

دو فصلنامه بین المللی تحقیقات حقوق قضایی

License Number: 86227 Article Number: Y4N13545 ISSN-P: 2717-1132

چالش های نظام عدالت قضایی ایران در قبال جرائم مرتبط با

ارز دیجیتال

(تاریخ دریافت ۱۴۰۲/۰۴/۱۵ تاریخ تصویب ۱۴۰۲/۰۶/۱۲)

نسیم فقها زاده

کارشناس ارشد، حقوق، جزا و جرم شناسی، دانشکده علوم انسانی، واحد علوم تحقیقات اهواز، دانشگاه پردیس علوم تحقیقات، خوزستان، ایران

کوثر رفیعی پور^۱

کارشناس ارشد، حقوق، جزا و جرم شناسی، دانشکده علوم انسانی، واحد اهواز، دانشگاه آزاد اسلامی، خوزستان، ایران

چکیده

ارز دیجیتال یکی از اقسام دارائی های دیجیتال می باشد که در سالیان اخیر بسیار مورد توجه قرار گرفته است. رمز ارز پدیده نوینی است که بر بستر اینترنت و با استفاده از فناوری های نوین استخراج و منتقل می شوند. و یکی از انواع آن بنام بیت کوین توانسته نظام های مالی دنیا را تحت تأثیر قرار دهد. غیرمتمرکز بودن، فرامرزی بودن، گمنام بودن کاربران، رمزنگاری و برگشت ناپذیر بودن تراکنش ها، ویژگی هایی است که بهره گیری از ارزهای مجازی در فعالیتهای مجرمانه را مورد توجه بزهکاران قرار می دهد. پژوهش حاضر سعی بر آن دارد تا در دو بخش با روش تحلیل محتوا به این مهم بپردازد. بنابراین در بخش اول جرایم مرتبط با رمز ارزها مورد بررسی قرار می گیرد و در بخش دوم به نظام قضایی حاکم بر جرایم مرتبط با ارز دیجیتال و چالش های آن پرداخته می شود. نتیجه چنین پژوهشی آشکار ساخت که در ایران قوانین مدونی به طور خاص به ارزهای دیجیتال اختصاص نیافته است و صرفا پیش نویسی در سال ۱۳۹۷ و اصلاحاتی به دنبال آن در سالهای بعد مورد بررسی قرار گرفت که قطعیت پیدا نکرده است همچنین با عنایت به عدم حاکمیت قانونی خاص بر قلمرو پول مجازی با استفاده از آن می توان به پول شویی، فرار مالیاتی و سایر جرائم اینترنتی دامن زد و زمینه ارتکاب این پدیده ها را تسهیل نمود.

واژگان کلیدی: ارزهای دیجیتال، ارتکاب جرم، نظام قضایی

^۱ نویسنده مسئول

بخش اول: کلیات

رمز ارزها پدیده نوینی است که بر بستر اینترنت و با استفاده از فناوری‌های نوین استخراج و منتقل می‌شوند. غیرمتمرکز بودن، فرامرزی بودن، گمنام بودن کاربران، رمزنگاری و برگشت ناپذیر بودن تراکنش‌ها، ویژگی‌هایی است که بهره‌گیری از ارزهای مجازی در فعالیت‌های مجرمانه را مورد توجه بزهکاران قرار می‌دهد. ویژگی‌های ارزهای مجازی به همراه ابهام در وضعیت قانونی و قلمرو فعالیت‌های مجرمانه، چالش‌هایی برای نظام عدالت کیفری در حوزه دادرسی جرایم، بوجود آورده است (سلطانی، اسدی، ۱۳۹۴: ۸۳).

استقبال روزافزون مردم از ارزهای دیجیتال و معاملات الکترونیکی موجب توجه اندیشمندان حوزه‌های مختلف علوم اقتصادی، اجتماعی، سیاسی و ... به این پدیده نوظهور اقتصادی شده است. پژوهشگران و اندیشمندان رمز ارزها را از زوایای گوناگون اقتصادی، اجتماعی و فرهنگی مورد توجه قرار داده‌اند. با این حال و علیرغم اهمیت و ضرورت انجام بررسی‌های حقوقی، فعالیت جامع پژوهشی از منظر حقوقی تاکنون در این باره به انجام نرسیده است. از سوی دیگر پژوهشی مشخصاً به بررسی ارزهای دیجیتال از منظر حقوقی نپرداخته است. از همین رو در این پژوهش به بررسی رمز ارزها در حقوق ایران، جرایم مرتبط با آنها و چالش‌های نظام عدالت قضایی با این پرسش که آیا نظام حقوقی ایران در قبال جرائم مرتبط با رمز ارزها سیاستی را در پیش دارد؟ در دو بخش پرداخته شده است.

چرا که رمز ارز یا ارز دیجیتال یا ارز الکترونیکی یکی از اقسام دارائی‌های دیجیتال می‌باشد که در سالیان اخیر بسیار مورد توجه قرار گرفته است. ارز دیجیتال با توجه به گسترش آن در دنیا و یکی از انواع آن به نام بیت کوین توانسته نظام‌های مالی دنیا را تحت تأثیر قرار دهد. امروزه حدود ۳۰ پول مجازی منتشر شده در دنیا وجود دارد که مهمترین آنها بیت کوین است. رمز ارزها به عنوان پدیده‌ای نو در فضای مجازی، همراه با سود و زیان‌هایی است. افزایش سرعت، کاهش هزینه، افزایش حریم خصوصی و سهولت استفاده از این ارزها موجب محبوبیت و رونق آنها شده است. گمنامی و فقدان نهاد مرکزی برای نظارت و اعمال



قوانین موجب شده است تا امکان استفاده از این پدیده در فعالیت‌های مجرمانه فراهم شود. ویژگی‌های مذکور به همراه ابهام در وضعیت قانونی و عدم شناخت کافی مردم، سیاست‌گذاران و نهادهای مجری قانون از این پدیده، چالش‌هایی را پیش روی نظام عدالت کیفری در دادرسی جرایم مرتبط با آنها قرار داده است. (نواب پور، و دیگران، ۱۳۹۷: ۱۸) ابهام در ماهیت ارزش‌های مجازی، چگونگی اعمال قوانین و مقررات بر ارزش‌های مجازی، چگونگی شناسایی و کشف جرایم، توقیف و مصادره و نگهداری ارزش‌های مجازی، استفاده از ادله الکترونیک و تعیین قلمرو صالح قضایی از چالش‌های اصلی در دادرسی جرایم مرتبط با ارزش‌های مجازی است. نگارندگان در این پژوهش سعی به بررسی آن دارند.

