

## جنبه‌های حقوقی پرداخت با رمزارز در تجارت بین‌الملل

امین حقیقت

دانشجوی دکترای حقوق تجارت بین‌الملل و سرمایه‌گذاری خارجی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

aminhaghighatlaw@gmail.com

سعید حبیبیا (نویسنده مسئول)

استاد، گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

habiba@ut.ac.ir

### قابل انتشار در دوره ۲۵، شماره ۶۵ (بهار ۱۴۰۵) نشریه پژوهش‌های حقوقی

چکیده:

یکی از پرسش‌های نوین در عرصه تجارت بین‌الملل این است که آیا می‌توان انجام تعهد یکی از طرفین که اغلب به صورت پرداخت پول می‌باشد را در قالب «رمزارز» انجام داد؟ بدین معنا که برای مثال، به جای پرداخت از طریق ارز معتبر یا مورد توافق (مانند دلار یا یورو)، از پرداخت رمزارزی (مثل بیت‌کوین یا تتر و...) استفاده شود. پاسخ این پرسش، نمی‌تواند منفی باشد، اما در حال حاضر با چالش‌های متعدد و گاه جدی روبرو می‌باشد. از یک سو، با توجه به آزادی تجارت، اقتصاد بازار و آزادی شهروندان در سایه جهانی شدن تجارت، پرداخت از طریق رمز ارز نباید ممنوع باشد و از سوی دیگر، عدم امکان نظارت دولت، فقدان یک مرکز پاسخگو یا پشتیبان در سطح جهانی نسبت به رمزارزها، ابهام در ماهیت آنها و چالش‌های ایمنی و امنیتی و مسأله دشواری اثبات پرداخت یا عدم پرداخت از طریق رمزارز، در کنار مسایلی مانند بهره‌گیری مجرمانه از رمزارز برای پولشویی، تأمین مالی تروریسم و... امکان پرداخت از طریق رمز ارز را با چالش‌های جدی روبرو ساخته است. این مقاله، پس از بررسی این موضوعات و چالش‌ها، بر پایه مطالعات و با در نظر گرفتن واقعیتها و رویکرد دولتها، راهکارهای عملی در خصوص پرداخت با رمزارز در تجارت بین‌الملل ارائه می‌نماید. واژگان کلیدی: پرداخت، رمزارز، تجارت بین‌الملل، امنیت، چالش‌ها.

## مقدمه

دارایی‌های رمزی که عموماً با نام رمزارز Cryptocurrency شناخته می‌شوند، در بستر اینترنت و به این منظور توسعه یافته‌اند که بدون مداخله بانک یا بدون نظارت نهادهای حکومتی از شخصی به شخص دیگر منتقل می‌شوند.<sup>1</sup> دارایی‌های رمزی<sup>2</sup> (رمز دارایی‌ها) مفهوم بهتری از رمزارز می‌باشد، زیرا که وجه نقد یا ارز در حقوق موضوعه مفهوم مشخص دارد و رمزارزها تمام ویژگی‌های پول - ارز را نداشته یا گاه ویژگی‌های بیشتر و متفاوتی از پول دارند.

عدم تمرکز در مورد رمزارز بدین معناست که بانک مرکزی یا دولتی وجود ندارد که مقررات حاکم بر آنها را تعیین کند یا پشتوانه این نوع از دارایی‌ها باشد.<sup>3</sup> داشتن پشتوانه دولتی هرچند یک امتیاز می‌باشد، اما با این ایراد روبروست که مداخله، نظارت تعیین محدوده و به طور کلی مقررات‌گذاری از جانب دولت و بانک مرکزی را هم ایجاب و هم توجیه می‌کند.

رمزارزها چنین پشتوانه‌ای ندارند. ارزش‌گذاری آنها از معیارهای متفاوتی در مقایسه با ارزهای مرسوم تبعیت می‌کند. ارزش آنها تابع مقبولیت (گرایش) عمومی، اعتماد و شرایط بازار است. با این وصف، استفاده از آنها به عنوان ابزار پرداخت می‌تواند با مسایل حقوقی متعددی روبرو باشد که در ادامه برخی از آنها را بررسی می‌کنیم.

ماهیت وسیله پرداخت باید مشخص باشد. تقریباً هیچ قانونی ماهیت حقوقی و اقتصادی رمزارزها را تعیین نکرده و دیدگاه‌های متعدد و گاه متعارضی در این خصوص وجود دارد. تشبیه به پول یا ارز یا کالا یا نهادی جدید، از جمله این دیدگاهها است. پرسش این است که وقتی شخص، رمزارز را به عنوان ابزار پرداخت می‌پذیرد، آیا باید بداند که به چه عنوانی (با چه ماهیتی) آن را قبول می‌کند یا ماهیتی که متعهدله از رمزارز به عنوان وسیله پرداخت قصد می‌کند، امکان دارد با ماهیت واقعی (غالب) آن متفاوت باشد؟ در واقع، پرسش این است که آیا شناخت متعهدله از ماهیت رمزارز شرط قبول این وسیله برای پرداخت است یا همین که وی مقبولیت رمزارز را می‌بیند و آن را به عنوان ابزار پرداخت می‌پذیرد، کافی است؟

پاسخ دادن به این پرسش ساده نبوده و هر پاسخی امکان دارد با ایراداتی مواجه شود. در عین حال، با لحاظ قاعده العقود تابعه التصود، باید پذیرفت که وقتی شخص رمزارز را به عنوان وسیله پرداخت می‌پذیرد و چنین امری در رابطه طرفین قصد می‌شود، برای اعتبار عقد و صحت شیوه پرداخت کفایت می‌کند. زیرا رمزارزها - با وجود نوسان متعارف یا ناشناخته در ارزش ریالی - دلاری آنها - به هر حال، ارزش مالی دارند.

از این حیث، باید تعامل یا پرداخت با رمزارز را به معامله‌ای تشبیه نمود که ثمن در آن وجه نقد نبوده، بلکه عین است. زیرا رمزارز خاصیتی دارد که در مورد پول قابل تحقق نیست و به همین دلیل باید حداقل از این جهت آن را با کالا(عین) قیاس نمود. خاصیت رمزارز این است که امکان دارد ارزش مالی آن در مدت کوتاهی به صفر برسد. چرا که برخی از رمزارزها با هدف بازاریابی عرضه می‌شوند و اگر توسط افراد یا شرکتهای مشهور یا صرافی‌های شناخته شده در حوزه معاملات رمزارز، پشتیبانی یا

<sup>1</sup> SELISTEANU, Citilin Cristian, The Bitcoin Currency - a New Instrument Used in Conducting Business? Diversity and Interdisciplinarity in Business Law, 2017, p. 218. Chohan, Usman W., Cryptocurrencies: A Brief Thematic Review (January 8, 2022). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3024330>

<sup>2</sup> Crypto-assets

<sup>3</sup> Morton, D. Towne, The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy, Loyola University Chicago International Law Review, Vol. 16, 2020, p. 130.

تبلیغ نشوند، به سرعت امکان دارد از بازار رمزارز محو شوند.

در فرضی که رمزارزی از این نوع (شت کوین)<sup>۴</sup> به عنوان وسیله پرداخت قبول می‌شود و در فاصله تاریخ عقد تا تاریخ پرداخت، ارزش آن به صفر می‌رسد، باید قایل به انفساخ عقد بود؛ مانند حالتی که مبیع در زمان عقد قابل تسلیم بوده، اما در آجل، غیر قابل تسلیم می‌شود. بدیهی است که اگر بعد از تسلیم، ارزش رمزارز به صفر برسد، تاثیری در اعتبار معامله نخواهد داشت.

