

جرم پولشویی به واسطه رمز ارزها

(تاریخ دریافت ۱۴۰۲/۰۳/۱۷، تاریخ تصویب ۱۴۰۲/۰۸/۱۲)

محمد جواد چراغی

دانشجوی کارشناسی ارشد حقوق کیفری و جرم شناسی دانشگاه آزاد اسلامی واحد تهران شمال^۱

چکیده

با ظهور رمزارزها به دنیای حقیقی پیشرفت قابل توجهی در حوزه اقتصادی به ویژه عملیات دریافت و پرداخت صورت گرفت. فناوری سرعت بالا و کارمزد ناچیز رمز ارزها باعث شد که در ابتدا شرکت ها، سازمان ها و حتی مردم عادی هم برای تراکنش های خود از رمزارزها بهره ببرند. رمزارزها در فضای شفاف بلاکچین فعالیت می کنند و این فضا علاوه بر این که بسیار شفاف است برای شناخت هویت افراد بسیار بسیار غیر شفاف است و به بیان دیگر در بازار رمز ارزها هویت افراد معلوم نیست و هویت افراد آدرس کیف پولی است که از یک مبدا به یک مقصد می رود. همین موضوع باعث شده است که از رمزارزها استفاده غیر مشروع در قالب پولشویی شود و قاطعانه می توان گفت که علاوه بر شرکت هایی که برای پولشویی تاسیس شده اند و از مردم برای پولشویی رمز ارزها استفاده می کنند، رژیم های صهیونیستی نیز برای خرید سلاح و مهمات جنگی و حتی کمک به کشور های هم پیمان خود از رمز ارزها استفاده می کنند تا ردپایی از هویت آنها در تراکنش باقی نماند. در این مقاله در ابتدا مفاهیم پایه و حقوقی پولشویی را بررسی می کنیم و در ادامه به بررسی مفاهیم پایه رمز ارزها و پولشویی رمز ارزی و هشدار های صادر شده در این حوزه می پردازیم.

واژگان کلیدی: رمزارز، بازار مالی، پولشویی، کلاهبرداری رایانه ای، ارز دیجیتال



مقدمه

سیستم های مالی در جوامع روزانه در حال آپدیت شدن هستند و بر فناوری های خود می افزایند و شبکه بلاکچین هم از همین نوع شبکه هاست که اطلاعات سنتی پاسخگوی فناوری تازه ای نیست و در صورت فقدان بستر مناسب جهت نظارت و پیگیری باعث پدید آمدن مشکل های بسیاری می گردد و لازمه فناوری جدید رشد اطلاعات به نسبت رشد فناوری است. اصلی ترین مشکل که در سیستم های مالی پدید می آید ظهور مجرمان و کلاهبرداران است تا بتوانند از این خلا اطلاعاتی بهره کافی ببرند و خود به سود برسند که در بازار رمز ارزها آزادی کامل دارند و هر نوع جرمی که بخواهند می توانند انجام دهند. از جمله جرایمی که رونق بسیاری برای مجرمان دارد و در همین کشور خودمان هم رواج یافته پولشویی می باشد که از این طریق پول های بسیار زیاد و هنگفتی را مبادله می کنند و در نهایت خود به سود بزرگی می رسند و با این عملیات رد و آثاری از آنها باقی نماند و یک سری قربانی وجود دارند که وسوسه کرایه کارت و اکانت و حساب و... شده اند. صادقانه باید گفت که صرافی های داخلی تاکنون راهکار درستی برای این مسئله ارائه نکرده اند. همین حالا هم بزرگترین صرافی های ایرانی دارند با وجود چنین معضلات و مخاطراتی کار می کنند و این ریسک ها همچنان پابرجاست. متأسفانه در کشور ما این موضوع بسیار رواج پیدا کرده و قربانی های بسیاری هم بر جای گذاشته است و تنها دلیل آن هم ضعف اطلاعاتی مردم نسبت به فناوری های نوپا و عدم فرهنگ سازی و اطلاع رسانی دولت و سازمان و نهاد های پیشگیری کننده از این نوع جرایم می باشد. کلاهبرداران هر روز روش های جدیدی برای پولشویی و پاک کردن رد ارزهای دیجیتال دزدی پیدا می کنند. از طرفی، مراجع قضایی نیز با وضع قوانین سخت گیرانه سعی دارند از پولشویی و فعالیت های مجرمانه جلوگیری کنند. ارزهای دیجیتال علی رغم ذات رمزنگاری شده خود، به راحتی قابل ردیابی هستند. میکوشیم به امید آن روز که مردم کشور با اطلاعات کافی وارد بازار های مالی به خصوص رمز ارزها شوند و بتوانند از این طریق به اقتصاد خانواده ایرانی کمک کنند و درد دام کلاهبرداران و شیادین این بازار نیفتند.

