اندیشه‌های حقوق عمومی ـــــــــــــ سال دوازدهم، شماره دوم، پیاپی ۲۳، بهار و تابستان ۱۴۰۲، ص ۶۱ـ۸۲

نوع مقاله: ترویجی

واکاوی حقوقی کارکرد فناوری رمزارزها در برون‌رفت از بحران ناشی از تحریم‌های مالی و پولی

حسین صادقی/ دانشیار حقوق خصوصی دانشگاه تهران
hosadeghi@ut.ac.ir orcid.org/0000-0002-4513-6177
فاطمه نوری/ دکترای حقوق خصوصی دانشگاه علوم قضایی fnouri67@yahoo.com
مهدی ناصر/ دانشجوی دکتری حقوق خصوصی دانشگاه علوم قضایی mn.ujsasac0077@yahoo.com
دریافت: ۱۴۰۱/۱۰/۲۳ ـ **پذیرش:** ۱۴۰۲/۰۲/۱۰

چکیده

«رمزارز» پدیده‌ای نوین است که ازیک‌سو دارای کارکرد پولی بوده و می‌توان از آن به‌منزله وسیله پرداخت بین‌المللی استفاده کرد و از سوی دیگر دارای ویژگی‌هایی همچون پنهان بودن اطراف مبادلات، آزادی در پرداخت و عدم امکان پایش دارایی توسط ثالث است. این موضوع سبب می‌شود فکر استفاده از رمزارزها به منظور برون‌رفت از تحریم‌های مالی تقویت شود. با این وجود، تجویز به استفاده از آن می‌تواند مخاطراتی را نیز در پی داشته باشد. با تبیین و تحلیل این مزایا و مخاطرات در پژوهش کیفی حاضر که دربردارنده روش تحقیق اسنادی و تحلیلی توصیفی می باشد، درمی‌یابیم که اولاً، از رمزارزها نباید توقع معجزه داشت، به‌گونه‌ای‌که با خلق و استفاده از آنها بتوان تمام مشکلات ناشی از تحریم‌ها را برطرف ساخت. ثانیاً، لازم است با اعمال راهکارهایی (همچون قانونگذاری مناسب، ایجاد واسطه‌های مجاز، به‌کارگیری راهکارهای احراز هویت، رفع ممنوعیت استفاده از رمزارزها در مبادلات بین‌المللی، رایزنی با کشورهای منطقه به منظور خلق رمزارز مشترک) از آسیب مخاطرات کاست و در جهت استفاده مطلوب از آن گام برداشت.

کلیدواژه‌ها: رمزارز، تحریم، بحران بین‌المللی.

مقدمه

یکی از موضوعاتی که چندسالی است در حوزه پول دیجیتال مطرح شده «رمزارز» است. «رمزارز» به معنای پولی است که با به‌کارگیری علوم رمزنگاری و بدون دخالت حاکمیت‌ها تولید و مدیریت می‌شود. این پول اولین بار در سال ۲۰۰۹ با خلق ارزی به نام «بیت‌کوین» ظهور پیدا کرد و هدف از معرفی آن، ایجاد پول بین‌المللی بدون تمرکز دولتی بود (ناگپال، ۲۰۱۹، ص ۴ـ۵).

این پول به تدریج با تولید ارزهای مشابه، معنای وسیع‌تری به خود گرفت، به‌گونه‌ای‌که حتی ارزهای دیجیتال ملی (رمزارزهایی که ساخته یک حاکمیت بوده و متمرکزند و کارکردی همچون پول ملی دارند و صرفاً مطابق فناوری جدید تولید شده‌اند) و یا مشترک (رمزارزهایی که ساخته مشترک میان چند حاکمیت هستند و به قصد نیل به اهداف اقتصادی مشترک میان کشورها ایجاد و منتشر می‌شوند) که از سازوکار و فناوری رمزارز تبعیت می‌کردند نیز به این مفهوم اضافه شدند. با این حال هنوز هم «رمزارز» در معنای اصلی و اخص خود، به معنای «پول دیجیتالی غیرمتمرکز» است. این مقاله «رمزارز» را با عنایت به مفهوم موسع آن بررسی و تحلیل کرده است.

بالاترین هدفی که از ابتدای خلق رمزارز وجود داشته جایگزینی آن با پول کاغذی بوده و ازاین‌رو از میان کارکردهای متنوع رمزارزها، بیشترین توجه به کارکرد پولی و استفاده از آن به‌مثابه وسیله پرداخت است. بررسی‌ها در این تحقیق نیز بر پایه همین کارکرد صورت گرفته است.

از سوی دیگر یکی از چالش‌های موجود برای کشورهایی همچون ایران از ابتدای حرکت‌های استقلال‌طلبانه، اعمال انواع تحریم‌ها توسط کشورها و سازمان‌های بین‌المللی بوده که رفته‌رفته این تحریم‌ها گسترش یافته و تمام ابعاد را دربر گرفته است. یکی از اقسام تحریم‌ها که در دهه‌های اخیر تمرکز بیشتری بر اعمال آن وجود داشته، تحریم‌های مالی ـ پولی بوده است؛ زیرا اولاً، این تحریم‌ها از سایر تحریم‌ها آسان‌تر اعمال می‌شود. ثانیاً، دور زدن آن مشکل‌تر است. ثالثاً، در اقتصادهای بازاری امروزی، تجارت و دیگر فعالیت‌های اقتصادی به شدت به منابع مالی و پولی وابسته است (طغیانی و درخشانی، ۱۳۹۳). بدین‌روی این نوع تحریم‌ها مؤثرترین قسم شناخته می‌شود.

با تحریم مالی ـ پولی، راه مبادله پول مسدود می‌شود و وقتی انتقال پول با چالش مواجه گردد حتی در برابر کشورهایی که حاضر به معامله با ایران هستند هم مشکل انتقال ثمن قراردادی به وجود می‌آید که این مشکل موجب انصراف کشورها در معامله با ایران می‌شود و یا هزینه تمام‌شده قراردادها را افزایش می‌دهد. تحریم‌های مالی ـ پولی اقسام متنوعی دارد که مهم‌ترین آنها عبارتند از: تحریم ارزی، تحریم بانکی، و انسداد دارایی.

با عنایت به کارکرد پولی رمزارز و ویژگی‌های آن، بعضاً تصور برون‌رفت از تحریم با توسل به رمزارزها وجود دارد، به‌گونه‌ای‌که از ابتدای ورود این فناوری، کم و بیش در نوشته‌ها و پژوهش‌ها به این نتیجهٔ بخصوص هم اشاره شده

است. اهمیت موضوع با عنایت به مفاد بند ۸ قانون «کاتسا» (Countering America's Adversaries Through Sanctions Act (CATSA) که توسط کنگره ایالات متحده امریکا علیه کشورهای ایران، روسیه و کره شمالی مبنی بر «نظارت بر عدم استفاده از رمزارزها برای دور زدن تحریم توسط کشورهای فوق» وضع شده، بیشتر جلوه‌گر خواهد شد. لیکن از زاویه‌ای دیگر چنین استفاده‌ای می‌تواند مخاطراتی را هم در پی داشته باشد که همین موضوع سبب شده است سیاستمداران در این عرصه با احتیاط بیشتری گام بردارند.

گاهی همان وصف که از یک منظر به‌عنوان امتیاز در نظر گرفته می‌شود، از بعد دیگر آسیب‌هایی را نیز ایجاد می‌نماید.

این پژوهش بر آن است طی دو گفتار مجزا، به بررسی ابعاد حقوقی، مزایا و خطرپذیری استفاده از رمزارزها به‌منزله یک وسیله پرداخت، بنگرد و در نهایت نتیجه‌گیری کند که کفه کدام‌یک بر دیگری فزونی می‌یابد و بر این اساس به این سؤال پاسخ دهد که آیا استفاده از رمزارزها در معاملات بین‌المللی به هدف برون‌رفت از تحریم با عنایت به امتیازات و مخاطرات موجود، توجیه حقوقی دارد یا خیر؟

در این‌باره توجه به دو نکته لازم است:

اول. این مقاله صرفاً از نقطه‌نظر تحریم به تبیین امتیازات و مخاطرات می‌پردازد. ازاین‌رو ممکن است اوصافی در رمزارزها وجود داشته باشد که به سبب بی‌ارتباطی آن به تحریم، در نوشته حاضر مدنظر قرار نگیرد.

دوم. در بیان اوصاف مذکور باید میان انواع رمزارزهای ملی، مشترک (منطقه‌ای) و بین‌المللی تفکیک قائل شد؛ زیرا برخی از ویژگی‌ها مختص برخی از انواع رمزارزهاست که ممکن است در دیگران کمتر یا اصلاً وجود نداشته باشد.

۱. مزایای استفاده از رمزارزها

۱ـ۱. تمرکزگرایی

تمام ارزهای جهان تا قبل از خلق رمزارزها، پول‌هایی متمرکز بودند؛ یعنی به فرمان یک دولت یا نهاد بین‌المللی ایجاد و منتشر می‌شدند و اعتبار خود را از آنها می‌گرفتند. بنابراین دولت‌ها هستند که با خلق پول، اقتصاد جوامع خود را تحت تأثیر قرار داده، سیاست‌های پولی کشور را متأثر می‌سازند. این در حالی است که طبیعت غیرمتمرکز رمزارزهای بین‌المللی چشم‌انداز مهار یا مالکیت دولتی را از بین می‌برد (پدرو، ۱۳۹۷، ص ۲۶ـ۲۷).