در این مقاله ضمن پنج گفتار به شرح زیر به بررسی جنبه‌های حقوقی پرداخت با رمزارز در تجارت بین‌الملل خواهیم پرداخت:

گفتار اول. نقش دولتها و موضوع آزادی شهروندان در پرداخت از طریق رمزارز

گفتار دوم. اعتبار قرارداد و ادله اثبات معاملات و تعاملات در بستر بلاک‌چین

گفتار سوم. چالش‌های بهره‌گیری از رمزارز به عنوان وسیله پرداخت

گفتار چهارم. ساز و کار نظارت بر رمزارز به عنوان وسیله پرداخت

گفتار پنجم. جرایم و تخلفات مرتبط با حوزه پرداخت با رمزارز

در پایان نیز نتایج و راهکارهای عملی و اجرایی ارائه می‌گردد.

## ۱. نقش دولتها و موضوع آزادی شهروندان در پرداخت از طریق رمزارز

تاثیر راهبردی دولتها در وسیله پرداخت بودن رمزارز و رابطه رمزارز و آزادی شهروندان، دو موضوعی است که در این گفتار، به ترتیب مورد بررسی قرار می‌گیرد.

### ۱-۱. تاثیر راهبردی دولتها در وسیله پرداخت بودن رمزارز

بسیاری از کشورها، تاکنون موضع خود را در مورد اعتبار یا بی‌اعتباری معاملات منعقد در بستر زنجیره بلوکی (بلاک‌چین) و نیز استفاده از این فناوری (قالب رمزارز برای پرداخت) مشخص نکرده‌اند.

با این وصف باید بررسی کرد که رویکرد کشورها چه تاثیری در اعتبار یا بی‌اعتباری پرداخت از طریق رمزارز خواهد داشت. در عین حال، باید قبول کرد که در وضعیت فعلی (سکوت دولتها)، با توجه به اصل صحت (ماده ۲۲۳ قانون مدنی) و نیز اصل لزوم (مواد ۱۰ و ۲۱۹ ق.م)، اصل بر اعتبار معاملات و پرداختهای مبتنی بر رمزارز می‌باشد.

رویکرد احتمالی اول، تایید اعتبار رمزارزها و پذیرش آنها به عنوان وسیله پرداخت می‌باشد. در این صورت، برخی از مسایل حقوقی و اقتصادی مرتبط با رمزارز با اعمال حاکمیت از جانب دولت تداخل پیدا خواهد کرد. زیرا دولت حداقل مجبور به تدوین قواعد نظارتی بر رمزارزها خواهد بود. قواعدی که به جهت عدم تمرکز در سازوکار بلاک‌چین، معلوم نیست که تا چه میزان قابل اجرا، قابل مدیریت یا اساساً از جانب بازیگران عرصه رمزارز قابل قبول و تحمل باشد.

حداقل کاری که در رویکرد اول باید از جانب دولتها انجام گیرد، ارائه رهنمودها، آموزش و احتیاطهای لازم برای کاربران به صورت یکنواخت (متحدالشکل) می‌باشد. چیزی که در حال حاضر وجود ندارد و همین امر، کاربران غیرحرفه‌ای در حوزه رمزارز را

<sup>4</sup> Shitcoin See: Hazar, H. B. 2020. Anonymity in Cryptocurrencies. In: Bilgin, M.H., Danis, H. & Demir E. (eds.), Eurasian Economic Perspectives, Eurasian Studies in Business and Economics, Vol. 14 (1), Springer, pp. 171-178.

با مشکلات عدیده‌ای مانند از دست دادن دارایی، عدم ذخیره اطلاعات ضروری و ناتوانی در اثبات تقلبها و زیان‌های وارده، روبرو ساخته است. حال آنکه دولت می‌تواند از طریق صرافی‌ها و کانال‌های مرتبط با معاملات رمزارز، رهنمودهای لازم را به شهروندان ارائه نموده و سوءاستفاده از بلاک‌چین را به حداقل ممکن برساند.

رویکرد دوم، تصریح به بی‌اعتباری رمزارز و هرگونه معامله و تراکنش در این حوزه می‌باشد. در صورت اتخاذ این رویکرد، دولت بر این امر قایل خواهد بود که چون رمزارز و به طور کلی سامانه‌های مبتنی بر بلاک‌چین را به رسمیت نمی‌شناسد، لذا هرگونه دریافت، پرداخت و تراکنش نیز در این فضا ممنوع است. اتخاذ این رویکرد، در بادی امر ساده به نظر می‌رسد، اما صرف اتخاذ آن، مسایل و چالش‌های متعددی در پی دارد.

اولین پرسش این خواهد بود که چرا دولت، رمزارز را به رسمیت نمی‌شناسد؟ پاسخ احتمالاً این خواهد بود که در حال حاضر، امکان نظارت بر آن را نداشته و به نوعی آن را رقیب پول سنتی و تحت سلطه و اختیار خود قلمداد می‌کند. این پاسخ، خود موجب طرح پرسش‌های دیگری می‌شود: آیا دولت امکان نظارت ندارد؟ آیا حتی با فرض ناتوانی دولت از نظارت، می‌توان روبروی عرف و رسم بازرگانی در خصوص شناسایی و اعتبار بخشی به رمزارز ایستاد؟ پاسخ به این پرسش‌ها و چالش‌های مرتبط دیگر، از موضوعات مورد طرح در این مقاله خواهد بود.

## ۲-۱. رابطه رمزارز و آزادی شهروندان

جنبش وال استریت یکی از نمونه‌های منفعت‌طلبی دولت‌ها در ترجیح منافع خود بر منافع مردم بود. اما در دنیای امروز این تنها نمونه از خودسری دولتها در ترجیح منافع خود بر جامعه نیست. محدودیت‌های مالی تحمیل شده به سازمان ویکی لیکس نمونه دیگری از محدودیت غیرقانونی و خودسرانه اعمال شده بر آزادی‌های فردی و قراردادی افراد است.

حامیان ویکی لیکس معتقدند که اگر افراد ضعیف، دارای قدرت فاش کردن شواهد مربوط به رفتارهای غیراخلاقی به صورت ناشناس باشند، در این صورت مؤسسات قدرتمند، دارای احساس مسئولیت بیشتری خواهند بود. در این بین، منتقدان ویکی لیکس معتقدند که این کار امنیت ملی و روابط بین‌المللی را تهدید می‌کند و معمولاً اینکه کدام کشور مورد هدف این افشاگری‌ها قرار گیرد (مثلاً آمریکا نه روسیه) ناعادلانه انتخاب می‌شود. در نتیجه این اختلاف نظر، در سال ۲۰۱۰ چندین کمپانی پرداخت‌کننده بزرگ جهان از جمله ویزا<sup>۵</sup>، مستر کارت<sup>۶</sup>، بانک آمریکا<sup>۷</sup>، پی پال<sup>۸</sup> و وسترن یونین<sup>۹</sup> ترتیبی دادند که مردم نتوانند از شبکه‌های پرداخت آنها به ویکی لیکس کمک کنند.

این قضیه ضربه محکمی به ویکی لیکس که یک سازمان غیرانتفاعی است و برای پابرجا ماندن به کمک‌های مردمی نیاز دارد، وارد کرد. چنین انسداد مالی هیچ پایه و اساس قانونی نداشت و ویکی لیکس به هیچ‌گونه جرمی متهم یا محکوم نشده بود. به نظر می‌رسد این انسداد کاملاً دل‌بخواه و مستبدانه بود. اما همین کمپانی‌ها هرگز لازم ندیدند که کمک‌های مردمی به

<sup>5</sup> VISA.

<sup>6</sup> MasterCard.

<sup>7</sup> Bank of America.

<sup>8</sup> PayPal.

<sup>9</sup> Western Union.

