

تحلیل حقوقی ارز دیجیتال و تاثیر آن بر امنیت ملی

احمدعلی ثالث مؤید^۱

سعید سیاه‌بیدی کرمانشاهی^۲

DOR: 20.1001.1.17358671.1399.19.69.3.2

محسن کوهستانی^۳

چکیده

امروزه رشد چشمگیر ارزهای دیجیتال، باعث شده است که توجه زیادی به این پدیده جلب شود. در این میان بررسی حقوقی این مسئله و نحوه سیاست‌گذاری قانون‌گذاران کشورها نیز تبدیل به یکی از دغدغه‌های پژوهشگران این حوزه شده است. یکی از مهم‌ترین مباحث حقوقی در ارتباط با ارزهای دیجیتال، تحلیل ماهیت حقوقی این ارزها و نیز بررسی تأثیر رواج این ارزها بر امنیت ملی کشور است. در این مقاله تلاش شده است ماهیت این ارزها، رویکرد سایر کشورها نسبت به آن‌ها نیز رویکرد قانون‌گذار ایرانی نسبت به آن‌ها تبیین شده و سپس به بررسی این مهم پرداخته شود که رواج این ارزها چه تأثیری بر امنیت ملی کشور خواهد داشت. به نظر می‌رسد رویکرد فعلی کشور ما از حیث عدم قانون‌گذاری در خصوص ارزهای مجازی مشابه کشورهای محتاط بوده و از این حیث که عملاً بانک‌ها و مؤسسات مالی و اعتباری از معامله ارزهای دیجیتال ممنوع نموده است، موضعی مشابه کشور چین اتخاذ نموده است؛ لیکن نبود قانون‌گذاری مناسب در این حوزه راه را برای تأثیرات منفی بر امنیت ملی باز گذاشته است؛ زیرا رواج ارزهای دیجیتال نیازمند آن است که الزامات پایش‌داری‌ها در خصوص آن رعایت شود و عدم رعایت این الزامات موجب آسیب سامانه اقتصادی کشور در نتیجه ارتکاب جرائم پول‌شویی و در معرض خطر تارشگری قرار گرفتن کشور در نتیجه ارتکاب جرم تأمین مالی تارشگری می‌شود.

کلیدواژگان: ارز دیجیتال، بلاک‌چین، رویکرد قانون‌گذار، امنیت ملی، پایش‌داری.

law744330@gmail.com

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه علوم قضایی (نویسنده مسئول)

۲. دانشجوی دکتری حقوق خصوصی دانشگاه تهران

۳. کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه آزاد اسلامی واحد تهران مرکز

۱- مقدمه

رشد چشمگیر به رسمیت شناختن و رواج بیت کوین در سال‌های اخیر، توجه وافری را به کاربردهای بالقوه تمام اشکال ارز دیجیتال جلب کرده است. این توجه باعث می‌شود بحث در مورد مسائل قانونی، مقرراتی و سیاست‌گذاری عمومی در ارتباط با استفاده گسترده از پول‌های مجازی بیشتر شود. در خصوص ماهیت این ارزها و سازوکار آن‌ها تحقیقات متعددی صورت پذیرفته است؛ لیکن یکی از مهم‌ترین پژوهش‌ها در این حوزه، پژوهشی است که با توجه به وضعیت و شرایط خاص هر کشور صورت پذیرد؛ یعنی در هر کشور با توجه به شرایط حاکم بر آن بررسی شود که رویکرد مقنن نسبت به این پدیده چگونه بوده یا چگونه باید باشد؟

پاسخ به پرسش یادشده از جنبه‌های گوناگونی قابل بررسی است. ممکن است برخی به رواج ارزهای دیجیتال به‌عنوان یک فرصت اقتصادی برای کسب ارزش بنگرند؛ درواقع ارزهای دیجیتال را به‌عنوان یک معدن باارزش تصور نمایند که افراد متعددی می‌توانند به‌عنوان معدنچی این ارزها را استخراج نموده و از عواید آن بهره‌مند شوند.

برخی دیگر ممکن است به جنبه‌های شرعی مسئله توجه نمایند و این بحث را از منظر آن‌که آیا استخراج این ارزها و معاملات آن‌ها دارای مشروعیت است یا خیر، مورد بررسی قرار دهند و نیز آیا استخراج این ارزها با فرهنگ کار و تلاش که از آموزه‌های دینی ماست مطابق دارد یا خیر؟

برخی دیگر ممکن است استخراج ارز دیجیتال را آفتی برای انرژی‌های ارزان‌قیمت بدانند؛ توضیح آن‌که در کشور ماکه برق برای رفاه حال مردم و نیز پایین آوردن هزینه‌های تولید به‌صورت ارزان‌تر از قیمت واقعی عرضه می‌شود. حال چنانچه شخصی بخواهد از این برق ارزان‌قیمت برای مقاصد شخصی خود و استخراج ارزهای دیجیتال استفاده نماید با فلسفه ارائه انرژی‌های ارزان‌قیمت در تعارض خواهد بود.^۱ رویکردهای یادشده هرکدام در جای خود شایسته بحث و بررسی هستند، اما یکی از عرصه‌های مهم پژوهش در این حوزه، بررسی تأثیر شیوع ارزهای دیجیتال بر امنیت ملی است. با توجه به اهمیت امنیت ملی در هر کشور و نیز این امر که وجود امنیت در کشور، پیش‌زمینه و لازمه هر فعالیت اقتصادی دیگر است، بحث تأثیر رواج ارزهای دیجیتال بر امنیت ملی نیز دارای اهمیت بیشتری نسبت به سایر مباحث خواهد بود؛ لذا پرسش اساسی این پژوهش آن است که با توجه به ماهیت خاص ارزهای دیجیتال، رواج این ارزها چه تأثیری بر امنیت ملی خواهد داشت؟

لازم به ذکر است که پاسخ پرسش یادشده از جنبه‌های متعددی قابل طرح است، لیکن مقاله حاضر درصدد بررسی حقوقی مسئله و ارائه پاسخ حقوقی به پرسش یادشده است؛ بر این اساس در نوشتار

۱. در حال حاضر، قرار است دولت نرخ برق مصرفی برای ارزهای مجازی را از سایر نرخ‌ها مجزا نموده و به‌صورت نرخ ارز صادراتی محاسبه نماید:
/https://arzdigital.com/export-electricity-prices-for-bitcoin-mining-in-iran

حاضر برای شناخت بهتر ارزهای دیجیتال، در قسمت مبانی نظری پژوهش، به ترتیب ماهیت ارزهای دیجیتال، جایگاه بلاک چین در عملکرد ارز مجازی، رویکرد مقنن کشورها نسبت به ارز دیجیتال و رویکرد مقنن ایران نسبت به ارزها مورد بررسی قرار می گیرد. این مباحث زمینه را برای ورود به بحث تأثیر این ارزها بر امنیت ملی هموار می کند. در قسمت یافته های پژوهش نیز بعد از شناخت جرائم پول شویی و تأمین مالی تارشگری، با توجه به نظریه تأثیر پایش دارایی ها بر پایش جرم، به بررسی تأثیر رواج ارزهای دیجیتال بر جرائم پول شویی و تأمین مالی تارشگری پرداخته شده و از این منظر تأثیر رواج این ارزها بر امنیت ملی مورد بررسی قرار می گیرد.

۲- مبانی نظری پژوهش

در این قسمت مباحثی مطرح می شوند که شناخت آن ها لازمه ورود به بحث اصلی بوده و به عنوان طرح مباحث اصلی را هموار می سازد. مبانی نظری پژوهش حاضر به شرح زیر قابل طرح و بررسی است.

۲-۱- ماهیت ارز دیجیتال

در خصوص مفهوم «ارز دیجیتال»^۱ قدری ابهام وجود دارد. برخی معتقدند که ارزهای دیجیتال اغلب به عنوان ارزهای مجازی نیز شناخته می شوند (Matsuura, 2016: 3)؛ لیکن باید دانست که «ارز دیجیتال» یک مفهوم گسترده است. در تعریف ارز دیجیتال گفته اند که ارز دیجیتال، حالت غیر ملموس ارز و به شکل الکترونیکی است که می تواند میان طرفین از طریق استفاده از فناوری های فعلی نظیر رایانه، اینترنت و تلفن های هوشمند جابه جا شود (Girasa, 2018: 9). مطابق این تعریف تمامی ارزهایی که در فضای حقیقی وجود خارجی ندارند ولی در فضای الکترونیکی ایجاد و منتقل می شوند داخل در تعریف ارز دیجیتال هستند؛ لذا ارزهای مجازی^۲ و رمزارزها^۳ نیز ارز دیجیتال محسوب می شوند. ارزهای مجازی دارای یک تعریف پذیرفته شده جهانی نیستند. (Rothchild, 2016: 39) با وجود این در تعریف آن ها گفته اند که ارز مجازی، نمود دیجیتالی^۴ ارزشی است که از سوی دولت یا بانک مرکزی ایجاد نشده است و می تواند به صورت دیجیتالی معامله شوند و به عنوان (۱) ابزار مبادله؛^۵ (۲) واحد محاسبه^۶ و یا (۳) ذخیره ارزش^۷ عمل می کنند (Girasa, 2018: 9). گونه دیگری از ارزهای که زیرمجموعه ارزهای دیجیتال محسوب می شوند (Lee Kuo Chuen, 2015: 8) عبارت اند از رمزارزها و مشهورترین آن ها بیت کوین^۸ است. این ارزها بر اساس فناوری رمزنگاری عمل می کنند.