در نظام پولی رمزارزها، پرداخت‌ها نظیر به نظیر صورت می‌گیرد و هیچ واسطه‌ای در پرداخت وجود ندارد. ازاین‌رو با این سازوکار می‌توان به هرکسی در هر جای دنیا بدون وجود کارمزد نهاد واسط و با سرعت و بدون دخالت، وجه دلخواه خود را پرداخت (نوری و نواب پور، ۱۳۹۷، ص ۱۵).

قبل از خلق رمزارزهای غیرتمرکز، عموماً در هر پرداختی واسطه‌ها حضور داشتند؛ یعنی اگر «الف» از یک نقطه می‌خواست مبلغی را به «ب» در نقطه دیگر برساند که دسترسی فیزیکی نیز به وی نداشت، باید از واسطه‌هایی نظیر بانک‌ها استفاده می‌نمود.

در عرصه پرداخت‌های بین‌المللی حضور این واسطه‌ها و تأثیر آنها بر پرداخت‌ها بیشتر جلوه می‌نماید. در مجموع می‌توان از حضور این واسطه‌ها در مبادلات سه اثر عمده را که در بحث تحریم نیز مؤثر است، برشمرد:

۱-۱-۱. افشای اطلاعات

منطقاً وقتی مبادله پولی از طریق یک واسط انجام شود، اطلاعات هویتی و تابعیتی دو طرف مبادله و اطلاعات مربوط به جزئیات معامله (مانند مبلغ، روش پرداخت، موضوع معامله اصلی) توسط واسط دریافت و نگهداری می‌شود. مطابق اصول حقوقی موجود، واسطه‌ها ملزم به حفظ حریم اشخاص هستند. ازاین‌رو حق افشای اطلاعات را ندارند. با این وجود به سبب وابستگی واسطه‌ها به حاکمیت کشورها و تبعیت از قوانین و احکام قضایی آنها، اقدام به افشای قانونی و یا بعضاً غیرقانونی اطلاعات می‌کنند که این موضوع موجب رصد اطلاعات توسط دولت‌های تحریم‌کننده و اعمال سیاست‌ها و دخالت‌های آنها متناسب با اطلاعات کسب‌شده نسبت به کشورهای تحریم‌شده (همچون ایران) می‌گردد.

۱-۱-۲. محدودیت یا ممنوعیت در پرداخت

مطابق اصل «آزادی قراردادی» هر کس حق دارد با هر شخصی که صلاح می‌داند وارد معامله شود و مابازای معاملاتی را پرداخت نماید. با این حال این حق توسط عواملی همچون نظم عمومی محدود می‌شود (کاتوزیان، ۱۳۸۸، ج ۱، ص ۱۴۴ـ۱۴۸).

مصادیق «نظم عمومی» توسط قوانین تحت سلطه حاکمیت‌ها وضع می‌شود. در فضای بین‌المللی نیز سازمان‌هایی که در ظاهر داعیه‌دار نظم جهانی هستند، می‌توانند با اعمال محدودیت‌ها و نظارت‌هایی آزادی پرداخت را از کشورها و اتباع آنها در قالب تحریم‌های اقتصادی سلب نمایند (ضیائی بیگدلی، ۱۳۸۶، ص ۲۲).

همچنین هریک از کشورها نیز با عنایت به اصل «حاکمیت» می‌توانند روابط خود و اتباع خود را با کشور یا کشورهای خاصی محدود سازند. وقتی مبادلات پولی از طریق ارزهای متمرکز و در حضور واسطه‌ها انجام شود، کشورهای تحریم‌کننده به‌راحتی می‌توانند با شناسایی معاملات، به بهانه‌های مذکور دستور ممنوعیت یا اعمال محدودیت در پرداخت را به واسطه‌ها بدهند. ازاین‌رو با اعمال تحریم‌ها، کشور تحریم‌شده عملاً نمی‌تواند با هویت اصلی خود اقدام به تبادل پول از طریق واسطه‌ها نماید. به همین علت است که تحریم‌های بانکی را از مؤثرترین تحریم‌ها می‌شمارند.

لیکن رمزارزهای بین‌المللی از خصیصه غیرمتمرکز بودن برخوردارند؛ یعنی هیچ دولت و حاکمیتی نمی‌تواند بر روی آن نظارت نماید و تبعاً قادر نخواهد بود پرداختی را محدود یا ممنوع سازد. ازاین‌رو قدرت‌های جهانی نمی‌توانند به بهانه تحریم، از پرداخت بین‌المللی ممانعت به عمل آورند. کاربران فضای رمزارز قادرند بدون هرگونه محدودیت و ممنوعیتی در هر مکانی از جهان، هر مبلغی را به هر مکان دیگری در جهان و به هر شخصی با هر تابعیت و ملیتی ارسال کنند یا دریافت دارند (بانجاکو و دیگران، ۲۰۱۷، ص ۳۸).

حتی گاهی رمزارزهای ملی و منطقه‌ای هم که تحت نظارت یک یا چند دولت هستند، سایر دولت‌ها (از جمله دولت‌های غربی مجری تحریم) قادر به مهار و اعمال محدودیت و ممنوعیت در تراکنش‌ها و پرداخت‌ها نیستند.

۳-۱-۱. توقیف حساب‌ها

یکی از عناصر لازم در مبادلات پولی با حضور واسطه‌ها، توقیف پول در مرجع واسط در زمان ارسال و دریافت پول است. به عبارت دیگر وقتی فرستنده از واسطه‌ای برای تبادل پول استفاده می‌کند پول در مرجع واسط باقی می‌ماند تا عملیات تسویه انجام پذیرد. در همین زمان امکان توقیف پول از طرف دولت‌های تحریم‌کننده وجود دارد.

مطابق اصول و مبانی حقوقی، مال اشخاص محترم است و هر کس حق هرگونه دخل و تصرف نسبت به مایملک خود را دارد و هیچ کس نمی‌تواند این حق را محدود کند. همچنین هیچ مالی را نمی‌توان از تصرف صاحبش بدون رضایت وی خارج ساخت. «مالکیت» حقی مطلق، انحصاری و دائمی است که شخص نسبت به مالی دارد و به او اجازه می‌دهد از تمام منافع اقتصادی آن بهره‌مند گردد و از این نظر «انحصاری» نامیده می‌شود که منحصر به مالک است و تمام افراد باید آن را محترم بشمارند و به آن تجاوز نکنند (امامی، ۱۳۸۶، ج ۱، ص ۴۹).

با این وجود محدود ساختن مالکیت اشخاص به موجب قانون امکان‌پذیر است؛ همچنان‌که در ماده ۳۱ قانون مدنی ایران آمده است: «هیچ مالی را از تصرف صاحب آن نمی‌توان بیرون کرد، مگر به حکم قانون».

در دستگاه‌های پرداخت متمرکز، به واسطه نظارت مرکزی بر وجوه، قدرت مرکزی می‌تواند در چارچوب قانون، حساب اشخاص را مسدود سازد و دارایی آنان را توقیف کند و اجازه هرگونه استفاده از مبالغ حساب‌ها را از صاحب آن سلب گرداند، حتی گاهی آن وجوه را از دست صاحبش خارج نماید و به تصرف شخص دیگری درآورد.

چنین حقی در فضای بین‌المللی و در چارچوب قوانین تحریمی به کشورها و سازمان‌های بین‌المللی نیز اعطا شده است. ازاین‌رو یک پرداختْ بین‌المللی باشد و از مجاری تحت رصد و نظارت کشورهای غربی (همچون بانک‌های بین‌المللی و سوئیفت «جامعه جهانی ارتباطات مالی بین بانکی») گذر کند، این کشورها و یا سازمان‌ها به‌راحتی می‌توانند به بهانه تحریم، حساب اشخاص را مسدود و دارایی آنها را توقیف نمایند.

این در حالی است که شبکه رمزارزی فارغ از این تمرکز و نظارت یا دخالت است. ازاین‌رو پایش دارایی در فرض پرداخت به وسیله رمزارزها امکان‌پذیر نیست. در این ساختار، دارایی متعلق به کسی است که کلید خصوصی یک حساب را دارد و هیچ کس غیر از صاحب حساب که دارنده کلید خصوصی آن است، نمی‌تواند خروجی‌ها و ورودی‌های تراکنش‌های او را پایش نماید. خارج از دسترس بودن موجودی حساب‌ها، امکان توقیف و مصادره کردن آن را از قدرت‌های جهانی می‌گیرد (بانجاکو و دیگران، ۲۰۱۷، ص ۳۸).

با عنایت به غیرمتمرکز بودن رمزارزها و سازوکار خاص آن که حضور واسطه‌ها را کمرنگ نموده است، سه اشکال فوق برطرف می‌گردد و آزادی در پرداخت تأمین می‌شود. بنابراین استفاده از رمزارزها در مبادلات پولی بین‌المللی موجب نفی دخالت کشورهای ثالث در مبادلات میان دو یا چند کشور شده، آزادی در پرداخت‌های بین‌المللی را فراهم ساخته و دولت‌ها را در مصادره و توقیف دارایی‌های پولی کشورهای تحریم‌شده ناتوان ساخته است.

۲ـ۱. بین‌المللی بودن

رمزارزها ساخته شده‌اند تا تمام مردم جهان از آن استفاده کنند؛ همان‌گونه که از ابتدای خلق آن این‌گونه بوده است. بنابراین در تمام جهان بدون در نظر گرفتن نژاد و ملیت قابلیت استفاده دارند. این ویژگی بین‌المللی و جهانی بودن رمزارزها را نمایان می‌سازد.

مبادلات جهانی بر پایه ارزهای جهان‌روا و جهان‌شمول همچون دلار و یورو صورت می‌گیرد و همین موضوع نیز به کشورهای غربی قدرت لازم برای دخالت در اقتصاد جوامع را از طریق تحریم‌های ارزی داده است.