بخش دوم: جرایم مرتبط با رمز ارزها

برخی ویژگی‌های بازار رمز ارزها از جمله عدم وجود قوانین جهانی و پذیرفته نشدن توسط کشورها، محصور نبودن مبادلات رمزارزها در جغرافیای سرزمینی، عدم امکان/ سخت بودن شناسایی و پیگیری مجرمین و تعیین سازمان خاص جهت رسیدگی به درخواست‌ها، هزینه‌ی پایین ارتکاب جرم، قبح اخلاقی پائین ارتکاب جرم در این حوزه و برخی ویژگی‌های مثبت این بازار از جمله جدید و تازگی برای سرمایه‌گذاران، انجام مبادلات تجاری بین المللی و بهره‌گیری در جهت شد کسب و کارهای مجازی و بسیاری از ویژگی‌های دیگر باعث افزایش ارتکاب جرم مرتبط با این فناوری جدید به خصوص در کشورمان شده است. این موارد تنها بخشی از جرایم حوزه رمز ارز در ایران می‌باشد چرا که این بازار به صورت لحظه‌ای در حال گسترش بوده و بالطبع طیف جرایم مرتبط نیز روز به روز گسترده می‌شود. این جرایم در کشور ما سابقه وقوع داشته و می‌تواند برای هر سرمایه‌گذار به وجود آید. خرید و فروش رمزارزها در هر بستری و به هر صورتی که انجام شود خطرات خاص مربوط به خود را دارد (بانک مرکزی، ۱۳۹۷) در این بخش در دو مبحث به جرایم عمومی و اختصاصی مرتبط با رمز و رازها می‌پردازیم.



بند اول: جرایم عمومی مرتبط با رمز رازها

الف: پولشویی

واژه‌های پول شویی، شستشوی پول آلوده، تطهیر پول و تعبیری از این قبیل، به این منظور نام گذاری گردیده است که آن چه را در این جرم رخ می دهد، به طور کامل شرح داده است. یعنی پول غیرقانونی و کثیف به گردش می افتد، به نحوی که در پایان کار شکل پول قانونی و پاک را به خود میگیرد (شهریاری، ۱۳۸: ۶) پول شویی فرآیندی است که طی آن، منبع اصلی درآمدهای حاصل از اعمال مجرمانه، مخفی نگه داشته شده و به این درآمدها جلوهای پاک و حاصل از اعمال قانونی بخشیده می شود (موسوی مقدم، ۱۳۸۶: ۱۹-۲۰)

جرم پول شویی دارای ویژگیهای خاص خود است که عبارتند از:

- مسبوق بودن به وقوع جرم
- فراملی بودن در اکثر مواقع
- متعدد بودن مباشرین آن
- تخصصی و پیچیده بودن
- از جرائم سازمان یافته بودن جرم

با توجه به درآمدهای بالای اعمال مجرمانه، پول شویی را بزرگ ترین جرم سازمان یافته هزاره سوم دانسته اند. از این رو کشوری چون ایران که در همسایگی کشوری چون افغانستان قرار دارد که درآمدهای نامشروع حاصل از موادمخدر آن سر به فلک می کشد، و ایران که در مسیر ترانزیت مواد مخدر آن می باشد؛ در کنار عواملی چون اقتصاد نابسامان و بی نظم، توسعه روزافزون مناطق اقتصادی، مناطق آزاد اقتصادی و تجاری با هدف گسترش سرمایه گذاری خارجی و داخلی؛ بستری مناسب برای رشد و گسترش پول شویی را مهیا نموده است (شهریاری، ۱۳۸۶: ۹۱-۹۵)



ب: کلاهبرداری سنتی

جرم کلاهبرداری در ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری بدین صورت تصریح گردیده است که: «هرکس از راه حيله و تقلب مردم را به وجود شرکت‌ها یا تجارت‌خانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیر واقع امیدوار نماید یا از حوادث و پیشامدهای غیر واقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر وجوه و یا اموال و یا اسناد یا حوالجات یا قبوض یا مفاسد حساب یا امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و مجازات کلاهبردار علاوه بر رد مال به صاحبش، حبس از ۱ تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است می باشد.

ج: قاچاق

واژه «قاچاق» از کلمه ترکی «قاچماق» به معنای فرار کردن مشتق شده است. (دهخدا: ج ۱۸: ۲۸) در لغت نامه دهخدا این کلمه «آنچه ورود آن به کشور و یا معامله آن از طرف دولت ممنوع است»، معنا شده است. برخی دیگر از نویسندگان آن را به معنای «کاری برخلاف قانون که پنهانی انجام می شود، یا متاعی که در معامله با ورود آن به کشور ممنوع است»، دانسته اند. (معین، ۱۳۷۱: ۲۶۰)

فرهنگ لغت وبستر (websters) علاوه بر ذکر نکات فوق، عوامل دیگری نیز به این تعریف افزوده است، بدین ترتیب که قاچاق: وارد کردن یا خارج کردن اقام ممنوع انسان از کشور بر خلاف قانون و با قصد تقلب (و حيله گری)، واردات و صادرات بدون پرداخت مالیاتهای مقرر توسط قانون و همچنین انتقال یا راهنمایی کردن به روش نهایی برای وارد یا صادر کردن هر چیزی بر خلاف قانون معنا شده است.