ارزهای دیجیتال مبتنی بر الگوریتم های ریاضی هستند. این الگوریتم ها در قلب ارزهای دیجیتال قرار دارند

1. Digital currencies.
2. Virtual currencies.
3. Cryptocurrencies
4. Digital representation.
5. Medium of exchange.
6. Unit of account.
7. Store of value.
8. Bitcoin.

و به نرم‌افزار منبع باز^۱ متصل می‌شوند که برای همه شرکت‌کنندگان در جامعه ارز دیجیتال قابل دسترسی است. فعالیت‌های حساس در سامانه ارز دیجیتال مانند ایجاد ارز و اعتبارسنجی معاملات، درواقع از طریق فرایند توسعه راه‌حل‌های پازل‌های ریاضی بسیار پیچیده انجام می‌شود. به‌عنوان مثال در شبکه بیت کوین، کاربران، نرم‌افزار مجانی که همان نرم‌افزار مشتری بیت کوین است را بارگیری (دانلود) می‌کنند و آن را بر روی کامپیوتر خود نصب می‌کنند. نرم‌افزار مشتری بیت کوین به‌عنوان یک کیف پول^۲ و با سامانه ذخیره‌سازی برای بیت کوین عمل می‌کند و قابلیت رمزنگاری و امضای دیجیتال مورد نیاز برای شرکت در سامانه بیت کوین را فراهم می‌کند (Matsuura, 2016: 3-4).

سامانه عامل‌های امن ارز مجازی مانند بیت کوین که مبتنی بر رمزنگاری هستند، کاملاً وابسته به سامانه اصلی (کلیدی) رمزنگاری عمومی و خصوصی‌اند. این قابلیت رمزنگاری و تأیید نیز با نرم‌افزار سرویس‌گیرنده (مشتری) که بر روی رایانه‌هایشان نصب شده یکپارچه شده است. برای بیت کوین، کلیدهای عمومی تولیدشده برای اعضای جامعه مشتمل بر ردیف‌هایی از کاراکترهای الفبایی و عددی هستند که اصولاً طول آن‌ها بین ۲۴ تا ۳۷ حرف است. کلیدهای خصوصی بیت کوین نیز ردیف‌هایی از کاراکترهای الفبایی و عددی است که به‌صورت تصادفی تولیدشده و طول آن‌ها ۶۴ کاراکتر است. کاربران می‌توانند چندین کلید عمومی ایجاد کنند و برای هر کلید عمومی یک کلید اختصاصی مرتبط نیز ایجاد می‌شود. کلیدهای عمومی به‌راحتی در دسترس سایر کاربران سامانه است. آن‌ها درواقع، حساب‌های ارز دیجیتالی قابل شناسایی برای کاربران محسوب می‌شوند. هر کلید خصوصی از لحاظ ریاضی مرتبط با یک کلید عمومی است. کلیدهای خصوصی برای هیچ شخصی غیر از صاحب حساب در دسترس نیست. کلیدهای خصوصی برای تأیید هویت صاحب حساب قبل از انجام مبادله ارز دیجیتال ضروری هستند. کلیدهای خصوصی در اصل همان ارز دیجیتال است؛ زیرا دسترسی به این کلیدها دسترسی به تمام ارزهای مرتبط با آن حساب کاربری خاص را فراهم می‌کند (Matsuura, 2016: 4). در استفاده از نرم‌افزار دانلود شده مشتری، یک کاربر بیت کوین باید میزان ارز مورد انتقال و نیز دریافت‌کننده آن را مشخص نماید. کاربر همچنین باید هویت خود را تأیید نماید و از طریق امضای دیجیتال، انجام معامله را تأیید نماید. تمام این مراحل برای انجام معاملات پردازش شده توسط نرم‌افزار مشتری لازم است. کلید خصوصی کاربر برای دسترسی به کیف پول امن که در آن بیت کوین‌های کاربر ذخیره می‌شود، مورد نیاز است. استفاده از کلید خصوصی امضای دیجیتالی لازم برای تأیید معامله را فراهم می‌کند. در سامانه‌های ارزی مجازی، امنیت کلید خصوصی ضروری است، زیرا این روش تأیید هویت کاربر و مجوز انجام تمام معاملات است. شخصی که کلید خصوصی مربوط به حساب ارز دیجیتال را دارد پایش کامل آن حساب را دارد (Matsuura, 2016: 4).

1. Open source software.
 2. Wallet.

۲-۲- جایگاه بلاک چین^۱ در عملکرد ارز مجازی

بیت کوین و سایر سامانه عامل‌های مجازی مبتنی بر رمزنگاری، از یک دفترچه «بلاک چین» برای ثبت و تأیید همه معاملات استفاده می‌کنند. بلاک چین، رشته‌ای از بلوک‌ها است که سوابق کامل معاملات را مانند یک دفتر کل عمومی نگهداری می‌کند (Lee Kuo Chuen, 2015: 49). درواقع بلاک چین، مستندسازی (بایگانی سوابق) همه معاملات مربوط به ارز دیجیتال است. سابقه معامله یا اسنادی که در بلاک چین موجود است، کامل، غیرقابل تغییر و قابل دسترسی برای همه کاربران این سامانه عامل است. این اطلاعات، به ترتیب زمانی، یک سابقه کامل از طرفین معامله، مقدار ارز دیجیتال پردازش شده در هر معامله و همچنین زمان و تاریخ هر معامله است. اطلاعات موجود در بلاک چین برای پردازش تمام معاملات و برای اطمینان از یکپارچگی پایدار سامانه ارز استفاده می‌شود. هر مرتبه که معامله ارز دیجیتال (تأیید) شود، جزئیات آن معامله به بلاک چین اعلام می‌گردد. جزئیات مربوط به هر معامله عبارت‌اند از آدرس عمومی صاحب قبلی ارزی که در حال حاضر منتقل می‌شود (آدرس عمومی منتقل کننده ارز به شخصی که اکنون معامله فعلی را تأیید می‌کند)، مقدار ارزی که در حال حاضر ارسال می‌شود و آدرس عمومی گیرنده پیشنهادی. هنگامی که اطلاعات معامله به بلاک چین منتقل می‌شود، معامله برای مدت زمان کوتاهی در انتظار باقی ماند؛ زیرا بلاک چین، پردازش اطلاعات معامله و در نهایت معامله را تأیید می‌کند. برای معاملات بیت کوین، معمولاً فقط چند دقیقه طول می‌کشد تا تأیید دریافت شود. تأیید معامله درواقع فرایندی است که توسط آن شرکت کنندگان در شبکه، به صورت ریاضی بررسی می‌کنند که ارز مربوط به معامله پیشنهادی درواقع متعلق به طرف درخواست کننده معامله است و قبلاً به شخص دیگری منتقل نشده است (Matsuura, 2016: 4-5).

۲-۳- رویکرد مقنن کشورها نسبت به ارز دیجیتال

کشورها به طور کلی سه رویکرد نسبت به ارز دیجیتال اتخاذ نموده‌اند، برخی از کشورها رویکرد محتاطانه اتخاذ نموده‌اند، برخی کشورها استفاده از این ارزها را ممنوع ساخته‌اند و برخی دیگر رویکرد سهل گیرانه با هدف توسعه این فناوری‌ها را در پیش گرفته‌اند.

۲-۳-۱- احتیاط در استفاده از ارزهای دیجیتال

برخی کشورها نظیر بلژیک در ارتباط با سامانه‌های ارز مجازی محتاط باقی مانده‌اند. به نظر می‌رسد که در حال حاضر اکثریت دولت‌ها در سراسر جهان موضع ایستادن و تماشا کردن را اتخاذ کرده‌اند؛ موضعی مشابه بلژیک. به نظر می‌رسد اتخاذ موضع ایستادن و تماشا کردن تا اندازه زیادی ناشی از عدم توانایی این دولت‌ها در پایش مستقیم ایجاد و استفاده از ارز مجازی است. سامانه‌های ارز دیجیتال مانند بیت کوین سامانه‌های خصوصی هستند که بر اساس توافق دوجانبه و رضایت طرف‌های دخیل عمل می‌کنند.

1. Blockchain.

اعمال پایش بر این سامانه‌های خصوصی برای دولت‌ها بسیار دشوار است (Matsuura, 2016: 7).

۲-۳-۲- تسهیل توسعه سامانه‌های ارزی دیجیتال

در ایالات متحده آمریکا، مرکز درآمدهای داخلی این کشور که در زمینه امور مالیاتی مقررات‌گذار محسوب می‌شود، بیت‌کوین را یک مایملک و دارایی تلقی و قوانین و مقررات مربوط به دارایی را بر آن حاکم می‌داند؛ در نتیجه در این کشور استفاده از بیت‌کوین برای مقاصد قانونی مانند خرید و فروش و مبادله با دلار برای کاربران آزاد است؛ با این حال بر تولیدکنندگان، مبادله‌کنندگان و کسب‌وکارهای مرتبط با بیت‌کوین قوانین بسیار دقیقی اعمال می‌گردد (معاونت پژوهش‌های زیربنایی و امور تولیدی مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۳: ۲).

