷۳	پاکستان	۷۱۳۷	اندونزی	۴۳۲۹
دانمارک	۱۴۲۷۵	عراق	۶۵۴۳	امارات	۳۵۶۹
آلمان	۱۴۲۷۵	اسرائیل	۶۰۸۷	هند	۳۲۷۴
ایتالیا	۱۰۳۱۰	آفریقای‌جنوبی	۵۹۴۸	**ایران**	**۳۲۱۷**
استرالیا	۹۹۱۳	سنگاپور	۵۹۳۶	چین	۳۱۷۲
هلند	۹۴۴۹	مالزی	۵۱۴۷	عربستان	۳۱۷۲
ژاپن	۸۷۲۳	ترکیه	۴۹۸۴	بنگلادش	۲۳۷۹
انگلیس	۸۴۰۲	آمریکا	۴۷۵۸	کویت	۱۹۸۳
فرانسه	۷۹۳۰	سوئد	۴۷۴۶	**ونزوئلا**	**۵۳۱**

اتحاد استخراج‌کنندگان نیز از مواردی است که می‌تواند باعث تمرکز نهادها شود. درصورتی‌که تعدادی از استخراج‌کنندگان با هم متحد شوند، تا بیش از پنجاه درصد توان محاسباتی استخراج یک کوین را کنترل کنند، می‌توانند حمله ۵۱٪ را رقم بزنند.

یکی دیگر از مواردی که باعث ازبین‌رفتن تمرکز زنجیره بلوکی می‌شود، پهنای باند است. محدودیت پهنای باند دستگاه‌های متصل به اینترنت موجب می‌شود که هر دستگاهی با پهنای باند بیشتر، سریع‌تر بتواند بلوک‌ها را دریافت و منتشر کند.

۵-۱-۳- اعتماد مردم

جنبه محیطی از بعد اعتماد مردم بررسی شده است که به شرح زیر به آن‌ها اشاره می‌شود یکی از ویژگی‌های شاخص بازار رمزارزها، نوسانات شدید قیمت و نبود ثبات در آن است. عوامل مختلفی چون عرضه و تقاضا، کاربردی‌بودن رمزارز، هیجان بازار، دشواری استخراج باعث قیمت‌گذاری بر رمزارزها می‌شود. این خود یکی از چالش‌هایی است که مردم برای سرمایه‌گذاری بر رمزارزها با آن مواجه می‌شوند. این موضوع در رمزارزهای رایجی مانند بیت‌کوین، اتریوم و ... به شهود پیداست. در شکل زیر نوسانات قیمت در بیت‌کوین از سال ۲۰۱۳ تا ۲۰۱۸ به تصویر کشیده شده است.

(شکل-۴): نوسانات قیمت بیت‌کوین [۳۲]

۶-۱-۳- حاکمیت

جنبه حاکمیتی از چهار بعد تضعیف بخش دولتی، گمنامی، پول‌شویی و خروج سرمایه از کشور بررسی شده است که به شرح زیر به آن‌ها اشاره می‌شود. در بخش حاکمیت با چالش‌های زیادی روبه‌رو هستیم. جدول (۲) نشان‌دهنده این است که بیش‌تر کشورها در مورد رمزارزها موضع مشخصی را اعمال نکرده‌اند و بیش‌تر آن‌ها مواضع‌شان در هاله‌ای از ابهام است.

تضعیف بخش دولتی: با رواج رمزارزها، نقش بانک مرکزی و نهادهای واسطه در تراکنش‌ها کمرنگ‌تر می‌شود. این موضوع می‌تواند خطری جدی برای نظام مالی یک کشور به‌وجود آورد؛ زیرا دراین‌صورت برای توجیه اعمال سیاست‌های مالی جایی باقی نمی‌ماند و هیچ نظارتی بر تراکنش‌های روزانه، وجود نخواهد داشت؛ به‌عنوان مثال بانک مرکزی یکی از نهادهایی است که در صورت تولید رمزارز ملی با مشکل روبه‌رو خواهد بود.