د: تحصیل مال نامشروع

منظور از تحصیل مال نامشروع کسب آگاهانه اموال دیگران از راه ممنوع می‌باشد. عبارت نامشروع به این معنی است که روش کسب اموال به صورت غیرقانونی بوده و ربطی به شرع و دین ندارد. تحصیل مال نامشروع در مفهوم عام خود در بردارنده بسیاری از عناوین مجرمانه در جرائم علیه اموال است. به عنوان مثال جرایمی چون سرقت، اختلاس، خیانت در امانت با شرط تصاحب، کلاهبرداری و نظایر آن همگی از مصادیق تحصیل مال از طریق نامشروع هستند. (داوری، ۱۳۹۸: ۴) لیکن در مفهوم خاص به هر نوع تحصیل مال از طریق نامشروع گفته می‌شود که نتوان عنوان مجرمانه دیگری به آن نسبت داد. در معنای اخص تحصیل مال از طریق نامشروع وقتی است که فرد مالی را از طریق رشوه یا ربا یا قمار و غیره که خودش عنوان خاصی دارد بدست نیاورده باشد بلکه از طریق زد و بند با مقامات یا سوء استفاده از موقعیت شغلی مثل نمایندگی مجلس یا مدیریت کلان در کشور بدست آورده است.

بند دوم: جرایم اختصاصی مرتبط با رمز ارزها

الف: کلاهبرداری اینترنتی

کلاهبرداری یکی از مهم ترین جرائم علیه اموال و مالکیت می‌باشد که برخی از آن به عنوان بحران قرن بیستم نام برده اند (میر محمد صادقی، ۱۳۸۳: ۲۸). در حقوق رم جرائم سرقت، خیانت در امانت و کلاهبرداری از یکدیگر تفکیک نشده و «Furtum» شامل هر سه جرم می گردیده است. (پاد، ۱۳۸۲: ۷) اما با پیشرفت علم و تکنولوژی کلاهبرداران هم برای رسیدن به اهداف خود از این پیشرفت‌ها استفاده نموده‌اند و با استفاده از رایانه و فضای سایبر اقدام به کلاهبرداری های رایانه ای نموده اند. کلاهبرداری رایانه ای همانند کلاهبرداری سنتی جرمی مقید به حصول نتیجه مجرمانه است و باید به واسطه سوء استفاده از رایانه از طریق افعالی نظیر ایجاد، محو، توقف داده و یا اختلال در سیستم رایانه ای، مال یا منفعت یا مزایای مالی عاید مرتکب شود. در حقوق کیفری رایانه ای همانند حقوق کیفری سنتی، سوء استفاده از نرم



افزارهای رایانه ای برای تحصیل مال یا منفعت یا مزایای مالی وجه تمایز بین کلاهبرداری رایانه ای از سایر جرائم مشابه است (پیشین، ص ۳۰). ماده ۱۳ قانون جرائم رایانه ای (م ۷۶۱ قم ۱) رکن قانونی این جرم محسوب می شود.

ب: سرقت های سایبری

سرقت رایانه ای در ماده ۱۲ ق جرائم رایانه ای پیش بینی نشده است. این بزه، یک بزه رایانه ای محض است چرا که ربودن داده در جایی که عین داده در جای خود باقی است، مانند جاسوسی و شنود غیر مجاز است که بر ضد محرمانگی داده رخ می دهد و در جایی که به وسیله برش، عین داده از سامانه برداشته می شود، همانند تخریب داده است. بنابراین در دسته جرایمی قرار دارد که رایانه، هدف یا موضوع بزه است و نباید در کنار کلاهبرداری که در آن رایانه نقش ابزار انجام بزه را دارد آورده شود. ماده ۷ ق جرائم رایانه ای (ماده ۷۳۵ ق. م.ا)، رکن قانونی بزه استفاده از داده مجعول به شمار می رود. داده، کارت های الکترونیکی و تراشه ها موضوع رفتار مجرمانه در این جرم می باشند. استفاده کردن از داده مجعول که باید در فضای سایبر و سامانه های رایانه ای و مخابراتی یا داده برها و کارت های حافظه انجام شود، رفتار مرتکب در بزه استفاده از داده مجعول را تشکیل می دهد. بنابراین اگر کسی در فضای بیرونی و فیزیکی از داده مجعول استفاده کند، این بزه رخ نمی دهد. به عنوان مثال اگر فردی جعل رایانه ای کند و متن یک قرارداد الکترونیکی را تغییر دهد و یا اینکه چنین قرارداد مجعولی را بیابد یا دریافت دارد و سپس آن را چاپ کرده و به نهاد یا کسی ارائه دهد مرتکب جرم استفاده از سند مجعول شده است نه جرم استفاده از داده مجعول، چرا که استفاده کردن در فضای بیرونی انجام شده است. آگاهی مرتکب به جعلی بودن، برجسته ترین عنصر رکن روانی است. همچنین لازم است که مرتکب عمد در استفاده کردن از داده مجعول را نیز بر اساس ماده ۷ ق جرائم رایانه ای هرکس با علم به مجعول بودن داده ها با کارت ها یا تراشه ها از آنها استفاده کند، بنا به تصریح ماده ۶ ق جرائم رایانه ای به حبس از یک تا پنج سال یا



جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم می شود (کمرخانی، ۱۴، ۱۳۸۸).