برخی از کشورها در حال تغییر چارچوب قانونی و مقرراتی خود برای تسهیل توسعه سامانه‌های ارزی دیجیتال هستند. برای نمونه، این قسم تلاش‌ها در برزیل در حال انجام است. در سال ۲۰۱۳، دولت برزیل قانونی را تصویب کرد که راه را برای افزایش استفاده از ارزهای دیجیتال و دیگر اشکال پرداخت‌های الکترونیکی و موبایلی هموار نمود. قانون مزبور ایجاد ارزهای الکترونیکی را مجاز نمود و ارزهای الکترونیکی را به‌عنوان منابعی معرفی نمود که بر روی یک دستگاه یا یک سامانه الکترونیکی ذخیره شده و کاربران نحایی را قادر می‌سازد که عملیات پرداخت را انجام دهند. این قانون و مجوزهای مربوطه بر ارزهای دیجیتال مانند بیت‌کوین و طیف وسیعی از دیگر سامانه‌های پرداخت الکترونیکی و موبایلی اعمال می‌شود (Matsuura, 2016: 7).

قانون‌گذاری برزیل در مورد ارز دیجیتال از حیث تعریفی که از ارز الکترونیک ارائه نموده نیز قابل توجه است. قانون برزیل تعریف به‌ظاهر گسترده‌ای از ارز دیجیتال را پذیرفته است که قلمرو قانون را به نحو قابل توجهی گسترده کرده است. برزیل ارز دیجیتالی را به گونه‌ای تعریف کرده که شامل سامانه‌های مبتنی بر رمزنگاری مانند بیت‌کوین و طیفی از سامانه‌های دیجیتال فعلی می‌گردد. علاوه بر این، در طبقه‌بندی ارز دیجیتال، قانون برزیل اساساً شامل تمام سامانه‌های پرداخت است که از ارتباطات دیجیتال و دستگاه‌ها و شبکه‌های پردازش اطلاعات استفاده می‌کند. دامنه کاربرد قانون برزیل گسترده است. دولت برزیل اساساً طیف گسترده‌ای از سامانه‌های پرداخت الکترونیکی را به‌عنوان ارز الکترونیکی دسته‌بندی می‌کند. این رویکرد گسترده برای نظارت بر ارز دیجیتال می‌تواند در آینده تأثیر قابل توجهی داشته باشد (Matsuura, 2016: 8).

مطابق قانون بانکداری آلمان (KWG) بیت‌کوین، اگرچه یک واحد پرداخت و واحد ارزش است و از این جهت مشابه ارز است؛ لیکن ارز محسوب نمی‌گردد؛ زیرا از لحاظ قانونی، وسیله پرداخت به حساب نمی‌آید (معاونت پژوهش‌های زیربنایی و امور تولیدی مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۳: ۴).

۲-۳-۳- ایجاد محدودیت در استفاده از ارزهای دیجیتال

یک نمونه از دولت‌هایی که در حال حاضر استفاده از ارز دیجیتال را به شدت محدود کرده، دولت چین است. مقامات چینی، بیت کوین و دیگر ارزهای دیجیتال را به جای ارز، به عنوان «کالاها مجازی»^۱ توصیف می‌کنند (Matsuura, 2016: 9) و از این جهت رویکرد آن‌ها تا اندازه‌ای مشابه رویکرد ایالات متحده آمریکا است (معاونت پژوهش‌های زیربنایی و امور تولیدی مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۳: ۲). در چین، بانک‌ها و دیگر مؤسسات پرداخت از معامله در بیت کوین و دیگر ارزهای دیجیتال منع شده‌اند. آن‌ها از خرید یا فروش ارزهای دیجیتال منع شده‌اند. آن‌ها همچنین از پذیرش یا استفاده از ارز دیجیتال به عنوان وسیله پرداخت برای کالاها یا خدمات منع شده‌اند. بانک‌ها و مؤسسات پرداخت در چین همچنین از تبدیل بیت کوین و دیگر ارزهای دیجیتال به ارزهای سنتی منع شده‌اند. این رویکرد مقررات‌گذاری در چین، نوعی مقررات‌گذاری غیرمستقیم برای دولت‌ها را نشان می‌دهد. بعضی از دولت‌ها به جای اینکه مستقیماً ایجاد، توزیع و استفاده از ارزهای مجازی را ممنوع کنند، استفاده یا پذیرش این ارزها توسط مؤسسات کلیدی تحت نظارت نظیر بانک‌ها و سایر ارائه‌دهندگان خدمات مالی را ممنوع کرده‌اند. به این ترتیب، توسعه و استفاده از ارزهای مجازی بدون نیاز به اقدام قانونی برای ممنوعیت ارزهای دیجیتال محدود شده است (Matsuura, 2016: 9).

۲-۴- رویکرد مقنن ایران نسبت به ارز دیجیتال

در خصوص ارزهای دیجیتال قوانین یا مقررات خاصی در کشور به تصویب نرسیده است؛ لذا برای بررسی قواعد حاکم بر آن باید به قواعد عمومی رجوع کرد.

این ارزها با توجه به آن‌که فاقد جنبه فیزیکی هستند و وجود و اعتبار آن‌ها در فضای مجازی محقق می‌شوند از جنس «داده‌پیام» هستند. مطابق بند «الف» ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲: داده‌پیام (Data Message): هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و با فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود؛ نظر به آن‌که این ارزها از جنس داده‌پیام هستند از حیث نقل و انتقال و مبادله اطلاعات تابع قانون تجارت الکترونیک هستند، مطابق ماده ۱ قانون تجارت الکترونیکی: «این قانون مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطه‌های الکترونیکی و با استفاده از سامانه‌های ارتباطی جدید به کار می‌رود.»

در نظام حقوقی ما تنها در یک قانون، به تعریف ارز اشاره شده است. در قانون مبارزه با قاچاق کالا و ارز مصوب ۱۳۹۲ واژه ارز به نحوی تعریف شده که شامل ارزهای مجازی نیز می‌شود. مطابق بند «پ» ماده ۱ «قانون مبارزه با قاچاق کالا و ارز» ارز عبارت است از: «ارز رایج کشورهای خارجی، اعم از

1. Virtual commodities.

اسکناس، مسکوکات،^۱ حوالجات ارزی و سایر اسناد مکتوب یا الکترونیکی است که در مبادلات مالی کاربرد دارد.»

از میان موارد یادشده در این بند عبارت «سایر اسناد مکتوب یا الکترونیکی...» که در مبادلات مالی کاربرد دارد» نیازمند توضیح بیشتری است. همان‌طور که بیان شد به نظر می‌رسد مراد از اسناد مکتوبی که در مبادلات مالی کاربرد دارد اسنادی نظیر چک، برات و سفته است. لیکن در باب اینکه مراد از اسناد الکترونیکی دارای کاربرد در مبادلات مالی چیست و چگونه می‌توان قاچاق این اسناد را تصور نمود، محل بحث است.

به نظر می‌رسد این اسناد باید به گونه‌ای باشند که ارزش مادی آن‌ها در خود سند متجلی باشد و درواقع به‌نوعی سند در وجه حامل الکترونیکی باشند تا نقل و انتقال این سند را بتوان نقل و انتقال ارز دانست؛ زیرا اگر غیرازاین باشد و استفاده از این داده‌های الکترونیکی صرفاً به‌منزله یک دستور پرداخت به بانک باشد که مبالغ معین ارز را از یک حساب به حساب دیگر منتقل نماید، موضوع تابع بحث حواله‌های ارزی خواهد بود و این داده‌های الکترونیکی موضوعیت نخواهند داشت. لذا آنچه در حال حاضر به‌عنوان چک الکترونیکی و یا مستر کارت^۲ (دبیت کارت^۳ یا کردیت کارت^۴) شناخته می‌شود نمی‌تواند ارز موضوع بند «پ» ماده ۱ «قانون مبارزه با قاچاق کالا و ارز» محسوب گردد. با لحاظ مطالب پیش‌گفته می‌توان بتوان بیت‌کوین^۵ را به‌عنوان مصداقی برای اسناد الکترونیکی دارای کاربرد در مبادلات مالی، معرفی نمود (سیاه‌بیدی کرمانشاهی و همکاران، ۱۳۹۶: ۱۴۳-۱۴۴)؛ لیکن باز هم مشمول تعریف قانونی ارز نخواهد بود؛ زیرا شرط دیگر ارز محسوب شدن بیت‌کوین این است که پول رایج کشورهای خارجی باشد و ازآنجا که در حال حاضر بیت‌کوین پول رایج هیچ کشوری محسوب نمی‌گردد، مشمول تعریف ارز در قانون ما نمی‌گردد و طبعاً ضمانت‌نامه قانون مبارزه با قاچاق کالا و ارز در خصوص آن اعمال نمی‌گردد. در میان صاحب‌نظران کشور ما پدیده ارز مجازی از جنبه‌های مختلفی بررسی شده است؛ به‌عنوان مثال آیا ارز مجازی کالا است یا ارز؟ آیا مالیت دارد یا خیر؟ آیا خصوصی بودن ارز مجازی و نبود دخالت دولت در آن در مشروعیت با عدم مشروعیت آن تأثیری دارد یا خیر؟ (ناصری مقدم، ۱۳۹۶: ۱۲؛ سلیمانی‌پور، ۱۳۹۶: ۱۶۷-۱۹۲؛ میرزاخانی، ۱۳۹۶: ۳۱-۴۲).