گروه‌های ستیزه‌جو مانند کو کلاکس کلن<sup>۱۰</sup> را مسدود کنند. حتی منتقدان ویکی‌لیکس علی‌رغم میل باطنی خود به ناچار پذیرفتند که این انسداد مالی الگوی خطرناکی برای آزادی پولی به‌جا می‌گذارد.<sup>۱۱</sup>

با اختراع بیت‌کوین اولین قدم در راه احیای آزادی‌های فردی بشر که همان استقلال اقتصادی بود، محقق شد. برای اولین بار در جهان ارزی به وجود آمد که پشتوانه آن نه قدرت دولتها بلکه حمایت ملتها بود. این ارز قادر بود تسلط دولتها را بر اموال و اراده مردم تا حدود زیادی کاهش داده و قدرت اقتصادی آنان را به چالش بکشد. اما فارغ از مشکلات فنی که لازم بود در ادامه مسیر مرتفع شود، این سیستم پاسخگوی تمام نیازهای مالی جامعه خصوصاً در پرداخت‌های خرد نبود. پرداختهای کلان اصولاً فیما بین دولتها، بانکها و شرکتهای بزرگ انجام می‌گیرد. اما مردم عادی برای انجام تعهدات مالی خود در قرارداد های خصوصی نیاز به یک سیستم مالی مناسب برای پرداختهای خردشان داشتند.

از یک سو امکان تامین استقلال اقتصادی افراد توسط رمزارزها<sup>۱۲</sup> و از سوی دیگر افزایش عدم اعتماد جوامع به دولت‌ها برای مدیریت پول و اموال، موجب بالاگرفتن تقاضاها برای اجتناب از تکیه بر سیستم‌های دولتی شد. مهندسين علوم کامپیوتر با بهره‌گیری از تکنولوژی پشتوانه رمزارزها، تلاش زیادی را برای تامین استقلال افراد در سایر موضوعات جامعه بشری نمودند. یکی از مهم‌ترین تلاش‌ها، در زمینه تامین آزادی حقوقی و قراردادی شکل گرفت. نتیجه این تلاش‌ها فراهم کردن بستری برای اجرای خودکار قراردادهای می‌باشد.<sup>۱۳</sup>

بدین‌گونه، رمز ارز و پرداخت از این طریق به یک نقطه تلاقی و گاه تداخل میان حقوق و منافع شهروندان از یک طرف و دولت از طرف دیگر، بدل گردید. در این میان، قدرت دولتها و توان تصمیم‌گیری آنها در سطح بین‌المللی، تاکنون بر حقوق ادعایی شهروندان، برتری داشته و مانع از بهره‌گیری از رمزارزها، به ویژه در پرداختهای کلان در سطح بین‌المللی شده است.

## ۲. اعتبار قرارداد و ادله اثبات معاملات و تعاملات در بستر بلاک‌چین

به لحاظ حقوقی، اعتبار قراردادهایی که با استفاده از فناوری بلاک‌چین منعقد می‌شود، محل بحث است. برای مثال، پرسش این است که اولاً: آیا اطلاعاتی که در زنجیره بلوکی ذخیره می‌شود، می‌تواند مبین مالکیت واقعی باشد؟ ثانیاً: برفرض که چنین باشد، چه شخصی مالک است و چگونه می‌تواند مالکیت خود یا اعمال حقوقی انجام شده، مانند پرداخت از این طریق را اثبات نماید؟

### ۲-۱. اعتبار قرارداد در بستر بلاک‌چین

<sup>10</sup> Ku Klux Klan- KKK.

<sup>11</sup> امیری، سمانه، ۱۳۹۷، آیا نسبت به آینده بیت‌کوین بدبین یا از آن متنفر هستید، برگرفته از لینک < /https:// arzdigital.com/hate-bitcoin-this-might-change-your-mind >

<sup>12</sup> Cryptocurrency.

<sup>13</sup> رجوع کنید: خرمی، یاسر، بررسی اعتبار حقوقی قرارداد هوشمند در بستر فناوری زنجیره بلوکی از منظر حقوق ایران، به راهنمایی دکتر پرویز ساورایی، پایان‌نامه کارشناسی ارشد حقوق خصوصی، دانشکده حقوق دانشگاه شهید بهشتی، شهریور ۱۳۹۸، صص ۱۱-۱۲.

قانون نمونه آنسیترال درباره سوابق الکترونیکی قابل انتقال (آنسیترال ۲۰۱۷)<sup>۱۴</sup> سعی کرده که برابری کارکرد<sup>۱۵</sup> را در مورد سوابق و اسناد تولید شده در بستر بلاک‌چین از قبیل بارنامه، راهنما، سفته و قبش‌های انباری که در فضای الکترونیکی رمزدار تولید شده یا قابل تولید هستند، شناسایی کند. با این حال، چنین مقرره‌هایی و نیز قانون نمونه تجارت الکترونیکی (آنسیترال ۱۹۹۶) و قانون نمونه امضاهای الکترونیکی (آنسیترال ۲۰۰۱) تا زمانی که به عنوان قانون داخلی تصویب نشوند، نمی‌توانند به عنوان بخشی از حقوق داخلی برای حل و فصل اختلافات و سایر مسایل حقوقی مرتبط با رمزارز و بستر بلاک‌چین به کار گرفته شوند. در حقوق فرانسه، به موجب ماده ۱-۱۳۱۶ قانون مدنی، ارزش اثباتی نوشته الکترونیکی با نوشته کاغذی برابر است؛ البته به شرطی که بتوان هویت صادرکننده آن را تشخیص داد و تولید و ذخیره آن به نحوی باشد که تمامیت آن تضمین شود. در ایران، به تصریح ماده ۶ قانون تجارت الکترونیکی (مصوب ۱۳۸۲)، «هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده پیام» در حکم نوشته است...». همچنین به موجب ماده ۱۲ همین قانون، «اسناد و ادله اثبات دعوی ممکن است به صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی «داده‌پیام» را صرفاً به دلیل شکل و قالب آن رد کرد».

به موجب ماده ۶۵۵ قانون آیین دادرسی کیفری (مصوب ۱۳۹۲)، «در هر مورد که به موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رای، امضاء، اثر انگشت، ابلاغ اوراق قضائی، نشانی و مانند آن لازم باشد، صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است.

تبصره ۱- در کلیه مراحل تحقیق و رسیدگی حقوقی و کیفری و ارائه خدمات الکترونیک قضائی، نمی‌توان صرفاً به لحاظ شکل یا نحوه تبادل اطلاعات الکترونیکی از اعتبار بخشیدن به محتوا و آثار قانونی آن خودداری نمود...». از این‌رو، اعتبار معاملات انجام شده در بستر بلاک‌چین، مورد تأیید مقنن می‌باشد و تاکنون نص دیگری بین این شیوه برای تجارت و کسب و کار الکترونیکی و شیوه‌های سنتی‌تر - از حیث اعتبار و بی‌اعتباری یا میزان اعتبار - قابل به تفکیک نشده است.

## ۲-۲. ادله اثبات معاملات و تعاملات در بستر بلاک‌چین

چالش ادله اثبات و به طور کلی نحوه و فرایند اثبات دعوا در حوزه رمزارز به این جهت پیچیده است که شبکه بلاک‌چین سامانه‌ای غیرمتمرکز می‌باشد. در این سامانه شخص می‌تواند با هویت ساختگی وارد شود و عملاً سازمان مستقل یا به عبارت بهتر، هیچ سازمانی بر بستر بلاک‌چین نظارت ندارد.

در چنین فضایی برای اثبات انعقاد قرارداد یا تحقق رابطه غیرقراردادی، ذینفع باید انتساب حساب کاربری شبکه را به طرف دعوا اثبات کند. ماده ۱۸ قانون تجارت الکترونیکی فرایند مبهم و نسبتاً قدیمی شده‌ای را برای انتساب داده‌پیام مشخص کرده و مقرر داشته است: «در موارد زیر «داده پیام» منسوب به اصل‌ساز است:

<sup>14</sup> UNCITRAL Model Law on Electronic Transferable Records ("MLETR", UNCITRAL 2017).