گمنامی: یکی از مسائلی که در برخی رمزارزها وجود دارد و دولت را با چالش مواجه کرده، مبحث گمنامی است. اگرچه کلیه تراکنش‌های انجام‌شده اعم از تاریخچه و موجودی هر حساب در سیستم، دردسترس همگان قرار دارد، ولی حساب‌ها تنها با یک نشانی نامشخص از نگاه دیگران نمایان است و در نتیجه به‌ظاهر مالک یک حساب رمزارز، گمنام و ناشناس خواهد بود. در رمزارزهایی همچون مونرو، Dash و Zcash طراحی به‌گونه‌ای است که گمنامی به‌شدت در آن لحاظ شده است. بسته به سیاست دولت در طراحی رمزارز ملی این ویژگی باید مورد توجه قرار گیرد.

پول‌شویی: برخی رمزارزهای موجود بستری مناسب برای

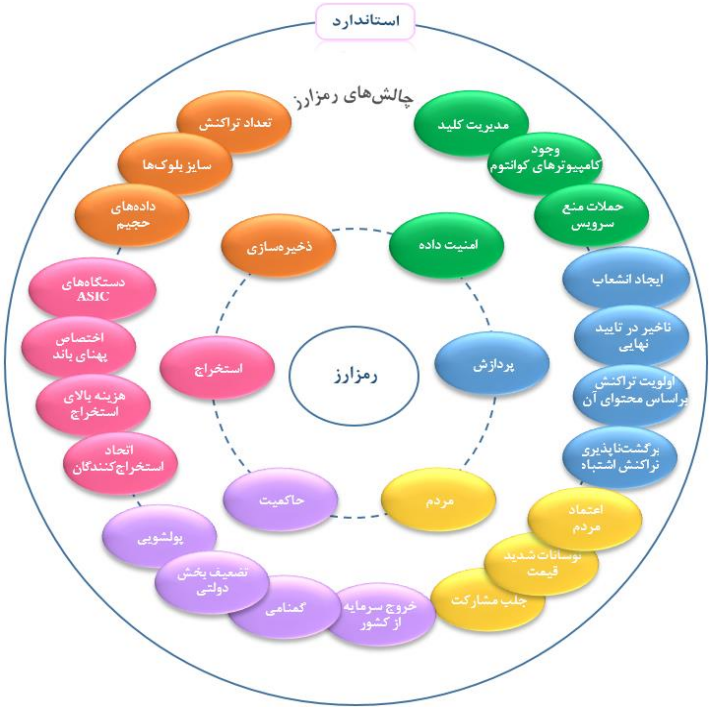
[DOR: 20.1001.1.24763047.1399.9.1.6.9]

پول‌شویی به‌حساب می‌آید. این ویژگی برای رمزارزها در تضاد کامل با مسیر حرکت و قوانین حاکم بر کشورها در شفاف‌سازی انتقالات پولی است. تعبیه سازوکارهای مبارزه با پول‌شویی در رمزارز ملی طبق قوانین پول‌شویی با نظارت FATF باید لحاظ شود. سازوکارهای مبارزه با پول‌شویی باید به‌گونه‌ای در طراحی رمزارز ملی اعمال شود که ضمن این‌که امکان ارتباط مبادلات پولی با هویت افراد مهیا نیست، اما نهادهای مبارزه با پول‌شویی در شبکه بتوانند در صورت لزوم هویت افراد را شناسایی کنند. برای نمونه می‌توان در سامانه مشخص کرد که به‌ازای ارسال مبالغ زیاد، هویت شخص شناسایی شود، که البته یکی از راه‌کارهایی که افراد مخرب می‌توانند انجام دهند این است که به‌ازای نشانی‌های مختلف و مبالغ پایین این کار انجام گیرد. این مسأله مستلزم اعمال روش‌های فنی و تعریف سطوح مختلف معاملاتی است.

خروج سرمایه از کشور: ویژگی رمزارزها می‌تواند برای خروج سرمایه از کشور تهدیدکننده باشد؛ به‌خصوص در شرایط اعمال‌شده برای محدودیت معامله و انتقال ارز در کشور طی هفته‌های اخیر، ممکن است، برخی از کاربران رمزارز را به‌عنوان راه‌حلی برای رفع این محدودیت‌ها و خروج سرمایه از کشور استفاده کنند. به‌خصوص اگر بتوان رمزارز تولیدشده را در سطح بین‌الملل مورد استفاده قرار داد.