ج: جعل رایانه‌ای

رکن قانونی بزه جعل رایانه ای ماده ۶ قانون جرائم رایانه‌ای (م ۷۳۶ ق.م.) می‌باشد. بستر انجام بزه جعل رایانه ای، فضای سایبر است و فضای سایبر فضایی غیر مادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه ای به وجود آمده است و دنیایی مجازی را در کنار دنیای واقعی ما به وجود آورده است. در واقع فضای سایبر همان فضای مجازی بیکرانی است که از طریق اتصال شبکه های رایانه ای به هم به وجود آمده است. (فضلی، ۱۳۸۹: ۱۷) به لحاظ فنی « شبکه رایانه ای در پایه‌ای ترین سطح خود شامل دو کامپیوتر می‌باشد که به وسیله کابل به یکدیگر متصل شده‌اند به گونه‌ای که بتوانند از داده ها به طور مشترک استفاده نمایند این ارتباط در حال حاضر از طریق کابل مسی است، البته ارتباط رایانه‌ها با یکدیگر ممکن است از طریق کابل خطوط تلفن نباشد و از طریق؛ « فیبر نوری، مایکروویو، اشعه مادون قرمز و ماهواره های ارتباطی نیز می‌توان برای ارتباط استفاده کرد.» (تنباوم، ۱۳۸۳: ۱۴) بنابراین همه رفتارهای پیش بینی شده در این ماده باید از رهگذر کنش‌های رایانه‌ای و در بستر رایانه و مخابرات انجام شود. بنابراین اگر کسی داده رایانه‌ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ شده، تغییراتی را ایجاد کند، جعل رایانه‌ای محقق نیست و ممکن است با وجود تمام شرایط جعل سنتی باشد. همچنین انجام رفتارهای موضوع جعل رایانه‌ای، باید به صورت غیر مجاز باشد یعنی با اجازه نداشته و یا برخلاف قانون و قرارداد بوده است.



د: استفاده از داده مجعول

ماده ۷ ق جرائم رایانه ای (ماده ۷۳۵ ق.م.ا)، رکن قانونی بزه استفاده از داده مجعول به شمار می رود.

داده، کارت های الکترونیکی و تراشه ها موضوع رفتار مجرمانه در این جرم می باشند. استفاده کردن از داده مجعول که باید در فضای سایبر و سامانه های رایانه ای و مخابراتی یا داده برها و کارت های حافظه انجام شود، رفتار مرتکب در بزه استفاده از داده مجعول را تشکیل می دهد. بنابراین اگر کسی در فضای بیرونی و فیزیکی از داده مجعول استفاده کند، این بزه رخ نمی دهد. به عنوان مثال اگر فردی جعل رایانه ای کند و متن یک قرارداد الکترونیکی را تغییر دهد و یا اینکه چنین قرارداد مجعولی را بیابد یا دریافت دارد و سپس آن را چاپ کرده و به نهاد یا کسی ارائه دهد مرتکب جرم استفاده از سند مجعول شده است نه جرم استفاده از داده مجعول، چرا که استفاده کردن در فضای بیرونی انجام شده است(اسراری، ۱۳۹۷، ۵۷).

ه: دسترسی غیر مجاز به داده ها با سیستم رایانه ای

دسترسی غیرمجاز عبارت است از رخنه غیرقانونی به سامانه رایانه ای حفاظت شده. رکن قانونی این بزه ماده ۱ قانون جرائم رایانه ای (ماده ۷۲۹ ق.م.ا) می باشد. دسترسی غیر مجاز در حقوق کیفری سنتی همانند با هیچ یک از جرائم نیست و جزء جرایمی است که با پیدایش رایانه به وجود آمده و مادر بیشتر جرائم رایانه ای است. البته شاید بتوان گفت که این جرم با هتک حرمت منزل یا ورود با قهر و غلبه به ملک دیگری (موضوع ماده ۶۹۴ ق.م.ا) در حقوق کیفری سنتی همسان است. لیکن تفاوتی که با هم دارند این است که در جرم موضوع ماده ۶۹۴ ق.م.ا نیازی نیست که منزل یا مسکن بسته یا حفاظت شده باشد و صرف ورود همراه با عنف و تهدید به منزل یا مسکن دیگری برای تحقق جرم کافی است. اما در بزه دسترسی غیر مجاز لازم است که سامانه رایانه ای ویژگی حفاظت شدگی را داشته



باشد(دره شامی، ۱۳۹۷: ۴۳) این بزه در مقایسه با بزه‌هایی مانند کلاهبرداری رایانه‌ای، اختلال در سیستم و تروریسم سایبری به عنوان یک رفتار مقدماتی به شمار رفته و در اندازه شروع به جرم است که هنوز با نتیجه که در بر دارنده زیان به دیگری است فاصله دارد و از این رو آن را دروازه جرائم رایانه‌ای می‌دانند.

و: شنود و دریافت غیر مجاز (جاسوسی) داده‌های رایانه‌ای

شنود غیر مجاز همچون دسترسی غیرمجاز ناشی از عدم رضایت دارنده واقعی یا قانونی داده یا محتوای در حال انتقال می‌باشد. همچنین شرط غیرقانونی بودن نیز به شرط رضایت اضافه می‌شود، رکن قانونی این جرم ماده ۲ قانون جرائم رایانه (ماده ۷۳۰ ق. م.ا) می‌باشد، این جرم در واقع همان تعرض به حریم ارتباطات به وسیله شنود سنتی و ضبط مکالمات تلفنی افراد را بیان می‌کند(جلالی فراهانی، ۱۳۸۹: ۲۸)همچنین موضوع بزه در شنود غیرمجاز، محتوای است. برای محتوا ویژگی در حال انتقال پیش بینی شده است یعنی این بزه تنها داده‌های در حال رفت و آمد را در بر میگیرد و نسبت به داده‌های دیگر، شنود همان دسترسی است. محتوای در حال انتقال باید در یک پیوند خصوصی میان دو یا چند نفر انجام گیرد تا شرط انتقال غیر عمومی مفهوم محرمانگی پیدا کند.