لیکن باید توجه داشت که پرداختن به این مسائل خارج از موضوع مقاله حاضر است و در مقاله حاضر باید رویکردی تقنینی و مقرراتی کشور در خصوص پدیده ارزهای مجازی مورد بررسی قرار گیرد.

بیان شد که در خصوص ارزهای مجازی به‌طور خاص قانون یا مقرره‌ای در کشور ما وجود ندارد؛ لیکن

۱. نظریه مشورتنی شماره ۷/۹۳/۲۳۸ مؤرخ ۱۳۹۳/۲/۹ اداره کل حقوقی قوه قضائیه: «با توجه به بند «پ» ماده ۱ قانون مبارزه با قاچاق کالا و ارز مصوب ۱۳۹۲/۱۰/۳، مسکوکات خارجی که در مبادلات مالی کاربرد دارد، می‌تواند مشمول تعریف ارز باشد.»

2. Master card
3. Debit card
4. Credit card
5. Bitcoin

به گزارش روابط عمومی بانک مرکزی در جلسه سیام شورای عالی مبارزه با پولشویی در تاریخ ۹ دی ماه ۱۳۹۶، «به کارگیری ابزار بیت کوین و سایر ارزهای مجازی در تمام مراکز ارزی و مالی کشور ممنوع اعلام شد. از آنجایی که انواع ارزهای مجازی از این قابلیت برخوردار هستند که به ابزاری برای پولشویی و تأمین مالی تارشگری و به طور کل، جابه جایی منابع ارزی مجرمان بدل شوند، حوزه نظارت بانک مرکزی برای پیشگیری از وقوع جرائم از طریق ارزهای مجازی، موضوع ممنوعیت به کارگیری ارزهای مجازی را به بانکها ابلاغ کرده است؛ از این رو، با توجه به اهمیت موضوع، تمام شعب و واحدهای تابعه بانکها و مؤسسات اعتباری و صرافیها باید از انجام هرگونه خریدوفروش ارزهای یادشده و با انجام هرگونه اقدامی که به تسهیل و یا ترویج ارزهای یادشده بینجامد، به طور جد اجتناب کنند. همچنین لازم به ذکر است با متخلفین، برابر قوانین و مقررات مربوط برخورد خواهد شد.» (<https://www.cbi.ir/showitem/17722.aspx>).

به نظر می رسد رویکرد فعلی کشور ما از حیث عدم قانون گذاری در خصوص ارزهای مجازی مشابه کشورهای محتاط نظیر بلژیک است؛ لیکن از این حیث که عملاً بانکها و مؤسسات مالی و اعتباری از معامله ارزهای دیجیتال ممنوع نموده است، موضعی مشابه کشور چین اتخاذ نموده است.

۳- روش شناسی پژوهش

تحقیق پیش رو را باید پژوهشی تبیینی دانست که مبتنی بر روش تحلیلی - توصیفی صورت گرفته است. بر این اساس این تحقیق به بررسی و تحلیل حقوقی ارزهای دیجیتال با تأکید بر آثار آن ها بر امنیت ملی می پردازد که متناسب با این موضوع اطلاعات مورد نیاز با ابزار کتابخانه ای گردآوری شده است.

۴- یافته های پژوهش

امنیت ملی از مفاهیمی است که ابعاد گسترده ای دارد. به طور سنتی قدرت نظامی به عنوان تنها شاخص امنیت ملی مطرح می شود و تهدیدات خارجی تنها عاملی است که امنیت ملی را مخدوش می سازد. (Nwanegbo & Odigbo, 2013) اما در حال حاضر، شاخص امنیت ملی، منحصر در حوزه نظامی نمی شود و زمینه های اجتماعی و اقتصادی را نیز در برمی گیرد. (Okechukwu & Anyadike, 2013) در یک تعریف وسیع از امنیت ملی این مفهوم با امنیت انسان مترادف شده است. (Pogson, 2013) بنابراین مشاهده می شود که شاخص های متعددی وجود دارد که بر اساس آن ها سطح امنیت ملی سنجیده می شود. یکی از مهم ترین این شاخص ها، شاخص میزان جرائم ارتكابی یافته در قلمرو یک کشور است. شاخص جرائم ارتباط مستقیمی با امنیت ملی دارد، به این صورت که هرچه میزان جرائم ارتكابی یافته در یک سرزمین بیشتر باشد، امنیت ملی آن سرزمین بیشتر در معرض خطر قرار گرفته یا به عبارتی سطح امنیت ملی آن سرزمین کاهش می یابد. در این میان سهم جرائم خشونت بار بیشتر از

سایر جرائم، مؤثر در سنجش میزان امنیت ملی است. یکی از مهم‌ترین نظریات جرم‌شناسی که در حال حاضر مبنای عمل برخی نهادهای داخلی و بین‌المللی نیز قرار گرفته است، پایش دارایی‌ها است. در جرائم مالی پایش دارایی‌ها مانع بهره‌برداری مرتکب از سود حاصل از جرم می‌شود و در جرائم خشونت‌بار ابزار ارتکاب جرم را از مرتکبان آن سلب نموده در حقیقت موجب خلع سلاح شدن مرتکبین این جرائم می‌شود.

صرف‌نظر از بحث بنیادین در خصوص اینکه این نظریه تا چه حد می‌تواند موجب پایش جرم شود، با پذیرش و تکیه بر آثار این نظریه، تأثیر ارزهای مجازی به‌عنوان یک نوع از دارایی بر امنیت ملی مورد بررسی قرار می‌گیرند.

به‌طور خلاصه پیش‌فرض‌های این پژوهش عبارت است از اینکه پایش دارایی‌ها موجب پایش جرم و پایش جرم موجب افزایش سطح یکی از شاخص‌های امنیت ملی می‌شود.

به‌منظور پایش دارایی‌ها، سامانه اقتصادی جامعه باید در قبال پول‌شویی و تأمین مالی تارشرگی ایمن شود. ایمن شدن سامانه اقتصادی جامعه در قبال این جرائم در گرو سلسله اقدامات کیفری و غیر کیفری است. بر این اساس ابتدا باید جرم پول‌شویی و تأمین مالی تارشرگی را شناخت و سپس باید الزاماتی که موجب افزایش ایمنی سامانه اقتصادی جامعه در قبال جرائم مالی و خشونت‌بار می‌شود را بررسی کرد. بر همین اساس در ادامه رابطه ارزهای مجازی با الزامات مبارزه با پول‌شویی و تأمین مالی تارشرگی بررسی می‌شود.

نکته‌ای که قبل از آغاز بحث باید بدان توجه نمود آن است که نباید تمام الزامات به شکل یکسان در همه زمینه‌های اقتصادی به کار گرفته شود؛ بلکه باید ابتدا خطر هر حوزه و تعاملات کاری مربوط به آن سنجیده شده و الزامات ضد پول‌شویی و تأمین مالی تارشرگی به نسبت آن اعمال شود. دو فاکتور تهدید و آسیب‌پذیری ازجمله عواملی است که برای سنجش خطر از آن استفاده می‌شود.

تهدید	H	M	M	MH	H	H
	MH	M	M	MH	MH	H
	M	ML	M	M	MH	MH
	ML	ML	ML	M	M	M
	L	L	ML	ML	M	M
		L	ML	M	MH	H
آسیب‌پذیری						

چنانچه وضعیت حوزه و تعاملات کاری مربوط به آن در وضعیت H یعنی سطح بالای تهدید و آسیب‌پذیری وجود داشت، الزامات باید به‌صورت حداکثری اعمال شود و بالعکس چنانچه وضعیت در

حالت L یعنی سطح پایین تهدید و آسیب پذیری وجود داشت الزامات به صورت حداقلی اعمال می شود.

۴-۱- شناخت جرائم مؤثر بر امنیت ملی

اگرچه در سنجش شاخص ارتکاب جرائم به عنوان یکی از شاخص های امنیت ملی تمام جرائم مدنظر قرار می گیرد اما مرتبط ترین جرائم به بحث ارز دیجیتال عبارت از جرم پول شویی به عنوان مهم ترین تهدید علیه اقتصاد کشور و جرم تأمین مالی تارشگری به عنوان مهم ترین تهدید علیه تمامیت جسمانی ساکنان یک کشور است.

