

## پولشویی از طریق ارزهای دیجیتال

### (تجزیه و تحلیل پدیده و اقدامات پیشگیرانه مناسب)

(تاریخ دریافت ۱۴۰۱/۰۲/۱۵، تاریخ تصویب ۱۴۰۱/۰۶/۰۶)

سهیلا مرادی قلعه

#### چکیده

نیاز به آموزش و کسب دانش در حوزه ارزهای دیجیتال، هم برای کاربران عادی احساس می‌شود و هم برای نهادهای قانون‌گذار. هرچه این نهادها از دانش بیشتری در رابطه با ارزهای دیجیتال برخوردار باشند، بهتر می‌توانند زوایای پیدا و پنهان و چالش‌های موجود در این صنعت را کشف کنند و برای آنها راه‌حل‌های کاربردی ارائه کنند. پولشویی به عنوان تلاش یا اقدام در پنهان کردن هویت درآمدهای غیرقانونی و سعی بر قانونی جلوه دادن آنها تعریف می‌شود؛ مجرمان برای پنهان کردن منشا غیرقانونی وجوه خود از طرق مختلفی وارد عمل می‌شوند ولی یکی از راحت‌ترین این روش‌ها آن است که این پول‌های کثیف تحت نام ارزهای دیجیتال معامله شود. اگرچه ارز رمزنگاری شده برای فعالیت‌های غیرقانونی قابل استفاده است اما تأثیر کلی بیت کوین و سایر ارزهای رمزی پایه در پولشویی و جرایم دیگر مرتبط با پولشویی در مقایسه با معاملات نقدی بسیار ناچیز است چراکه در سال ۲۰۱۹ حجم پولشویی‌هایی انجام شده با استفاده از بیت کوین به ۲ میلیارد و ۸۰۰ میلیون دلار رسید این اتفاق در حالی افتاد که در سال ۲۰۱۸ تنها ۱ میلیارد پول کثیف با استفاده از بیت کوین جابه‌جا شد و از ابتدای سال جاری نیز حجم کل پولشویی‌های انجام شده با استفاده از بیت کوین تنها ۸۲۹ میلیون دلار تخمین زده شده است؛ این بدان معناست که از ابتدای سال جاری تاکنون تنها ۰.۵ درصد از بیت کوین‌های استخراج شده برای هدف پولشویی مورد استفاده قرار گرفته‌اند؛ با اینحال باگ‌های بلاکچین‌ها در تایید هویت مشتریان خود منجر شده است تا پولشویی‌های گسترده‌ای در این حوزه صورت بگیرد. با این تفاسیر باید این راه پولشویی را در قالب یک مقاله علمی مورد تجزیه و تحلیل قرار داد و اقدامات پیشگیرانه مناسب در این راستا را بیان کرد.

**واژگان کلیدی:** بیت کوین، ارز دیجیتال، جرایم اقتصادی اینترنتی، هکر، پولشویی

الکترونیکی و سنتی، پول‌های نامشروع

## مقدمه

مجرمان برای کسب درآمد از طریق فعالیت‌های غیرقانونی مانند فروش مواد مخدر، کلاهبرداری، قاچاق اسلحه یا قاچاق انسان، باید راهی داشته باشند که وجوه غیرقانونی را به پولی تبدیل کنند که در ظاهر قانونی باشد. به این فرایند «پول‌شویی» می‌گویند. ارزهای دیجیتال ویژگی‌هایی دارند که آنها را به گزینه‌های مناسبی برای پول‌شویی و انتقال مبالغ غیرقانونی تبدیل می‌کند. ردیابی این ارزها سخت است، تراکنش‌های آنها ناشناس است، قانون‌گذاری مشخص و سفت‌وسختی درمورد آنها وجود ندارد، هزینه انتقال آنها پایین است، بدون نیاز به واسطه منتقل می‌شوند، می‌توان در چند دقیقه آنها را از کشوری به کشور دیگر منتقل کرد و به سایر ارزهای دیجیتال یا حتی دارایی‌های ملموس تبدیل کرد و بسیاری دلایل دیگر که دست به دست هم داده‌اند تا ارزهای دیجیتال را به ابزار پرداخت محبوب مجرمان و کلاهبرداران تبدیل کنند. پیش از ظهور ارزهای دیجیتال، پول‌شویی با ارزهای فیات به این شکل بود که مجرمان چندین حساب بانکی مختلف را ایجاد می‌کردند و پول‌های خود را با عناوین مختلف، در بین این حساب‌ها جابه‌جا می‌کردند. برای ایجاد هریک از این حساب‌ها، شخص مجرم باید مراحل احراز هویت را طی می‌کرد و اطلاعات هویتی خود را در اختیار بانک قرار می‌داد. نقل‌وانتقال پول در این سیستم سنتی، به‌شدت تحت‌کنترل بانک‌های مرکزی قرار داشت. انتقال پول در قالب ارز دیجیتال دقیقاً در نقطه مقابل ارزهای فیات قرار دارد. برای انتقال ارزهای دیجیتال، تنها چیزی که به آن نیاز دارید آدرس کیف پول طرف مقابل است. تراکنش‌های ارزهای دیجیتال کنترل نمی‌شوند و هیچ قدرت مرکزی یا واسطه‌ای آنها را بررسی نمی‌کند. البته برای تبدیل ارزهای دیجیتال به پول فیات، باید از یک صرافی ارز دیجیتال کمک بگیرید. یکی از راهکارهایی که صرافی‌ها برای کاهش پول‌شویی از طریق ارزهای دیجیتال اندیشیده‌اند، ملزم‌کردن کاربران به احراز هویت است. امروزه اکثر صرافی‌های بزرگ دنیا که حجم معاملات بالایی دارند، کاربران خود را ملزم به احراز هویت می‌کنند؛ اما همچنان صرافی‌های (غالباً) کوچک‌تری وجود دارند که الزامی را برای احراز هویت در نظر نگرفته‌اند.

## بخش اول: بررسی طرق و روش‌های پولشویی مجرمان در بیت کوین

پولشویی با بیت کوین به دلیل پیچیدگی و ریسک بالا یک استراتژی ناکارآمد محسوب می‌شود. براساس گزارش سازمان ملل، پولشویی سالانه بین ۸۰۰ میلیارد دلار تا ۲ تریلیون

دلار برای اقتصاد جهانی هزینه برمی‌دارد. این میزان تقریباً مبلغ ۲ تا ۵ درصد تولید ناخالصی داخلی جهانی است.<sup>۱</sup> امروزه با وجود توسعه در فناوری که موجب ظهور ابزارهای جدیدتر و سریع‌تر شده است اما هنوز بیش از ۹۰ درصد پولشویی‌ها هنوز کشف نشده‌اند. در واقع مجرمان از این توسعه و پیشرفت برای ادامه پولشویی استفاده می‌کنند. در همین زمان، مقامات دولتی و کمپانی‌های فین تک برای شناسایی ویژگی‌های معاملات و کمک به افشای کلاهبرداری‌ها به تکنولوژی نفوذ کرده‌اند و از آن استفاده می‌کنند.<sup>۲</sup>