۷-۱-۳- استاندارد

درحال حاضر در دنیا قوانین مشخص و واضحی در رابطه با رمزارزها اعمال نشده است و این امر می‌تواند به یک چالش جدی برای دولت‌ها و حتی سرمایه‌گذاران در این عرصه بدل شود. قوانین حاکم بر رمزارزها ثبات چندانی ندارد و ممکن است در چند ماه آینده تغییرات زیادی را شاهد باشیم. در نتیجه تغییر قوانین کشورها، بازار رمزارزها را تحت تأثیر خودش قرار می‌دهد. مانند کره‌جنوبی که به یک‌باره رویکرد خود را نسبت به رمزارزها تغییر داد.



(شکل-۵): تصویر جامع از چالش‌های رمزارزها

۲-۳- چالش‌های رمزارزهای ملی

به‌دلیل سیاست‌هایی که در رمزارز ملی قائل خواهیم بود، برخی از چالش‌هایی که در رمزارزهای عمومی وجود دارد، در اینجا کاربرد نخواهد داشت (شکل ۶)؛ مانند استفاده از دستگاه‌های ASIC و اتحاد استخراج‌کنندگان؛ زیرا به‌دلیل ماهیت رمزارز ملی لازم است، زنجیره بلوکی آن به‌صورت خصوصی پیاده‌سازی شود (ازاین‌رو نیازی به طراحی مسائل محاسباتی سخت برای بخش استخراج وجود ندارد). در ادامه به بررسی چالش‌های مختص رمزارز ملی همانند رمزارز عمومی براساس سه جنبه فناورانه (گفتنی است کلیه چالش‌های مرتبط با پردازش و ذخیره‌سازی در رمزارز عمومی در اینجا صادق است)، محیطی و حاکمیتی پرداخته خواهد شد.

۱-۲-۳- امنیت داده (جنبه فناورانه)

امنیت الگوریتم پیاده‌سازی‌شده در رمزارز ملی باید به‌دقت بررسی شود. هسته اصلی رمزارزها، الگوریتم‌های چکیده‌سازی و رمزنگاری است. الگوریتم‌های جست‌وجوی

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

کامل فضای حالت‌های کلید رمزنگاری و محاسبهٔ زمان لازم برای حمله به این الگوریتم‌ها از جمله مواردی است که پیچیدگی به‌کارگیری یک رمزارز در سطح ملی را بیشتر می‌کند؛ زیرا قدرت محاسباتی مبتنی بر توان محاسباتی در سطح کشورهای متخاصم خواهد بود.

در حال حاضر کشورهای معدودی در حال پیاده‌سازی رمزارز ملی هستند. در این بین کشور ونزوئلا اقدامی عملی در پیاده‌سازی یک رمزارز ملی (پترو مبتنی بر توکن) به تعداد مشخص و غیرقابل تغییر انجام داده است. این کشور برای خروج از مشکلات شدید اقتصادی و فرار از تحریم به راه‌اندازی پترو اقدام کرده ولی به هدف خود دست نیافته است.

در صورت استفاده از توکن و پلتفرم غیرمستقل، موجب عدم استقلال در یک رمزارز ملی خواهد شد و بنابراین می‌توان گفت چالش‌های بستر انتخابی به‌نوعی به توکن ایجادشده منتقل می‌شود.

یکی دیگر از چالش‌های این لایه جرم‌یابی است که رمزارز ملی باید به‌نحوی طراحی شود که حافظ حریم‌خصوصی کاربران باشد؛ ولی از طرفی اگر جرمی اتفاق بیافتد، بتوان آن را پیگیری نمود.