۴-۱-۱- جرم پول شویی

پول شویی برگردان فارسی ترکیب «Money Laundering» است؛ این تعبیر، مرکب از دو واژه «Money» به معنی پول و «Laundering» به معنی شست و شو یا تطهیر است که جمع آن ها را می توان «تطهیر پول» نامید. در باب وجه تسمیه این عملیات باید گفت همان طور که اشاره شد اصولاً پول یا درآمد در یک تقسیم بندی به پول پاک یعنی پول ناشی از اعمال مشروع و طرق قانونی و پول ناپاک، یعنی پول ناشی از اعمال خلاف قانون تقسیم می شود. درجایی که شخصی بخواهد پول ناشی از اعمال خلاف قانون را به عنوان پول پاک معرفی نماید و منشأ غیرقانونی آن را مخفی نمایند، عمل وی را پول شویی می نامند. به تعبیر برخی «دلیل انتخاب واژه پول شویی برای این عمل، آن است که این روند مثل یک رخت شوی خانه یا ماشین لباس شویی که چرک و کثافت را از لباس ها جدا می کند، با جدا کردن کثافات ناشی از جرم، آن را پاک می کند.» (میرمحمد صادقی، ۱۳۹۵: ۳۳۳)

معنای اصطلاحی پول شویی از معنای لغوی آن دور نیفتاده است. در خصوص تبیین مفهوم این فرایند، تعاریف گوناگونی مطرح شده است که در ادامه به برخی از آن ها اشاره می شود.

برخی معتقدند پول شویی عبارت است از تبدیل عواید مجرمانه به دارایی هایی که ردیابی آن ها به جرم مبنا ممکن نیست. (Reuter, 2004:1)

همچنین آمده است پول شویی به طور مرسوم به سه مرحله تقسیم می شود: جای گذاری وجوه ناشی از عمل غیرقانونی، لایه گذاری وجوه مزبور به وسیله جابه جایی آن ها میان بسیاری از نهادها و حوزه ها برای پنهان کردن منبع آن ها و ادغام وجوه مزبور در اقتصاد که مشروع به نظر برسد. (Ibid:3)

نویسنده کتاب حقوق جزای بین الملل بیان می دارد: «منظور از تطهیر مال، مخفی کردن منبع اصلی اموال ناشی از جرم و تبدیل آن ها به اموال پاک است به طوری که یافتن منبع اصلی مال غیرممکن یا بسیار دشوار گردد.» (میرمحمد صادقی، ۱۳۹۵: ۳۳۲)

برخی دیگر گفته اند: «پول شویی فرایندی است که به موجب آن فرد علماً و به قصد رهایی از عواقب رفتار مجرمانه، منبع اصلی درآمدهای حاصل از اعمال مجرمانه را مخفی نگه داشته و به این درآمدها جلوه ای پاک

و حاصل از اعمال قانونی می‌بخشد.» (باقرزاده، ۱۳۹۴: ۳۱) برخی نیز معتقدند: «پول‌شویی یک رشته اقداماتی است که به‌منظور پنهان ساختن منشأ نامشروع یا تغییر ماهیت غیرقانونی درآمدهای حاصل از جرائم سازمان‌یافته فراملی و تبدیل آن به سرمایه و دارایی به‌ظاهر قانونی صورت می‌گیرد.» (ولیدی، ۱۳۹۴: ۲۶۵)

تعریف قانونی جرم پول‌شویی عبارت است از: «تحصیل، تملک، نگهداری، استفاده، تبدیل، مبادله یا انتقال عواید حاصل از جرم یا اخفا یا پنهان کردن یا کتمان کردن ماهیت واقعی، منشأ، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عواید حاصل از جرم».

تعریف جرم پول‌شویی در حقوق ایران تا حد زیادی برگرفته از اسناد بین‌المللی است. مطابق توصیه شماره ۳ گروه ویژه اقدام مالی (FATF): «کشورها باید بر مبنای کنوانسیون وین^۱ و کنوانسیون پالرمو^۲ پول‌شویی را جرم‌انگاری کنند. کشورها باید جرم پول‌شویی را به همه جرائم شدید تسری دهند با این هدف که دامنه وسیع‌تری از جرائم منشأ را در برگیرد.» (زارع قاجاری، ۱۳۹۲: ۲۱)

تعاریف جرم پول‌شویی به‌وضوح نشان می‌دهد که هدف از جرم‌انگاری آن جلوگیری از بهره‌برداری مرتکبان جرائم مالی از سود به‌دست‌آمده از جرم و به‌تبع خنثی شدن آثار اقتصادی جرم اصلی از یک‌طرف و کاهش وقوع این نوع از جرائم از طرف دیگر است.

۴-۱-۲- جرم تأمین مالی تارشرگی

ارائه تعریف واحدی که جامع همه مصادیق مفهوم تارشرگی باشد، بسیار مشکل به نظر می‌رسد؛ زیرا «آن شخص که از نظر یک شخص تروریست محسوب می‌شود، از نظر دیگری یک مبارز راه آزادی است.»^۳ در قوانین آمریکا، اقدامات تروریستی به معنی «تشکیل، معاونت یا مشارکت در یک عمل خشونت‌آمیز غیرموجه یا بی‌پروایانه با بی‌تفاوتی کامل نسبت به خطر کشتن یا ایراد صدمه شدید جسمانی به کسانی که در مخاصمات مسلحانه شرکت ندارند» دانسته شده است. (میرمحمد صادقی، ۱۳۹۴: ۱۵۸) در حقوق داخلی تا قبل از تصویب «قانون الحاق دولت جمهوری اسلامی ایران به کنوانسیون سازمان کنفرانس اسلامی جهت مبارزه با تارشرگی بین‌المللی» مصوب ۱۳۸۷، تعریفی از «تارشرگی» به عمل نیامده بود؛ لیکن با تصویب این قانون، گزاره‌های جدیدی وارد نظام حقوقی داخلی شد و بر غنای آن افزود. مطابق بند دو ماده یک این کنوانسیون: «اصطلاح «تارشرگی» به هرگونه عمل خشونت‌آمیز یا تهدیدکننده اطلاق می‌شود که علی‌رغم مقاصد یا انگیزه‌اش به‌منظور اجرای طرح جنایی فردی یا گروهی که با هدف ایجاد رعب بین مردم یا تهدید به آسیب‌رساندن یا به خطر انداختن جان، حیثیت، آزادی‌ها، امنیت یا حقوق آنان، یا به خطر انداختن محیط زیست یا هرگونه تأسیسات یا اموال

۱. کنوانسیون ملل متحد علیه قاچاق مواد مخدر و داروهای روان‌گردان ۱۹۸۸.

۲. کنوانسیون ملل متحد علیه جرائم سازمان‌یافته فراملی ۲۰۰۰.

3. One man's terrorist is another man's freedom fighter.

عمومی یا خصوصی یا اشغال یا تصرف آن‌ها یا به خطر انداختن منابع مالی یا تأسیسات بین‌المللی یا تهدید کردن ثبات، تمامیت ارضی، وحدت سیاسی یا حاکمیت کشورهای مستقل انجام گیرد.» بند سوم همین ماده نیز مقرر می‌دارد: «اصطلاح «جرم تروریستی» به معنای ارتکاب، آغاز یا مشارکت در هر جرمی است که به‌منظور تحقق هدف تروریستی در هر یک از کشورهای متعاقد یا علیه اتباع، دارایی‌ها یا منافع آن کشور یا تأسیسات و اتباع مقیم در آن قلمرو که مطابق با قوانین داخلی آن کشور مشمول مجازات قرار می‌گیرد، صورت می‌پذیرد.» همچنین از ماده یک «قانون مبارزه با تأمین مالی تارشرگی» مصوب ۱۳۹۴ نیز می‌توان مصادیق تارشرگی در حقوق داخلی را استخراج نمود؛ مطابق این ماده: تهیه و جمع‌آوری عمداً و علماً وجوه و اموال به هر طریق چه دارای منشأ قانونی باشد یا نباشد و یا مصرف تمام یا بخشی از منابع مالی حاصله از قبیل قاچاق ارز، جلب کمک‌های مالی و پولی، اعانه، انتقال پول، خریدوفروش اوراق مالی و اعتباری، افتتاح مستقیم یا غیرمستقیم حساب یا تأمین اعتبار یا انجام هرگونه فعالیت اقتصادی اشخاص توسط خود یا دیگری جهت ارائه به افراد تروریست یا سازمان‌های تروریستی که مرتکب یکی از اعمال زیر می‌شوند، تأمین مالی تارشرگی بوده و جرم محسوب می‌شود:

الف- ارتکاب یا تهدید به ارتکاب هرگونه اقدام خشونت‌آمیز از قبیل قتل، سوءقصد، اقدام خشونت‌آمیز منجر به آسیب جسمانی شدید، ربودن، توقیف غیرقانونی و گروگان‌گیری اشخاص و یا اقدام خشونت‌آمیز آگاهانه علیه افراد دارای مصونیت قانونی یا به مخاطره انداختن جان یا آزادی آن‌ها به قصد تأثیرگذاری بر خطمشی، تصمیمات و اقدامات دولت جمهوری اسلامی ایران، سایر کشورها و یا سازمان‌های بین‌المللی دارای نمایندگی در قلمرو جمهوری اسلامی ایران

ب- ارتکاب اعمال زیر با مقاصد یادشده در بند (الف):