<sup>15</sup> Functional equivalence

الف. اگر توسط اصل ساز و یا به وسیله شخصی ارسال شده باشد که از جانب اصل ساز مجاز به این کار بوده است.

ب. اگر به وسیله سیستم اطلاعاتی برنامه‌ریزی شده یا تصدی خودکار از جانب اصل ساز ارسال شود».

قانون تجارت الکترونیکی ایران در مواد ۱۸ تا ۲۲ که برداشت شده از ماده ۱۳ قانون نمونه تجارت الکترونیکی آنسیترال می‌باشد، بدون ارایه تعریف، به موضوع انتساب داده‌پیام پرداخته و ضوابطی را برای تشخیص شرایط انتساب داده‌پیام به اصل ساز، معین نموده است، مانند شرایطی که طبق ماده ۱۹ قانون ایران علی‌رغم ارسال داده‌پیام توسط اصل ساز و همچنین اصل عدم انتساب داده‌پیام، داده منتسب به او فرض می‌شود و در این راستا از مفاهیمی استفاده نموده که یا در خصوص مفهوم دقیق یا در مورد کاربرد آن‌ها در این زمینه ابهاماتی وجود دارد.<sup>۱۶</sup>

در بستر بلاک‌چین، اجرای ضوابط مقرر در مواد ۱۸ تا ۲۲ قانون تجارت الکترونیکی برای احراز انتساب، حداقل در مقام عمل و اثبات، چندان ساده نیست. زیرا برخلاف پیام‌های که بر مثال در بستر واتساپ یا تلگرام یا پیام‌رسان‌های داخلی مانند بله و ایتا یا همراه اول انجام می‌گیرد، بستر بلاک‌چین تحت مالکیت یا کنترل یا نظارت هیچ دولتی نیست؛ به همین دلیل، اثبات پیام‌های رد و بدل شده در آن، اغلب بر مبنای مدارکی انجام می‌شود که مدعی (اغلب زیان‌دیده) ارایه می‌کند و راستی‌آزمایی این مدارک و مستندات - که اغلب روگرفتی از منشأ اصلی الکترونیکی است - امری دشوار، فنی و در بیشتر موارد، نیازمند بهره‌گیری از کارشناس توانمند می‌باشد.

به هر حال، مهمترین موضوع این است که به هنگام گشایش حساب کاربری توسط شخصی که برای اولین بار وارد فضای بلاک‌چین می‌شود، باید دقت کافی به عمل آید. در غیر این صورت، شخصی که هویت واقعی ندارد، می‌تواند در سامانه عضو شده، صاحب حساب کاربری و کیف پول مجازی گردیده و بتواند حسب مورد معاملات خرد و کلان انجام دهد. هویت غیرواقعی این خطر را برای سایر کاربران ایجاد می‌کند که از دارایی یا اطلاعات مالی آنها سوء استفاده شده یا اگر معامله‌ای انجام گرفت، اثبات آن غیرممکن یا حتی برفرض اثبات، بی‌فایده شود. به ویژه که هر شخص از هر کشوری می‌تواند با استفاده از صرافی‌های مجازی اقدام به ثبت نام کاربری و انجام معامله در بستر بلاک‌چین نماید.

برای حل مشکل یا حداقل برای کاستن از چالش بی‌هویتی یا گمنامی در بستر بلاک‌چین، سامانه‌ها و صرافی‌های دیجیتال اقدام به ارایه نرم‌افزارها و سیستم‌های چندمرحله‌ای برای احراز هویت کاربران نموده‌اند. با این وجود، چون هویت کاربر در هر تراکنشی مجدداً احراز نمی‌گردد، این خطر وجود دارد که ابتدا حساب کاربری توسط یک شخص واقعی در فضای بلاک‌چین ایجاد و هویت وی واقعا احراز شود؛ سپس همان نام کاربری در اختیار شخص یا اشخاص دیگری قرار گیرد.

این واگذاری یا اعطای نمایندگی می‌تواند در قبال دریافت وجه یا بلاعوض، دانسته یا ندانسته انجام گیرد. در چنین فرضی، زیان‌دیده با کاربری روبرو خواهد شد که اطلاعی از تراکنش او و معاملاتی که با نام کاربری وی انجام شده، ندارد؛ چه بسا شخص مذکور در کشوری بسیار دورتر از کشور محل ورود زیان، اقامت داشته باشد و برفرض شناسایی و محکومیت، به احتمال زیاد،

<sup>۱۶</sup> رجوع کنید: فیضی چکاب، غلام نبی و مه‌افروز کلانتر هرمزی، جنبه‌های حقوقی انتساب داده پیام در ارتباطات الکترونیک، مجله پژوهش حقوق خصوصی - دانشگاه علامه طباطبائی، دوره ۶، شماره ۲۳، تیر ۱۳۹۷، ص ۱۴۱.

فاقد توان کافی برای جبران خسارت می‌باشد. به علاوه، اجرای احکام قضایی داخلی در کشورهای دیگر، نیز چالش بزرگ دیگری است که به طور خاص، در مورد کشورمان مطرح می‌باشد.

در روند جمع‌آوری ادله اثبات، دستورهای مقام قضایی و جزئیاتی که در قرار کارشناسی ذکر می‌کند، از اهمیت زیادی برخوردارند. برای مثال در یک پرونده<sup>۱۷</sup> افراد ناشناسی اقدام به انعقاد قرارداد و سرقت از حساب طرف مقابل کردند. دادگاه عالی سنگاپور دستورهایی را برای جلوگیری از اتلاف دارایی‌های رمزنگاری شده، همراه با دستورات افشای جانبی برای کمک به ردیابی رمز ارزهای سرقت شده و شناسایی طرف‌های مسئول صادر کرد. سی ال ام اقدامی را برای ردیابی و بازیابی ۱۰۹/۸۳ بیت کوین و ۱۴۸۷/۵۴ اتریوم که ظاهراً توسط افراد ناشناس مورد سوء استفاده قرار گرفته بود، آغاز کرد. بخش از دارایی‌های دزدیده شده را می‌توان در کیف پول‌های دیجیتالی که توسط صرافی‌های ارز دیجیتال با عملیات در سنگاپور کنترل می‌شد، ردیابی کرد. سی ال ام به دنبال یک حکم مسدودی در سراسر جهان بود که از دفع دارایی‌های آن کیف پول‌های دیجیتال که ۷/۱ میلیون بود، حفاظت کند.<sup>۱۸</sup>

در این پرونده دادگاه عالی سنگاپور دریافت که هیچ مشکلی در مورد صدور حکم علیه افراد ناشناس براساس رویه قضایی وجود ندارد. لذا حکمی برای بازیابی دارایی‌های سی ال ام که توسط افراد ناشناس سوء استفاده و سرقت شده بود را صادر کرد.<sup>۱۹</sup> در خصوص چگونگی اثبات ادعاها در دعاوی مربوط به رمز ارزها می‌توان گفت که باید بین ادعاهای مربوط به شبکه بلاک‌چین و رمز ارزها و ادعاهای مربوط به خارج شبکه مزبور و عالم واقع قائل به تفکیک شد. بدین معنا که ادعاهای مربوط به شبکه بلاک‌چین و سیستم رمز ارزها با توجه به سیستم رمزنگاری شده و نگهداری معاملات در دفتر کل توزیع شده با مشکل همراه نیست. بلکه کافی است مدعی به دفتر کل مزبور استناد کند و مقام قضایی با مشاهده دفتر مذکور صحت یا عدم صحت ادعای مدعی را احراز می‌کند. اما در خصوص ادعاهای مربوط به خارج از شبکه و عالم واقعی باید اظهار داشت که در خصوص این ادعاها مدعی بایستی به ادله اثباتی استناد کند که در دعاوی عادی به آن استناد می‌شود. مانند شهادت شهود، اسناد و...<sup>۲۰</sup>

### ۳. چالش‌های بهره‌گیری از رمز ارز به عنوان وسیله پرداخت

در مورد اینکه رمز ارزها می‌توانند وسیله پرداخت باشند، تردیدهای جدی وجود دارد. این چالش‌ها را می‌توان به شرح زیر خلاصه کرد:

<sup>17</sup> CLM v CLN [2022] SGHC 46.