### بند اول: امکان پولشویی با بیت کوین

بسیاری از مجرمان از رمز ارزها برای رسیدن به اهداف خود بهره می‌گیرند و در این بین، بیت کوین یکی از محبوب‌ترین انتخاب‌های آن‌هاست. بیت کوین و سایر رمز ارزها به ابزار اصلی مجرمان سایبری برای پول‌شویی و پنهان کردن رد منابع اصلی دارایی‌های غیرقانونی تبدیل شده است. سادگی پول‌شویی با استفاده از رمز ارزها نسبت به سایر روش‌ها، یکی از اصلی‌ترین دلایل محبوبیت بیت کوین در میان مجرمان و کلاهبرداران است. معمولاً تصور ما از پول‌شویی آن چیزی است که در فیلم‌ها و سریال‌ها دیده‌ایم که فرد یا گروهی پول‌های نامشروع خود را با استفاده از کیف‌ها و ساک‌های بزرگ یا چمدان‌ها از مرز رد می‌کنند تا نهادهای نظارتی را دور بزنند، اما در زندگی واقعی این‌گونه نیست.<sup>۳</sup> به جای این روش‌های دراماتیک، تبدیل پول‌های نامشروع به بیت کوین یا رمز ارزهای دیگر از طریق صرافی‌های آنلاین و سپس تبدیل آن رمز ارزها به پول نقد روشی بسیار آسان‌تر و کم‌دردتر خواهد بود. تراکنش‌های آنلاین توسط مرزهای جغرافیایی محدود نمی‌شوند و زحمت جابجایی‌های فیزیکی پرخطر پول‌ها را هم از بین می‌برد. علاوه بر این، رمز ارزها به دلیل ثبت نکردن نام کاربر در آدرس عمومی مورد استفاده در تراکنش‌ها، درجه‌ای از ناشناس بودن را ارائه می‌کنند که برای مجرمان سایبری ایده‌آل است. اگرچه تمامی تراکنش‌های انجام شده با بیت کوین به صورت عمومی در بلاک‌چین ثبت می‌شوند، اما فقط شخصی که تراکنش را انجام داده می‌تواند به حساب و کیف پول دسترسی داشته باشد. همین عامل امکان اتصال

۱ محمودی، حسین، (۱۳۸۴)، مبارزه با جرائم اقتصادی، نشر جهان جام جم، چاپ اول، ص ۱۱۱

۲ عارفی مسکونی، محمد، جرایم پولشویی، ۱۳۸۴، چاپ اول، تهران، انتشارات آریان، ص ۸۰

۳ هادیان، ابراهیم، پولشویی و ارتباط با جرائم دیگر، ۱۳۸۲، همایش بین المللی مبارزه با پولشویی، دانشگاه شیراز، نشر

تراکنش‌های بیت‌کوین به یک شخص یا نهاد را به یک چالش تبدیل می‌کند. با این حال، رهگیری تراکنش‌ها کاملاً غیرممکن نیست. هنگامی که پول‌شویی انجام شد، آن‌ها می‌توانند بدون هیچ نگرانی از دستگیری و مجازات، رمز ارزها را به پول نقد تبدیل کنند. در ادامه به روش‌های رایج استفاده از بیت‌کوین برای پول‌شویی اشاره می‌کنیم:

- **میکسر بیت‌کوین:** میکسرهای بیت‌کوین دارایی‌های دیجیتال نامشروع و مشروع از چند آدرس مختلف را پیش از عرضه‌ی مجدد آن‌ها به کیف پول‌ها یا آدرس‌های مقصد، با یکدیگر ترکیب می‌کنند. این فرایند ترکیب دارایی‌ها باعث افزایش درجه‌ی ناشناس ماندن تراکنش‌ها خواهد شد، بنابراین مجرمان اغلب برای پنهان کردن رد انتقال دارایی‌های خود به کسب‌وکارهای مشروع یا صرافی‌های بزرگ از این روش بهره می‌گیرند.
- **صرافی‌های نامعتبر:** اگرچه بسیاری از صرافی‌های بزرگ دنیای رمز ارزها قوانین ضد پول‌شویی و شناسایی کاربران را به کار گرفته‌اند، اما خیلی از صرافی‌های غیرمعتبر فرایند احراز هویت را انجام نمی‌دهند. هنگامی که یک رمز ارز در یک صرافی نامعتبر مکرر به رمز ارز دیگری تبدیل شود، به مرور تبدیل به یک دارایی تمیز می‌شود. این فرایند به کلاه‌برداران اجازه می‌دهد با کمک سرویس‌های میکسینگ، دارایی نامشروع خود را با امنیت به یک کیف پول اکسترنال انتقال بدهند. گزینه‌ی دیگر تبدیل رمز ارز به پول نقد است. اما این روش رواج کمتری دارد، زیرا بیشتر صرافی‌های غیرقانونی بازار فیات ندارند و اگر داشته باشند، کسب‌وکارشان دوام چندانی نخواهد داشت.
- **شرط‌بندی و وب‌سایت‌های گیمینگ:** پلتفرم‌های شرط‌بندی و گیمینگ اغلب از دریافت بیت‌کوین یا سایر رمز ارزها به‌عنوان روش پرداخت پشتیبانی می‌کنند و همین موضوع آن‌ها را به یکی از مقاصد مورد علاقه‌ی کلاه‌بردارانی تبدیل کرده‌است که از رمز ارزها برای پول‌شویی استفاده می‌کنند. این دسته از مجرمان از رمز ارزهای خود برای خرید اعتبار، آیتم‌های مجازی یا ارز بازی‌های مورد نظر روی این پلتفرم‌ها استفاده می‌کنند و پس از چند تراکنش روی وب‌سایت، دارایی خود را نقد می‌کنند. زمانی که وب‌سایت‌های مذکور پول را به یک حساب منتقل کنند، این پول اعتبار قانونی پیدا می‌کند.

- **سرویس‌های شبکه‌ای:** سرویس‌های شبکه‌ای یا Nested Services که طیف گسترده‌ای از سرویس‌ها را در برمی‌گیرد در یک صرافی یا بیشتر فعالیت می‌کند. این سرویس‌ها از آدرس صرافی‌های میزبان استفاده می‌کنند تا به امکان تبدیل سریع کوین‌ها به پول نقد که در اختیار صرافی‌هاست دسترسی پیدا کنند و از فرصت‌های مناسب برای معامله بهره بگیرند. بعضی از صرافی‌ها استانداردهای سختگیرانه‌ای در برابر سرویس‌های شبکه‌ای ندارند و این نقص سبب شده تا پول‌شویی برای مجرمان ساده‌تر شود. هنگامی که سرویس‌های شبکه‌ای یک تراکنش را تکمیل می‌کنند، این تراکنش در دفترکل بلاک‌چین ظاهر می‌شود، اما به‌جای آدرس این سرویس‌ها یا آدرس شخصی، تحت آدرس صرافی ثبت می‌شود. کارگزاران غیرقانونی رایج‌ترین نوع از سرویس‌های شبکه‌ای هستند. زمانی که مجرمان از این کارگزاران استفاده می‌کنند، می‌توانند به‌صورت ناشناس مبالغ هنگفتی از رمز ارزها را معامله کنند و کارگزاران غیرقانونی هم نقش تسهیل‌کننده‌ی معاملات بین دو طرف در خارج از صرافی‌ها را اجرا می‌کنند. این معاملات امن و سریع هستند و کارگزاران هم برای پیدا کردن دو طرف تراکنش حق کمیسیون دریافت می‌کنند، اما خودشان در مذاکرات مشارکتی ندارند. هنگامی که طرفین تراکنش بر شرایط معامله به توافق رسیدند، دارایی‌ها از طریق کارگزار منتقل می‌شوند.
- **سرویس پنهان‌سازی هویت:** با توجه به این که تراکنش‌های بیت‌کوین و سایر رمز ارزها در بلاک‌چین‌های مورد استفاده‌ی آن‌ها ثبت می‌شوند، معمولاً می‌توان منبع اصلی را ردیابی کرد. به همین دلیل، بعضی از مجرمان سایبری از سرویس‌های مخفی‌سازی هویت برای پنهان کردن منبع دارایی خود استفاده و ارتباطات میان تراکنش‌های بیت‌کوین را قطع می‌کنند. مردم اغلب از نیاز به حفظ حریم شخصی به‌عنوان دلیل اصلی برای استفاده از این سرویس‌ها یاد می‌کنند، اما کلاه‌برداران با سوء استفاده از این موضوع از قابلیت این سرویس‌ها برای اهداف مجرمانه‌ی خود بهره می‌گیرند. شرکت در عرضه‌ی اولیه‌ی یک کوین با استفاده از کوین دیگر برای خرید کوینی متفاوت، مانند خرید اتریوم با بیت‌کوین، یکی از راه‌های پنهان کردن منبع اصلی ارز در هنگام استفاده از خدمات صرافی‌های بزرگ است.
- **ادغام:** هنگامی که بیت‌کوین یا رمز ارز دیگری با موفقیت در یک فرایند پول‌شویی به