بخش اول: مفاهیم پایه پولشویی

پولشویی در لغت عبارت است از شستن پول های کثیف. بانک تجارت ایران پول شویی را چنین بیان میدارد: ^۱ فعالیتی غیر قانونی است که در طی انجام آن، عواید و درآمدهای ناشی از اعمال خلاف قانون، مشروعیت می یابد. به عبارت دیگر پولهای کثیف ناشی از اعمال خلاف قانون به پول های تمیز تبدیل گردیده و در بدنه اقتصاد جایگزین می شود. پول شویی به مشروع جلوع دادن پول هایی که از راههای غیرقانونی و نامشروع بدست می آیند با استفاده از روش هایی که باعث پنهان شدن منشاء غیرقانونی آن پول ها می شوند، گفته می شود. پولشویی به عنوان یک جرم حدود سه دهه سابقه دارد و عملاً از دهه ۱۹۸۰ و اساساً در مورد قاچاق داروهای روان گردان و مواد مخدر مطرح گردید. ولی سابقه پولشویی و مباحث مربوط به آن بیش از این است.

درباره واژه پولشویی به عنوان یک جرم، چندین دیدگاه و نظریه متفاوت وجود داد: یک نظریه معتقد است که این لغت ریشه در قرن بیستم دارد، و به زمانی که قمار در ایالات متحده ممنوع شد باز می گردد.

دکترین حقوقی نیز پولشویی را فرایندی که در راستای آن مرتکب اموالی را که از ارتکاب جرم و به صورت غیر قانونی به دست می آورند و به پول تمیز یا ثروتی که به ظاهر مشروع است تبدیل می کنند، می دانند.

قانون گذار تعریفی از جرم پولشویی ندارد و صرفاً در ماده ۲ قانون اصلاح قانون مبارزه با پولشویی مصادیق آن را بیان کرده است.

ماده ۲- ماده (۲) قانون به شرح زیر اصلاح می شود:

ماده ۲- پولشویی عبارت است از :

الف - تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از ارتکاب جرائم با

علم به منشأ مجرمانه آن

ب - تبدیل، مبادله یا انتقال عوایدی به منظور پنهان یا کتمان کردن منشأ

مجرمانه آن با علم به اینکه به طور مستقیم یا غیرمستقیم از ارتکاب جرم به دست



آمده یا کمک به مرتکب جرم منشأ به نحوی که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نشود.

پ - پنهان یا کتمان کردن منشأ، منبع، محل، نقل و انتقال، جابه جایی یا مالکیت عوایدی که به طور مستقیم یا غیرمستقیم در نتیجه جرم تحصیل شده باشد.

تبصره ۱- هرگاه ظن نزدیک به علم به عدم صحت معاملات و تحصیل اموال وجود داشته باشد مانند آن که نوعاً و باتوجه به شرایط امکان تحصیل آن میزان دارایی در یک زمان مشخص وجود نداشته باشد مسئولیت اثبات صحت آنها برعهده متصرف است. منظور از علم در این تبصره و تبصره (۳) همان است که در قانون مجازات اسلامی برای علم قاضی تعریف شده است.

تبصره ۲- داراشدن اموال موضوع این قانون منوط به ارائه اسناد مثبته می باشد. علاوه بر این چنانچه ارزش اموال مزبور بیش از ده میلیارد (۱۰.۰۰۰.۰۰۰.۰۰۰) ریال برای سال پایه و معادل افزایش یافته آن بر اساس نرخ تورم برای سالهای بعد باشد وجود سابقه از آن در سامانه های مربوطه مطابق قوانین و مقررات لازم است. عدم تقدیم اسناد مثبته که قابل راستی آزمایی باشد به حکم دادگاه مستوجب جزای نقدی به میزان یک چهارم ارزش آن اموال خواهد بود، در این صورت اصل مال موضوع قانون تا زمان رسیدگی قضائی توقیف می شود. چنانچه پس از رسیدگی اثبات شود دارا شدن مشروع بوده از مال رفع توقیف و در غیراین صورت ضبط می شود.