۲-۲-۳- استخراج (جنبه فناورانه)

برخلاف رمزارزهای عمومی که یکی از اهداف آن تمرکززدایی است، در رمزارز ملی نمی‌توان به این صورت عمل کرد و لازم است بر افرادی که اجازه استخراج دارند نظارت شود. اعمال سیاست‌های مالی در رمزارزهای ملی یکی از اهداف محورهای آن به‌شمار می‌رود؛ بنابراین شبکه استخراج باید تحت کنترل تولیدکنندگان رمزارز قرار داشته باشد تا سیاست‌های مالی را به نفع کشور اعمال کنند. بدین‌ترتیب ایجاد سازوکارهایی در پیاده‌سازی رمزارز (استفاده زنجیره‌بلوکی خصوصی[1]) لازم است تا فهرست استخراج‌کنندگان مجاز ثبت شود. همچنین لازم است اگر مشکلی در روش‌ها، کدهای رمزارز و یا الگوریتم‌ها پیش آمد، به‌سرعت استخراج‌کنندگان، روش‌های جدید را جایگزین روش‌های پیشین کند.

۳-۲-۳- اعتماد مردم (جنبه محیطی)

یکی از مهم‌ترین عوامل موفقیت یک رمزارز ملی، پذیرش آن بین فعالان اقتصادی و مردم است. بدون رواج و پذیرش یک رمزارز در بین فعالان اقتصادی و مردم، درعمل هیچ کاربردی برای آن نمی‌توان متصور شد. تفاوت اساسی یک رمزارز عمومی مانند بیت‌کوین و اتریوم با رمزارزهای ملی، این است که در سازوکار رمزارز عمومی، هیچ دولت یا قدرتی (البته به‌ظاهر) بر عرضه و کنترل نقل و انتقالات تراکنش‌ها دخالتی ندارند که این خود یکی از دلایل استقبال مردم به رمزارزهاست؛ ولی در رمزارز ملی با وجود نظارت حاکمیت در بخش‌هایی از این فناوری، این مزیت از بین خواهد رفت. یکی از راه‌کارهایی که به نظر می‌رسد اعتماد کاربران را افزایش می‌دهد، آموزش است. کاربر باید مفاهیم زنجیره‌بلوکی، فاکتورهای امنیتی که این فناوری را برایش به ارمغان می‌آورد، چگونگی استخراج، ایمن‌نگه‌داشتن کیف‌پول و از بسیاری مسائل مرتبط آگاه باشد.

۴-۲-۳- حاکمیت

این بخش بر اساس جنبه حاکمیتی شامل چالش‌های اساسی زیر است:

انتخاب پشتوانه مناسب: اهمیت انتخاب پشتوانه‌ی مناسب به اندازه‌ای است که در صورت انتخاب نادرست می‌تواند به‌طورکامل فرآیند تولید رمزارز ملی را مختل کند برای مثال می‌توان به شکست کشور ونزوئلا در حوزه رمزارز ملی اشاره کرد. رمزارز پترو در ونزوئلا با پشتوانه نفت تولیدی آن کشور برخلاف هیاهوی اولیه، موفقیتی درپی نداشته است. دلیل این امر این است که درهمین‌اواخر آمریکا در بسته تحریم‌های جدید ونزوئلا، این رمزارز را جای داده است و وزارت خزانه‌داری ایالات متحده اعلام کرده که پترو می‌تواند به منزله وابستگی با دولت ونزوئلا باشد که زیر تحریم‌های دولت آمریکا است و شهروندانی که وارد معاملات این رمزارز می‌شوند، ممکن است شامل تحریم‌ها شوند؛ بنابراین این کشور اقدام به ایجاد رمزارز ملی دیگری به نام Petro Oro کرده است که پشتوانه آن طلا است؛ بنابراین در طراحی باید پشتوانه رمزارز به‌درستی تعیین شود تا تحریم‌های بین‌المللی نتواند مانع از به‌کارگیری آن شود.

توافقات بین‌الملل: با توجه به مسائل سیاسی، کاربری

[1] در حالت کلی دو نوع شبکه زنجیره بلوکی خصوصی داریم. نوع نخست با قابلیت نوشتن و خواندن خصوصی است که توسط پروژه‌هایی مانند هایپرلجر فابریک انجام می‌شود. نوع دوم با قابلیت نوشتن اختصاصی و خواندن عمومی است که توسط رمزارزهایی مانند ریپل استفاده می‌شود. با توجه به این که اعمال سیاست‌های مالی در رمزارزهای ملی یکی از اهداف محوری است نوع دوم شبکه زنجیره بلوکی خصوصی به نظر مناسب برای به‌کارگیری در حوزه رمزارز ملی است.