کار گرفته شد، به سطح ادغام رسیده است که در آن ارتباط با فعالیت‌های مجرمانه دشوار است. در حالی که پول مورد نظر دیگر ارتباطی با جرم اتفاق افتاده ندارد، افرادی که پول‌شویی را انجام داده‌اند همچنان باید توضیحی برای چگونگی دسترسی به این پول بیاورند. مجرمان برای مشروع‌سازی رمز ارزهای کثیف، به ایجاد یک شرکت آنلاین اقدام می‌کنند که بیت‌کوین را به‌عنوان یک روش پرداخت قبول دارد. از این روش پول کثیف جابجا شده در قالب بیت‌کوین به پول تمیز و مشروع تبدیل می‌شود.

- روش دیگر برای اعتبار بخشیدن به پول کثیف این است که ادعا شود این مبلغ از راه سرمایه‌گذاری در تجارتي سودده یا رشد ارزش دارایی‌های بهادار و کسب سود به‌دست آمده است. با توجه به اینکه بازار آلت‌کوین‌ها پرنوسان است، کسب سود و نابودی دارایی در این بازار در عرض چند دقیقه ممکن است و بنابراین، اثبات چنین ادعایی می‌تواند چالش برانگیز باشد.

#### **بند دوم: مجرمان چه میزان رمز ارز را برای پول‌شویی استفاده می‌کنند؟**

بر اساس داده‌های منتشر شده از سوی پلتفرم بلاک‌چین Chainalysis، برآورد شده مجرمان از سال ۲۰۱۷ حجمی از رمز ارزها به ارزش ۳۳ میلیارد دلار را برای پول‌شویی استفاده کرده‌اند. در سال ۲۰۲۱، میزان پول‌شویی‌های سایبری با ۳۰ درصد رشد نسبت به سال پیش از خود، به مبلغی با ارزش ۸/۶ میلیارد دلار رسید. با توجه به افزایش فعالیت‌های قانونی و غیر قانونی در حوزه رمز ارزها در سال‌های گذشته، رشد چشمگیر فعالیت‌های مجرمانه مرتبط با این حوزه اتفاق شگفت‌انگیزی نیست. اپلیکیشن‌های DeFi مسئول حدود ۱۷ درصد از پول‌شویی‌های سال ۲۰۲۱ شناخته شده‌اند و پس از آن میکسرها، صرافی‌های پرخطر و استخرهای ماینینگ هم افزایش قابل توجهی را مشاهده کرده‌اند.

#### **بند سوم: آیا می‌توان مجرمانی را که از بیت‌کوین برای پول‌شویی استفاده می‌کنند متوقف کرد؟**

پول‌شویی با استفاده از بیت‌کوین یک تکنیک کاملاً حرفه‌ای نیست و هنوز نقاط خطای زیادی وجود دارند که در موارد بسیاری منجر به به‌دام افتادن مجرمان بزرگ شده‌اند. در حالی که رمز ارزها به ناشناس بودن مشهور هستند، تمامی تراکنش‌های مرتبط با آن‌ها به‌صورت دائمی در دفتر کل بلاک‌چین‌ها ثبت می‌شوند. مجرمان با هدف دور زدن نهادهای مسئول و عدم شناسایی منبع اصلی دارایی خود به استفاده از رمز ارزها برای پول‌شویی روی

می‌آورند. با این حال، اگر در این مسیر اشتباهی انجام دهند، تمام برنامه‌هایشان نقش بر آب خواهد شد. با توجه به پیشرفت روز افزون تکنولوژی، این افراد هم با راه‌های جدیدتری خلاف‌های مالی خود را پنهان خواهند کرد و تلاش خواهند کرد همیشه یک گام جلوتر از مراجع قانونی باشند.<sup>۱</sup>

### بخش دوم: بررسی حقوقی غرامت‌های مبارزه با قوانین ضد پولشویی (AML)

سال ۲۰۱۹ با توجه به تعداد جریمه‌های تحمیل شده سال رکوردداری از این جهت بود. مقامات ۵۸ مورد جریمه مبارزه قوانین پولشویی (AML) که در مجموع ۸۰۱۴ میلیارد دلار بود را اعمال کردند. این رقم دو برابر مبلغی بود که در سال ۲۰۱۸ تحمیل شد. در سال ۲۰۱۸ تنها ۲۹ جریمه به مبلغ ۴۰۲۷ میلیارد دلار به ثبت رسید. براساس آخرین گزارش‌ها، تنظیم‌کننده‌های قانون آمریکا سرسخت‌گیرانه‌تر بودند و تنها ۲۵ غرامت به مبلغ ۲۰۲۹ میلیارد دلار تعیین کردند و پس از آن انگلیس با ۱۲ جریمه به مبلغ ۳۸۸۰۴ میلیون دلار در رتبه دوم قرار دارد. دو سوم جریمه‌های AML به بانک‌ها تحمیل شد در حالیکه تقریباً ۱۷ درصد جریمه برای بخش‌های قمار و ارزهای دیجیتالی برخی سازمان‌ها اعمال شد. این صنایع در معرض بررسی و تحقیقات بیشتری از سوی تنظیم‌کننده‌های قانون قرار دارند زیرا آنها کانال‌های مشتری برای پولشویی نیز هستند. مجازات AML از سال ۲۰۱۵ رو به افزایش بوده است. میانگین جریمه ۱۴۵۰۳۳ میلیون دلار در سال ۲۰۱۹ بود. در سال ۲۰۲۰ در حال حاضر دو جریمه با مبلغ بیش از ۱ میلیارد دلار مشاهده شده است که بیشتر مبلغ این جریمه متعلق به دولت فرانسه به مبلغ ۵۰۱ میلیارد دلار است.<sup>۲</sup>

### بخش سوم: پرداختن به قوانین ضد پولشویی (AML) و تنظیم قوانین ارز دیجیتال

ظهور ابزارهای جدید برای پرداختن قوانین ضد پولشویی (AML) معمولاً توسط تنظیم‌کننده‌های قانون قبل از پذیرش با دقت بررسی می‌شوند. در سال ۲۰۱۹، قوانین ضد پولشویی قوی‌تری در مورد پول و دارایی‌های دیجیتالی مانند ارز دیجیتال وضع شدند. بهر حال حوزه ارز رمزپایه همچنان به رشد خود ادامه می‌دهد. گروه ویژه اقدام مالی