تبصره ۳- چنانچه ظن نزدیک به علم بر تحصیل مال از طریق نامشروع وجود داشته باشد در حکم مال نامشروع محسوب و مرتکب در صورتی که مشمول مجازات شدیدتری نباشد به حبس درجه شش محکوم می شود. در هر صورت مال مزبور ضبط خواهد شد مگر اینکه تحصیل مشروع آن اثبات شود.»

در واقع هدف از جرم پولشویی توجه به مبدا مال و هدف از جرم انگاری تامین مالی تروریسم توجه به مقصد مال است.^۱ جرم پولشویی از حیث رکن مادی در



حقوق کیفری، ایران جرمی ساده و مطلق است.^۱

هرگاه ظن نزدیک به علم به عدم صحت معاملات و تحصیل اموال وجود داشته باشد مانند آن که نوعاً و با توجه به شرایط امکان تحصیل آن میزان دارایی در یک زمان مشخص وجود نداشته باشد، مسئولیت اثبات صحت آنها برعهده متصرف است منظور از علم در این تبصره و تبصره (۳) همان است که مجازات اسلامی برای علم قاضی تعریف شده است.^۲

دارا شدن اموال موضوع این قانون منوط به ارائه اسناد مثبت می باشد چنانچه ارزش اموال موضوع این قانون بیش از ۱۰ میلیارد ریال برای سال پایه و معادل افزایش یافته آن بر اساس نرخ تورم برای سالهای بعد باشد وجود سابقه از آن در سامانه های مربوطه مطابق قوانین و مقررات لازم است. عدم تقدیم اسناد مثبت که قابل راستی آزمایی باشد به حکم دادگاه مستوجب جزای نقدی به میزان یک چهارم ارزش آن اموال خواهد بود در این صورت اصل مال موضوع قانون تا زمان رسیدگی قضائی توقیف می شود.^۳

هرگاه اثبات شود دارایی مشروع بوده = رفع توقیف

*هرگاه اثبات شود دارایی نامشروع بوده = ضبط *

چنانچه ظن نزدیک به علم بر تحصیل مال از طریق نامشروع وجود داشته باشد در حکم مال نامشروع محسوب و مرتکب در صورتی که مشمول مجازات شدیدتری نباشد به حبس درجه ۶ (یعنی حبس بیش از شش ماه تا دو سال محکوم میشود در هر صورت مال مزبور ضبط خواهد شد مگر اینکه تحصیل مشروع آن اثبات شود.^۴

ماده ۱- اصطلاحات مندرج در این قانون در معانی مشروح زیر به کار می رود :

الف - جرم منشأ: هر رفتاری است که مطابق ماده (۲) قانون مجازات اسلامی مصوب ۱/۲/۱۳۹۲ جرم محسوب شود. از منظر این قانون تخلفات مذکور در قانون

^۱آزمون وکالت ۱۳۸۹

^۲تبصره ۱ ماده ۲ قانون اصلاح پولشویی

^۳تبصره ۲ ماده ۲ قانون اصلاح پولشویی

^۴تبصره ۳ ماده ۲ قانون اصلاح پولشویی



مبارزه با قاچاق کالا و ارز با اصلاحات بعدی جرم محسوب می شود.

ب - مال: هر نوع دارایی اعم از مادی یا غیر مادی، منقول یا غیرمنقول، مشروع یا غیرمشروع و هر نوع منفعت یا امتیاز مالی و همچنین کلیه اسناد مبین حق اعم از کاغذی یا الکترونیکی نظیر اسناد تجاری، سهام یا اوراق بهادار.

پ - مال حاصل از جرم: هر مالی که به طور مستقیم یا غیرمستقیم از جرم منشأ به دست آید از قبیل مالی که از جرائم اقتصادی و جرم تأمین مالی تروریسم حاصل می شود همچنین، مال موضوع جرم یا مالی که برای ارتکاب جرم اختصاص داده شده است در حکم مال به دست آمده از جرم است.

ت - اشخاص مشمول: اشخاص مذکور در مواد (۵) و (۶) این قانون.