در چنین شرایطی وجود ارزی بین‌المللی که اولاً، ارزش و اعتبار یکسانی در فضای بین‌المللی داشته باشد و تمام مردم جهان بدون نگرانی از تبدیل آن به سایر ارزها بتوانند با آن مبادله نمایند و ثانیاً، وابسته به هیچ دولت یا حکومتی نباشند تا امکان تحریم آن وجود داشته باشد، می‌تواند راه را برای انجام مبادلات مالی در شرایط تحریمی هموار سازد.

این دو خصیصه با هم در رمزارزها وجود دارد؛ زیرا ازیک‌سو رمزارزها ارزهایی بین‌المللی و جهان‌شمول با قابلیت کاربرد در مبادلات مالی و پولی بین‌المللی هستند. علاوه بر آن فناوری رمزارزها، امکان تولید و انتشار ارزهای دیجیتالی مشترک میان چند کشور و در نتیجه معاهدات دو یا چندجانبه را مهیا می‌سازد. از سوی دیگر ویژگی «غیرمتمرکز بودن» آن نیز موجب غیرقابل پایش بودن آن توسط حاکمیت‌ها می‌گردد و در نتیجه به علت آنکه در سلطه و اراده هیچ حاکمیتی نیست، قابلیت رهگیری و تحریم را هم ندارد.

۳ـ۱. ناشناخته بودن طرف‌های مبادله

شناسایی هویت دو طرف مبادله از لوازم ایجاد تعهد حقوقی و ایفای آن است؛ اما فراتر از رابطه میان دو طرف، این می‌تواند تبعات منفی و مؤثری در تحریم داشته باشد. چنانچه کشور تحریم‌کننده به‌عنوان طرف ثالث، هویت مبادله‌کنندگان را کشف و احراز نماید، به اطلاعاتی دست یافته است که می‌تواند با آن تحریم اعمال کند؛ زیرا ممنوعیت، محدودیت و تحریم بر کشور تحریم‌شده و اتباع آن ازیک‌سو و کشورها و اتباعی که با کشور تحریم‌شده معامله می‌کنند از سوی دیگر اعمال می‌شود و شناسایی هویت به معنای شناسایی تابعیت اشخاص است. در چنین شرایطی مخفی ماندن هویت اطراف مبادله برای طرف ثالث، راهگشا خواهد بود.

یکی از ویژگی‌های استفاده از رمزارزها غیرقابل شناسایی بودن اطراف پرداخت است که معروف به وصف «گمنامی» است. کاربران شبکه رمزارزی با یک کلید عمومی که شماره حساب آنهاست، شناخته می‌شوند و هویت واقعی آنان پشت این کلید پنهان است (جوریک، ۲۰۲۱، ص ۲۶).

در مبادلات رمزارزها دو طرف مبادله ناشناخته هستند. آنها یکدیگر را با ارسال رمزهای خاص ـ و نه با هویت شناسنامه‌ای خود ـ می‌شناسند و ردیابی می‌نمایند. اگرچه تمام اطلاعات مربوط به تراکنش‌ها به صورت عمومی ذخیره می‌شوند، اما هویت دو طرف تراکنش تقریباً ناشناس باقی می‌ماند (ابوبکر، ۱۳۹۸، ص ۱۰ـ۱۱).

۴ـ۱. قابلیت ایجاد رغبت جهانی

رمزارزها به واسطه سه خصیصه «سرعت بالا»، «هزینه پایین» و «وجود امنیت» این قابلیت را دارند که به‌عنوان وسیله تبادل پول در جهان مورد استقبال قرار گیرند. متعاقب این استقبال و رغبت جهانی است که می‌توان انتظار جایگزینی نظام پرداخت مبتنی بر رمزارز با ساختارهای بانکی در پرداخت‌های بین‌المللی در شرایط تحریمی را داشت.

۱-۴-۱. سرعت

در شرایطی که پرداخت بین‌المللی میان دو بانک، چندین روز زمان می‌برد و یا پرداخت‌های غیربانکی همچون پرداخت چمدانی و حواله‌ای ممکن است تا هفته‌ها طول بکشد، پرداخت رمزارزی از یک نقطه جهان به نقطه دیگری از جهان حداکثر سی دقیقه زمان می‌برد (کرنل، ۲۰۱۷، ص ۶۷).

جدیدترین شیوه‌های پرداخت بین بانکی هم نمی‌توانند چنین سرعتی داشته باشند. به طریق اولی نظام‌های غیربانکی که کشورهای مشمول تحریم مجبور به استفاده از آنها هستند نیز قادر به فراهم ساختن چنین سرعتی نیستند.

۲-۴-۱. هزینه پایین

در پرداخت مبتنی بر رمزارز، هزینه انجام تراکنش در مقایسه با هزینه تراکنش‌های بین‌المللی بین بانکی و به طریق اولی هزینه حواله و پرداخت چمدانی در وضعیت تحریمی بسیار پایین است. قسمت اصلی تراکنش با انجام فرایند ریاضی است که به پول نیاز ندارد (بانجاکو و دیگران، ۲۰۱۷، ص ۳۷). پرداخت بدون نیاز به طی مسیر پیچیده بانکی انجام می‌شود و با حذف واسطه‌ها از میزان هزینه‌ها نیز کاسته شده است.

تنها هزینه تعلق‌گرفته به این ساختار، کارمزدی (Fee) است که به گره‌ها اختصاص می‌یابد. این کارمزد برای ایجاد انگیزه و رغبت در گره‌ها برای تأیید تراکنش تعبیه شده است.

بااین‌حال میزان کارمزد برخلاف نظام بانکی یک مبلغ مقطوع و ازپیش‌تعیین‌شده نیست، بلکه می‌تواند بسته به نظر ارسال‌کننده وجه، تغییر کند. تمام تراکنش‌های رمزارزی در فضای الکترونیکی به نام «استخر حافظه» (Mempool) جمع می‌شوند و منتظر تأیید باقی می‌مانند. گره‌ها (ساختار فعال در شبکه که در سرتاسر جهان استقرار دارند) تراکنش‌ها را انتخاب نموده، آن را تأیید می‌کنند. میزان کارمزد اعلامی از سوی ارسال‌کننده وجه عملاً مهم‌ترین عامل برای گره‌ها در جهت انتخاب یک تراکنش برای تأیید است. ازاین‌رو هر تراکنشی که کارمزد بیشتری داشته باشد رغبت بیشتری برای تأیید آن از سوی گره‌ها وجود دارد. بنابراین بهتر است در تراکنش‌های با مبالغ بالا، کارمزد بالاتری قرار داده شود تا زودتر تأیید شوند؛ زیرا تا قبل از تأیید گره‌ها، پرداختْ نهایی نمی‌شود (جوریک، ۲۰۲۱، ص ۲۷). بنابراین ایفای تعهد و سقوط آن منوط به تأیید توسط گره‌هاست.

۳-۴-۱. امنیت

یکی از مهم‌ترین گزاره‌ها در پرداخت بین‌المللی که دو طرف قرارداد بدان توجه می‌کنند، انتخاب «نظام پرداخت» است که امنیت لازم را برقرار سازد، ولو آنکه دارای هزینه بوده، سرعت آن کم باشد؛ زیرا اولاً، ممکن است دو طرف هیچ‌گونه شناختی از یکدیگر نداشته باشند تا این شناخت مبنای اطمینان آنها گردد. ثانیاً، اقدامات قضایی به‌مثابه ضمانت اجرا و راهکار درمانی ـ نه پیشگیرانه ـ به سبب بین‌المللی بودن قرارداد، با تحمیل هزینه‌های هنگفتی روبه‌روست. بنابراین اگر در نظام پرداخت مبتنی بر رمزارز، امنیت فدای مزایای فوق‌الذکر گردد، قطعاً رغبتی به پذیرش چنین ساختاری وجود نخواهد داشت.

منظور از «امنیت پرداخت» به‌مثابه یک داده‌پیام که در فضای الکترونیکی منتقل می‌شود، آن است که وقتی داده‌پیام در فضای ناامن اینترنت که قابل رؤیت و در دسترس همگان است، عبور می‌کند، باید قادر باشد محرمانگی و تمامیت خود را حفظ نماید؛ یعنی اولاً، رؤیت و فهم پیام برای شخصی غیر از مخاطب خاص خود امکان نداشته باشد. ثانیاً، بدون هرگونه تغییر از فرستنده به دست گیرنده برسد. در این حالت است که مخاطب مطمئن می‌شود پیامْ محرمانگی خود را حفظ نموده و از تغییرات مصون مانده است.

دانش «رمزنگاری» امروزه برای رسیدن به این مقصود به کار گرفته می‌شود. این فناوری در مسیر انتقال رمزارز و حفظ اطلاعات پرداخت توسط آن به کار گرفته شده است. وجود فناوری رمزنگاری در رمزارزها علاوه بر ایجاد اطمینان در طرف‌های یک مبادله پولی، ردیابی مبادلات در حال انجام و اخلال یا توقف آنها را نیز ناممکن می‌سازد که این خصیصه در اوضاع تحریم مؤثر خواهد بود. تراکنش‌ها در عین ناشناس بودن در «بلاکچین» ذخیره می‌شوند و بررسی معاملات در این دفتر کل، وضعیت تجاری و معاملاتی یک نشانی را هویدا می‌سازد، بدون آنکه هویت آن نشانی مشخص شود (جوریک، ۲۰۲۱، ص ۲۸).