۱ الهام جمشیدیان ۱۲ اسفند ۱۳۹۷ اخبار بلاک چین، خبر روز، برگرفته از سایت [www.excoino.com](http://www.excoino.com)

۲ تذهیبی اصفهانی، فریده، پولشویی (تطهیر پول)، ۱۳۸۱، چاپ اول، تهران، انتشارات زعیم، ص ۱۷۹

(FATF) یک سازمان غیردولتی است که در سال ۱۹۸۹ برای مبارزه با پولشویی تاسیس شد. این سازمان رهنمودهای رمزیایه را برای بسیاری از کشورهایی که تنظیم کنندگان قوانین در مورد بانک‌ها احتیاط می‌کنند وضع کرد. هنک کنگ به بانک‌ها توصیه کرد که برای این بخش رویکرد مبتنی بر ریسک اتخاذ کنند. شبکه اجرایی جرایم مالی (FinCEN)، به مبارزه با پولشویی و تامین مالی تروریست‌ها می‌پردازد و همچنین بانک‌ها را مجبور کرد تا فعالیت‌های مشکوک مربوط به ارزهای دیجیتال را گزارش دهند. سنگاپور، ژاپن و کره جنوبی نیز قرار است تا اواخر سال ۲۰۲۰ یک چارچوب نظارتی ارز رمزیایه راه اندازی کنند. در همین حال، بانک‌ها اقدامات مهمی برای کاهش خطرات تمام بخش‌های رمزیایه انجام داده‌اند. گروه ویژه اقدام مالی (FATF) اعلام کرده است که این رویکردهای کاهش خطر در طولانی مدت پایدار نیستند زیرا ارزهای رمزنگاری شده در آینده رشد پیدا می‌کنند.<sup>۱</sup>

### بند اول: نگاهی به مباحث جدید در سال ۲۰۲۰

همانطور که می‌دانیم پیرو اختیار جدید انتظار می‌رود کسب و کارها مورد ارزیابی قرار گیرند و ریسک‌های مالی مربوط به استفاده از ارزهای دیجیتالی تشخیص داده شوند. با آمدن تکنولوژی‌های جدید شاهد اختیارات جدید نیز خواهیم بود. سال ۲۰۲۰ سالی است که وضوح نظارتی بیشتری در مورد ارزهای رمزیایه ارائه می‌شود. امسال هند، ژاپن، کره جنوبی و فرانسه قوانین مطلوب‌تری برای نگرانی‌های مردم در مورد ارزهای رمزنگاری شده تنظیم کنند. این اقدامات موجب ایجاد بحث‌هایی در دوائر دولتی در مورد تاسیس یک بانک مرکزی ویژه ارز دیجیتال، قوانین و اختیارات پولی آن شده است. ظهور پروژه‌هایی مانند Libra یکی از پروژه‌های غول شبکه‌های اجتماعی یعنی فیس بوک است. در واقع این شرکت قصد داشت یک استیبل کوین (ارز دیجیتالی با پشتوانه پول ملی مثل دلار) ارائه دهد. چنین پروژه‌هایی نیاز به تنظیم کنندگانی دارد که با نوآوری‌ها همگام باشند و به درک بیشتری از آخرین فناوری‌ها و پیامدهای آنها دست پیدا کنند.

۱ مطالبی برگرفته از سایت خبر آنلاین [www.khabaronline.ir](http://www.khabaronline.ir) درخصوص روند خاص پولشویی در عصر جدید

## بخش چهارم: نگاهی به مراحل پولشویی ارز دیجیتال و تجزیه و تحلیل این

### پدیده نوظهور

مجرمانی که ارز دیجیتالی را به حساب واریز می‌کنند باید بازپرداخت نهایی خود را به صورت نقدی دریافت کنند. این امر مستلزم پنهان کردن محل سرمایه‌های آنهاست. متأسفانه چندین ابزار و سرویس پیشرفته وجود دارند که به مجرمان در این امر کمک می‌کنند. از این گذشته اگر هیچ راهی هم برای این دسته مجرمان که ارز دیجیتالی را نقد کنند وجود نداشت از روش‌های غیرقانونی آن را دریافت می‌کردند.

### بند اول: نمونه‌ای از فرآیند پولشویی

مرحله جایگذاری، نقطه شروع: جابه جایی پول از مبدا آن. پول درسیستم پولی موجود از طریق واسطه‌ها مانند موسسات مالی، فروشگاه‌ها و صرافی‌های ارز دیجیتال در گردش قرار می‌گیرد. نمونه‌هایی از این فعالیت‌ها می‌توان به قاچاق ارز به خارج از کشور، همدستی در جرم بانکی، صرافی‌های ارز دیجیتال، خرید دارایی و غیره اشاره کرد.

مرحله خواباندن (لایه گذاری): در مرحله دوم، هدف این است که پرده برداری از فعالیت پولشویی را به چالش کشید. برای اینکار، مجرمان باید هزینه‌های خود را طبقه بندی و ردیابی پول غیرقانونی را دشوار کنند. این کار معمولاً با تبدیل پول نقد به ابزارهای پولی یا خرید دارایی‌ها با سرمایه غیرقانونی برای فروش مجدد آنها انجام می‌گیرد.<sup>۱</sup>

مرحله ادغام و یکپارچه سازی: این آخرین مرحله از پولشویی است که پول غیرقانونی دوباره وارد سیستم مالی می‌شود به طوری که به نظر می‌آید از راه قانونی بدست آمده. این مرحله می‌تواند با خرید اموال غیر منقول، اتومبیل و جواهرات و فلزات گرانبها صورت بگیرد. با توجه به ماهیت دیجیتالی و خصوصیات طبیعی به نظر می‌رسد که بیت کوین در مراحل تزریق پول و لایه بندی مناسب است. با شروع مرحله جای گذاری، بیت کوین می‌تواند ابزار مفیدی برای تبدیل ارز فیات به بیت کوین و سپس دوباره تبدیل بیت کوین به ارز فیات و جا به جایی پول از یک کشور به کشور دیگر نیز باشد. با این حال، بیشتر مجرمان برای دریافت پول از بیت کوین استفاده می‌کنند، مسئله اصلی آنها ادغام یعنی گذاشتن جای

---

۱ سمیع زنور، حسین و حبیب زاده، محمد جعفر و صابر، محمود، (۱۳۹۵)، تحلیل جرم «اخلال در نظام اقتصادی کشور» از طریق قبول سپرده ی اشخاص در حقوق ایران، مجله آموزه های حقوق کیفری، شماره ۱۱: ۲۷-۵۱.

خود گذاشتن سرمایه‌ها در اقتصاد برای پنهان کردن فعالیت غیرقانونی خودشان است.