ث - مشاغل غیرمالی: مشاغلی که شاغلین آن معاملات زیادی را به صورت نقدی انجام داده و از نظر پولشویی در معرض خطر قرار دارند از قبیل پیش فروش کنندگان مسکن یا خودرو، طلافروشان، صرافان، فروشندگان خودرو، فرش های قیمتی، فروشندگان عتیقه جات و هر نوع محصول گران قیمت.

ج - خدمات پایه: خدماتی است که طبق مقررات مربوطه، پیش نیاز و لازمه ارائه سایر خدمات توسط اشخاص مشمول می باشد و پس از آن ارباب رجوع به منظور اخذ خدمات مکرر و متمادی به اشخاص مشمول مراجعه می کنند.

چ - معاملات و عملیات مشکوک

معاملات و عملیات مشکوک شامل هر نوع معامله، دریافت یا پرداخت مال اعم از فیزیکی یا الکترونیکی یا شروع به آنها است که براساس قرائن و اوضاع و احوالی مانند موارد زیر ظن وقوع جرم را ایجاد کند :

۱- معاملات و عملیات مالی مربوط به ارباب رجوع که 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 بیش از سقف مقرر در آیین نامه اجرائی این قانون



هر چند 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.^۱ عواید حاصل از جرم پولشویی به معنای هر نوع مال یا امتیازی است که به به طور مستقیم یا غیر مستقیم از ارتکاب جرایم اعم از منشا و پولشویی کسب شده است.

به جرم منشاء که در خارج از کشور واقع شده باشد، میتوان طبق اصل صلاحیت سرزمینی^۲ یا صلاحیت واقعی^۳ یا صلاحیت شخصی مثبت و منفی^۴ یا صلاحیت جهانی^۵ به منظور هماهنگی برای پیشگیری و مقابله با جرائم پولشویی و تأمین مالی تروریسم، شورای عالی مقابله پیشگیری از جرائم پولشویی و تأمین مالی تروریسم که در این قانون به اختصار شورا نامیده میشود، تشکیل می گردد.^۶

وظایف شورا عبارت است از: تعیین راهبردها و برنامه ریزی در جهت اجرای قانون، تهیه و پیشنهاد آیین نامه‌های لازم در خصوص اجرای قانون برای تصویب به هیأت وزیران، هماهنگ کردن دستگاههای زیر مجموعه دولت در امر جمع آوری پردازش و تحلیل اخبار اسناد، مدارک اطلاعات و گزارشهای واصله تهیه سامانه های هوشمند و شناسایی معاملات مشکوک و گزارش به مراجع ذی ربط جهت انجام اقدامات لازم.

مصادیقی از معاملات و عملیات مشکوک پولشویی :

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

*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.

*معاملات یا عملیات مالی که به هر ترتیب مشخص شود صوری یا ظاهری

^۱ ماده ۱ قانون اصلاح پولشویی

^۲ ماده ۴ ق.م.ا

^۳ ماده ۵ ق.م.ا

^۴ ماده ۷ و ۸ ق.م.ا

^۵ ماده ۹ ق.م.ا

^۶ ماده ۴ قانون اصلاح پولشویی



بوده و مالک شخص دیگری است.

*معاملات یا عملیات مالی که اقامتگاه قانونی هر یک از طرفین در مناطق پرخطر از نظر پولشویی واقع شده است. فهرست این مناطق توسط شورا مشخص می شود.

*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.

مرکز اطلاعات مالی یک مؤسسه دولتی تابع وزارت امور اقتصادی و دارایی است. در موارد فوری که به مقام قضائی دسترسی نیست که در این صورت مرکز اطلاعات مالی می تواند دستور توقیف و جلوگیری از انتقال وجوه و اموال مشکوک را حداکثر تا ۲۴ ساعت صادر و بلافاصله پس از حصول دسترسی مراتب را به مقام قضائی گزارش و مطابق دستور وی عمل کند چنانچه بعد از ۲۴ ساعت مجوز مراجع قضائی صادر نشود رفع توقیف می شود. رئیس مرکز اطلاعات مالی با رأی حداقل دوسوم اعضای شورا و با حکم رئیس شورا تعیین میشود و کارکنان مرکز اطلاعات مالی نیز توسط رئیس مرکز تعیین می شوند.^۱

مجازات جرم پولشویی براساس میزان درآمد حاصل از جرم منشا و پولشویی^۲ :

اگر تا ۱۰ میلیارد ریال باشد: (۱) مصادره اصل مال

(۲) حبس درجه ۵

(۳) جزای نقدی معادل پولشویی

بیش از ۱۰ میلیارد ریال باشد: (۱) مصادره اصل مال

(۲) حبس درجه ۴

(۳) جزای نقدی معادل پولشویی

* در صورتی که سازمان یافته باشد موجب تشدید مجازات به میزان ۱ درجه خواهد بود.