بنابراین استفاده از دانش «رمزنگاری» در رمزارزها به چند طریق در تحریم مؤثر خواهد بود:

اولاً، ایجاد امنیت در مبادلات پولی که هم موجب جلب اعتماد کشورهای ثالث برای انجام مبادله با کشور تحریم‌شده از طریق رمزارزها می‌شود و هم تبادل پولی میان کشورها را مطابق اسناد بین‌المللی در زمینه حقوق تجارت الکترونیک، معتبر، قابل دفاع و قابل استناد می‌نماید.

ثانیاً، حفظ محرمانگی، امکان رصد اطلاعات مبادلات پولی میان کشورها را کاهش داده، از این طریق از دخالت کشورهای تحریم‌کننده و اعمال سیاست‌های آنان درخصوص کشورهای تحریم‌شده جلوگیری به عمل می‌آورد.

۲. خطرپذیری ناشی از رمزارزها

۲ـ۱. فقدان قانون مشخص

در نظام حقوقی ایران هیچ مقرره‌ای که به طور دقیق چارچوب‌های حقوقی رمزارزها و آثار ناشی از پرداخت توسط آن و ضمانت اجراهای آن را بیان کند، تدوین نشده است.

به‌طورکلی، معاملات رمزارزی به سبب چالش‌هایی همچون بستر مناسب برای ارتکاب جرایم، تضعیف بانک مرکزی و نهادهای مالی و نظام پولی و بانکی کشورها (نوری و نواب‌پور، ۱۳۹۷، ص ۱۹ـ۲۰)، هنوز نتوانسته است جایگاه خود را در میان جوامع به دست بیاورد.

در بیشتر کشورها، قانونگذاری در این زمینه صورت نگرفته است؛ حتی کشورهایی که رمزارزها را به رسمیت شناخته‌اند نیز غالباً آن را به صورت کالای سرمایه‌ای در نظر گرفته‌اند، نه وسیله پرداخت. قانونگذاری در بیشتر کشورها به صورت موردی بوده و صرفاً برخی مسائل از جمله جلوگیری از ارتکاب جرایمی همچون پولشویی و فرار مالیاتی را مدنظر قرار داده و نسبت به آن مقرراتی تنظیم نموده‌اند و ازاین‌رو قوانین جامعی درخصوص رمزارزها تاکنون تدوین نشده است (عزیز، ۲۰۱۹، ص ۳۳).

در چنین فضای ناامن حقوقی کاربران نمی‌توانند با اطمینان‌خاطر دست به این‌گونه معاملات بزنند. مادام که قانونگذاری انجام نشود ریسک پرداخت با این ارز برای پرداخت‌کننده وجود دارد؛ اینکه این پرداخت به رسمیت شناخته می‌شود و می‌تواند پرداخت‌کننده را از مسئولیت مبرا سازد یا خیر؟

در پاسخ به اشکال فوق، باید خاطرنشان کرد که اگر قصد بر آن باشد از رمزارزها برای پرداخت به هدف برون‌رفت از تحریم استفاده کنیم، فقدان قانونگذاری صرفاً چالش امروز ماست و می‌توان با تدابیری آن را از پیش‌رو برداشت. بی‌تردید با توجه به نقش قانون و حاکمیت آن به‌مثابه یکی از ویژگی‌ها و ابعاد حمکرانی خوب، قانونگذاری مطلوب در پاسخ به ضرورت‌های حاصل از توسعه فناوری، به‌منزله سیاست‌گذاری تقنینی تلقی می‌گردد (صادقی و ناصر، ۱۳۹۹) که در شرایط کنونی در حوزه رمزارزها ضرورت تقنین مناسب و مطلوب باید در نظر گرفته شود. ساختار رمزارزی قابلیت‌های لازم برای انتخاب به‌مثابه یک وسیله پرداخت را مشروط به تدوین قوانین لازم دارد. ازاین‌رو کافی است ـ دست‌کم ـ در مبادلات بین‌المللی، آن هم در موضوعات تحریمی، این قوانین تنظیم و تدوین شوند.

همچنین می‌توان در سطح منطقه و میان کشورهایی که مبادلات کشور با آنها بیشتر است، اقدام به ایجاد رمزارز مشترک و تنظیم مقررات آن نمود و بدین طریق ـ دست‌کم ـ پرداخت را در میان این کشورها تسهیل گردانید.

۲ـ۲. امکان فنی شناسایی هویت نهفته در برخی رمزارزها

«گمنامی» خصیصه تمام رمزارزها نیست، صرفاً برخی از رمزارزها از این امتیاز برخوردارند؛ همچون «بیت‌کوین» و «مونرو». حتی در رمزارزهایی که گمنامی از ویژگی‌های آنهاست، این ناشناسی کامل نیست و امکان شناسایی هویت نهفته پشت کلید عمومی و نشانی حساب وجود دارد. همچنان‌که برخی گفته‌اند، فنون آماری و تجزیه و تحلیل الگویی می‌تواند هویت تا ۶۰ درصد از کاربران «بیت‌کوین» را آشکار سازد (کرنل، ۲۰۱۷، ص ۶۷).

علاوه بر این اگر مبادلات رمزارزی توسط واسطهایی همچون صرافی‌های دیجیتال صورت گیرد، هویت آشکار خواهد شد. کاربر برای استفاده از خدمات صرافی‌ها، ابتدا باید ثبت‌نام کند و در این زمان است که ضرورت دارد اطلاعات هویتی کابر در سامانه صرافی درج شود.

ممکن است گفته شود: ثبت‌نام با یک هویت و شناسه صوری غیرایرانی مشکل را حل خواهد نمود؛ اما لازم است یادآور شویم که بیشتر صرافی‌ها، صرفاً در مبادلات با ارقام پایین به این ثبت‌نام بسنده می‌کنند و اگر کاربر بخواهد مبادلاتی با ارقام بالا انجام دهد، ضرورت دارد ابتدا احراز هویت به طور کامل انجام شود که در این مرحله صرافی از کاربر می‌خواهد تصویری از چهره خود را در حالتی که کارت هویتی‌اش در کنار

صورت اوست برای آن صرافی ارسال نماید که در این صورت ملیت واقعی کاربر آشکار می‌شود و چناچه ایرانی باشد مشمول تحریم قرار می‌گیرد.

صرافی «بیترکس» یکی از این نمونه‌هاست که در سال ۱۹۹۶ اقدام به مسدود کردن حساب کاربران ایرانی خود به بهانه تحریم کرد (صمدی گرگانی و شهیر، ۱۳۹۶، ص ۹). صرافی «بایننس» هم در مقررات استفاده از خدمات خود، برخی کشورها را از دریافت خدمات ممنوع نموده که ایران ازجمله آنهاست (www.binance.com).

پیشنهاد می‌شود برای آنکه گمنامی کامل گردد، اشخاص برای هر تراکنش از یک نشانی منحصربه‌فرد استفاده کنند و تمام تراکنش‌های خود را با یک نشانی انجام ندهند (بانجاکو و دیگران، ۲۰۱۷، ص ۳۸). حتی در مبالغ بالا می‌توان کل مبلغ را به ارقام خرد تبدیل کرد و هر بخش را با یک نشانی، برای گیرنده ارسال نمود. با توجه به اینکه در رمزارزها ایجاد نشانی محدودیتی ندارد این مسیر تا حدی می‌تواند راهگشا باشد.

همچنین بسیاری از کاربران رمزارزها ثبت‌نام خود در این صرافی‌ها را به وسیله فیلترشکن انجام می‌دهند تا ملیت آنها آشکار نگردد.

استفاده از خدمت «میکسر» نیز می‌تواند موجب ناشناسی گردد. این خدمت توسط برخی از سامانه‌های عامل مجازی ارائه می‌شود، برای اطمینان از اینکه مشتریان آنها می‌توانند منشأ رمزارزهای ثبت‌شده در «بلاکچین» را پنهان نمایند. چنین سکو (پلتفرم)هایی رمزارزهای همه کاربران خود را مخلوط کرده، میان آنها مبادله می‌کنند و از این طریق امکان ردیابی تراکنش‌ها را از بین می‌برند (سانزباس و دیگران، ۲۰۲۱، ص ۱۴).

۳ـ۲. چالش حقوقی احراز هویت اشخاص وارد در مبادلات رمزارز

در مطالب پیشین گفته شد: هویت اشخاص در مبادلات رمزارزی به وسیله کلید عمومی و نشانی حساب آنان احراز می‌شود. اما این هویت واقعی افراد نیست، هویت واقعی پشت رشته‌ای از اعداد و حروف در قالب کلید و نشانی مخفی مانده است. این کلید و نشانی اتصال و انتساب آن به یک هویت را که در عالم واقع دارای حقوق و تکالیف است، اثبات نمی‌کند. به بیان ساده‌تر، مشخص نیست این کلید عمومی واقعاً متعلق به چه کسی است.

احراز هویت از بعد حقوقی آثار فراوانی دارد:

الف. تا هویت اشخاص احراز نشود انتساب عمل حقوقی به یک شخصِ معین امکان‌پذیر نیست. برای مثال نمی‌توان ثابت کرد که شخص «الف» پول را پرداخت نموده و شخص «ب» پول را دریافت کرده است. ممکن است اساساً «الف» پرداختی نکرده باشد و یا «الف» پرداخته نموده، اما به دست «ب» نرسیده باشد.

ب. تا زمانی که انتساب عمل به شخص معینی احراز نشود، نمی‌توان آثار حقوقی عمل را بر آن فرد بار کرد. برای مثال وقتی هویت فرستنده و گیرنده وجه مشخص نباشد، نمی‌توان پرداخت را به «الف» و دریافت

وجه را به «ب» منتسب نمود و متعاقب آن، نمی توان احراز کرد که دین شخص «الف» به «ب» پرداخت شده و تعهد او ساقط گردیده است. ازاین‌رو اثر حقوقی پرداخت ـ به‌مثابه مصداقی از ایفای تعهد ـ که همان سقوط تعهد است، بر «الف» بار نمی‌شود.