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

رمزارز ملی در سطح بین‌المللی لازم است با ایجاد بستری مقدمات لازم برای تبدیل رمزارز بومی برای استفاده در تبادلات جهانی را با توافقات بین‌المللی و منطقه‌ای فراهم آورد؛ زیرا در حالت کلی امکان ایجاد رمزارز مشترک میان دو یا چند کشور با توجه به عدم اعتمادی که در میان کشورها حکم فرما است، وجود ندارد؛ بنابراین هرگونه اقدام عمده در این خصوص باید با مقدمات و پیش‌نیاز توافقات چندجانبه انجام گیرد. این چالش به‌خصوص در کشورهای اروپایی مطرح می‌شود. در سال ۱۹۹۹ این کشورها واحد پول مشترکی به‌نام یورو را معرفی کردند که تمام کشورهای عضو، این واحد پول را جایگزین پول‌های ملی خود کردند. برای مثال یکی از مسائلی که باعث کنارگذاشتن رمزارز ملی در کشور استونی شد، نبود قوانین در رابطه با استفاده از جایگزینی رمزارز ملی این کشورها به‌جای یورو بود.

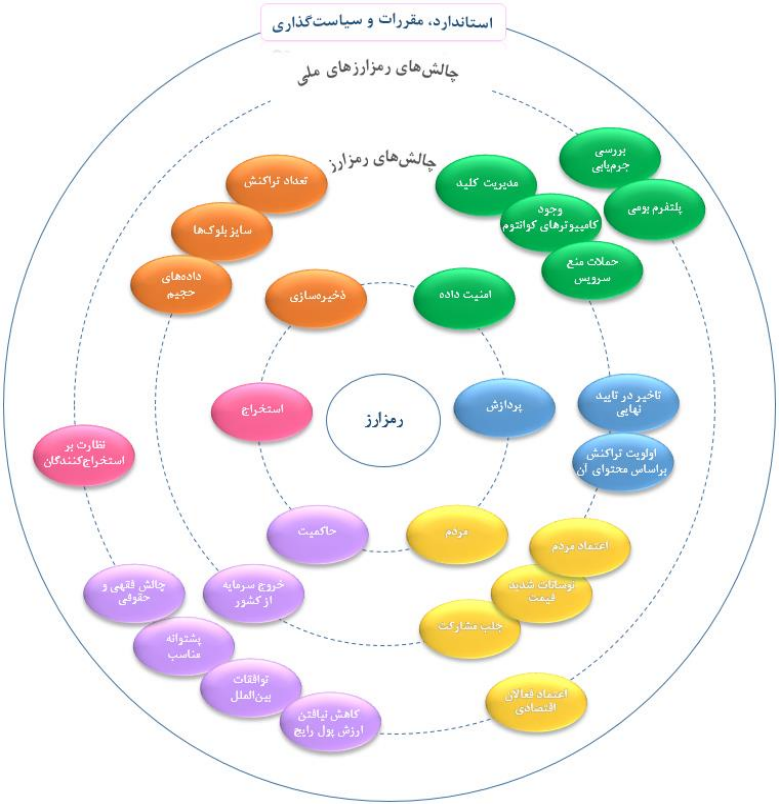
چالش فقهی و حقوقی: درمورد کشورهای مسلمانی چون ایران این چالش به‌طور جدی دنبال می‌شود. این مسأله که رمزارزها به‌طوراصولی مبنای شرعی دارند و یا خیر. برای آن‌که بتوان سازوکار مناسب و احکام فقهی در قبال این نوع پول اتخاذ کرد، مراکز و نهادهای فقهی در کشور می‌توانند با درنظرگرفتن ابعاد مختلف در اقتصاد کشور و شناخت دقیق احکام شرعی و فقهی متناسب با آن را تدوین کرده تا بتوان متناسب با احکام شرع و درنظر گرفتن اهداف نظام اقتصاد اسلامی، نحوه برخورد با آن را با اتخاذ قوانین و مقررات مناسب مشخص کرد.