^۱ شرح جزا اختصاصی بهزاد ستاری، ص ۳۳۱

^۲ شرح جزا اختصاصی بهزاد ستاری، ص ۳۴۲



در صورتی که اشخاص حقوقی مرتکب جرم پولشویی شوند علاوه بر مقررات ماده ۲۰ ق.م.ا به جزای نقدی معادل ۲ تا ۴ برابر وجوه یا ارزش مالی که پولشویی شده محکوم می گردند.

مرجع صالح به رسیدگی پولشویی شعبی از دادگاه عمومی در تهران و در صورت نیاز مراکز استان ها هستند و تخصصی بودن شعبه رسیدگی به جرم پولشویی مانع رسیدگی به سایر جرایم نمی باشد. در مواردی که مرتکب پولشویی از مقامات ماده ۳۰۷ و ۳۸۰ ق.ا.ک و مرتکب جرم منشا شخصی غیر از مقامات مذکور باشد به جرم پولشویی حسب مورد در دادگاه کیفری تهران یا مرکز استان رسیدگی می شود.^۱

مجازات شروع به پولشویی مطابق ماده ۱۲۲ ق.م.ا خواهد بود.

مجازات معاونت به پولشویی مطابق ماده ۱۲۷ ق.م.ا خواهد بود.

مجازات شرکت در پولشویی مطابق ماده ۱۲۵ همان مجازات فاعل مستقل جرم است.

طبق ماده ۴۷ ق.م.ا پولشویی قابل تعویق و تعلیق است مگر اینکه بطور سازمان یافته باشد.

بخش دوم: مفاهیم پایه رمزارز^۲

ارزدیجیتال= کریپتو= رمزارز= کریپتوکارنسی= رمزینه ارز

تمامی اسامی که ذکر شده همگی به یک معنی و یک عملکرد هستند و منظور بازار رمزارزها می باشد که فعالین بازار رمز ارزها هر کدام این بازار را به این اسامی نسبت می دهند. اولین رمز ارز موفق بازار بیتکوین است که در سال ۲۰۰۹ توسط شخصی با نام مستعار ساتوشی ناکاماتو به تعداد ۲۱ میلیون واحد در شبکه بلاکچین^۳ قرار گرفت و راه به دست آوردن آن فقط از طریق استخراج است که به وسیله ماینر ها^۴ انجام می شود و هر ۴ سال یک بار پاداش این استخراج نصف می

^۱ شرح جزا اختصاصی بهزاد ستاری، ص ۳۳۱

^۲ مقاله کلاهداری به واسطه رمزارزها mjcheraghi.ir

^۳ blockchain

^۴ miner



شود یعنی با گذشت زمان این ارزش این ارز افزایش پیدا می کند. در حقیقت یکی از مشکلات اقتصادهای وابسته به پول فیات (همان پول ملی کشورها)، افت ارزش پول در اثر چاپ پول بیشتر است که بیت کوین این مشکل را حل کرده و در اصطلاح ضدتورمی عمل می کند.