ج. اهلیت قراردادی که از شرایط اساسی صحت معاملات است، منوط به شناسایی هویت اشخاص است.

بنابراین با توجه به تأثیرات حقوقی بسزایی که احراز هویت بر قرارداد و پرداخت وجه می‌گذارد، لازم است راهکارهایی برای رفع این ایراد ارائه شود، وگرنه همین یک مخاطره برای انصراف از استفاده از رمزارزها کافی خواهد بود.

مشکل احراز هویت در معاملات رمزارزی را می‌توان به شیوه‌های ذیل رفع نمود:

۱-۳-۲. احراز هویت از طریق صرافی‌های مجاز

دولت‌ها می‌توانند با ایجاد صرافی‌های دیجیتال مشخص و قانونگذاری بر آنها، از طریق آنان اقدام به احراز هویت نمایند. همان‌گونه که در قسمت قبل هم گفته شد، بزرگ‌ترین صرافی‌های جهانی امروزه به روش ارسال تصویر همراه با کارت هویتی، مشکل احراز هویت را حل نموده‌اند. این صرافی‌ها فهرست مشخصی از کاربران خود و مشخصات آنها و معاملات انجام‌شده توسط ایشان را دارند که در مواقع لزوم قابل استناد در محاکم قضایی برای اثبات دعاوی مرتبط است.

۲-۳-۲. احراز هویت در قرارداد

اگر قرار باشد پرداخت مابازای قراردادی توسط رمزارز صورت گیرد طرفین یک توافق می‌توانند در قرارداد، اقدام به ابراز نشانی حساب و کلید عمومی نشانگر هویت خود کنند. در این صورت واریز تنها به شماره حساب متعلق به این کلید عمومی انجام خواهد گرفت. این اقدام ازیک‌سو رضایتِ گیرنده را به پرداخت از طریق رمزارز نشان می‌دهد و از سوی دیگر با توجه به اقرار خود شخص، هویت واقعی یک کلید عمومی را آشکار می‌سازد.

۳-۳-۲. احراز هویت توسط مراکز صدور گواهی الکترونیکی

یکی از زیرساخت‌های کلید عمومی به‌طورکلی ـ و نه فقط در مبحث رمزارز ـ ایجاد مراکزی برای صدور گواهی الکترونیکی است. این گواهی حاوی اطلاعاتی است که هویت اصلی دارنده یک کلید عمومی را مشخص می‌سازد.

مراجع صدور این گواهی‌ها همانند دفاتر اسناد رسمی در صدور «گواهی امضا» عمل می‌نمایند و چون این مراکز تحت نظارت حاکمیت بوده، مطابق قانون فعالیت می‌کنند، گواهی‌های صادرشده توسط آنان، قابلیت استناد در دادگاه را به‌عنوان یک مدرک معتبر خواهد داشت.

۲ـ۴. چالش دستیابی به رمزارز

یکی دیگر از چالش‌های پیش‌رو در بحث رمزارزها، دستیابی به آن است. مقدمه هر پرداخت، تصاحب آن پول یا ارز برای پرداخت است. اگر بخواهیم مابازای دلاری یا ریالی پرداخت کنیم ابتدا باید به همان میزان دلار یا ریال به دست آوریم.

رمزارزهای بین‌المللی مرجع صدور ملی ندارند و ازاین‌رو به‌راحتی و به صرف چاپ آن توسط دولت قابل دسترس نیستند. برای کسب این رمزارزها به سه طریق می‌توان عمل کرد: اول تولید؛ دوم دریافت آن به‌عنوان مابازای فروش؛ سوم خرید آن با پرداخت ارز خارجی.

مشکل تولیدْ از طریق استخراجِ برخی از اقسام رمزارز (همچون «بیت‌کوین») و نیز با ایجاد زیرساخت قانونی لازم و رفع ممنوعیت استفاده از رمزارز در مبادلات قابل حل است.

اما درخصوص نکته سوم، ممکن است گفته شود: چون رمزارزها عموماً در بازارهای جهانی با ارزهای جهان‌شمول (همچون دلار و یورو) مبادله می‌شوند، برای اکتساب آنها، مجبور به پرداخت مبالغ قابل‌توجهی دلار یا یورو هستیم و این موضوع ازیک‌سو موجب خروج ارز از کشور می‌شود و از سوی دیگر چالش تهیه این میزان دلار و یورو در وضعیت تحریمی را ایجاد می‌نماید.

در پاسخ باید گفت: اولاً، میزان قابل‌توجهی رمزارز بین‌المللی در مالکیت عموم مردم است که از راه‌های گوناگون (همچون استخراج یا انواع واسطه‌گری‌های مجازی و اخذ کارمزد به صورت رمزارز) کسب شده است که با مدیریت صحیح می‌توان آنها را با پرداخت مابازای ریالی تصاحب نمود.

ثانیاً، بحث خروج ارز را نیز نمی‌توان در این فضا مطرح ساخت؛ زیرا حتی اگر قرار بر پرداخت رمزارزی هم نبود، به همین میزان ارز برای دریافت کالا و خدمات، از کشور خارج می‌شد. خروج ارز در فرضی که قصد خرید خدمات یا کالا از کشور خارجی مطرح است، بی‌معناست. قرار است تمام آنچه از رمزارز خریداری می‌شود در خرید کالا یا خدمات صرف شود و این تبدیل ارزی صرفاً به علت دور زدن تحریم صورت می‌گیرد.

۲ـ۵. کافی نبودن رمزارز به‌مثابه عاملی برای برون‌رفت از آثار ناشی از تحریم‌های چندجانبه و چندبعدی

تحریم‌های کنونی علیه ایران چندجانبه است، صرفاً مبادله پولی با ایران ممنوع نیست که با جایگزینی رمزارز بتوان تمام مشکلات ناشی از تحریم را حل نمود، بلکه هرگونه مراوده تجاری با ایران ممنوع است. کشورها در هراس از هر نوع ارتباطی با ایران هستند و مسئله پرداخت یک مسئله ثانوی است. ازاین‌رو حتی اگر مسئله پرداخت مابازای قراردادی هم حل شود سه چالش پیش‌رو قراردارد:

ـ به عنوان مقدمهٔ هر پرداختی، آیا اساساً کشورها تمایل به انعقاد قرارداد با ایران دارند یا خیر؟

ـ در صورت انعقاد قرارداد و پرداخت مابازای آن به وسیله رمزارزها، حمل کالای خریداری شده چگونه اتفاق خواهد افتاد، درحالی‌که حمل و نقل از ایران و به آنجا مشمول تحریم است؟

علاوه بر آن، در فرایند حمل و نقل با توجه به ماهیت فیزیکی و ملموس آن، هویت دو طرف معامله آشکار می‌شود، مگر آنکه بتوان از مسیرهای دیگری برای دور زدن این بخش کمک گرفت.

ـ حتی اگر این مشکلات هم حل شود، چالش سوم آن است که رمزارز دریافتی توسط طرف معامله باید در کشور وی تبدیل به پول رسمی شود و مصرف گردد که قطعاً در این مسیر صرافی‌ها و مراکز دولتی از مبدأ آن پرس‌وجو نموده، از معامله با ایران مطلع خواهند شد.

مطابق مقررات گروه «اقدام ویژه مالی» (FATF) هر کشوری باید درخصوص دارایی‌های دیجیتال و رمزارزها تمهیداتی را رعایت نمایند، به‌گونه‌ای‌که امکان شناسایی جرایم پولشویی و تأمین مالی تروریسم فراهم باشد. در این زمینه کشورها موظف هستند نقل و انتقالات رمزارزی را نیز پایش نموده، گزارش دهند (توصیه‌های اف. ای. تی. اف، یادداشت‌های تفسیری به توصیه‌های ۱۵).

بدین‌روی انجام صحیح فرایند استفاده از رمزارز تا انتها، نیاز به همکاری و همراهی کشور متبوع طرف معامله با کشور ایران دارد.

۶ـ۲. امکان تحریم برخی رمزارزها

از میان اقسام رمزارزها، صرفاً رمزارزهای بین‌المللی هستند که مرجع صدور و انتشار آنها خارج از قلمرو حاکمیت‌هاست. رمزارزهای ملی و منطقه‌ای (مشترک) تحت حاکمیت یک یا چند دولت خاص صادر و منتشر می‌شوند. ازاین‌رو تحریم یک حاکمیت تحریم رمزارز منتسب به آن را نیز در پی دارد. بنابراین چنانچه رمزارز ملی ایران منتشر شود قطعاً تحریم خواهد گردید و معاملات آن نیز تحریم خواهد شد.

به اشکال مذکور می‌توان این‌گونه پاسخ داد که «گمنامی» مهم‌ترین ویژگی رمزارز به هدف دور زدن تحریم‌هاست. ازاین‌رو چنانچه طراحی ساختار رمزارز ملی به‌گونه‌ای باشد که اطراف معاملات آن تا حد قابل اطمینانی ناشناس باقی بمانند، رغبت جهانی برای خرید و فروش و انجام معاملات با آن و سرمایه‌گذاری در آن ایجاد می‌شود؛ زیرا در این صورت با وجود تحریم رمزارز ملی، امکان شناسایی معامله‌کنندگان وجود ندارد که هراسی از اِعمال آثار نقضِ تحریم داشته باشند.