بخش سوم: چالش‌های نظام عدالت قضایی در جرایم مربوط به رمز ارزها

با توجه به سیاست جنایی ایران در قبال جرایم مرتبط با ارزهای دیجیتال و گسترش روزافزون اینترنت در جهان و ایران، و ضریب نفوذ بالای آن در جوامع امروزی، علاوه بر روش‌های به کارگیری درست آن، بزهکاری‌هایی که اساس آن بر اینترنت است، نیز رو به افزایش است. در دهه اخیر به علت گسترش باورنکردنی اینترنت در جهان، کشورهای توسعه یافته و کشورهای در حال توسعه، بر اساس ضریب نفوذ اینترنت در کشورشان، با تبهکاریها و بزهکاریهای متعددی مواجهند. تنوع و میزان جرائم در کشورهای مختلف به سطح فرهنگی آن جامعه، میزان سواد و عوامل اجتماعی و غیره بستگی دارد. اما عموماً جرائم مالی یا



همان جرائم علیه اموال و مالکیت که در فضای مجازی (اینترنت) اتفاق می افتد، در اغلب کشورها در صدر میزان این نوع جرائم قرار دارد. البته خود این جرم نیز صور مختلفی دارد که کلاهبرداری سایبری (اینترنتی به علت گوناگونی در روش های اجرای آن و فراوانی افرادی که مورد بزه قرار می گیرند، بیشترین آمار را در جرائم علیه اموال در فضای اینترنت به خود اختصاص داده است. در این زمینه باید توجه کرد با اینکه در ایران ورود اینترنت به دهه ۱۳۷۰ بازمی گردد، اولین جرم در فضای کامپیوتری و اینترنت در سال ۱۳۸۱ اتفاق افتاد، که شروعی برای جرائم اینترنتی در ایران بود. به طوری که از آن سال به بعد، این نوع جرائم به ویژه جرم کلاهبرداری اینترنتی افزایش یافت و علت آن هم نبود قانونی مناسب و بازدارنده بود. بر این اساس، مؤثرترین قانون آن زمان، یعنی قانون تجارت الکترونیکی در سال ۱۳۸۲ تصویب شد که البته نواقص و کمبودهای زیادی داشت و همین امر باعث شد میزان این جرائم روز به روز بیشتر شود. این مسئله باعث شد قانون گذار این خلأ قانونی را بیش از پیش احساس کند و بر این اساس، در سال ۱۳۸۸ قانون جرائم رایانه ای به تصویب مجلس شورای اسلامی رسید. این قانون تا حدی خلأ قانونی مورد نظر را در آن برهه زمانی پوشش داد، ولی متأسفانه در آن فقط یک ماده به جرم کلاهبرداری اینترنتی تخصیص داده پدیدآورندگان آن دسته از نرم افزارهای رایانه ای را که مورد حمایت این قانون قرار گرفته اند، جرم تلقی کرده است. سومین واکنش قانون گذار ایران در مقابل جرائم کامپیوتری در سال ۱۳۸۲، تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۹/۱۰/۱۳۸۲ مجلس شورای اسلامی بود. براساس ماده این قانون، جعل اطلاعات و داده های رایانه ای، .. و سوءاستفاده مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی شده و مرتکب حسب مورد، به مجازات جرم ارتكابی محکوم می شود. چهارمین واکنش قانونی مرتبط با جرائم رایانه ای، تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی بود. بر اساس مواد ۶۶، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵، ۷۶ و ۷۷ این قانون، کلاهبرداری، جعل و دستیابی و افشای غیر مجاز اسرار تجاری، نقض حقوق مربوط به



مالکیت معنوی (کپی رایت) و غیره ... که از طریق رایانه و در بستر تجارت الکترونیکی انجام گیرد، جرم تلقی شده، و برای آن مجازات تعیین شده است. شایان ذکر است هر یک از چهار قانون یادشده در بستر خاص خود قابلیت اعمال دارند. همان طور که از مطالب پیش گفته مشخص شد، در آن زمان برای مقابله با سایر جرائم اینترنتی قانونی کامل وجود نداشت، از همین رو، نیاز به یک قانون جامع در این زمینه بیش از پیش احساس می‌شد، به این دلیل در سال ۱۳۸۸، بالاخره قانون جرائم رایانه‌ای تصویب شد و در ماده ۱۳ آن کلاهبرداری اینترنتی جرم انگاری شد (السان، ۱۳۸۶، ۶۳). بطور کلی برخی بر این باورند که به سیاست جنایی ایران درباره پیشگیری از جرائم سایبری و نیز ایرادهایی مانند نبود برنامه‌های مشخص و منسجم، وارد است که رفع این ایرادها نیز نیازمند یک برنامه‌ای جامع، مشخص و اجرashدنی است. (انصاری؛ میلانی، ۱۳۹۵: ۱۴۳) همین امر در خصوص ارزشهای دیجیتال نیز مورد تأیید و تاکید است. آنچه که امروزه در خصوص سیاست جنایی ایران در ارتباط با ارزشهای دیجیتال به چشم می‌آید. نوعی بلاتکلیفی و حالت انفعالی است که خود میتواند موجب سو استفاده و بروز جرائم گردد. از طرفی دیگر اتخاذ یک سیاست جنایی مشخص می‌تواند علاوه بر رشد اقتصادی، امنیت و آسایش را نیز برای کسانی که در این حوزه فعالیت دارند و یا افرادی که قصد ورود به مبادلات اینگونه ارزشها را دارند بیشتر فراهم آورد.