### بند دوم: ادغام

بر اساس گزارش جنایات رمزنگاری شده ۲۰۲۰ Chainalysis، بسیاری از مجرمان ارزهای دیجیتال‌شان را با کمک دلان سهام و اوراق بهادار پولشویی می‌کنند. دلان OTC یا فرابورس نمایندگان یا شرکت‌هایی هستند که معاملات را بین خریداران و فروشندگانی که نمی‌خواهند یا نمی‌توانند در صرافی ارز دیجیتال معامله کنند تسهیل می‌کنند. کارگزاران فرابورس در بین تجار و ماینرهای می‌توانند بر قیمت بازار تاثیر بگذارند به این صورت که بین تجار و ماینرهای که می‌خواهند موجودی وسیعی از دارایی‌های رمزیه را در یک قیمت توافقی نگه دارند و سپس با استفاده از یک صرافی آزاد حجم زیادی از آن را به فروش برسانند. اکثر معامله‌گران فرابورس با صرافی‌ها هم‌دستی می‌کنند، اما بسیاری از آنها احراز هویت کمتری نسبت به صرافی‌هایی که در آنجا فعالیت می‌کنند ارائه می‌دهند. گفتنی است بسیاری از آنها در خدمات پولشویی برای مجرمان بهره می‌برند و تخصص می‌یابند. صرافی‌ها همچنان برای تمیز کردن بیت کوین غیرقانونی روش ارجحی هستند. در طول سال ۲۰۱۹، بیش از ۲۰۸ میلیارد دلار بیت کوین از سوی مجرمان ارزی به صرافی‌ها فرستاده شده و ۵۲ درصد آن به دو صرافی برتر یعنی بایننس (Binance) و Huobi نیز ارسال شدند.<sup>۱</sup>

### بند سوم: لایه بندی

بیت کوین برای مرحله دوم پولشویی یعنی لایه بندی عملی‌تر است. در واقع بیت کوین یک ارز دیجیتال است که می‌تواند برای بدون محدودیت از مرزهای فیزیکی برای خرید در سراسر شبکه استفاده شود.<sup>۲</sup> اگر کسی به اندازه کافی توجه کند می‌تواند بیت کوین را برای خرید دارایی‌ها خرج یا اینکه از طریق معامله‌گران فرابورس آن را نقد کند. به عنوان مثال، شخصی ممکن است یک رلکس (Rolex) در بازار ثانویه خریداری کند و سپس آن را دوباره برای پول فیات بفروشد. با این حال برای مجرمان ارزی بسیار دشوار خواهد بود که دارایی‌های پولی بخرند زیرا بسیاری از آنها به وسیله واسطه‌گران خریداری شدند که نیاز به

۱ باقر زاده، احد، جرایم اقتصادی و پولشویی، مرداد ۱۳۸۳، چاپ اول، تهران، انتشارات مجد، ص ۷۹

۲ توسلی زاده، توران، پیشگیری از جرایم اقتصادی، ۱۳۹۲، چاپ اول، تهران، انتشارات جنگل جاودانه، ص ۱۸۰

احراز هویت و اقدامات ضد پولشویی دارند. با این وجود، شایان به ذکر است برخلاف پول نقد، ارزهای دیجیتالی به طور ذاتی شفاف هستند زیرا تمامی تراکنش‌ها در یک دفتر کل عمومی ضبط می‌شوند. همانطور که در گزارش منتشر شده توسط Chainalysis آمده است، تمام این سرمایه‌های غیرقانونی اثری از خود پشت آنها به جا می‌گذارند. اگر کسی مقدار قابل توجهی از اطلاعات را جمع‌آوری کند سپس معلوم شود که چه کسی پشت آدرس بیت کوین است برای پولشویی استفاده می‌شود. یکپارچه سازی مرحله آخر پولشویی با استفاده از ارزهای دیجیتال است و از آنجا که هر لحظه ارزش ارزهای دیجیتال در حال تغییر است برای نگه داشتن آن‌ها در بازار، نه تنها وارد کردن آنها، نیاز به شفاف بودن منابع است که یک روش ساده برای مشروعیت بخشیدن به درآمد غیرمجاز ارائه آن به عنوان نتیجه سرمایه گذاری سودآور یا افزایش ارزش پول دیگر است. مشابه نحوه استفاده از حساب بانکی ارز فیات خارج از کشور برای پولشویی پول‌های کثیف، یک شرکت آنلاین صوری که پرداخت‌های بیت کوین را می‌پذیرد می‌تواند برای مشروعیت بخشیدن به درآمد و تبدیل ارز رم‌پایه کثیف به بیت کوین تمیز و قانونی ایجاد شود و معمولاً این شرکت‌های صوری با نام‌های شرکت‌های بازی‌های آنلاین و یا ای تی ام‌ها دست به فعالیت می‌زنند. اصول زیربنایی پولشویی به طور کلی در چهار عنوان خلاصه می‌شود: ناشناس ماندن، سرعت، پیچیدگی و پنهان بودن؛ به این معنا که منبع پول باید ناشناس باقی بماند زیرا از طریق فعالیت‌های غیرقانونی استحصال شده است. در طول مرحله جایگذاری، وجوه مالی غیرقانونی به نام موجودیت‌های قانونی ثبت می‌شوند تا ماهیت واقعی آنها پنهان شود. اغلب به منظور کاهش حساسیت نسبت به تراکنش‌های حاوی مبالغ بالا، این وجوه در قالب چند تراکنش میان چند موسسه تقسیم می‌شوند. در مرحله ی لایه چینی، مجموعه ای از تراکنش‌ها به سرعت انجام می‌شود تا دنباله ای پیچیده ایجاد شود و به این ترتیب رد پای موسسات درگیر در مرحله ی جایگذاری پنهان شود. با انجام این حجم بالای تراکنش به مقصد کشورهای مختلف جهان، جا به جایی این وجوه غیرقانونی ماهیتی پیچیده می‌یابد که رهگیری آن را بسیار دشوار می‌کند. در این میان یکی از بزرگترین پولشویی‌های صورت گرفته در این صنعت توسط بنیانگذار صرافی بیت کوین اتفاق افتاده است. الکساندر وینیک روسی که سرویس مبادله بیت کوین را بنیان نهاده است و این سیستم را اداره می‌کند به جرم پولشویی مقصر شناخته شده است؛ وزارت دادگستری آمریکا از زمان تأسیس صرافی

در سال ۲۰۱۱ وینیک را به ۱۷ فقره پولشویی به ارزش ۴ میلیارد دلار متهم کرده است. وینیک و تیمش از بستر ایجاد شده برای رد و بدل پول هایی که از طریق حملات سایبری به نهادها به دست می آوردند استفاده می کردند.<sup>۱</sup>

### بخش پنجم: پولشویی با استفاده از بیت کوین

بیت کوین علاوه بر مرحله دوم یعنی لایه بندی برای مراحل جایگذاری در هنگام پولشویی نیز کاربردی باشد. با این حال آیا می تواند جایگزین بهتری برای سیستم فعلی فراهم کند؟ تنها ۱۰۱ درصد از مجموع حجم ارز رمزپایه گفته می شود که غیرقانونی است.<sup>۲</sup> اکثریت قریب به اتفاق جرایم مربوط به رمزپایه کلاهبرداری هایی با حجم معاملات بیشتر از ۸۰۶ میلیارد دلار بودند. به استثنای PlusToken، Bitconnect و OneCoin که سه تا از بزرگترین طرح های پانزی رمزپایه (کلاهبرداری هایی که تقریباً ۰٫۴۶ درصد تمام فعالیت های رمزنگاری شده را به خود اختصاص داده اند هستند. با توجه به نظریه های ناشناس بودن و احراز هویت، استدلال مبنی بر اینکه بیت کوین یک ابزار بهتر برای پولشویی محسوب می شود نادرست است. هویت ها در بلاک چین بیت کوین ناشناس نیستند بلکه نام مستعار هستند. هر هویتی با یک رشته حروف الفبا و اعداد باهم که کلید خصوصی نامیده می شوند همراه هستند. در حالیکه که گفته می شود بیت کوین دارای محافظتی بالایی در خصوص هویت کاربران دارد اما در واقع معاملات عمومی هستند. با توجه به ویژگی طبیعی اش، کلیه معاملات بلاک چین بین سرمایه گذاران به اشتراک گذاشته می شود. اگر نام مستعار برای حفظ حریم خصوصی کافی نباشد می توان از اصطلاح میکسر (Mixers) استفاده کرد. میکسر ها نرم افزار یا سرویس هایی هستند که به کاربران این امکان را می دهند معاملات را از طریق ترکیب کردن کوین های خود با دیگر کاربران رای حفظ حریم خصوصی انجام دهند. این کار کاربران را قادر می سازد بازده ها و آدرس هایشان و هویت واقعی خود را پنهان کنند. در سال ۲۰۱۹، میکسر های ارز دیجیتال، در کانون توجه اخبار بودند. با این حال طبق گزارش Chainalysis، میکسر ها برای حفظ حریم خصوصی بیشتر از فعالیت های غیرقانونی استفاده می شوند. تنها ۸۰۱ درصد کوین های ترکیب شده به