کاهش نیافتن ارزش پول رایج: کاهش ارزش پول یکی از مسائل اقتصاد است. در یک نظام اقتصادی اسلامی این موضوع از اهمیت دوچندانی برخوردار خواهد بود. در این نظام به‌کارگیری ابزارهای پولی و اتخاذ تصمیمات و

سیاست‌های پولی در راستای اهداف کلان اقتصادی باید منطبق بر احکام فقهی باشد؛ از این‌رو عدم تحقیق و شناخت ماهیت رمزارز به‌عنوان پولی مجازی، موجب ناکارآمدی سیاست‌های پولی و اعتباری در اقتصاد کشور خواهد شد.

۵-۲-۳- مقررات حاکمیتی

قوانین و مقررات زیادی در این باره باید تدوین شود؛ از آن جمله می‌توان به قوانین تجارت الکترونیک، قوانین حمایت از داده، قوانین فناوری‌های موجود و مشابه آن‌ها در کشور اشاره کرد. همچنین نقش بازیگران هر بخش و وظیفه‌ای که به عهده دارند، نحوه احراز هویت استخراج‌کنندگان و سیاست‌های مرتبط با آن نیز در زمره اقداماتی است که در این خصوص باید تصمیم‌گیری شود.



(شکل-۶): تصویری جامع از چالش‌های رمزارز ملی

۴- نتیجه‌گیری

این مقاله، نقاط ضعف و چالش‌های رمزارزها را با تحلیلی سه‌جانبه از دیدگاه‌های فناورانه، محیطی و حاکمیتی توصیف می‌کند و رویکرد استفاده از آن‌ها را در برخی از کشورها معرفی می‌کند. این مقاله همچنین با ارائه تصویری جامع فرصت امکان‌سنجی را برای شناسایی راه‌کارهایی نوآورانه در استفاده از رمزارز در کشور فراهم می‌کند. همانطور که می‌دانیم، رمزارزها در بستر فناوری زنجیره بلوکی پیاده‌سازی می‌شوند و این فناوری در مرحله نوآوری و رشد از لحاظ کاربرد و پیشرفت قرار دارد؛ از این رو عمده چالش‌های رمزارزها وابسته به چالش‌های زنجیره بلوکی است.

۵- مراجع

[1]S. Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. https://bitcoin.org/bitcoin.pdf 2008.

[2]https://coinmarketcap.com/currencies/bitcoin

[3]I. Takashima. *Blockchain: The Ultimate Guide to The World of Blockchain Technology, Bitcoin, Ethereum, Cryptocurrency, Smart Contracts*. CreateSpace Independent Publishing Platform, 2017.

[4]F. Bunjaku1, O. Gjorgieva-Trajkovska, E. MitevaKacarski. "Cryptocurrencies–advantages and disadvantages." *Journal of Economics*, Vol 2, No. 1, 2017.

[5]Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *IEEE Computer Society*, pp.557–564, October 2017.

[6] S. Olnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” Government Information Quarterly, Vol. 34, No 3, pp 355-364, 2017.

[7] I. Amsyaret al. "The Challenge of Cryptocurrency in the Era of the Digital Revolution: A Review of Systematic Literature." Aptisi Transactions on Technopreneurship (ATT) Vol 2. No 2 , 2020.

[8]https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocurrencies

[9] O. Drozd, Y. Lazur, and R. Serbin. "Theoretical and legal perspective on certain types of legal liability in cryptocurrency relations." *Baltic Journal of Economic Studies*, Vol 3, No. 5, pp 221-228, 2018

[10] O. Jackson, "Japan’s separate rules for crypto could be the answer." *International Financial Law Review*, 2018.

[11] Y. Zhao, "Cryptocurrency Brings New Battles into the Currency Market." *Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)* 91, 2015.

[12] R. F. Décourt, U. W. Chohan, and M. L. Perugini. "Bitcoin Returns and The Monday Effect." *Horizontes Empresariales*, Vol 16, No. 2, 2017.

[13] D. Schaffner, "Policy-Based Control and Augmentation of Cryptocurrencies and Cryptocurrency Security." U.S. Patent Application 14/691,463, filed November 2015.