همچنین در رمزارزهای منطقه‌ای، هدفْ ناشناسی معامله‌کنندگان با کشور تحریم‌شده (همچون ایران) نیست، بلکه تسهیل روابط تجاری میان چند کشور و حذف حاکمیت دلار انگیزهٔ اصلی است که توسط رمزارز تأمین می‌گردد، ولو آنکه مورد تحریم واقع شود.

۲ـ۷. جرم‌زا بودن فضای مبادلات رمزارز

یکی از مخاطرات قابل طرح و پراهمیت در حوزه رمزارزها، بسترسازی برای ارتکاب برخی جرایم است، به‌گونه‌ای‌که می‌توان این موضوع را یکی از علل جدی عدم رسمیت و اعتباربخشی حاکمیت‌ها به این حوزه دانست.

با وجود چنین مخاطره‌ای ممکن است این شائبه پیش آید که استفاده از رمزارزها در حوزه روابط بین‌المللی ــ در حقیقت ـ رسمیت دادن به آن و ایجاد مقدمه‌ای برای ارتکاب این جرایم خواهد بود. تبعات حقوقی سوء ناشی از این مخاطرات، موجب می‌شود حاکمیت از فواید و مزایای استفاده از رمزارزها در روابط بین‌المللی صرفاً به سبب وجود چنین جرایمی صرف‌نظر نماید.

با این وجود، دلایلی که در ادامه بدان خواهیم پرداخت، اثبات می‌نماید نه‌تنها وجود این جرایم نمی‌تواند دلیل معقولی برای ممنوعیت رمزارزها باشد، بلکه اتفاقاً نقش قانونگذاری در این حوزه را پررنگ‌تر نیز می‌نماید. قبل از ورود به بحث و ارائه راهکارهای پیشنهادی، مناسب است به اجمال عمده جرایم ارتکابی در حوزه رمزارزها را مطالعه و تبیین نماییم.

جرایمی را که در این بستر رخ می‌دهند می‌توان به دو دسته کلی تقسیم نمود:

۱-۷-۲. جرایم مستقیم

«جرایم مستقیم» به افعال مجرمانه‌ای گفته می‌شود که مستقیماً در فضای رمزارز رخ می‌دهد که مهم‌ترین آنها عبارتند از:

۱-۱-۷-۲. کلاهبرداری

«کلاهبرداری» تعریف می‌شود به: «تحصیل اموال اشخاص با توسل به اقدامات فریبکارانه و متقلبانه به نحو غیرقانونی و نامشروع» (قانون تشدید مجازات مرتکبان ارتشا و اختلاس و کلاهبرداری، ماده ۱).

کلاهبرداری در حوزه رمزارزها عموماً از طریق عرضه اولیه سکه و یا طرح‌های هرمی (پانزی) صورت می‌گیرد، بدین صورت که اشخاص حقیقی و یا حقوقی با طراحی یک سکه و عرضه آن به عموم مردم، به بهانه سرمایه‌گذاری در یک طرح و یا ارائه خدمات، اقدام به جمع‌آوری سرمایه از سرتاسر جهان می‌کنند. پس از سرمایه‌گذاری مردم در این طرح‌ها و پس از مدت زمانی مشخص می‌شود که طرح از اساس معدوم بوده و وجوه مردم توسط عرضه‌کنندگان ربوده شده است (سانزباس و دیگران، ۲۰۲۱، ص ۱۲).

تنها در ماه ژوئن ـ ژوئیه ۲۰۱۸ در انگلستان، ۲۰۳ نمونه کلاهبرداری از طریق رمزارزها گزارش شده که مجموع خسارات آن بیش از دو میلیون پوند برآورد شده است (هاینز و یاو، ۲۰۲۰، ص ۲۳).

۲-۱-۷-۲. سرقت

اگرچه امنیت ساختار «بلاکچین» و شبکه رمزارزی بالاست و تاکنون سکوی رمزارزهایی همچون «بیت‌کوین» به

طور قابل‌توجهی آسیب ندیده (هاینز و یاو، ۲۰۲۰، ص ۲۱)، اما حضور واسطه‌ها و عدم به‌کارگیری سازوکارهای امنیت در سکوهای آنان ازیک‌سو و آگاهی پایین معامله‌کنندگان از سوی دیگر، اغلب موجب ایجاد فرصت برای مجرمان برای سرقت رمزارزها می‌گردد.

شایع‌ترین الگوی سرقت در حوزه رمزارزها، سرقت از صرافی‌هاست. زمانی که معامله‌کنندگان از واسطه‌گری صرافی‌ها برای مبادلات رمزارزی استفاده می‌کنند، چنانچه سازوکارهای امنیتی صرافی قوی نباشد رخنه‌گر (هکر)ها و مهاجمان می‌توانند اقدام به سرقت رمزارزها نمایند. برای مثال، صرافی «مت گاکس» صرافی مستقر در توکیو که از بزرگ‌ترین صرافی‌های دیجیتال به شمار می‌رفت، در سال ۲۰۱۴ آماج حمله واقع شد و بیت‌کوین‌هایی به ارزش ۴۷۷ میلیون دلار از آن به سرقت رفت (گرشما، ۲۰۱۵، ص ۴). همچنین در سال ۲۰۱۸ تنها از صرافی ژاپنی «کوین‌چک» رمزارزهایی به ارزش تقریبی ۵۰۰ میلیون یورو به سرقت رفت (لاپوه بله، ۲۰۲۱، ص ۴).

حملات بدافزارها به کیف‌پول‌های آنلاین و حملات رمزگیری (فیشینگ) از طریق ارسال نامه‌های الکترونیکی نیز راهکارهای دیگری برای سرقت رمزارزهای اشخاص است. در حمله رمزگیری مهاجم از طریق ارسال نامه‌های الکترونیکی پیچیده برای قربانیان، سعی می‌کند آنان را به نسخه جعلی یک وبگاه رمزارز واقعی هدایت کند و سپس اطلاعات حساب و یا وجوه آنها را سرقت نماید. گزارش شده است که در جولای ۲۰۲۰ ***توبیتر*** هدف این نوع حمله قرار گرفت و رخنه‌گرها توانستند به ۱۳۰ شماره حساب، ازجمله *ایلان ماسک* و *بیل گیتس* دسترسی پیدا کنند و از آنها برای بهره‌برداری در کلاهبرداری استفاده نمایند (www.packetlabs.net).

سرقت شایع‌ترین جرمی است که در بستر رمزارزها رخ می‌دهد. یک گزارش نشان می‌دهد که تنها در ۹ ماه اول سال ۲۰۱۸ در امریکا، براساس حملات رخنه‌گرها، رمزارزهایی به ارزش ۹۲۷ میلیون دلار به سرقت رفته است (هاینز و یاو، ۲۰۲۰، ص ۲۲).

۳-۱-۷-۲. پولشویی

با عنایت به تعریف مصرح در ماده ۲ قانون «مبارزه با پولشویی» مصوب ۱۳۸۶ (اصلاحی ۱۳۹۷) می‌توان گفت: پولشویی از طریق رمزارزها طی سه مرحله انجام می‌شود: ابتدا وجوه تحصیل‌شده در یک فعالیت غیرقانونی به ارز مجازی تبدیل می‌شود. در مرحله بعد، عملیاتی برای از بین بردن قابلیت ردیابی جریان معاملاتی آن انجام می‌شود و در نهایت، رمزارزهای تحصیل‌شده تبدیل به وجوه قانونی و تمیز می‌شود و یا صرف کسب مال و خدمات می‌گردد (سانزباس و دیگران، ۲۰۲۱، ص ۱۲).

آمارها حاکی از آن است که در سال ۲۰۱۸، مبلغی قریب ۶/۴ میلیارد یورو تنها در اروپا از طریق رمزارزها پولشویی شده است (لاپوه بله، ۲۰۲۱، ص ۵).

۲-۷-۲. جرایم غیرمستقیم

منظور از «جرایم غیرمستقیم» جرایمی است که در نتیجهٔ جرم دیگری رخ می‌دهد و در حقیقت تأمین مالی جرایم دیگر را پوشش می‌دهد؛ یعنی جرایم در فضای دیگری رخ می‌دهند، اعم از فضای مادی یا مجازی و سپس تأمین مالی آن در بستر مجازی و از طریق رمزارزها شکل می‌گیرد؛ مانند تأمین مالی تروریسم و یا باجگیری. مجرمان از طریق باج‌افزارها اقدام به سرقت اطلاعات قربانی و یا قفل نمودن دستگاه او می‌کنند و سپس در ازای پرداخت مبالغی پول در قالب رمزارز، اقدام به بازنمودن دستگاه یا بازگرداندن اطلاعات وی می‌کنند. یکی از جدیدترین نمونه‌های این اقدام مجرمانه به سرقت رفتن اطلاعات یکی از کاروران (اپراتورهای) خط لوله نفت امریکایی به نام Colonial Pipeline و پرداخت بیت‌کوین به ارزش تقریبی ۵ میلیون دلار توسط آنان به رخنه‌گرها بود.