۱ مطالبی برگرفته از سایت خبر آنلاین [www.khabaronline.ir](http://www.khabaronline.ir) در خصوص روند خاص پولشویی در عصر جدید

۲ باقر زاده، احد، جرایم اقتصادی و پولشویی، مرداد ۱۳۸۳، چاپ اول، تهران، انتشارات مجد، ص ۸۳

سرقت رفته‌اند و تنها ۲۰۷ درصد کوین‌های ترکیب قبلا در بازارهای دارک نت استفاده شدند. کوین میکسرها دقیقا کاربرپسند نیستند. در واقع آنها هنوز قادر به ارائه همان میزان امنیت به عنوان روش‌های قدیمی برای پولشویی نیستند. شخصی ممکن است با استفاده از میکسر اعلام جنگ کند اما میکسرها تنها می‌توانند معاملات در صورتی که حجم گسترده‌ای از بیت کوین ترکیب شده باشد مخفی کنند. علاوه بر این، اقدامات متقابل پیشرفته‌تری نیز وجود دارد مانند تحلیل بلاک چین که حتی می‌تواند بیت کوین ترکیب شده را به آدرس‌ها وصل کند. برخلاف پول نقد، هریک از معاملات ارزهای دیجیتالی در یک دفترکل قابل رویت و عمومی ثبت می‌شوند. با یک ابزار صحیح می‌توانید بررسی کنید که فعالیت‌های رمزنگاری شده با جرم در ارتباط هستند یا خیر. این شرکت‌ها به قانون‌گذاران با ارائه اطلاعات ارزشمند به پرونده‌های کیفری کمک می‌کنند. پول نقد هنوز یکی از ساده‌ترین و امن‌ترین روش برای پولشویی است. داده‌های ارائه شده حاکی از آن است که بیت کوین می‌تواند ابزاری فرعی برای پولشویی در اختیار مجرمان نیز باشد. برای مثال، آنها ممکن است از آدرس‌های در معرض و روش‌های ترکیب کوین به عنوان یک احتیاط استفاده کنند تا اطمینان حاصل شود که سطح کافی از حریم خصوصی از آنها محافظت می‌کند. با این حال، هویت‌های مستعار، معاملات عمومی و پیچیدگی‌های سیستم ناوبری مورد نیاز برای استفاده از بیت کوین در حال حاضر جایگزینی موثرتر برای پولشویی ارائه نمی‌دهند. گفتنی است یک مجرم نمی‌خواهد اثر دائمی از فعالیت‌های غیرقانونی به طور عمومی منتشر شود. علاوه بر این بیت کوین نمی‌تواند حجم وسیعی از پول مورد نیاز برای پولشویی مجرمان را آماده کند. شبکه بیت کوین در مقایسه با سایر کلاس‌های دارایی روزانه حجم کمی را مشاهده می‌کند. (در تاریخ ژانویه ۲۰۲۰ این حجم ۲۵ میلیارد دلار بود). جا به جایی چنین مبلغی از پول، بلافاصله زنگ هشدار را برای شرکت‌های جرم یابی قانونی بلاک چین به صدا درمی‌آورد و به واسطه‌های بیشتر و مبادلات متمرکز شده‌ای نیاز دارد. در سال ۲۰۱۷ و ۲۰۱۸، گروه هکری لازاروس کره شمالی (Lazarus Group)، بخش عمده‌ای از بودجه خود را از طریق صرافی‌های دارای احراز هویت نقد کرد. با این حال در سال ۲۰۱۹، روش این گروه پیچیده‌تر شد زیرا آنها نیمی از بودجه خود را از طریق کیف پول‌های (میکسرها) CoinJoin (تمیز کردند در حالیکه نیمی دیگر در کیف پول‌های آنها بدون فعالیت باقی مانده‌اند. اجرای قانونی و تنظیم‌کننده‌های قانون باید برای بهبود

توانایی‌های خود برای جلوگیری و پاسخ به شکل‌های مختلف جرایم رمزیابه کارشناسی تر شوند. همچنین انتظار می‌رود صرافی‌ها ارزیابی صلاحیت گسترده روی کاربران، کارگزاران فرابورس و اشخاص ثالث دیگر انجام دهند. تنظیم قانون مبارزه با پولشویی (AML) برای وضعیت فعلی امور طراحی نشده است. همکاری و نظارت بین المللی بیشتر برای فعال کردن آزادی جا به جایی پول و سرمایه نیاز است. متأسفانه قانون گذاران نتوانسته‌اند از پیشرفت‌های سریع فناوری پیروی کنند. برای جایگزینی سیستم‌های بانکی سنتی، قوانین و مقررات جدیدی نیاز است تا بتوانند حاکمیت کافی در سطح جهانی را تضمین کند.<sup>۱</sup>

### بخش ششم: دستورالعمل‌های ارز دیجیتال FATF برای مبارزه با پولشویی

FATF که به آن گروه ویژه اقدام مالی می‌گویند. یک سازمان بین دولتی است که هدف آن توسعه سیاست‌های مبارزه با پول‌شویی ست. این سازمان به تازگی دستورالعمل‌های مقدماتی برای ارز دیجیتال روی وبسایت خود منتشر کرده است. گروه ویژه اقدام مالی در مورد موارد اولیه ای که لازم است درباره ارزهای دیجیتال انجام شود، جلسه ای برگزار کرد. طبق گفته این سازمان، متن جدیدی به این اقدام اضافه شد که در آن موارد لازم برای تنظیم و نظارت بر خدمات دیجیتالی که ارائه داده می‌شود، مشخص شود. انتظار می‌رود که در ماه می که قرار است جلسه در رابطه با همین موضوع ترتیب داده شود، FATF بتواند از مشاوره‌های بخش خصوصی کمک بگیرد و از کارآفرینان تقاضا کند تا تاریخ ۸ آپریل، نظرات و پیشنهادات خود را به سازمان ارائه کنند. پس از جمع بندی و نهایی شدن این پیشنهادات، به صورت رسمی توسط FATF تصویب می‌شود. آخرین نشستی که برای این موضوع برنامه ریزی شده است، ژوئن ۲۰۱۹ است.<sup>۲</sup>

### بند اول: قوانین FATF برای ارز دیجیتال

در سال ۲۰۱۸ نسخه قبلی FATF به امضا رسید که در آن از کشورها خواسته شده بود که برای جلوگیری از پول شویی و تامین مالی تروریسم به کمک ارز دیجیتال، از دستورالعمل‌های ذکر شده پیروی شود. علاوه بر این، تمام کسانی که دارایی دیجیتال دارند، موظف هستند تا مجوز کسب کنند یا در مراکز قانونی که توسط این گروه به وجود آمده