رمزارزها به طور کلی تحت قاعده غیرمتمرکز بودن هستند این به این معنی است که به دولت ها یا سازمان ها و یا واسطه ای وابسته نیستند و این ها هم به طور مستقیم نمی توانند قانون گذاری یا نظارت مستقیمی بر روی رمز ارزها داشته باشند و اگر نظارت و عملی بخواهد انجام دهند فقط در قلمرو خود و تا جایی که بلاکچین به آنها دسترسی می دهد ادامه خواهد داشت پس رمزارزها به طور کاملاً مستقل از دنیای حقیقی در فضای بلاکچین به کار خود ادامه می دهند. اولین و مهم ترین تقسیم بندی ای که میتوان برای رمز ارزها نام برد تقسیم بندی ارزها به توکن^۱ و کوین^۲ است. کوین و توکن از لحاظ فنی با یکدیگر تفاوت دارند. کوین ها رمزارزهای بومی یک بلاکچین هستند یعنی کوین ها بلاکچین اختصاصی به خود را دارند و از بلاکچین بقیه ارزها تغذیه نمی کنند اما توکن ها بلاکچین اختصاصی خود را ندارند و از بلاکچین یک کوین جهت ایجاد قرارداد هوشمند بر روی بلاکچین آن کوین و تولید توکن تغذیه می کنند. به عنوان مثال ارز اتریوم^۳ خود یک کوین است که دارای بلاکچین اختصاصی به نام ای آر سی - ۲۰ است اما ارزی مثل شیبا یک توکن است که در شبکه اتریوم قرارداد نویسی شده و از این شبکه تغذیه می کند. دسته بندی بعدی که میتوان از بازار رمزارزها نام برد، دسته بندی کل بازار به بیتکوین و آلت کوین^۴ است که درباره بیتکوین صحبت کردیم و حالا آلت کوین ها که در بازار رمز ارزها به هر چیزی (کوین و توکن) آلت کوین گفته میشود این تقسیم بندی کلی است چون خود آلت کوین ها بسته به پروژه و عملکردی که دارند به شاخه های مختلفی تقسیم می گردند. در آخرین تقسیم بندی به بررسی شت کوین ها یا هرز رمز ارز می پردازیم. شت کوین ها در واقع توکن هایی هستند کاملاً بی ارزش و بی کاربرد و هدف خاصی را به دنبال نمی کنند و

^۱ token

^۲ coin

^۳ eth

^۴ Alt coin



صرفا با یک سری حواشی به وجود می آیند و با حواشی دیگر از بین می روند و بیشتر این شت کوین ها جنبه کلاهبرداری و اسکم را دارند. تا به اینجای کار با انواع رمز ارز آشنا شدیم حال وقت آن است که به صرافی هایی که در این بازار حضور دارند بپردازیم. به طور کلی صرافی ها به دو نوع متمرکز و غیر متمرکز تقسیم بندی می شوند. صرافی های غیرمتمرکز صرافی هایی هستند که در فضای بلاکچین ایجاد شده اند و بدون حضور فیزیکی و احراز هویت و ملیت و... می توان معامله و مبادله رمز ارزها را به طور کاملا شفاف انجام داد و تمامی تراکنش های این صرافی در اکسپلورر آن بلاکچین قابل مشاهده خواهد بود. اما صرافی های متمرکز که صرافی فیزیکی هم از آن یاد می شود یعنی صرافی ای که دارای اداره و سازمان است و از یک سری قوانین پیروی می کند که این قوانین، قوانین کشوریست که آن صرافی در قلمرو آن کشور واقع شده است این قوانین می تواند قوانین مالیاتی و یا حتی قوانین نظارتی باشد. اما این به این معنی نمی باشد که در صرافی های متمرکز جرمی رخ نمی دهد بالعکس تمامی جرایم در همین صرافی ها رخ می دهد که انسان در عملکرد آن دخالت دارد. آخرین موردی که از مفاهیم پایه رمزارزها بررسی می کنیم کیف پول های رمزارز است. کیف پول های رمز ارز تا به امروز تغییرات زیادی داشته اما هم اکنون تقسیم بندی که از آن ها می توان نام برد کیف پول فیزیکی و کیف پول نرم افزاری است. کیف پول فیزیکی که به اشکال مختلف تولید شده اند و روانه بازار گردیده دارای امنیت بیشتری نسبت به کیف های نرم افزاری است اما به دلیل رایگان نبودن آن مورد استقبال عموم مردم قرار نگرفته است. کیف پول های الکترونیکی یا نرم افزاری کیف پول هایی هستند که در قالب اپلیکیشن و یا بستر وب فعالیت دارند و مردم می توانند به صورت رایگان از این کیف پول ها استفاده کنند. البته هر کیف پول نیاز به ایجاد امنیت و نوعی نگهداری از طرف کاربر دارد که باید به آن ها عمل کند تا سرمایه اش به خطر نیفتد.

بند دوم: استاندارد های رمز ارز

هر رمز ارزی که به وجود می آید حالا می خواهد توکن یا کوین باشد باید یک سری استانداردها داشته باشد که بتوان تشخیص داد که این پروژه واقعا وجود دارد و آن را در بین ارزهای معتبر بازار طبقه بندی کرد.