اقدامات غیرقانونی که در فضای حقیقی و یا مجازی صورت می‌گیرد نیاز به این دارد که منابع مالی آن تأمین و پرداخت شود. فضای مجازی در لایه زیرین خود، دارای سطحی است که می‌تواند میان مجرمان در تمام جرایم ارتباط برقرار نماید که به آن «اینترنت تاریک» گفته می‌شود. پس از ظهور رمزارزها غالب پرداخت‌ها در این فضا از طریق رمزارزها صورت می‌گیرد. بر حسب معمول، وقتی اقدامات مجرمانه انجام می‌شود اگر مابازای آن و یا منابع مالی آن از طریق ارزهای متمرکز انجام شود به سبب شفافیت و نظارت مرکزی، جرایم ردیابی و کشف می‌شوند. اما رمزارزها به واسطه غیرمتمرکز بودن و گمنامی می‌توانند گزینه مناسبی برای تأمین مالی بدون شناسایی و نظارت حاکمیت باشند. برای مثال وبگاه «جاده ابریشم» که یک بازار غیرقانونی در ***دارک نت*** بود و در آن خرید و فروش محصولات غیرقانونی، از جمله مواد مخدر، اسناد جعلی هویت، داده‌های سرقت‌شده و بدافزارها از طریق رمزارزها انجام می‌شد، توسط اداره تحقیقات فدرال امریکا در سال ۲۰۱۲ کشف و بسته شد (سانزباس و دیگران، ۲۰۲۱، ص ۱۱). تخمین زده شده که ۴٫۵ تا ۹ درصد از کل مبادلات بیت‌کوین در آن سال برای تجارت مواد مخدر در جاده ابریشم بوده است (گرشما، ۲۰۱۵، ص ۴).

با وجود ارتکاب جرایم مذکور از طریق رمزارزها، نفس رمزارزها را نمی‌توان جنایتکارانه قلمداد نمود (همان، ص ۲) و با تحلیل صحیح رفتاری مجرمان و علل رغبت آنها به رمزارزها و بستر دیجیتال، می‌توان راهکارهای مناسبی برای جلوگیری و مبارزه با این نوع اقدامات ارائه نمود.

دفتر «مواد مخدر و جنایت» سازمان ملل متحد (UNODC) و «کارگزاری مبارزه با مواد مخدر» ایالات متحده امریکا (DEA) طی پژوهش‌های انجام‌شده دریافتند که گمنامی، سرعت مبادلات، فراملیتی بودن، و ارتباط آسانِ از راه دور در فناوری رمزارزها از جمله علل استقبال مجرمان به منظور استفاده در جرایمی همچون پولشویی، فرار مالیاتی و مانند آن است (سانزباس و دیگران، ۲۰۲۱، ص ۱۲). همچنین در مطالعات دیگری نبودِ نظارت

مرکزی، وضعیت حقوقی نامعلوم (گرشما، ۲۰۱۵، ص ۲) و فقدان قانونگذاری مناسب (لاپوه بله، ۲۰۲۱، ص ۵) ازجمله علل ارتکاب جرایم در این بستر معرفی شده است.

۳. راهکارها

با عنایت به جرایم مذکور و علل ترغیب ارتکاب آن توسط رمزارزها ازیک‌سو و هدف مؤلف از به‌کارگیری رمزارزها در مبادلات بین‌المللی برای برون‌رفت از شرایط تحریمی از سوی دیگر، راهکارهای ذیل پیشنهاد می‌شود:

۳-۱. احراز هویت از طریق واسطه‌گران مجاز

گفته شد که عمده علت انجام جرایم در بستر رمزارزها، گمنامی مجرمان است. برای رفع این معضل، روش‌های احراز هویت به منظور شناسایی مشتریان (KYC) به کمک ما می‌آید. در مبادلات رمزارزی که به طور مستقیم انجام می‌شود، امکان احراز هویت معامله‌کنندگان وجود ندارد، اما وقتی پای واسطه (مانند صرافی) به میان بیاید احراز هویت قابل تحقق است؛ زیرا واسطه‌گران می‌توانند در زمان ثبت‌نام، شرط استفاده از خدمات را احراز هویت اعلام نمایند. بنابراین دولت‌ها می‌توانند با اعطای مجوز به صرافی‌های رمزارزی و الزام قانونی آنها به احراز هویت، زمینه ارتکاب جرم را کاهش دهند؛ همچنان‌که در کشور ژاپن صرافی‌های بیت‌کوین ملزم به شناسایی مشتریان خود شده‌اند (هاینز و یاو، ۲۰۲۰، ص ۲۱).

شناسایی مشتریان (KYC) موضوع جدیدی نیست و سابق بر این هم در ارائه خدمات مالی مدنظر دولت‌ها قرار گرفته و در قوانین وارد شده است که می‌تواند درخصوص رمزارزها هم اعمال گردد؛ همچنان‌که مطابق فصل دوم «آیین‌نامه اجرایی قانون مبارزه با پولشویی»، ارائه‌دهندگان خدمات مالی، همچون مؤسسات مالی موظف به شناسایی مشتریان خود هستند. همچنین در توصیه‌نامه شماره ۱۰ اف. آی. تی. اف. هم به الزام شناسایی کافی مشتریان تصریح شده است (www.cfatf-gafic.org).

۳-۲. نظارت بر معاملات از طریق واسطه‌های مجاز

مطابق قوانین، یکی از راهکارهایی که در جهت جلوگیری از ارتکاب جرایمی همچون پولشویی می‌تواند مؤثر واقع شود، نظارت بر نهادهای ارائه‌دهنده خدمات مالی و الزام آنان به ارائه گزارش است. در رمزارزها نیز می‌توان از این تدابیر کلی بهره برد؛ با این توضیح که با اعطای مجوز به صرافی‌ها آنها را ملزم به رعایت قوانین کنند؛ قوانینی که آنها را موظف می‌نماید معاملات و اطلاعات مربوط به آن را ثبت نموده، از مبدأ و مقصد رمزارزها و وجوه اطمینان حاصل کنند و معاملات مشکوک را به سازمان‌های ذی‌ربط گزارش دهند. اعمال نظارت و الزام به ارائه گزارش، علاوه بر آنکه جنبه پیشگیرانه دارد و ارتکاب جرایم را کاهش می‌دهد، امکان ردیابی و کشف جرم را نیز تسهیل می‌گرداند.

۳-۳. تدوین قوانین

مقدمه دو مطلب مزبور قانونگذاری بموقع و مناسب است تا فضای دیجیتال از دست حاکمیت رها نشود. بدون وجود قانون مناسب، جرایم نه‌تنها کاهش نمی‌یابد، بلکه ارتکاب آن به سبب آنکه فضای دیجیتال بدون صاحب و رها شده، افزایش نیز می‌یابد. قانون مناسب می‌تواند بسترهای وقوع جرایم را از بین ببرد و یا ـ دست‌کم ـ محدود سازد. علاوه بر آن بدون قانونگذاری، روابط صحیح از ناصحیح قابل تشخیص نخواهند بود. وقتی قانونی نباشد صرافی مجاز از غیرمجاز و فعالیت قانونی از غیرقانونی قابل تشخیص نیست و این موضوع علاوه بر اینکه بستر بهتری را برای انجام جرم ایجاد می‌کند، با حمایت نکردن از قربانیان، تبعات سوءاجتماعی و حقوقی بیشتری نیز برای حاکمیت به دنبال خواهد داشت.

۴-۳. استفاده از رمزارزهای متمرکز

بیشتر جرایم در بستر رمزارزهای غیرمتمرکز انجام می‌شود. بنابراین رمزارزهای مشترک و ملی به سبب وجود نظارت مرکزی از این مخاطرات تا حد زیادی در امان هستند. ازاین‌رو می‌توان برای بهره‌گیری از رمزارزها در تحریم، از این نوع آنها بیشتر حمایت و استفاده نمود.

۵-۳. محدود ساختن بهره‌گیری از رمزارزها به تحریم‌های مالی ـ پولی

تا زمان تدوین قوانین مناسب و ایجاد زیرساخت‌های نظارت بر معاملات رمزارزی، می‌توان مشروعیت استفاده از رمزارزها را محدود به معاملات خاص به هدف برون‌رفت تحریم و با نظارت حاکمیت نمود.

۶-۳. الزام به تأمین امنیت در سکوهای واسطه‌گران

گفته شد: مطالعات و گزارش‌ها نشان می‌دهد که بیشتر سرقت‌ها به علت نبود امنیت شبکه صرافی‌ها و یا کیف‌پول‌هاست. بنابراین دولت می‌تواند با الزام این واسطه‌گران به تأمین امنیت لازم در زمان اعطای مجوز و نظارت بر عملکرد آنان، تا حد زیادی از این مخاطرات بکاهد.

۷-۳. آگاهی‌بخشی

بسیاری از کلاهبرداری‌ها و سرقت‌ها در این حوزه به علت ناآگاهی عموم مردم است. حاکمیت می‌تواند با تدابیر لازم به منظور آگاهی‌بخشی، بستر ایجاد ارتکاب جرم از طرف قربانی را برای مجرمان از میان ببرد.

۸-۳. اعطای مجوز عرضه اولیه سکه

در خصوص طرح‌های سرمایه‌گذاری و کلاهبرداری از طریق آن، دولت‌ها می‌توانند با اعطای مجوز و تأییدیه به طرح‌ها، سرمایه‌گذاران را ارشاد کنند تا طرح‌های مورد حمایت و صحیح را از سایران تشخیص دهند.

۹-۳. استفاده از قراردادهای هوشمند

«قراردادهای هوشمند» قراردادهای الکترونیکی هستند که در بستری عمومی مانند «بلاکچین» منعقد می‌گردند و از زمان انعقاد تا تأیید نهایی توسط قوه حاکم و هوش مصنوعی بر آنها نظارت می‌شود و دو طرف و هوش مصنوعی در زمان انعقاد تا نهایی شدن قرارداد، امکان دریافت هرگونه اطلاعات را از معامله یا دو طرف عقد دارند (صادقی و ناصر، ۱۳۹۸).