- ۱- خرابکاری در اموال و تأسیسات عمومی دولتی و غیردولتی
 - ۲- ایراد خسارت شدید به محیط‌زیست از قبیل مسموم کردن آب‌ها و آتش زدن جنگل‌ها
 - ۳- تولید، تملک، اکتساب، انتقال، حمل، نگهداری، توسعه یا انباشت غیرقانونی، سرقت، تحصیل متقلبانه و قاچاق سموم، عناصر و مواد هسته‌ای، شیمیایی، میکروبی و زیست‌شناسی (بیولوژیک)
 - ۴- تولید، تهیه، خریدوفروش و استفاده غیرقانونی و قاچاق مواد منفجره، اسلحه و مهمات
- پ- ارتکاب اعمال زیر صرف‌نظر از انگیزه مرتکب و نتیجه حاصله:
- ۱- اعمال خطرناک علیه ایمنی هواپیما یا هوانوردی
 - ۲- تصرف هواپیمای در حال پرواز و اعمال پایش غیرقانونی بر آن
 - ۳- ارتکاب خشونت علیه مسافر یا مسافران و خدمه هواپیما یا اعمال خطرناک علیه اموال موجود در هواپیمای در حال پرواز

۴- تولید، تملک، اکتساب، انتقال، حمل، نگهداری، توسعه یا انباشت، غنی سازی و انفجار غیرقانونی، سرقت، تحصیل متقلبانه و قاچاق عناصر و یا مواد هسته‌ای به میزان غیرقابل توجیه برای اهداف درمانی، علمی و صلح‌آمیز

۵- تولید، تملک، اکتساب، انتقال، سرقت، تحصیل متقلبانه، قاچاق، حمل، نگهداری، توسعه یا انباشت و استفاده یا تهدید به استفاده از سلاح‌های هسته‌ای، شیمیایی، میکروبی و زیست‌شناسی (بیولوژیک) ۶- دزدی دریایی، تصرف غیرقانونی کشتی و یا اعمال پایش غیرقانونی بر آن و یا به خطر انداختن ایمنی کشتیرانی از طریق ارائه آگاهانه اطلاعات نادرست یا تخریب و واردکردن آسیب شدید به کشتی، محموله و خدمه یا مسافران آن

۷- تصرف یا پایش غیرقانونی سکوها یا تأسیسات مستقر در مناطق دریایی، ارتکاب اعمال خشونت‌بار علیه افراد حاضر در آن‌ها و هرگونه اقدام برای تخریب یا صدمه به این سکوها یا تأسیسات به قصد ایجاد خطر برای ایمنی این مناطق

۸- مبادله در اماکن عمومی، تأسیسات دولتی، شبکه حمل‌ونقل عمومی یا تأسیسات زیرساختی ت- ارتکاب جرمی که به موجب قوانین داخلی یا کنوانسیون‌های بین‌المللی جرم تروریستی شناخته شده؛ در صورت الحاق دولت جمهوری اسلامی ایران به آن‌ها».

یکی از مهم‌ترین راه‌های مبارزه با پدیده تارشگری به‌عنوان پدیده‌ای که یکی از شاخص‌های اصلی سنجش امنیت ملی است، مبارزه با تأمین مالی آن است. به همین منظور کشورها رأساً یا از طریق سازمان ملل متحد، مبادرت به تهیه اسناد و مقرراتی جهت مسدود نمودن راه‌های تأمین مالی تارشگری نموده‌اند. از حیث اهمیت و اعتبار شکلی و وصف الزام‌آور آن‌ها، قطعنامه‌های شورای امنیت، به‌ویژه قطعنامه ۱۳۷۳ مصوب ۲۰۰۱، در وهله اول اهمیت قرار دارند؛ در وهله دوم، کنوانسیون بین‌المللی مبارزه با تأمین مالی تارشگری ۱۹۹۹ سازمان ملل متحد است؛ سپس توصیه‌های ویژه هشت گانه و نیز برخی توصیه‌های مرتبط چهل‌گانه گروه اقدام مالی است. اگرچه توصیه‌های گروه اقدام مالی برخلاف قطعنامه ۱۳۷۳ از پشتوانه ماده ۲۵ منشور ملل متحد برخوردار نیستند، ولی در عرصه بین‌المللی واجد اهمیت بسیارند.

۴-۲- الزامات مربوط به پایش ارزهای دیجیتال

به‌منظور مقابله با پول‌شویی و تأمین مالی تارشگری با استفاده از ارزهای دیجیتال الزاماتی باید رعایت شود. البته این اقدامات باید مبتنی بر میزان ریسکی که از ارزهای دیجیتال در هر حوزه اقتصادی وجود دارد اتخاذ شود.

۴-۲-۱- شناسایی ارباب رجوع و نگهداری سوابق هویتی و معاملاتی او

اولین مورد از الزامات مقابله با پول شویی و تأمین مالی تارشگری شناسایی ارباب رجوع و نگهداری سوابق هویتی و معاملاتی او است. توصیه شماره ۱۰ گروه ویژه اقدام مالی (FATF) ذیل عنوان «شناسایی مشتریان»^۱ مقرر می دارد: مؤسسات مالی باید از نگهداری حساب های بی نام و حساب هایی که جعلی بودن نام صاحب آن ها محرز است، منع شوند. مؤسسات مالی باید ملزم شوند که در موارد زیر نسبت به شناسایی کافی مشتریان اقدام کنند:

۱- برقراری روابط کاری؛

۲- انجام معاملات موردی:

الف- بیش از سقف مقرر (۱۵۰۰۰ دلار یا یورو)، یا

ب- نقل و انتقالات الکترونیکی مشمول شرایط مندرج در یادداشت تفسیری توصیه شماره ۱۶؛

۳- در مواردی که ظن به پول شویی و یا تأمین مالی تارشگری وجود داشته باشد؛

۴- زمانی که مؤسسه مالی نسبت به صحت و یا کفایت اطلاعات اخذ شده قبلی درباره هویت مشتری، تردید داشته باشد.

اجرای این الزام اقتضائاتی دارد؛ از جمله این که باید اولاً از فعالیت نهادهای مالی و غیرمالی ارائه دهنده خدمات غیرمجاز جلوگیری به عمل آید؛ در غیر این صورت مشتریان که معمولاً تمایل دارند بدون شناسایی شدن به فعالیت اقتصادی بپردازند، این نهادها را جایگزین نهادهای رسمی خواهند کرد. ثانیاً نهادهای رسمی باید به شدت تحت پایش و نظارت باشند تا مشخص شود تا چه میزان به نحو صحیح اقدام به شناسایی مشتریان خود می کنند. ثالثاً ابزارهای شناسایی باید ایجاد شده و به نهادهای رسمی معرفی شود.

اقتضائات یاد شده علاوه بر این که زمینه های قانونی لازم دارد، نیازمند روش های ساماندهی کشف و برخورد است. متأسفانه در قدم اول یعنی زمینه های قانونی جز در مورد ارائه برخی خدمات صرافی یا بانکی، ضمانت اجرای قوی برای نهادهای مالی و غیرمالی غیرمجاز وجود ندارد به نحوی که ایجاد سامانه های مبارزه با این نوع فعالیت ها در عمل بیهوده و بی نتیجه می شود. نهادهای رسمی و مجاز نیز در صورت تخلف از مقررات شناسایی جز در برخی موارد مربوط به خرید و فروش ارز، چندان با ضمانت اجرای قوی مواجه نیستند و در سخت ترین برخورد بر اساس تبصره ۳ ماده ۴ قانون مبارزه با پول شویی مجازات انفصال موقت از ۲ تا ۵ سال برای کارمند خاطی در نظر گرفته می شود و شخصیت حقوقی خاطی هیچ انگیزه ای برای نظارت بر این امر ندارد.

این زمینه های قانونی در خصوص ارزش های مجازی کمرنگ تر نیز می شوند تا جایی که اساساً مشخص نیست آیا ارائه این خدمات نیاز به اخذ مجوز دارد یا خیر و اگرچه مقرراتی در این حوزه وضع شده و

1. Customer due diligence.

در بخش نخست نیز بدان اشاره شد اما پشتوانه قانونی برای مجازات خاطیان هنوز به وجود نیامده است.

۴-۲-۲- گزارش دهی اجباری

یکی از روش‌های متداول برای تطهیر پول، استفاده از سامانه بانکی، مؤسسات مالی و اعتباری و دفاتر اسناد رسمی است؛ لذا توجه به این نهادها و تهیه یک سازوکار برای کشف این موارد در نهادهای مزبور، به مبارزه با پول‌شویی کمک شایانی می‌نماید.

اکثر کشورها و ازجمله ایران، برای همین منظور، نظام «گزارش دهی اجباری» را تأسیس نموده‌اند. توصیه شماره ۹ گروه ویژه اقدام مالی (FATF) نیز ذیل عنوان «قوانین ناظر بر رازداری در مؤسسات مالی» مقرر می‌دارد: «کشورها باید اطمینان ایجاد کنند که قوانین داخلی آن‌ها در زمینه رازداری در مؤسسات مالی، مانع از اجرای توصیه‌های گروه ویژه نمی‌شوند.» (زارع قاجاری، ۱۳۹۲: ۲۵)

فصل چهارم از آیین‌نامه اجرایی «قانون مبارزه با پول‌شویی» به «گزارش‌های الزامی» اختصاص یافته است؛ مطابق این مقررات، گزارش دهی اجباری یا ناظر به «معاملات بیش از سقف مقرر» است و یا ناظر به «معاملات و عملیات مشکوک».