اولین استاندارد یک رمزارز وجود وایت پیپر آن رمز ارز است. وایت پیپر نوعی شناسنامه ارز است که در آن اطلاعات پروژه، اهداف، نقشه راه و عملکرد آن پروژه را نشان می دهد که



توسط توسعه دهندگان و پدید آورندگان آن پروژه ایجاد می شود. دومین مورد وجود دامنه وبسایت با پسوند معتبر و درج وایت پیپر و اطلاعات پروژه داخل این وبسایت است.

سومین مورد کامیونیتی قوی و فعالیت در شبکه های مجازی و سوشال مدیا. چهارمین مورد لیست شدن رمز ارز در وبسایت های مرجع رمزارز مانند کوین مارکت کپ، کوین جکو و... است که این وبسایت ها هم مانند صافی ای هستند که ارزها از آن عبور می کنند.

پنجمین و مهم ترین استاندارد یک رمزارز که به آن اعتبار می بخشد پول لیکوییدیتی یا استخر نقدینگی است. هر چه میزان استخر نقدینگی یک ارز بیشتر باشد نوسانات آن ارز کم تر است و می توان گفت ارز امن تری جهت سرمایه گذاری است. آخرین استاندارد لیست شدن در صرافی های معتبر است که برای لیست شدن و قابل معامله بودن در این صرافی ها باید تمامی موارد گفته شده را کسب کنند تا بتوانند از فیلتر صرافی ها عبور کنند اما باید توجه داشت که هر رمز ارزی که در صرافی لیست می شود معتبر نیست.

بخش سوم: پولشویی رمزارزی

مجرمان از پولشویی با استفاده از رمز ارزها استفاده می کنند تا منبع درآمد های غیرقانونی خود را پوشش دهند. این کار با روش های متعددی انجام می گیرد؛ ساده ترین روش این است که آنها می توانند با نام های مستعار تراکنش ها را انجام دهند. ۳ مرحله برای پولشویی رمز ارزها وجود دارد^۱:

(۱) قرارگیری

(۲) پنهان کردن

(۳) یکپارچه سازی

• قرارگیری

رمز ارزها می توانند توسط پول فیات و یا رمز ارزها خریداری شوند. بازارهای آنلاین معاملات کریپتو (صرافی ها) سطوح مختلف پیروی از قوانین تراکنش های مالی دارند؛ صرافی های قانونی از قوانین مربوط به احراز هویت و ضد پولشویی

^۱ Mihanblockchain /blog



تبعیت می‌کنند. زمانی که صرافی‌ها قانون گذاری می‌شوند، مجبورند که قوانین احراز هویت و پروتکل‌های امنیتی را برای مشتریان در نظر بگیرند. این باعث می‌شود که اطلاعات تراکنش مشتریان ثبت و تایید شود. بدین ترتیب، ناشناس بودن تراکنش‌ها و مشتریان، از بین می‌رود. صرافی‌ها اطلاعات شخصی کاربران را ذخیره نمی‌کنند؛ به جای آن، از اطلاعات هویتی افراد استفاده می‌کنند تا اطلاعات تراکنش‌ها را با هم تطبیق دهند.

• پنهان کردن

تراکنش‌های بر پایه رمز ارزها را می‌توان با استفاده از بلاک چین دنبال کرد. با این حال، زمانی که بحث رمز ارز غیرقانونی به میان می‌آید، مجرمان می‌توانند از یک سرویس ناشناس‌سازی استفاده کنند تا منبع تراکنش را پنهان کنند. این کار می‌تواند هم در صرافی‌های قانونی انجام شود و هم در عرضه اولی‌ها، که از یک کوین برای خرید کوین دیگر استفاده می‌شود.