بند اول: چالش های نظام عدالت قضایی

رمزگذاری صحیح داده های الکترونیکی جهت انجام آنچه توسعه دهنده نرم افزار می خواهد، می‌تواند بسیار مشکل تر از برنامه ریزی نرم افزار سنتی باشد.^۱ به علاوه به جهت

^۱. Kevin Delmolino, Mitchell Amett, Ahmed Kosba, Andrew Miller & Elaine Shi, Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, <https://eprint.iacr.org/T.۱۰/۴۸۰.pdf> ("Our lab experiences show that even for very simple smart contracts (e. g. a 'Rock, Paper, Scissors' game), designing and implementing them correctly was



ماهیت خود اجرای دیال.تی، حتی اشتباهات کوچک منجر به نتایج و آثار بزرگی می‌شود. برای مثال یک سازمان مستقل غیر متمرکز مبتنی بر اتریوم - که به طور فراگیر به آن اشاره می‌شود، دائو است که براساس رمز رایانه‌ای قراردادهای الکترونیکی عمل می‌کند. کد حاوی یک اشکال شناخته شده بود که برنامه ریزان به طور فعال جهت درست نمودن آن کار می‌کردند که در نهایت به یکی از شریکان دائو اجازه داد تا ۳.۶ میلیون اتر که تقریباً ۵۰ میلیون دلار ارزش داشت را منتقل کند. برنامه نویس دانو "کریستف جتزج" یک کهنه سرباز اتریوم با مدرک دانشگاهی فیزیک و ریاضی نظری است. او یک طراح سیستم‌های نرم افزاری یا کد نویس نیست. اما او شخص باهوشی بود که متوجه اتریوم شد و آن را فهمید. او حتی تجربه حرفه‌ای به عنوان آزمایش کننده نرم افزار داشته است. به عبارت دیگر حتی دانشمندان رایانه ای خوب آموزش دیده و با تجربه در این زمینه و با فهم عمیق از اتریوم ممکن است زمانی که قراردادهای الکترونیکی را برنامه‌ریزی می‌کنند دچار اشتباه شوند. در واقع به علت مشکلات رمزگذاری قراردادهای الکترونیکی، پیشروها در صنعت تلاش می‌کنند تا ممیزی‌های کد قرارداد هوشمند استاندارد را توسعه دهند. نکته اینجاست که علاوه بر هر موضوع ذاتا قانونی دیگر که حاکم بر مورد کاربردی قرارداد هوشمند باشد، کسب و کارهای ارائه دهنده خدمات مبتنی بر قراردادهای الکترونیکی باید مواظب مسئولیت بالقوه در خصوص اشتباهات در برنامه ریزی باشند. چنین موضوعات حقوقی ممکن است شامل مسئولیت محصول تولید شده، نقض (نرم افزار به عنوان یک خدمت) قرارداد، رویه‌های تجاری ناعادلانه و فریبنده، امنیت سایبری و غیره باشد. موارد کاربردی در حال ظهور که تحت رژیم های حقوقی کاملا متفاوت قرار می گیرند. (صادقی نشاط، ۱۳۸۳: ۱۹)

بند دوم: نارضایتی از تمرکز زدایی در فرایند دادرسی

تجزیه و تحلیل انجام شده تاکنون نشان می‌دهد که فن‌آوری‌های ارزهای دیجیتال جاییکه



قواعد داوری می تواند بدون تکیه بر دادگاههای دولتی اجرا شود منجر به ظهور سیستمهای تصمیم‌گیری و قضاوت خصوصی می شود. این به نوبه خود نشان می‌دهد که همچنان که خود اجرایی فن آوری محور حرکت و جنب و جوشی به دست می‌آورد، ممکن است برای دادگاه های ملی به طور فزاینده‌ای دشوار گردد که محتویات نتایج حل اختلاف را به دقت مورد بررسی قرار دهند. با این حال این ارزیابی به جای وضعیت فعلی آینده امور را نگاه می‌کند. در حال حاضر فن آوری‌های دیجیتال هنوز در حاشیه سازی دادگاه های کشور موفق نبوده اند اما در واقع منجر به وقوع پدیده های متضادی شده‌اند. میزان قابل توجهی از دادرسی دادگاه به ویژه در ایالات متحده آمریکا مربوط به افزایش آی.سی.او.هاست. در طول دو سال گذشته آی.سی.او.ها، چشم انداز سرمایه گذاری خطرپذیر، بازارهای مالی و قوانین مالی شرکتی را مختل کرده اند اما همچنین برخی از پرونده های دادگاهی با ارزش قابل توجه را افزایش داده اند (فتحی زاده، ۱۳۹۹: ۱۱) این پرونده ها سوالات جذاب و بی پاسخی به خصوص در مورد صلاحیت پیش رو قرار می‌دهند.

بند سوم: صحت اعتبار سنجی

این مشکل از زمان ورود بیت کوین به دوران بحران مالی خود و نوسان شدید قیمت این ارز در بازارهای مالی جهان به وجود آمد. به این جهت بسیاری از کشورهای در حال توسعه با مشاهده چنین نوسانی به دلایلی همچون عدم وجود قوانین در جهت مشروعیت بخشیدن به استفاده از این ارزها در نظام اقتصادی خود یا نبود سیستم مرکزی پرداخت این ارزها در به کارگیری آنها در معاملات متعاملین، استفاده از این ارزها را ممنوع اعلام نمودند. به دنبال آن در سطح بین الملل جهت جلوگیری از تاثیر تجارت جهانی از نوسانات شدید بیت کوین، ارز اتریوم جایگزین آن در معاملات میان تجار گردید (قلی زاده، ۱۳۸۶: ۲) کشورهای جهان نیز مبادرت به تصویب کنوانسیون یکنواخت سازی معاملات مبتنی بر ارزهای مجازی در سال ۲۰۱۷ نمودند. با رعایت مقررات این کنوانسیون و الحاق کشورها به آن می‌توان