۴-۲-۲-۱- گزارش دهی معاملات بیش از سقف مقرر

ماده ۲۶ آیین‌نامه مقرر می‌دارد: کارکنان تحت امر اشخاص مشمول موظفند تمامی معاملات بیش از سقف مقرر را که ارباب رجوع وجه آن را به صورت نقدی پرداخت می‌نماید، ثبت و همراه با توضیحات ارباب رجوع به واحدهای مسئول مبارزه با پول‌شویی در هر دستگاه و در صورت عدم وجود این واحد، به بالاترین مقام شخص مشمول اطلاع دهند. واحدهای مسئول مبارزه با پول‌شویی در هر دستگاه و یا بالاترین مقام شخص مشمول (در صورت عدم وجود واحد) موظفند خلاصه فرم‌های یادشده را در پایان هر هفته به نحوی که واحد اطلاعات مالی مشخص می‌سازد ارسال و اصل آن را به نحو کاملاً حفاظت شده، نگهداری نمایند.

تبصره ۱- ارائه‌دهندگان وجه نقد بیش از سقف مقرر موظفند توضیحات مورد نیاز یادشده در فرم ابلاغ شده را به اشخاص مشمول ارائه نمایند.

تبصره ۲- در صورت نقل و انتقال وجه نقد بیش از سقف مقرر با استفاده از روش‌های غیر بانکی مانند پست، کارکنان اشخاص مشمول موظف به ارائه گزارش به واحدهای مسئول مبارزه با پول‌شویی در هر شخص مشمول هستند. در صورت عدم وجود این واحد، گزارش‌ها باید به بالاترین مقام شخص مشمول جهت انجام اقدامات مقتضی ارسال گردد.

تبصره ۳- فرم‌ها، میزان و نحوه اخذ اطلاعات از ارباب رجوع، نحوه و میزان اطلاعات اولیه ارسالی به واحد اطلاعات مالی و نحوه نگهداری و دسترسی به اطلاعات در هر شخص مشمول مطابق آیین‌نامه‌ای

خواهد بود که به تصویب شورا خواهد رسید.»

«سقف مقرر» مطابق بند «ز» ماده یک آیین نامه عبارت است از: «مبلغ یک صد و پنجاه میلیون (۱۵۰,۰۰۰,۰۰۰) ریال وجه نقد یا معادل آن به سایر ارزها و کالای گران بها».

این شیوه می تواند مورد سوءاستفاده واقع شود؛ بدین صورت که اشخاص مترصد پول شویی، مبادلات و سرمایه گذاری های خود را به میزان کمتر از سقف مقرر انجام دهند (همان: ۸۴) یا آن که مبالغ کلان را به مبالغ خردتر تبدیل کرده و توسط اشخاص دیگر مثل فرزندان، مستخدمان و نظایر آنها در بانک ها و مؤسسات سرمایه گذاری نمایند. (احد باقرزاده، ۱۳۹۴: ۲۹۵) این نقایص، مقتضی تمهید یک سازوکار مکمل است؛ لذا در «قانون مبارزه با پول شویی» و نیز آیین نامه اجرایی آن، گزارش دهی «معاملات و عملیات مشکوک» نیز پیش بینی شده است.

۲-۲-۲-۲-۴ گزارش دهی معاملات و عملیات مشکوک

گزارش معاملات و عملیات مشکوک از مهم ترین الزامات مبارزه با پول شویی و تأمین مالی تارشرگری به حساب می آید. اجرای کامل این الزام نیز اقتضائاتی دارد، اول این که به مانند مورد قبل از فعالیت نهادهای غیرمجاز جلوگیری شود و بر فعالیت نهادهای مجاز از این جهت که در موارد تعیین شده گزارش ها به درستی ارسال می شود، نظارت صورت گیرد. دوم این که مصادیق عملیات مشکوک به درستی تبیین شود، سوم این که زیرساخت های شناسایی معاملات مشکوک باید ایجاد شود. برای مثال اگر سامانه هایی برای مستند کردن دارایی ها نظیر املاک، طلا، ارز و ... وجود نداشته باشد، امکان شناسایی و در نتیجه ارسال گزارش عملیات مشکوک به وجود نمی آید؛ بنابراین دارایی ها نیز باید مانند انسان ها شناسه هویتی و شناسنامه داشته باشند تا رصد آنها امکان پذیر شود.

ماده هفت «قانون مبارزه با پول شویی» مقرر می دارد: اشخاص، نهادها و دستگاه های مشمول این قانون (موضوع مواد ۵ و ۶) برحسب نوع فعالیت و ساختار سازمانی خود مکلف به رعایت موارد زیر هستند: ... پ- ارائه گزارش معاملات یا عملیات یا شروع به عملیات بیش از میزان مصوب شورا یا معاملات و عملیات مشکوک بانکی، ثبتی، سرمایه گذاری، صرافی، کارگزاری و مانند آنها به مرکز اطلاعات مالی. تبصره- معاملات و عملیات مشکوک شامل هر نوع معامله، دریافت یا پرداخت مال اعم از فیزیکی یا الکترونیکی یا شروع به آنها است که بر اساس اوضاع و احوالی مانند ارزش، موضوع یا طرفین آن برای انسان به طور متعارف ظن وقوع جرم را ایجاد کند؛ نظیر:

۱- معاملات و عملیات مالی مربوط به ارباب رجوع که به نحو فاحش بیش از سطح فعالیت مورد انتظار وی باشد.

۲- کشف جعل، اظهار کذب یا گزارش خلاف واقع از سوی مراجعان، قبل یا بعد از آنکه معامله یا

عملیات مالی صورت گیرد و نیز در زمان اخذ خدمات پایه.

۳- معاملات یا عملیات مالی که به هر ترتیب مشخص شود صوری یا ظاهری بوده و مالک شخص دیگری است.

۴- معاملات یا عملیات مالی که اقامتگاه قانونی هریک از طرفین در مناطق پرخطر (از نظر پول شویی) واقع شده است. فهرست این مناطق توسط شورا مشخص می شود.

۵- معاملات یا عملیات مالی بیش از سقف مقرر در آیین نامه اجرائی. هرچند مراجعان، قبل یا حین معامله یا عملیات مزبور از انجام آن انصراف داده یا بعد از انجام آن بدون دلیل منطقی نسبت به فسخ قرارداد اقدام نمایند.»

ماده ۱۴ قانون مبارزه با تأمین مالی تارشگری نیز مقرر می دارد: «کلیه اشخاص مشمول قانون مبارزه با پول شویی موظفند گزارش عملیات مشکوک به تأمین مالی تارشگری را به شورای عالی مبارزه با پول شویی موضوع ماده (۴) قانون مذکور ارسال کنند.»

تخلف از این مقررات نیز همان طور که در بند قبل بیان شد، جز در برخی موارد معدود، متناسب، مؤثر و بازدارنده نیست. افزون بر آن، سازوکاری سامانمند برای کشف میزان گزارش های ارسال نشده وجود ندارد. دارایی های باارزش نظیر املاک و ارزها و طلا و خودرو به درستی نظام مند نشده اند. در این میان ماهیت ارزهای مجازی نیز به عنوان یکی از دارایی های باارزش به گونه ای است که مستند کردن آن بسیار دشوارتر از دارایی های یادشده است.

یکی دیگر از مسائلی که مربوط به این بند می شود آن است که سطح فعالیت افراد یعنی میزان دارایی متصور برحسب نوع فعالیت اقتصادی آنها باید مشخص شود؛ با توجه به این که برخلاف دیگر دارایی ها که ایجاد آن عملاً خارج از دست مشتریان است، ارزهای مجازی ممکن است توسط افراد ایجاد شود؛ بنابراین اگر در مرحله ایجاد این دارایی ها هیچ پایشی صورت نگیرد، هر نوع اختلاف در سطح فعالیت می تواند از طریق ادعای ایجاد یا مشارکت در ایجاد این دارایی توجیه شود. متأسفانه در این حوزه توجه دولت با توجه به مصوبات در دست اقدام در زمان نگارش این سطور معطوف به هزینه های برق مصرفی شده و به مسئله تأثیر استخراج بدون پایش بر سطح فعالیت افراد توجه چندانی نمی شود.

۴-۲-۳- توقیف دارایی های مشکوک

اساسی و بنیادی ترین الزام مبارزه با پول شویی و تأمین مالی تارشگری مسئله توقیف دارایی های مشکوک است. مسئله ای که علاوه بر اقتضائات بیان شده در مباحث یادشده به شدت وابسته به ایجاد سازوکار توقیف و انسداد است. سازوکاری که از لحظه شناسایی مال مشکوک آغاز و تا پایان رفع انسداد یا مصادره ادامه می یابد. مقررات فعلی متأسفانه در این زمینه چندان واضح نیست و نمی توان گفت چنین

سازوکاری در حال حاضر وجود دارد. قانون مبارزه با تأمین مالی تارشگری و قانون مبارزه با پول شویی صرفاً به بیان جواز توقیف در این زمینه اکتفا نموده‌اند.