<sup>18</sup> CLM v. CLN and others [2022], Singapore high court (SGHC).

<sup>19</sup> . Utasy Clark, Andrea, Cryptocurrency disputes increasingly referred to arbitration, with unique issues arising, 2022 September 27, p. 12

<https://www.pinsentmasons.com/out-law/analysis/cryptocurrency-disputes-increasingly-referred-to-arbitration-with-unique-issues-arising>

رجوع کنید: شعبانی، علی، آسیب‌شناسی بهره‌گیری از رمز ارزها در حوزه تجارت بین‌الملل از منظر اصول امنیت و شفافیت، پایان‌نامه کارشناسی ارشد رشته حقوق تجارت بین‌الملل، به راهنمایی دکتر مصطفی‌السان، دانشکده حقوق دانشگاه شهید بهشتی، تابستان ۱۴۰۲، صص ۸۷-۸۶.

<sup>۲۰</sup> شعبانی، پیشین، ص ۸۹.

### ۳-۱. محدود بودن ظرفیت و کارایی و مقبولیت رمزارز

یکی از ویژگی‌های پول، آزادی تجارت با آن، کاهش تشریفات و عدم محدودیت در نقل و انتقال است. در مورد رمزارزها، محدودیتهایی به لحاظ فنی و عملیاتی وجود دارد. برای مثال، شبکه بیت‌کوین تراکنش‌های محدودی را در هر ثانیه (۷ مورد) پشتیبانی می‌کند. این محدودیت در مورد سایر رمزارزها هم وجود دارد. به طوری که توان اتریوم دوبرابر بیت‌کوین است. در حالی که سامانه‌های پرداخت الکترونیکی مانند ویزا ۵۶۰۰۰ تراکنش را در ثانیه می‌توانند پردازش کنند. هرچند با افزایش استفاده از رمزارزها، میزان پشتیبانی اتریوم در سال ۲۰۱۷ به ۵۰۰ تراکنش در ثانیه رسید؛ اما به هر حال این محدودیت وجود دارد. محدودیت دیگر در پرداخت از طریق رمزارز، وجود محدودیت و سقف در استخراج برخی از رمزارزها، به طور خاص بیت‌کوین می‌باشد. به این معنا که بیت‌کوین از حیث تعداد و میزان نحوه استخراج، محدود می‌باشد؛ در حالی که چنین محدودیتی در مورد پول کاغذی و پرداخت‌های الکترونیکی با پایه پولی کاغذی وجود ندارد.

یکی دیگر از چالش‌های جدی در مورد رمزارزها، فقدان اجماع بین المللی در خصوص اصل پذیرش یا عدم پذیرش آنها و به طور کلی نحوه رفتار و برخورد با این پدیده نوین است. در واقع، هیچ توافق جهانی در مورد نحوه دسته بندی، تعیین ماهیت و مقررات گذاری برای ارزهای دیجیتال وجود ندارد. این امر می‌تواند برای کسب‌وکارهایی که قصد دارند در تجارت بین‌المللی از این نوع وسیله برای پرداخت بهره ببرند، نوعی عدم اطمینان نسبت به این ابزار پرداخت ایجاد می‌کند.

### ۳-۲. مسأله کاربرپسندی

محدودیت دیگر، کاربرپسندی (User-friendly) شیوه‌های مبتنی بر رمزارز می‌باشد. فناوری بلاک‌چین برای بسیاری از مردم و نیز بازرگانان در سراسر جهان ناشناخته است. این فناوری به قدری پیچیده می‌باشد که اغلب تجار، ناچار از استفاده از دستیار فنی برای معاملات و پرداخت‌هایی که از این طریق انجام می‌شود، هستند. رویه قضایی کشورهای مختلف، از جمله ایران نشان می‌دهد که بسیاری از موارد سوء استفاده، توسط دستیار و از طریق اقداماتی همچون افشای اطلاعات، دسترسی غیرمجاز به اطلاعات شبکه تاجر و سوء استفاده از داده‌های شخصی از جانب دستیار روی می‌دهند.

### ۳-۳. چالش شیوه پرداخت و ملاحظات زیست‌محیطی

استخراج بیت‌کوین و تراکنش‌های مربوط به سایر رمزارزها، عمدتاً مستلزم مصرف برق می‌باشد. در سال ۲۰۱۴، رمزارز بیت‌کوین، به اندازه برق کل کشور ایرلند، نیروی برق مصرف کرده است.<sup>۲۱</sup> در تصویب‌نامه در خصوص استفاده از رمزارزها (مصوب ۱۳۹۸، ۰۵، ۰۶ با اصلاحات و الحاقات بعدی هیأت وزیران)، ضوابط و محدودیتهایی برای استفاده از برق جهت استخراج بیت‌کوین تعیین گردیده است. با وجود تغییرات زیاد بعدی در این تصویب‌نامه، به هر حال، در اینکه استخراج بیت‌کوین، به شدت بر مصرف برق تأثیر می‌گذارد، تردیدی وجود ندارد.

<sup>21</sup> O'Dwyer, K.J. and Malone, D. (2014) Bitcoin Mining and Its Energy Footprint. 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies, Limerick, 26-27 June 2014, 280-285.

در عین حال، استفاده از این فناوری برای پرداخت می‌تواند با کاهش استفاده از کاغذ، کاستن از مراجعات حضوری به بانک یا مراجع دیگر، موجب کاهش مصرف انرژی شود. به‌علاوه فناوری‌های مرتبط با رمزارز همواره در حال به‌روز شدن است و می‌توان برای کاهش مصرف برق در مقام استفاده از این فناوری‌ها، چاره‌اندیشی کرد.

#### ۳-۴. چالش امنیت

هرچند رمزارزهای مبتنی بر بلاک‌چین به جهت تمرکززدایی و ماهیت توزیعی خود بسیار امن‌تر از شیوه‌های سنتی پرداخت می‌باشند؛ اما نمی‌توان آنها را کاملاً امن تلقی کرد. عدم آشنایی عموم شهروندان با این فناوری در بسیاری از موارد مداخله اشخاص ثالث و فنی را می‌طلبد که امکان دارد از توان خود سوء استفاده کنند؛ بدون اینکه ردپایی بر جای گزارند. برای مثال، لجرهای سخت‌افزاری برای ذخیره رمزارز به کار گرفته می‌شوند. این لجرها دارای کدهای مشخصی برای تعیین شناسه و رمز ورود می‌باشند. به‌علاوه، بر فرض گم شدن یا خرابی یک لجر (کیف پول سخت‌افزاری) می‌توان با تعریف کلماتی که سابقاً به دارنده لجر داده شده، همان لجر را بازسازی کرد. حتی به لحاظ فنی غیرممکن نیست که برای مقدار مشخصی از رمزارز که متعلق به شخص معینی می‌باشد، همزمان بیش از یک لجر وجود داشته باشد. با این فرض، هر شخصی که کلمات بازشناسی لجر را در اختیار دارد؛ می‌توان آن را بازتولید کرده و با استفاده از یک لجر بازتولید شده (کپی) تمام رمزارزهای ذخیره شده در لجر اصلی را به لجر دیگری انتقال دهد که شناسایی مالک/دارنده آن، تقریباً غیرممکن است.