[14] U. W. Chohan, "Assessing the Differences in Bitcoin & Other Cryptocurrency Legality across National Jurisdictions.", Discussion Paper. University of New South Wales, 2017.

[15]https://cdn.crowdfundinsider.com/wp-content/uploads/08/2018/Middle-Africa-Briefing-EcoBank-Note-Digital-African-crypto-regulation-August-2018.pdf

[16]http://www.fsb.org/wpcontent/uploads/r_111017.pdf

[17] www.fsb.org/wp-content/uploads/P160718-1.pdf

[18]https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocurrencies.

[19] N. Elena, "Analysis of Cryptocurrency Risks and Methods of their Mitigation in Contemporary Market Conditions." Review of Business and Economics Studies, No. 3, pp. 65-78, 2018.

[20] D. K. C. LEE, “The cryptocurrency revolution and its impact.” Self-published, 2014.

[21]A. Loera. “Method of making, securing, and using a cryptocurrency wallet”, February 11 2014. US Patent App. 14/178,234.

[22] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks. "A brief survey of cryptocurrency systems." In Privacy, Security and Trust (PST), 2016 14th Annual Conference on, pp. 745-752. IEEE, 2016.

[23] R. Farell, “An analysis of the cryptocurrency industry”. available at repository.upenn.edu, 2015.

[24] J. Bucko, D. Pal'ová, and M. Vejacka. "Security and Trust in Cryptocurrencies." In Central European Conference in Finance and Economics, pp. 14-24. 2015.

[25] F.R. Batubara, J. Ubacht, and M. Janssen. "Challenges of blockchain technology adoption

[DOR: 20.1001.1.24763047.1399.9.1.6.9]

for e-government: a systematic literature review." In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, p. 76. ACM, 2019.

[26] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, ‘‘Current trends in sustainability of bitcoins and related blockchain technology,’’ Sustainability, Vol. 9, No. 12, p. 2214, 2017.

[27]C. Decker and R. Wattenhofer, ‘‘Information propagation in the bitcoin network,’’ in Proc. IEEE 13th Int. Conf. Peer-Peer Comput. (P2P), Trento, Italy, pp. 1–10, Sep 2013.

[28] M. Conti, C. Lal, S. Ruj et al., “A survey on security and privacy issues of bitcoin,” arXiv preprint arXiv:1706.00916, 2017.

[29]W. Shor, ‘‘Algorithms for quantum computation: Discrete logarithms and factoring,’’ in Proc. IEEE 35th Annu. Symp. Found. Comput. Sci., Santa Fe, NM, USA, pp. 124–134, Nov. 1994.

[30]https://www.ccn.com/cryptocurrency-exchange-etherdelta-hacked-in-dns-hijacking-scheme/

[31]https://www.cryptocompare.com/mining/#/equipment?f3=ASIC

[32]https://coinmarketcap.com/currencies/bitcoin/#charts.

[33]https://medium.com/@Swissonecapital/crypto-regulation-2019-summary-update-ea08c77bc3ff

مرجان بحرالعلوم تحصیلات خود را در مقطع کارشناسی‌ارشد مهندسی الکترونیک در دانشگاه صنعتی امیرکبیر در سال ۸۱ به اتمام رسانده است. از سال ۱۳۸۶ تاکنون عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات است و زمینه‌های پژوهشی مورد علاقه ایشان امنیت شبکه و سامانه‌ها، زنجیره بلوکی و رمزارزها است.

زهرا فردوسی هر سه مدرک کارشناسی - کارشناسی ارشد و دکتری را از دانشگاه صنعتی امیرکبیر رشته ریاضیات کاربردی گرایش تخصصی کد و رمز طی سال‌های ۲۰۰۹، ۲۰۱۱ و ۲۰۱۸ اخذ کرده است. زمینه‌های مورد علاقه ایشان که در حال حاضر در قالب تدریس و تحقیق و پژوهش به آنها می‌پردازد شامل حوزه‌های مختلف کاربرد نظریه کدگذاری و رمز (نظریه اطلاعات و امنیت داده) و ترکیبات است.