مسأله اعتبارسنجی معاملات این نوع ارزها و همچنین نوسانات قیمت آنها را به جهت تعیین رسمی مالکیت هر فرد بر هر ارز تعیین نمود. چنین امری می تواند از وقوع پولشویی در بازارهای پولی نیز جلوگیری نماید. ارزهای رمزنگاری شده پول های دیجیتالی نظیر به نظیرا و آنلین جهت مدیریت و توزیع معاملات می باشند. میزان ارزش مالی این ارزها تابع عرضه و تقاضا بوده و در معاملات الکترونیکی جهت انجام امور تجاری مورد استفاده قرار می گیرد. این ارزها فایل های کامپیوتری در فرمت های text می باشند که از قابلیت تخریب پذیری برخوردار هستند. این ارزها در کامپیوترهای شخصی یا سرویس های آنلین تایید شده توسط حکومت مانند فضا های ابری، قابلیت ذخیره داشته و پرداخت عوض معامله از طریق آنها همانند ارسال ایمیل به صورت کاملاً ساده می باشد. برای آن که ارزهای رمزنگاری شده امکان پرداخت و دریافت را داشته باشند باید معاملات انجام شده توسط آن بین طرفین در یک سربرگ عمومی مانند بلاک چین منعقد گردند... مطابق با توضیحات بیان شده تنها تفاوت پول های دیجیتالی با پول های کاغذی در دیجیتالی بودن آن می باشد و نوسانات قیمت آن در بازارهای مالی جهانی امری طبیعی بوده که می تواند در بسیاری از کالاهای مشابه دیجیتالی و حتی کالاهای مادی مانند طلا و نفت نیز رخ دهد (همان، ص ۱۴). بنابراین چالش هایی که توسط برخی دکترین در خصوص خطرات به کارگیری این ارزها در نظام مالی بیان شده است با تصویب برخی قوانین و الحاق به کنوانسیون های بین المللی مصوب در این خصوص قابل حل است.

بند چهارم: بدون پشتوانه بودن و غیر متمرکز بودن

ارز دیجیتال می تواند اولین نظام پرداخت دیجیتال کاملاً غیر متمرکز جهان بدون نیاز به بانک مرکزی باشد. نظام پرداختی بیت کوین یک سامانه خصوصی است، اما هیچ موسسه مالی سنتی متعارفی در تراکنش ها وجود ندارد. بر خلاف ارزهای دیجیتالی اولیه که یک شخص یا موجودیت مرکزی داشتند، نظام بیت کوین کاملاً غیر متمرکز است و همه



تراکنش‌ها توسط کاربران نظام پرداخت بیت کوین انجام می‌شود. همین امر می‌تواند در نظام پرداختی قراردادها اختلال ایجاد کرده و ضمانت اجرایی آنها را به خطر بیندازد (محمودی، ۱۳۸۸: ۱۸)

بند پنجم: سهولت ارتکاب جرایم

با عنایت به عدم حاکمیت قانونی خاص بر قلمرو پول مجازی با استفاده از آن می‌توان به پول شویی، فرار مالیاتی و سایر جرائم اینترنتی دامن زد و زمینه ارتکاب این پدیده‌ها را تسهیل نمود. ریشه این مسأله در امکان عدم تطابق مشخصات کاربری مالکان این پول‌ها با هویت حقیقی آنها است. در واقع، صاحبان این وجوه نه بینام، که گمنام هستند و از این رو زمینه ارتکاب چنین تخلفات و جرایمی برای آنها ساده‌تر است. (ریاضی مند، ۱۳۹۷: ۴۶)

اگر چه امکان رهگیری تراکنش‌ها و شناسایی ردپای یک کاربر در این شبکه‌ها وجود دارد، اما سیاست‌گذاری بر شفافیت و تعقیب چنین امری نبوده است.

بند ششم: نقش داوری در حل و فصل اختلافات ناشی از دعاوی مرتبط با ارزهای

دیجیتال

در سیستم ارزهای دیجیتال نظیر بیت کوین کاربران یک سیستم قضاوتی خصوصی طراحی کرده‌اند که کمی پیچیده‌تر از ساز و کار سپرده‌گذاری است که در ابتدا توسط ناکاموتو پیش‌بینی شده بود؛ نشانی چند امضا. این ابزار اساساً مانند یک قفل دو کلیده است که اگر دو کلید استفاده شود قفل باز می‌شود. دو طرفی که وارد معامله می‌شوند می‌توانند تا زمانی که تعهدات ناشی از آن معامله انجام می‌شود، از این ابزار برای ذخیره سکه‌ها استفاده کنند (به عنوان مثال قیمت فروش کالاهایی خاص). هر دو طرف با یک کلید دیجیتال به نشانی مجهز می‌شوند. در صورت عدم اختلاف آنها می‌توانند از هر دو کلید برای باز کردن قفل سکه‌ها استفاده کنند که به طور مشترک مقصد نهایی خودشان را (معمولاً نشانی فروشنده



تعیین می‌کنند (سلطانی، اسدی ۱۳۹۴: ۱۲) با این وجود در صورت اختلاف، هیچ یک از طرفین نمی‌توانند سکه خود را مستقلاً برداشت نمایند، اما هر یک از آنها می‌توانند یک داور خصوصی برای بررسی حقایق پرونده و تعیین اینکه کدام یک از دو طرف اختلاف نسبت به وجوه مورد اختلاف مستحق است را درخواست نمایند.