۱. توسلی زاده، توران، پیشگیری از جرایم اقتصادی، ۱۳۹۲، چاپ اول، تهران، انتشارات جنگل جاودانه. ص ۱۸۷

۲. الهام جمشیدیان ۱۲ اسفند ۱۳۹۷ اخبار بلاک چین خبر روز برگرفته از سایت [www.excoino.com](http://www.excoino.com)

است، ثبت نام کنند. صاحبان این مراکز قانونی هم باید اطلاعاتی که هویت آن‌ها را نشان می‌دهد، به مقامات مربوطه ارائه کنند.<sup>۱</sup>

### نتیجه‌گیری و جمع‌بندی بحث

ارزش ارزهای دیجیتال در یک سال گذشته نوسانات شدیدی را تجربه کرده؛ اما این باعث نشده است که چیزی از جذابیت آن‌ها برای کلاهبرداران کم شود. ارزهای دیجیتال با حجم بالای ارزشی که در آن‌ها ذخیره و ردوبدل می‌شود، همیشه منابعی جذاب برای کلاهبرداری و اقدامات مجرمانه بوده‌اند. در طی سال‌هایی که از تولد ارزهای دیجیتال می‌گذرد، همواره اخباری را مبنی بر کلاهبرداری در این حوزه و به‌سرقت‌رفتن دارایی‌های کاربران شنیده‌ایم. این کلاهبرداری‌ها می‌توانند طیف گسترده‌ای را شامل شوند؛ از هک و سرقت گرفته تا طرح‌های پانزی و هرمی؛ حملات فیشینگ؛ کوین‌ها و توکن‌های بی‌ارزش؛ صرافی‌های تقلبی و حتی دست‌کاری عامدانه قیمت برای کسب سود. یکی از مهمترین و بارزترین اعمال مجرمانه که ضربه بسیار سنگینی بر اقتصاد جامعه و کشور می‌زند پولشویی از طریق ارزهای دیجیتالی است که در این خصوص توضیح دادیم.<sup>۲</sup> با اتفاقات رخ داده خیلی از کشورهای خارجی از جمله فرانسه برای جلوگیری از پولشویی با استفاده از ارزهای دیجیتال قوانین ارزهای دیجیتال را تقویت کردند به طوری که در ۹ دسامبر سال جاری چندین وزارتخانه در فرانسه مشترکاً دستوری را برای جلوگیری از معاملات دارایی‌های دیجیتال ناشناس با ممنوع کردن حساب رمزگذاری ناشناس ارائه دادند. وزارتخانه‌های فرانسه اعتراف کرده‌اند که دارایی‌های دیجیتال یا ارزهای رمزیابه "فرصت‌های قابل توجهی برای اقتصاد" فراهم می‌کنند و خاطرنشان کردند که دولت فرانسه کاملاً از اهمیت آن آگاه است؛ این مقامات همچنین اظهار داشتند، با وجود فرصت‌های امیدوار کننده، رمزنگاری همچنین خطرات قابل توجهی در ارتباط با فعالیت‌های مالی غیرقانونی دارد. وزرا به طور خاص به دستگیری‌های سپتامبر ۲۰۲۰ شامل یک شبکه تأمین مالی تروریسم با استفاده از دارایی‌های دیجیتال برای پوشاندن آثار خود اشاره کردند. وزرا گفتند، مقامات و سازمان‌های بزرگ جهانی مانند گروه ویژه اقدام مالی جی ۷ و جی ۲۰ خواستار تدابیری برای جلوگیری

۱ غلامی، علی و پوریخش، سید محمد علی، مبارزه با پولشویی در قوانین ایران و اسناد بین المللی، فصلنامه علمی تخصصی مطالعات اقتصاد اسلامی، زمستان ۱۳۹۰، سال چهارم، شماره اول.

۲ رحیمی مقدم، علیرضا، پولشویی در تجارت بین الملل، دیماه ۱۳۹۷، نشریه بانک ملی ایران، شماره ۲۳۴، ص ۵۸

از فعالیت‌های غیرقانونی با استفاده از رمزنگاری شده اند. نهایتاً راهکارهای و روش‌های مقابله با پولشویی از طریق ارزش‌های دیجیتال و دیگر جرایم اقتصادی مشابه را می‌توان در قالب دو راهکار پیشنهاد داد:

### راهکار اول: دانش افزایی

یکی از اولین موانع پیش روی مجریان قانون در برخورد با ارزش‌های دیجیتال، درک این فناوری جدید است. ارزش دیجیتال یک حوزه جدید و در حال پیشرفت است و به همین دلیل، مردم آن را پیچیده می‌دانند. بنابراین واضح است که آموزش و یادگیری در این زمینه امری بسیار مهم است. شیوه‌ها و تکنیک‌هایی که پلیس و نهادهای نظارتی برای مقابله با جرایم استفاده می‌کنند بسیار مهم هستند؛ اما آنها باید برای بهینه‌سازی تکنیک‌های خود و نتیجه‌گیری حداکثری، ابتدا به درک درستی از مفهوم ارزش‌های دیجیتال برسند و دانش ابتدایی خود را در این زمینه تقویت کنند. متأسفانه این امکان وجود دارد که مقامات ارشد پلیس به‌علت جدیدبودن حوزه ارزش‌های دیجیتال، ضرورت آموزش در این حوزه را به‌طوری که باید درک نکنند. این شرایط دقیقاً مشابه وضعیتی است که در دهه پیش، در رابطه با تلفن‌های همراه شاهد آن بودیم. در این دوره، بسیاری از نهادهای ارشد قانونی اهمیت بررسی تلفن‌های همراه را درک نمی‌کردند. بسیاری از تیم‌ها به این دلیل که ابزارهای لازم و دانش کافی برای بررسی داده‌های مربوط به تلفن‌های همراه را نداشتند، به‌طور کلی از این کار صرف‌نظر می‌کردند؛ اما امروزه می‌بینیم که تقریباً هر جرمی به‌نوعی به تلفن‌های همراه مرتبط است. در آینده‌ای نزدیک همین اتفاق درباره ارزش‌های دیجیتال رخ خواهد داد. با توجه به این حقیقت غیرقابل‌انکار که ارزش‌های دیجیتال آینده پول هستند، در آینده همه جرایم مالی به‌شکلی به این ارزش‌ها مرتبط خواهند بود.

### راهکار دوم: ابزارهای نوین

گزینه دومی که برای مقابله با جرایم در دنیای ارزش‌های دیجیتال اهمیت دارد، ابزارهای تحقیقاتی است. منظور از آن، هم ابزارهای فیزیکی برای جمع‌آوری داده‌ها از دستگاه‌هاست و هم نرم‌افزارهایی برای تحلیل داده‌های جمع‌آوری‌شده. برای اینکه بتوان بهترین ابزارها را برای محققان بلاک چین توسعه داد، به یک موتور جست‌وجوی جامع بلاک چین نیاز داریم که حجم زیادی از داده‌ها را گردآوری کند و از آنها برای ردیابی آدرس‌های ارزش‌های دیجیتال در بازارهای دارک نت، صرافی‌ها و خودپردازهای ارزش‌های دیجیتال استفاده کند. امروزه