ماده ۵ قانون تأمین مالی تارشگری مقرر می‌دارد: مراجع قضائی و ضابطان دادگستری تحت نظارت و تعلیمات و یا دستور مقام قضائی حسب مورد، مکلفند اقدامات زیر را انجام دهند:

پ- توقیف اموال و عواید موضوع جرم که با اموال قانونی امتزاج یافته؛ به نحوی که اموال مزبور به اندازه تخمین زده شده قابل توقیف باشد.

تبصره- اشخاص موضوع این ماده موظفند حسب دستور مقام قضائی نسبت به مسدود کردن وجوه و توقیف اموال و دارایی‌های افراد، گروه‌ها و سازمان‌های تروریستی و همچنین افراد موضوع قانون مبارزه با پول شویی مصوب ۲/۱۱/۱۳۸۶ با اصلاحات و الحاقات بعدی برابر فهرست اعلامی شورای عالی امنیت ملی اقدام نمایند. در موارد فوری و ضروری که دسترسی به مقام قضائی ممکن نیست باید برابر فهرست یادشده اقدام نموده و مراتب را ظرف مدت بیست و چهار ساعت به مراجع قضائی اعلام کنند. (الحاقی مصوب ۱۳۹۷/۴/۳۱)

تبصره ۱ ماده ۷ مکرر قانون مبارزه با پول شویی نیز به همین شکل مقرر داشته است: توقیف و جلوگیری از نقل و انتقال وجوه یا اموال مشکوک به جرائم پول شویی و تأمین مالی تارشگری و یا انجام هرگونه تحقیقات منوط به اخذ مجوز از مراجع قضائی ذی صلاح است؛ مگر در موارد فوری که به مقام قضائی دسترسی نیست که در این صورت مرکز اطلاعات مالی می‌تواند دستور توقیف و جلوگیری از انتقال وجوه و اموال مشکوک را حداکثر تا بیست و چهار ساعت صادر و بلافاصله پس از حصول دسترسی، مراتب را به مقام قضائی گزارش و مطابق دستور وی عمل کند. چنانچه بعد از بیست و چهار ساعت مجوز مراجع قضائی صادر نشود، رفع توقیف می‌شود.

افزون بر مشکلات کلی که در این زمینه وجود دارد در خصوص ارزهای مجازی باید گفت نحوه توقیف این دارایی‌ها نیز به موجب قوانین و مقررات مشخص نشده است. به لحاظ فنی نیز تبیین دقیقی در خصوص فرآیند توقیف این دارایی‌ها ارائه نشده است.

۵- نتیجه گیری

نتایج نوشتار حاضر را به شرح زیر می‌توان تبیین نمود:

۱- ارز دیجیتال، حالت غیرملموس و الکترونیکی ارز است که می‌تواند میان طرفین از طریق استفاده از فناوری‌های فعلی نظیر رایانه، اینترنت و تلفن‌های هوشمند جابه‌جا شود. تمامی ارزهایی که در فضای حقیقی وجود خارجی ندارند ولی در فضای الکترونیکی ایجاد و منتقل می‌شوند داخل در تعریف ارز دیجیتال هستند؛ لذا ارزهای مجازی و رمزارزها نیز ارز دیجیتال محسوب می‌شوند.

۲- فناوری بلاک‌چین نقش مهمی در سازوکار ارزهای دیجیتال ایفا می‌کند. بلاک‌چین، رشته‌ای از بلوک‌ها است که سوابق کامل معاملات را مانند یک دفتر کل عمومی نگهداری می‌کند. بیت‌کوین و سایر سامانه‌های مجازی مبتنی بر رمزنگاری، از یک دفترچه «بلاک‌چین» برای ثبت و تأیید همه معاملات استفاده می‌کنند.

۳- کشورها به‌طورکلی سه رویکرد نسبت به ارز دیجیتال اتخاذ نموده‌اند، برخی از کشورها رویکرد محتاطانه اتخاذ نموده‌اند، برخی کشورها استفاده از این ارزها را ممنوع ساخته‌اند و برخی دیگر رویکرد سهل‌گیرانه با هدف توسعه این فناوری‌ها را در پیش گرفته‌اند. به نظر می‌رسد رویکرد فعلی کشور ما از حیث عدم قانون‌گذاری در خصوص ارزهای مجازی مشابه کشورهای محتاط نظیر بلژیک است؛ لیکن از این حیث که عملاً بانک‌ها و مؤسسات مالی و اعتباری از معامله ارزهای دیجیتال ممنوع نموده است، موضعی مشابه کشور چین اتخاذ نموده است.

۴- رواج ارزهای دیجیتال نیازمند آن است که الزامات پایش دارایی‌ها در خصوص آن رعایت شود؛ زیرا عدم رعایت این الزامات موجب آسیب سامانه اقتصادی کشور در نتیجه ارتکاب جرائم پول‌شویی و در معرض خطر تارشگری قرار گرفتن کشور در نتیجه ارتکاب جرم تأمین مالی تارشگری می‌شود. آسیب به این دو حوزه نیز یکی از شاخص‌های امنیت ملی کشور را تحت تأثیر قرار داده و موجب کاهش سطح امنیت ملی خواهد شد.

۵- این پژوهش نشان می‌دهد که اولاً ماهیت ارزهای دیجیتال به‌گونه‌ای است که اتخاذ الزامات پایش دارایی‌ها در قبال آن به‌طور ذاتی با دشواری روبه‌رو است. ثانیاً زمینه‌های قانونی و اجرایی کشور نیز برای اتخاذ الزامات ضد پول‌شویی و تأمین مالی تارشگری در وضعیت مطلوبی قرار ندارد؛ بنابراین صرف نظر از سنجش میزان مخاطراتی که در نتیجه استفاده از این نوع دارایی‌ها وجود دارد، به نظر می‌رسد رواج ارزهای دیجیتال در وضع فعلی حداقل در سطح استفاده عمومی از آن (نه استفاده توسط دولت در مراودات بین‌المللی) با چالش اساسی روبه‌روست.

فهرست منابع

- باقرزاده، احد (۱۳۹۴)، پول‌شویی در حقوق ایران و انگلستان و اسناد بین‌المللی، تهران: میزان.
- زارع قاجاری، فردوس و دیگران (۱۳۹۲)، استانداردهای بین‌المللی مبارزه با پول‌شویی و تأمین مالی تارشگری، تهران: نشر تاش.
- سلیمانی‌پور، محمد مهدی (۱۳۹۶)، بررسی فقهی ارز مجازی، تحقیقات مالی اسلامی، شماره ۲.
- سیاه‌بیدی کرمانشاهی، سعید و همکاران (۱۳۹۶)، حقوق کیفری اقتصادی: جرائم و تخلفات مالیاتی - اخلاص در نظام اقتصادی کشور - قاجاق ارز و تخلفات ارزی - پول‌شویی، تهران: جنگل.
- معاونت پژوهش‌های زیربنایی و امور تولیدی (۱۳۹۶)، سیاست‌گذاری کشورهای آمریکا، چین و آلمان در زمینه ابزارهای مالی دیجیتال جدید مانند بیت‌کوین، تهران: مرکز پژوهش‌های مجلس شورای اسلامی.
- میرزاخانی، رضا (۱۳۹۶)، بیت‌کوین و ماهیت مالی - فقهی ارز مجازی، تهران: مرکز پژوهش، توسعه و مطالعات اسلامی سازمان بورس و اوراق بهادار.
- میرمحمد صادقی، حسین (۱۳۹۴)، جرائم علیه امنیت و آسایش عمومی، تهران: میزان.
- میرمحمد صادقی، حسین (۱۳۹۵)، حقوق جزای بین‌الملل (مجموعه مقالات)، تهران: میزان.
- ناصری مقدم، حسین (۱۳۹۶)، ارز مجازی و چالش‌های فقهی پیش‌رو، جستارهای فقهی و اصولی، شماره ۷.
- ولیدی، محمد صالح (۱۳۹۴)، حقوق کیفری اقتصادی، تهران: میزان.
- Girasa, Rosario (2018), **Regulation of Cryptocurrencies and Blockchain Technologies**, Springer International Publishing; Palgrave Macmillan.
- Lee Kuo Chuen, David (2015), **Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data**, Academic Press.
- Matsuura, Jeffrey H. (2016), **Digital Currency: An International Legal and Regulatory Compliance Guide**, Bentham Science Publishers.
- Nwanegbo, C.J. & Odigbo, J. (2013), **Security and National Development in Nigeria: Threat of book Haram**, International Journal of Humanities and Social Science, 3(4).
- Okechukwu, E. I. & Anyadike, N. (2013), **Security Challenges and Votes in Nigeria**, 2008-2013, Kuwait Chapter of Arabian Journal of Business and Management Review, 2(8).
- Pogson, A. I. (2013), **Nigeria's National Security in an Age of Terrorism**, Ibadan: Department of Political Science, University of Ibadan.
- Reuter, Peter, Truman, Edwin M. (2004), **Chasing Dirty Money: The Fight against Money Laundering**, Peterson Institute.
- Rothchild, John A. (2016), **Research Handbook on Electronic Commerce Law**, Edward Elgar Publishing.

- <https://arzdigital.com/export-electricity-prices-for-bitcoin-mining-in-iran/>
- <https://www.cbi.ir/showitem/17722.aspx>