نتیجه گیری

فن‌آوریهای دیجیتال در زمینه مبادلات مالی و رمز ارزها تاثیر دوگانه‌ای بر آینده دارند. تسهیل در تشریفات قراردادی از یکسو و چالش‌هایی نظیر صحت اعتبار سنجی و بدون پشتوانه بودن ارزهای دیجیتال و همچنین جرائم مرتبط با آنها از مهم‌ترین دلایلی است که ارزهای دیجیتال ملزم به بررسی و واکاوی از ابعاد متفاوت می‌باشند. از یک سو با نگاهی به تحولات احتمالی آینده این فن‌آوری‌ها به نظر می‌رسد که این توانایی را دارند که با ایجاد سیستم‌های خود اجرای حل و فصل اختلافات خصوصی، دادگاه‌های دولتی را به حاشیه ببرند. واضح است که استفاده از انواع ارزهای دیجیتال و پول الکترونیک انواع جدیدی از اختلافات و جرائم را به وجود می‌آورد که نیازمند شکل‌های جدید حل اختلاف است. در بیشتر موارد چنین اختلافاتی همچنان نیازمند مداخله انسانی است. هنوز در کشور ما قوانین مدونی به طور خاص به ارزهای دیجیتال اختصاص نیفتاده است و صرفاً پیش‌نویسی در سال ۱۳۹۷ و اصلاحاتی به دنبال آن در سالهای بعد مورد بررسی قرار گرفت که قطعیت پیدا نکرده است. از طرفی با عنایت به عدم حاکمیت قانونی خاص بر قلمرو پول مجازی با استفاده از آن می‌توان به پول شویی، فرار مالیاتی و سایر جرائم اینترنتی دامن زد و زمینه ارتکاب این پدیده‌ها را تسهیل نمود. ریشه این مسأله در امکان عدم تطابق مشخصات کاربری مالکان این پول‌ها با هویت حقیقی آنها است. در واقع، صاحبان این وجوه نه بینام، که گمنام هستند و از این رو زمینه ارتکاب چنین تخلفات و جرایمی برای آنها ساده‌تر است. مهمترین راهکارهای به منظور جلوگیری از گسترش تخلفات در زمینه مبادلات ارزهای دیجیتال تصویب قوانین مدون، و اعمال نظارت‌های قانونی بر انجام این گونه



مبادلات می‌باشد. پیشنهاد پژوهش پیش رو آن است که:

۱_ اتخاذ سیاست‌های حقوقی و تصویب قوانینی برای جلوگیری از بلا تکلیفی و حالت انفعالی در مواجهه با ارزش‌های دیجیتال به منظور افزایش امنیت در فضای مذکور و توسعه و رشد اقتصادی صورت گیرد.

۲_ موافقت و ایجاد مرجع مرکزی برای فعالیت‌های مالی توسط ارزش‌های دیجیتال و نظارت مستقیم به منظور کاهش جرایم در این حوزه شناسایی شده و رفع چالش‌های مساله نظیر مشکلات امنیتی و برگشت پذیر نبودن پول، جرائم مرتبط مانند پولشویی، فرار مالیاتی و ... پیچیدگی فنی فراهم گردد.



منابع مآخذ

الف: منابع فارسی

- السان، مصطفی، تشکیل قراردادهای الکترونیکی، فصلنامه پژوهشنامه بازرگانی، شماره ۶۳، ۱۳۸۶.
- تفقدی اسراری، حسین، تاریخچه پول و روند تکاملی آن، تاریخ پژوهی شماره ۵۴، ۱۳۹۷.
- جعفری لنگرودی، محمد جعفر، ترمینولوژی حقوق، جلد اول، انتشارات گنج دانش، چاپ ششم ۱۳۷۲.
- جلالی فراهانی، امیرحسین، صاحت کلی سایبری در پرتو قوانین داخلی، در: حقوق فن آوری اطلاعات و ارتباطات (مجموعه مقالات)، انتشارات روزنامه رسمی جمهوری اسلامی ایران، چاپ نخست، ۱۳۸۸.
- دره شامی، قاسم، شرایط اعتبار قرارداد الکترونیکی، دانشگاه آزاد اسلامی واحد ماکو، ۱۳۹۷.
- ریاضی مند، مهران، بررسی ابعاد حقوقی ارزشهای دیجیتال، نشر برتر اندیشان، ۱۳۹۷.
- ریوار، ژان، تاریخ بانک و بانکداری، ترجمه شیرین هشترودی، تهران سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۹.
- صادقی نشاط، امیر، تحلیل حقوقی جنبه هایی از پرداخت الکترونیک، مجموعه مقالات همایش بررسی ابعاد حقوقی فن آوری اطلاعات، ۱۳۸۳.
- صفایی، سید حسین، حقوق مدنی، دوره مقدماتی، ج ۲، نشر میزان ۱۳۸۹.
- عمید، حسن، فرهنگ فارسی عمید، تهران، انتشارات امیر کبیر، ۱۳۸۰.
- فتحی زاده، امیر هوشنگ، حقوق بلاکچین، شرکت چاپ و بازرگانی، تهران، ۱۳۹۹.
- قلی زاده، احد، تحلیلی بر انعقاد الکترونیکی معاملات، پژوهش نامه بازرگانی، شماره ۲، ۱۳۸۶.



- کاتوزیان، ناصر، حقوق مدنی، قواعد عمومی قراردادها، جلد ۲، چاپ چهارم، شرکت انتشار، ۱۳۷۶.
- کمرخانی، پری، شرایط صحت قراردادهای الکترونیکی، دانشگاه آزاد اسلامی و احد ایلام، ۱۳۹۸.
- محمودی، محبوبه، انعقاد قرارداد الکترونیکی (با تاکید بر قانون تجارت الکترونیکی ایران و مقررات بین المللی)، مرکز پیام نور تهران، دانشکده علوم انسانی و پایه، ۱۳۸۸.
- بانک مرکزی، ج.ا.ایران، پیش نویس الزامات و ضوابط حوزه رمز ارزها، معاونت فن آوری-های نوین، ۱۳۹۷.
- سلطانی محمد، اسدی، حمید، ماهیت حقوقی پرداخت در پول الکترونیک، پژوهش نامه حقوق اسلامی، سال شانزدهم، شماره اول، پیاپی ۴۱، بهار و تابستان ۹۴.

ب: منابع انگلیسی

- *European Central Bank (2012). Virtual Currency Schemes. Frankfurt am Main: European Central Ban.*
- *Dominick Romeo, Hidden Threat: The Dark Web Surroundin.*
- *Cyber Security, 43 N. Ky. L. Rev. 73, 2016.*
- *Ethan D. Jeans, Funny Money or the Fall of Fiat: Bitcoin and Forward.*
- *Facing Virtual Currency Regulation, 13 J. on Telecomm. & High Tech .*