با این وصف، با ساخت / شبیه‌سازی یک لجر، لجر قبلی نیز می‌تواند کار کند. بدین معنا که برخلاف دیگر ساز و کارهای پرداخت الکترونیکی و کاغذی، یک وسیله پرداخت امکان دارد در آن واحد در اختیار بیش از یک نفر (یکی دارنده واقعی و دیگری دارنده با سوء نیت) بوده و از آن استفاده یا سوء استفاده شود.

به لحاظ فنی، بسیاری از مسایل ایمنی رمزارزها با استفاده از الگوریتم‌های دقیق‌تر پوشش داده شده و امکان نفوذ، هک و.. کاهش یافته است.<sup>۲۲</sup> اما این بدان معنا نیست که وقتی در مورد رمزارز برای پرداخت یا جابجایی و انتقال، اقدام به مداخله انسان یا ربات است، سوء استفاده غیرممکن باشد. در واقع ساز و کار رمزارز مانند یک هواپیماست. زمانی که در قلمرو بلک‌چین قرار دارد (مثل هواپیمایی که در آسمان است)، امن است؛ اما به هر حال فرایند رمزارزی، به ناچار باید زمانی به صورت فیزیکی درآید. مثل زمانی که خرید یا فروخته می‌شود یا از آن برای پرداخت دینی استفاده می‌شود. در این موارد، اقدامات فیزیکی مانند ورود به سامانه، احراز هویت دیجیتال، فرایند فیزیکی وارد کردن رمز یا رمزهای ورود برای انتقال از یک کیف پول الکترونیکی به کیف پول دیگر (اعم از سخت‌افزاری و نرم‌افزاری) و.. مورد نیاز است؛ دقیقاً در چنین مواقعی، احتمال سوء استفاده نیز به شدت افزایش می‌یابد.

#### ۳-۵. مساله تشخیص دادگاه دارای صلاحیت محلی در پرداخت از طریق رمزارز

<sup>22</sup> Buterin, Vitalik, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014; At: [https://ethereum.org/Ethereum\\_Whitepaper](https://ethereum.org/Ethereum_Whitepaper)

ضرورت دارد با تصویب قانون، تمهیداتی برای حمایت از مشتریان (به ویژه مصرف‌کنندگان) و کاربران رمزارز، از حیث تعیین دادگاه مناسب برای آنها (مانند دادگاه محل اقامت مصرف‌کننده)، اندیشیده شود.<sup>۲۳</sup> بدیهی است که توسعه صلاحیت محلی یا تفسیر قواعد این نوع از صلاحیت، باید به موجب قانون انجام گیرد. چراکه با توجه به «اصل قانونی بودن صلاحیت»، دولت یا هر نهاد دیگری اختیار دخالت و وضع قاعده در این حوزه را ندارد.

راهکار دوم بر قواعد موجود تکیه می‌کند. روابط طرفین یک رابطه مبتنی بر رمزارز در فضای مجازی در اکثر موارد، قالب «قرارداد» را دارد. با این وصف، می‌توان در دعوی مدنی ناشی از چنین قراردادهایی، از قاعده تعیین دادگاه (محلی) صالح در زمینه قرارداد استفاده کرد. این قاعده در ماده ۱۳ ق.آ.د.م مقرر شده است و به موجب آن، «در دعوی بازرگانی و دعوی راجع به اموال منقول که از عقود و قراردادهای ناشی شده باشد خواهان می‌تواند به دادگاهی رجوع کند که عقد یا قرارداد در حوزه آن واقع شده است یا تعهد می‌بایست در آنجا انجام شود».

برای تعیین مکان انعقاد یا اجرای قرارداد، از همان معیارهایی استفاده می‌شود که در قراردادهای الکترونیکی دیگر هم جاری است با تعیین مکان انعقاد یا اجرای قرارداد، در صورت بروز اختلاف به هر عنوان که از قرارداد مذکور ناشی شده باشد، هر یک از مشتری یا بانک مجازی می‌تواند علاوه بر محل اقامت خوانده،<sup>۲۴</sup> برای طرح دعوا به دادگاه محل انعقاد یا اجرای قرارداد مراجعه کند.

توافق طرفین بر صلاحیت دادگاه خاص، در ضمن قرارداد، قاعده فوق را از اثر می‌اندازد. در این خصوص می‌توان از محتوای آیین‌نامه بانک مجازی<sup>۲۵</sup> کمک گرفت.

#### ۴. ساز و کار نظارت بر رمزارز به عنوان وسیله پرداخت

استفاده از ساز و کار و سامانه‌های استاندارد در مورد تمام یا اکثر رمزارزهایی که می‌توانند به عنوان وسیله پرداخت به کار گرفته شوند، موضوعی است که نیاز به بررسی جدی دارد. اینکه هر شخصی می‌تواند رمزارز طراحی کرده و آن را در فضای مجازی (از طریق صرافی دیجیتال که امکان دارد، آن را هم خود راه‌اندازی کرده باشد)، به فروش رساند؛ اینکه بانک مرکزی بسیاری از کشورها، رمزارز را پشتیبانی نکرده، آن را به عنوان پول شناسایی نمی‌کنند و حتی شهروندان را از استفاده از این ساز و کار برای معامله و پرداخت برحذر می‌دارند، از جمله چالش‌های جدی در این حوزه محسوب می‌گردد.

پرسشی که مطرح می‌شود این است که با این فرض که رمزارز، به عنوان پول یا جایگزین یا معادل پول، توسط بانک مرکزی یا هر مرجع ذی‌صلاح دیگری، به رسمیت شناخته نشده باشد، آیا می‌توان آن را به عنوان وسیله پرداخت محسوب داشت؟

<sup>23</sup> Le, Yuxin. "Blockchain Application Risks and Solutions of International Commercial Arbitration in Chinese Mainland." *Foundation for Law and International Affairs Review*, vol. 2, no. 2, 2021, p. 95.

<sup>24</sup> بنابر رأی وحدت رویه ش ۹-۳/۲۶-۱۳۵۹، صلاحیت نسبی دادگاه محل اقامت خوانده با پیش‌بینی صلاحیت قراردادی نفی نشده و به عنوان قاعده عمومی (ماده ۱۱ ق.آ.د.م) اجرا می‌شود. ر. ک: مهاجری، علی، مبسوط در آیین دادرسی مدنی، جلد اول، چاپ دوم، انتشارات فکرسازان، تهران ۱۳۸۸، ص ۹۶.

<sup>25</sup> آیین‌نامه تأسیس و فعالیت بانک‌های مجازی، مصوب مورخ ۱۳۹۰/۲/۲۷ شورای پول و اعتبار.

در بند یک از تصویب‌نامه در خصوص استفاده از رمزارزها (مصوب ۱۳۹۸، ۰۵، ۰۶ با اصلاحات و الحاقات بعدی هیأت وزیران) تصریح شده: «استفاده از رمزارزها صرفاً با قبول مسئولیت خطرپذیری (ریسک) از سوی متعاملین صورت می‌گیرد و مشمول حمایت و ضمانت دولت و نظام بانکی نبوده و استفاده از آن در مبادلات داخل کشور مجاز نیست». در واقع، در این مصوبه، بانک مرکزی یا دولت، امکان استفاده از رمز ارز به عنوان وسیله پرداخت یا حتی معاملات رمزارز را غیرقانونی (ممنوع) اعلام نکرده، اما صریحاً اظهار داشته که رمزارزها، مورد حمایت دولت نبوده و از پشتیبانی دولت، برخوردار نیستند.

پرسش دیگر این است که آیا پرداخت با چنین ساز و کاری - که در برخی از کشورها، معادل قمار تلقی می‌شود - می‌تواند موجب سقوط تعهد به مفهومی شود که در قانون مدنی طرح گردیده و شرایط و ارکان آن ذکر شده است؟ بدیهی است که اگر رمزارز، از حمایت دولت برخوردار نباشد یا حداقل دولتها در مورد اعتبار آن سکوت نکنند، نمی‌توان آن را به عنوان ابزار پرداخت به رسمیت شناخت.