دو طرف قرارداد برای انعقاد این نوع قراردادها نیازمند برخورداری از کلیدهای خصوصی تخصیص داده‌شده در امضاهای دیجیتالی برای امضای قرارداد هستند و نحوه برخورداری از مجوز استفاده از این نوع امضاها نیازمند شناسایی هویت آنها توسط مراجع ذی‌صلاح و بررسی وضعیت حقوقی و سوابق کیفری آنهاست (همان، ص ۲۵۷).

نتیجه‌گیری

مزایایی همچون آزادی در پرداخت، غیرقابل پایش بودن دارایی، بین‌المللی بودن، وجود سرعت، و امنیت در رمزارزها می‌تواند در وضعیت تحریم مؤثر و کمک‌کننده باشد؛ اما در نقطه مقابل، مخاطراتی نیز وجود دارد که بدون حل آن نمی‌توان انتظار عملکرد مناسب از رمزارزها در حوزه تحریم را داشت. گاهی برخی اوصاف مانند مشخص نبودن هویت ازیک‌سو فرصت و مزیت در فضای تحریم به شمار می‌رود و از سوی دیگر می‌تواند یک تهدید به حساب آید. در این زمینه راهکارهایی ارائه شده است که در حل معایب می‌تواند راهگشا باشد که عمدتاً بر پایه قانون‌گذاری بموقع و مناسب متکی است.

حتی با وجود رفع معایب مذکور نمی‌توان از رمزارزها متوقع معجزه بود. اینکه با استفاده از آنها می‌توان تمام مشکلات ناشی از تحریم را برطرف نمود، نگاهی آرمان‌گرایانه و ناشی از بی‌دقتی در پیچیده و لایه‌لایه بودن تحریم‌ها علیه ایران است. با این وجود، می‌توان انتظار داشت که به‌کارگیری رمزارزها در پرداخت بین‌المللی ـ دست‌کم در کم‌اثر کردن فشارهای حاصل از تحریم ـ مؤثر خواهد بود.

در نتیجه و با عنایت به ابعاد حقوقی مزایا و مخاطرات مذکور در این پژوهش، برای استفاده از رمزارزها به هدف برون‌رفت از تحریم در سه نوع رمزارز بین‌المللی، ملی و مشترک، پیشنهادات ذیل ارائه می‌گردد:

در حوزه رمزارزهای بین‌المللی، تدوین قوانین، رفع ممنوعیت تبادلات رمزارزی ـ دست‌کم ـ در مبادلات بین‌المللی، ایجاد واسطه‌های مجاز (همچون صرافی‌ها)، به‌کارگیری سازوکارهای احراز هویت، الزام به افشای هویت دیجیتالی در قراردادها، و بسترسازی مناسب در حوزه استخراج برای تحصیل رمزارز، از لوازم و مقدماتی است که باید نسبت به آن اقدامات لازم از سوی حاکمیت صورت گیرد.

رمزارزهای ملی کارکردی همچون پول ملی دارند. ازاین‌رو به علت انتسابشان بـه یـک حاکمیـت، مـی‌تواننـد از طرف امریکا و کشورهای غربی تحریم شوند. بنابراین چنانچه قصد استفاده از این نوع رمزارز بـرای دور زدن تحـریم وجود داشته باشد، به نظر می‌رسد توجه به دو موضوع ذیل، مهم است:

الف. چنانچه هدف از طراحی رمزارز ملی مبادله با تمام کشورهاست، اعم از کشورهایی که تمایـل بـه شناسـایی ندارند و یا بعکس کشورهایی که واهمه‌ای از شناسایی و اعمـال تحـریم علیـه خـود بـه واسـطه معاملـه بـا کشـور تحریم‌شده ندارند، سازوکار عملیاتی آن به گونه‌ای طراحی شود که دو طرف آن ناشناس باقی بمانند.

ب. چنانچه هدف صرفاً تسهیل مبادلات با کشورهای منطقه یا کشورهایی است کـه نیـازی بـه پنهـان مانـدن هویت خود و ارتباطشان با کشور تحریم‌شده ندارند (همچون عراق یا روسیه یا چین) که خود نیز تحـریم هسـتند یـا منافع آنها در آشکار بودن روابط است، در این صورت هر رمزارز ملی می‌تواند پاسخگوی این نیاز باشد.

در حوزه تجارت منطقه‌ای، مسئله گمنامی در پرداخت مطرح نیست و هـدف صـرفاً بـه‌کـارگیری روشـی بـرای پرداخت است که مزایایی (همچون سرعت، سهولت، آزادی پرداخت و انجام پرداخت بدون دخالت سایر کشورها) بـه دنبال داشته باشد و بتواند جایگزین ساختارهای بین بانکی شود که در دوران تحریم عمل نمی‌کنند و یا ناقص عمـل می‌کنند. رمزارز مشترک یا منطقه‌ای هدف مذکور را به خوبی فراهم می‌آورد. ازاین‌رو مـی‌تـوان در حـوزه منطقـه‌ای اقدام به رایزنی‌ها و انعقاد توافق‌نامه‌ها و قراردادهایی برای ایجاد یک رمزارز مشترک در میان اعضا نمود.

منابع

ابوبکر، محمد، ۱۳۹۸، «بررسی جامع فقهی بیت‌کوین، ارزهای مجازی دیجیتال و بلاکچین»، ترجمهٔ محمد آذرنیوار، در: https://arzdigital.com/shariah-analysis-of-bitcoin-cryptocurrency-and-blockchain

امامی، سیدحسن، ۱۳۸۶، ***حقوق مدنی***، چ بیست و هفتم، تهران، اسلامیه.

پدرو، فرانکو، ۱۳۹۷، ***مفاهیم بیت‌کوین***، ترجمهٔ حسن مرتضی‌زاده، چ دوم، تهران، مؤسسهٔ کتاب مهربان نشر.

صادقی، حسین و مهدی ناصر، ۱۳۹۸ مهدی، «اعتبارسنجی و چالش‌های حقوقی به‌کارگیری قراردادهای هوشمند: با مطالعه تطبیقی نظام حقوقی ایران و آمریکا»، ***پژوهش حقوق خصوصی***، ش ۲۷، ص ۲۲۵ – ۲۸۸.

صادقی، حسین و مهدی ناصر، ۱۳۹۹، «ارائه چارچوب حقوقی مسئولیت‌پذیری در عملکرد ابزارهای اینترنت اشیاء در بستر دولت الکترونیک؛ تبیین الگوی سیاست‌گذاری مؤثر»، ***سیاستگذاری عمومی***، ش ۳، ص ۸۱ – ۱۰۳.

صمدی گرگانی، محمود و امید شهیر، ۱۳۹۶، «تب بیت‌کوین در ایران و تحلیل آن از دیدگاه مالی، حقوقی و فقه اسلامی»، در: ***اولین همایش ملی پژوهش‌های حسابداری مدیریت با رویکرد کسب و کارهای نوین***، دانشگاه آزاد اسلامی واحد تنکابن.

ضیائی بیگدلی، محمدرضا، ۱۳۸۶، ***حقوق بین‌الملل عمومی***، چ سی‌ام، تهران، گنج دانش.

طغیانی، مهدی و مرتضی درخشانی، ۱۳۹۳، «تحلیل عوامل تأثیرگذاری تحریم‌های اقتصادی بر ایران و راهکارهای مقابله با آن»، ***راهبرد***، ش ۷۳، ص ۱۱۵–۱۴۶.

کاتوزیان، امیرناصر، ۱۳۸۸، ***قواعد عمومی قراردادها***، چ هشتم، تهران، شرکت سهامی انتشار.

نوری، مهدی و علیرضا نواب‌پور، ۱۳۹۷، «مقدمه‌ای بر تنظیم‌گری رمزینه‌ارزها در اقتصاد ایران»، ***گزارشی از دفتر مطالعات اقتصادی مرکز پژوهش‌های مجلس شورای اسلامی***.

Aziz, Atif, 2019, "Cryptocurrency: Evolution and Legal Dimenesion", ***International Journal of Business, Economics and Law***, V. 18, p. 31-33.

Bunjaku, Flamur, Gjorgieva-Trajkovska, Olivera, Miteva-Kacarski, Emilija, 2017, "Cryptocurrency Advantages and Disadvantages", ***Journal of Economics***, V. 2, N. 1, p. 31-39.

Cornel Dumitrescu, Georg, 2017, "Bitcoin–A Brief Analysis of the Advantages and Disadvantages", ***Global Economic Observer***, V. 5, N. 2, p. 63-71.

Countering America's Adversaries Through Sanctions Act (CATSA).

FATF Recommendations، Interpretive Notes to Recommendations 15.

Greeshma, K V, 2015, "Crypto Currencies and Cybercrime", ***International Journal of Engineering and Technical Research***, Available at, www.researchgate.net/publication.

Haynes, Andrew & Peter Yeoh, 2020, ***Cryptocurrency and Cryptoassets: Regulatory and Legal Issues***, New York, Informa Law from Routledge.

Jurik, Pavol, 2021, "Benefits and Drawbacks of Virtual Currency Bitcoin", ***Available at***. www.researchgate.net/publication.

Lapuh Bele, Julija, 2021, "Cryptocurrencies as facilitators of cybercrime", ***SHS Web of Conferences***, Available at, https://doi.org/10.1051/shsconf.

Nagpal, Sushant, 2019, ***Cryptocurrency: The Revolutionary of Future Money***, p. 1-14, available at https://ssrn.com.

Sanz-Bas, David. del Rosal, Carlos, Náñez Alonso, Sergio Luis, Echarte Fernández, Miguel Ángel, 2021, "Cryptocurrencies and Fraudulent Transactions: Risks, Practices، and Legislation for Their Prevention in Europe and Spain", ***MDPI, Available*** at: https://doi.org.