راهکارهای جدیدی در بازار هست که می‌توان از طریق آنها، موارد غیرعادی را در تراکنش‌های ارزش‌های دیجیتال کشف کرد و از آنها به‌عنوان سرنخی برای شروع تحقیقات استفاده کرد. کلاهبرداران باتجربه با کمک‌گرفتن از پیشرفت‌های فناوری ارزش‌های دیجیتال، فعالیت‌های خود را به سطوح زیرزمینی ارتقا داده‌اند و از آنجاکه مجریان قانون عملاً هیچ حضوری در این فضا ندارند، شانس دستگیری آنها بسیار کم است. از این‌رو، مجریان قانون اکنون باید با تمرکز بر دانش، ابزار و خدمات، یک راهکار جامع تحقیقاتی ایجاد کنند تا بتوانند در مقابل این نوع جرایم هم حرفی برای گفتن داشته باشند. هوش دیجیتال در تجزیه و تحلیل اشتباهات و آماده‌شدن برای حوادث بعدی نقشی حیاتی دارد. البته گفتنی است که برای افزایش بهره‌وری، همه استراتژی‌های هوش دیجیتال باید قابلیت‌هایی برای آمادگی در مقابل رویدادهای پیش‌بینی نشده داشته باشند؛ قابلیت‌هایی که ابزارهای پیشرفته جهانی که منحصرراً برای ارزش‌های دیجیتال طراحی شده‌اند باید از آنها پشتیبانی کنند. با توجه به افزایش کاربرد و محبوبیت ارزش‌های دیجیتال، نهادهای اعمال قانون باید برای استخدام کارشناسان نخبه و ایجاد واحدهای تخصصی هوش دیجیتال در درون سازمان خود تلاش کنند. آنها باید تخصص و ابزار مناسب را برای واکنش به رویدادهای مرتبط با ارزش‌های دیجیتال در اختیار داشته باشند. این دو، یعنی تخصص و ابزار مناسب، اجزای سازنده یک استراتژی هوش دیجیتال قوی هستند. جرایم در دنیای ارزش‌های دیجیتال زمینه‌های مختلفی را در بر می‌گیرند؛ از کلاهبرداری‌های مالی گرفته تا قاچاق مواد مخدر و قاچاق حیوانات و انسان. از این‌رو، ارزش‌های دیجیتال بخشی اساسی از تحقیقات هوش دیجیتال را تشکیل می‌دهند؛ اما خوشبختانه فناوری ارزش‌های دیجیتال در عین پیچیدگی و کارکردهایی که می‌تواند برای مجرمان داشته باشد، فرایند تحقیقات جنایی را نیز تسهیل می‌کند. رسیدگی به این چالش‌های جدید مستلزم تکامل ابزارهای اعمال قانون، آموزش و راهبردهای مبتنی بر هوش دیجیتال و تحلیل داده‌هاست. خلاصه اینکه ارزش‌های دیجیتال ماندنی هستند و نهادهای مجری قانون باید همین امروز اقدامات لازم را انجام دهند تا برای افزایش جرم‌های مرتبط با این ارزش‌ها در آینده آمادگی داشته باشند. تردیدی نیست که افزایش محبوبیت ارزش‌های دیجیتال، جرایم مرتبط با این حوزه را نیز گسترده‌تر خواهد کرد. امروز ارزش‌های دیجیتال فقط یک ابزار در دست خلاف‌کاران هستند؛ همان طور که پول نیز همیشه این‌طور بوده است. اما مسئله این است که نهادهای مجری قانون نیز برای اینکه بتوانند

توانایی مقابله با مجرمان را داشته باشند، باید به این ابزار مجهز باشند و با آن آشنایی کامل داشته باشند.

## منابع و مأخذ

۱. تجلی، سید آیت اله، مبارزه با پولشویی و تامین مالی تروریسم در بانک ها، ۱۳۹۱، چاپ اول، تهران، انتشارات آزاد کتاب.
۲. تذهیبی اصفهانی، فریده، پولشویی (تطهیر پول)، ۱۳۸۱، چاپ اول، تهران، انتشارات زعیم.
۳. توسلی زاده، توران، پیشگیری از جرایم اقتصادی، ۱۳۹۲، چاپ اول، تهران، انتشارات جنگل جاودانه.
۴. روون بوسورث و گراهام سالت مارش، پولشویی، ۱۳۷۶، ترجمه نصرالله امیر بشیری، چاپ اول، تهران، انتشارات اداره کل آموزش نیروی انتظامی.
۵. زارع علی، جمالی جعفر، «تعهد بانک به حفظ اسرار مشتریان و عملیات تبدیل دارایی به اوراق بهادار»، بهار ۱۳۹۰، فصلنامه راهبرد، سال بیستم، شماره ۵۸.
۶. روزبهان، محمود، (۱۳۸۲)، مبانی علم اقتصاد، مرکز نشر دانشگاهی، چاپ چهارم.
۷. ساکی، محمدرضا، (۱۳۹۳)، حقوق کیفری اقتصادی، انتشارات جنگل، چاپ سوم.
۸. باقر زاده، احد، جرایم اقتصادی و پولشویی، مرداد ۱۳۸۳، چاپ اول، تهران، انتشارات مجد.
۹. محمودی، حسین، (۱۳۸۴)، مبارزه با جرائم اقتصادی، نشر جهان جام جم، چاپ اول.
۱۰. مهدی پور، اعظم، (۱۳۹۵)، سیاست کیفری افتراقی در قلمرو بزهکاری اقتصادی، نشر میزان، چاپ دوم.
۱۱. میرمعزی، سید حسین، (۱۳۹۰)، نظام اقتصادی اسلام «مبانی، اهداف، اصول راهبردی و اخلاق»، پژوهشگاه فرهنگ و اندیشه اسلامی، چاپ دوم.
۱۲. عارفی مسکونی، محمد، جرایم پولشویی، ۱۳۸۴، چاپ اول، تهران، انتشارات آریان.
۱۳. ملازمیان، مسعود، سیاست جنایی - تقنینی ایران در جرایم اقتصادی، ۱۳۸۷، معاونت آموزش قوه قضاییه، تهران، انتشارات جنگل جاودانه.
۱۴. جوانمرد، بهروز، جرم تطهیر در حقوق موضوعه ایران، زمستان ۱۳۹۱، کانون وکلای دادگستری مرکز، شماره ۲۱۹.
۱۵. چاووشی، حمید، (۱۳۸۰)، پدیده قاچاق از منظر حقوق کیفری، قسمت اول، مجله دادرسی، سال پنجم، شماره ۴۸

۱۶. سمیعی زنور، حسین و حبیب زاده، محمد جعفر و صابر، محمود، (۱۳۹۵)، تحلیل جرم «اخلال در نظام اقتصادی کشور» از طریق قبول سپرده ی اشخاص در حقوق ایران، مجله آموزه‌های حقوق کیفری، شماره ۱۱: ۲۷-۵۱.
۱۷. هادیان، ابراهیم، پولشویی و ارتباط با جرائم دیگر، ۱۳۸۲، همایش بین المللی مبارزه با پولشویی، دانشگاه شیراز، نشر وفاق.
۱۸. خمایی زاده، فرهاد، مبارزه با پولشویی در بانک‌ها و موسسات مالی نگاهی به قانون ضد تروریسم ایالات متحده آمریکا، مجله حقوقی، پاییز ۱۳۸۲، نشریه دفتر خدمات بین المللی جمهوری اسلامی ایران، شماره بیست نهم.
۱۹. غلامی، علی و پوربخش، سید محمد علی، مبارزه با پولشویی در قوانین ایران و اسناد بین المللی، فصلنامه علمی تخصصی مطالعات اقتصاد اسلامی، زمستان ۱۳۹۰، سال چهارم، شماره اول.
۲۰. رحیمی مقدم، علیرضا، پولشویی در تجارت بین الملل، دیماه ۱۳۹۷، نشریه بانک ملی ایران، شماره ۲۳۴