مسأله دیگر، نظارت بانک مرکزی و به طور کلی وجود یک ناظر بر این شیوه از پرداخت می‌باشد. وقتی بانک مرکزی، رمزارزها و پرداخت از طریق آنها را به رسمیت نمی‌شناسد، نظارتی نیز بر آنها نخواهد داشت.

در جلسه سی‌ام شورای عالی مبارزه با پولشویی (مورخ ۱۳۹۶/۱۰/۰۹) ۱۳۹۶، به کارگیری ابزار بیت کوین (Bit Coin) و سایر ارزهای مجازی در تمام مراکز پولی و مالی کشور ممنوع اعلام شد. از آنجایی که انواع ارزهای مجازی از این قابلیت برخوردار هستند که به ابزاری برای پولشویی و تامین مالی تروریسم و به طور کلی، جابه‌جایی منابع پولی مجرمان بدل شوند، حوزه نظارت بانک مرکزی برای پیشگیری از وقوع جرایم از طریق ارزهای مجازی، موضوع ممنوعیت به کارگیری ارزهای مجازی را به بانکها ابلاغ کرده است.

از این‌رو، با توجه به اهمیت موضوع، تمام شعب و واحدهای تابعه بانک‌ها و موسسات اعتباری و صرافی‌ها باید از انجام هر گونه خرید و فروش ارزهای مذکور و یا انجام هر گونه اقدامی که به تسهیل و یا ترویج ارزهای یاد شده بینجامد، به طور جد اجتناب کنند. همچنین لازم به ذکر است با متخلفین، برابر قوانین و مقررات مربوط برخورد خواهد شد. یکی دیگر از موانع نظارت بانک مرکزی بر رمزارزها، با ماهیت این نهاد نوپدید ارتباط می‌یابد. یک دیدگاه قوی این است که رمزارز، ماهیتاً «پول» (اعم از داخلی یا خارجی) نیست و همین امر موجب می‌شود تا خارج از حوزه نظارتی بانک مرکزی کشورها قرار گیرد.

## ۵. جرایم و تخلفات مرتبط با حوزه پرداخت با رمزارز

در حال حاضر، بسیاری از کشورها فاقد قانونگذاری در زمینه رمزارز هستند؛ همین امر می‌تواند زمینه سوء استفاده و بهره‌گیری از رمز ارز برای ارتکاب جرم را فراهم کند. برای مثال در سال ۲۰۱۷ بزهکاران فضای مجازی با گروگان گرفتن سامانه‌های رایانه‌ای، مالکین آنها را مجبور می‌کردند که پرداختهایی در قالب رمزارز به ایشان داشته باشند؛ سپس برای انتقال این رمزارزها به حسابهای بانکی و انجام پولشویی کوشیدند.

حذف واسطه، هرچند تجارت و پرداختهای بین‌المللی را تسریع می‌کند، اما با این خطر روبرو می‌باشد که به جهت امکان انتقال رمزارز از شخص به شخص (بدون وساطت و نظارت دولت یا بانک)، زمینه‌ای برای پولشویی و تأمین مالی تروریسم فراهم می‌آورد.<sup>۲۶</sup>

در سطح بین‌المللی نهادهایی چون کمیته بازل برای نظارت بانکی (The Basel Committee on banking supervision)، سازمان بین‌المللی کمیسیون اوراق بهادار برای نظارت بر اوراق بهادار در سطح بین‌المللی (The International Organization of Securities Commission (IOSCO)) و (Financial Action Task Force (FATF)) به عنوان نهاد بین‌المللی برای کنترل پولشویی و تأمین مالی تروریسم در حال فعالیت هستند؛ اما در کمال تعجب، حوزه فعالیت هیچ‌کدام از آنها - حداقل در وضعیت و شرایط فعلی - رمزارزها را شامل نمی‌شود.

گسترش جرایم مالی در سایه بهره‌گیری روزافزون از رمزارز، اینترپل را مجبور کرده که مرکز جرایم مالی و ضد فساد (Financial Crime and Anti-Corruption Centre (IFCACC)) را راه‌اندازی نماید.<sup>۲۷</sup>

جرم یا تخلف دیگر در حوزه رمزارزها، فرار مالیاتی است. دریافت مالیات برای تراکنش‌های تجاری بین‌المللی، امری مرسوم می‌باشد؛ اما در مورد پرداختهایی که از طریق رمزارز انجام می‌گیرد، دریافت مالیات با مشکلات عدیده‌ای روبرو می‌شود. اول اینکه، چگونه می‌توان نقل و انتقال رمزارز را ردیابی و رهگیری کرد؟ دوم اینکه، بفرض هم که بتوان بر چنین انتقالاتی نظارت کرد، ماهیت رمزارز - برای تعیین مالیات چیست؟ آیا باید قواعد مالیات بر پول اجرا شود یا مالیات بر سهام و اوراق بهادار بی‌نام؟<sup>۲۸</sup> پرسش‌هایی که تاکنون پاسخ روشنی به آنها داده نشده و به عنوان موارد ابهام در حوزه رمزارز و ماهیت آن باقی مانده‌اند.

## ۵. چالش مالیاتی در حوزه رمزارز

تردید در مورد امکان اخذ مالیات از دارایی‌هایی که تجسم عینی ندارند، امری مسبوق به سابقه می‌باشد. در یک پرونده،<sup>۲۹</sup> تردید در مورد اینکه نرم‌افزار «عین شخصی»<sup>۳۰</sup> محسوب می‌شود و در نتیجه مالیات بهره‌برداری بر آن تعلق می‌گیرد، دادگاه را مجبور به استدلال کرد: «شرکت خواهان ادعا کرده که نرم‌افزار صرفاً «دانش» یا «اندیشه» است و به همین دلیل، تجسم خارجی ندارد و نمی‌تواند مالیات به آن تعلق گیرد. با این توصیف، مخالفیم؛ نرم‌افزار موضوع بحث، اطلاعات صرف نیست، بلکه دانشی است که فرم فیزیکی و وجود خارجی دارد، فضای نوار، دیسکت یا حافظه سخت را اشغال می‌کند، امکان رویداد فیزیکی (مادی) را فراهم می‌سازد و می‌توان با حواس آن را درک کرد».<sup>۳۱</sup>

<sup>26</sup> Ligeti, K. & Simonato, M. (2017). Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU. UK: Bloomsbury Publishing.

<sup>27</sup> Juan Carlos Portilla, The Role of International Law to tackle the Dark Side of Cryptocurrencies April 26, 2022. At: <https://cilj.co.uk/2022/04/26/the-role-of-international-law-to-tackle-the-dark-side-of-cryptocurrencies/>

<sup>28</sup> Hoegner, S., (2015). The Law of Bitcoin. Bloomington : iUniverse.

<sup>29</sup> South Central Bell Telephone. Co. v. Sidney J. Barthelemy et al. [643. So.2d 1240 (La. 1994).

<sup>30</sup> Tangible personal property

<sup>31</sup> السان، مصطفی، حقوق فضای مجازی، چاپ بیست و دوم، انتشارات شهردانش، تهران ۱۴۰۲.

یکی از لوازم ضروری برای اخذ مالیات از فعالان بازار رمزارز، شناسایی هویت آن‌هاست. بدین منظور تمام صرافی‌های متمرکز رمزارز موظف به احراز هویت کاربران خود حداقل به هنگام ثبت نام یا اولین ورود می‌باشند که اغلب به صورت حضوری و گاه به صورت الکترونیکی و از طریق ارتباط زنده (به همراه مدرک احراز هویت) انجام می‌گیرد. اگر چنین چیزی در واقع محقق شود یا قابل تحقق باشد، محاسبه سود حاصل از فعالیت در این بازار و در نتیجه محاسبه مالیات متعلقه، تا حدود زیادی امکان‌پذیر است. البته بسیاری از معامله‌گران حرفه‌ای و تریدرها در صرافی‌ها و پلتفرم‌های غیرمتمرکز فعالیت می‌کنند. این امر، عملاً امکان شناسایی و تعیین مالیات برای ایشان را دشوار و یا غیرممکن می‌سازد. به علاوه، این فعالیت امکان دارد فراتر از مرزهای کشوری که در آن پول واقعی به ارز دیجیتال تبدیل می‌شود انجام گیرد. خود این امر مشکل‌ساز بوده و عملاً تعیین مالیات و اینکه چه کشوری به چه میزان می‌تواند مالیات بگیرد را دچار چالش جدی می‌سازد. نتیجه این وضعیت این است که بسیاری از کشورها در دریافت مالیات از تریدرهای حرفه‌ای دچار مشکل شوند. این امر به معنای فرارهای مالیاتی بزرگ و گاه غیرقابل ردیابی در این حوزه می‌باشد.

سختگیری مالیاتی برخی از کشورها در مقایسه با کشورهای دیگر که نظم خاصی در این مورد ندارند، موجب شده تا فعالیت صرافان دیجیتال و کریپتو به کشورهایی منتقل شود که در حوزه مالیات چندان سختگیر نیستند و یا دغدغه‌ای نسبت به خروج ارز واقعی (دلار و یورو و...) که ورود آن به بازار رمزارز ندارند؛ با این وصف، می‌توان ادعا کرد در شرایط فعلی هیچ کشوری نتوانسته بر تمام اجزای بازار رمزارز، مقررات مالیاتی وضع کرده یا بتواند آن را به مرحله اجرا گذارد.

## نتایج و راهکارها

تعیین ماهیت رمز ارز، موضوعی است که تاکنون، در محافل حقوقی و اقتصادی محل بحث بوده و این بحثها، به نتیجه واحد نینجامیده است. مسلماً، رمز ارز، پول به مفهوم سنتی آن نمی‌باشد. زیرا فاقد پشتوانه دولتی بوده و تعدد رمزارزها، نوسان شدید ارزش برخی از آنها، عدم قبول تمام یا برخی از رمزارزها در کشورهای مختلف، مانع از آن می‌شود که حداقل مؤلفه‌های پول را داشته باشد.

عدم امکان دستکاری ارزش رمزارزها توسط دولتها و نیز امکان بهره‌گیری از آنها برای دور زدن تحریم‌های اقتصادی از جمله مزایای رمزارز می‌باشد. در عین حال، فقدان ناظر دولتی یا حتی نبود نهاد بین‌المللی برای مدیریت، نظارت، سیاستگذاری و ارزش‌گذاری رمزارز، از جمله مسایلی است که در عین ایراد، می‌توانند از جنبه‌ای، مزیت رمزارز نیز به شمار آیند. با وجود تمام واقعیهایی که در این مقاله مورد بررسی قرار گرفت؛ باید پذیرفت که دوره گذار دیگری در راه است. زمانی، انسان از قرون وسطی به انقلاب صنعتی رسید و بعدها، فناوری‌های نوین ارتباطات، فاصله میان انسانها و کشورها را به حداقل ممکن رسانید. با این تفاوت، که در سابق، فاصله این تحولات بسیار زیاد بود و گاهی قرن‌ها طول می‌کشید؛ اما اکنون، سرعت تحولات در فناوری این امکان را فراهم ساخته که گذار از یک دوره به یک دوره دیگر، بسیار سریع باشد. آنقدر تند که گاهی، پیش از اینکه حکومت‌ها موضوع را درک کرده و سپس آن را منع کنند؛ آوازه و اثرش به تمام جهان رسیده و دولت، چاره‌ای جز پذیرش وضعیت و مدیریت آن ندارد.

در عین حال، به نظر می‌رسد که بستر بلاک‌چین یا هر بستر جدیدتری که در حوزه رمزارز در آینده معرفی می‌شود، باید تحت نظارت یک نهاد فراملی، بی‌طرف و به‌روز درآید. بدین‌سان، از چالش‌های موجود در این بستر، کاسته شده و اعتماد عمومی، امکان بهره‌گیری از این شیوه برای پرداختهای خرد و کلان داخلی و بین‌المللی را فراهم می‌سازد.

### فهرست منابع:

- آیین‌نامه تأسیس و فعالیت بانک‌های مجازی، مصوب مورخ ۱۳۹۰/۲/۲۷ شورای پول و اعتبار.
- خرمی، یاسر، بررسی اعتبار حقوقی قرارداد هوشمند در بستر فناوری زنجیره بلوکی از منظر حقوق ایران، به راهنمایی دکتر پرویز ساورایی، پایان‌نامه کارشناسی ارشد حقوق خصوصی، دانشکده حقوق دانشگاه شهید بهشتی، شهریور ۱۳۹۸.
- رأی وحدت رویه شماره ۹-۱۳۵۹/۳/۲۶.
- شعبانی، علی، آسیب‌شناسی بهره‌گیری از رمزارزها در حوزه تجارت بین‌الملل از منظر اصول امنیت و شفافیت، پایان‌نامه کارشناسی ارشد رشته حقوق تجارت بین‌الملل، به راهنمایی دکتر مصطفی‌السان، دانشکده حقوق دانشگاه شهید بهشتی، تابستان ۱۴۰۲.
- فیضی چکاب، غلام‌نبی و مه‌افروز کلانتر هرمزی، جنبه‌های حقوقی انتساب داده‌پیام در ارتباطات الکترونیک، مجله پژوهش حقوق خصوصی دانشگاه علامه طباطبائی، دوره ۶، شماره ۲۳، تیر ۱۳۹۷.
- مهاجرى، علی، مبسوط در آیین دادرسی مدنی، جلد اول، چاپ دوم، انتشارات فکرسازان، تهران ۱۳۸۸، ص ۹۶.
- Buterin, Vitalik, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014; At: [https://ethereum.org/Ethereum\\_Whitepaper](https://ethereum.org/Ethereum_Whitepaper)
- Chohan, Usman W., Cryptocurrencies: A Brief Thematic Review (January 8, 2022). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3024330>
- CLM v. CLN and others [2022], Singapore high court (SGHC).
- Eurasian Economic Perspectives, Eurasian Studies in Business and Economics, Vol. 14 (1), Springer, 2019.
- Hazar, H. B. 2020. Anonymity in Cryptocurrencies. In: Bilgin, M.H., Danis, H. & Demir E.
- Hoegner, S., (2015). The Law of Bitcoin. Bloomington : iUniverse.
- Juan Carlos Portilla, The Role of International Law to tackle the Dark Side of Cryptocurrencies April 26, 2022. At: <https://cilj.co.uk/2022/04/26/the-role-of-international-law-to-tackle-the-dark-side-of-cryptocurrencies/>
- Le, Yuxin. "Blockchain Application Risks and Solutions of International Commercial Arbitration in Chinese Mainland." Foundation for Law and International Affairs Review, vol. 2, no. 2, 2021.
- Ligeti, K. & Simonato, M. (2017). Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU. UK: Bloomsbury Publishing.

Morton, D. Towne, The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy, Loyola University Chicago International Law Review, Vol. 16, 2020.

O'Dwyer, K.J. and Malone, D. (2014) Bitcoin Mining and Its Energy Footprint. 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies, Limerick, 26-27 June 2014.

Selisteanu, Cătilin Cristian, The Bitcoin Currency - a New Instrument Used in Conducting Business? Diversity and Interdisciplinarity in Business Law, 2017. UNCITRAL Model Law on Electronic Transferable Records (UNCITRAL 2017).

Utasy Clark, Andrea, Cryptocurrency disputes increasingly referred to arbitration, with unique issues arising, September 27, 2022.