• یکپارچه سازی

زمانی که مرحله یکپارچه ساختن (مرحله آخر در پولشویی) انجام می‌شود، دنبال کردن تراکنش‌های غیرقانونی دیگر کار ساده‌ای نیست. این رمز ارز دیگر مستقیماً به یک عمل مجرمانه مرتبط نیست؛ اما پولشویان باید توضیح دهند که چگونه به این رمز ارز دست یافته‌اند. یکپارچه ساختن پاسخ این سوال است. یک روش ساده برای قانونی کردن این پول غیرقانونی، معرفی آن به عنوان درآمد از یک سرمایه گذاری موفق و یا افزایش قیمت رمز ارز است. رد کردن این ادعاها در بازاری که قیمت‌ها هر ثانیه تغییر می‌کند، بسیار سخت است. به هر حال، درست مثل یک حساب بانکداری خارج از کشور، که می‌توان از آن برای پولشویی استفاده کرد، یک شرکت نیز می‌تواند شیوه پرداخت با بیت کوین را انتخاب کند و درآمد خود را با تبدیل رمز ارز غیرقانونی به بیت کوین تمیز، قانونی جلوه دهد. برخی از مواردی که برجسته‌ترین روش‌های پولشویی شامل آنها می‌شوند به شرح زیر هستند :



۱) میکسر ها^۱: خدمات میکسر ها که با نام دست اندرکاران شناخته می‌شوند، می‌توانند جداسازی رمز ارزهای غیرقانونی را به طور موثر انجام دهند. میکسر ها این رمز ارزها را تقسیم می‌کنند و از چندین آدرس مختلف عبور می‌دهند و سپس دوباره آنها را دوباره ترکیب می‌کنند. این کار باعث می‌شود که یک رمز ارز تمیز و قانونی، که کارمزد آن نیز پرداخت شده، به وجود بیاید.

در بیشتر موارد پولشویی، رمز ارز به صورت قانونی در یک کیف پول قرار دارد. سپس قبل از قرار گرفتن در کیف پول مقصد در دارک وب، از یک کیف پول دارک وب دیگر عبور می‌کند. همین قضیه باعث می‌شود که رمز ارز به قدری تمیز و قانونی شود، که بتوان آن را به دنیای قانونی برگرداند و در صرافی معامله کرد و یا به ارز فیات تبدیل کرد.

۲) صرافی‌های غیر قانونی

یکی دیگر از راه‌هایی که مجرمان از آن برای پول‌شویی رمز ارزها استفاده می‌کنند، صرافی‌های غیر قانونی است؛ صرافی‌هایی که با قوانین ضد پولشویی سازگار نیستند و احراز هویت مناسبی انجام نمی‌دهند. تبدیل مداوم یک نوع رمز ارز به یک رمز ارز دیگر، آن را تبدیل به یک رمز ارز قانونی می‌کند، که مجرمان در نهایت آن را به یک کیف پول خارج از صرافی انتقال می‌دهند. در مواردی نادر، مجرمان ممکن است رمز ارز را به پول فیات تبدیل کنند؛ اما این که بازارهای فیات به صرافی‌های غیر قانونی سرویس دهند، غیر معمول است.

۳) شبکه‌های هم‌تا به هم‌تا^۲

برای کاهش ریسک پولشویی با بیت کوین، خیلی از مجرمان از شبکه‌های هم‌تا به هم‌تا غیرمتمرکز که غالباً بین المللی هستند استفاده می‌کنند. در اینجا، آنها می‌توانند غالباً از واسطه‌های نامشکوک برای ارسال دارایی‌هایشان به مقصد استفاده کنند. بیشتر طرح‌های پولشویی با رمز ارزها، از طریق صرافی‌هایی انجام می‌شوند که واقع در کشورهایی هستند که قوانین ضد پولشویی خاصی ندارند.

^۱ Mixer

^۲ P2p



اینجاست که مجرمان می‌توانند رمز ارز خود را تبدیل به پول فیات کنند و با آن کالاهای لاکچری مثل اتومبیل‌های گران قیمت و خانه‌های اشرافی بخرند.

(۴) کارت‌های پیش پرداخت

کارت‌های اعتباری پیش پرداختی که موجود آنها به صورت رمز ارز است، یک راه دیگر برای پولشویی با رمز ارز است.

این کارت‌ها می‌توانند برای فعالیت‌های مجرمانه مختلفی به کار روند و یا برای معامله با دیگر رمز ارزها استفاده شوند.

(۵) قمار و سایت‌های بازی^۱

قمار بازی آنلاین و سایت‌های بازی‌های آنلاینی که بیت کوین و دیگر رمز ارزها را به عنوان روش پرداخت قبول می‌کنند، یکی دیگر از طرح‌های پولشویی هستند. کریپتو می‌تواند برای خرید اعتبار یا چیپ‌های مجازی استفاده شود، که کاربران می‌توانند پس از چند تراکنش کوچک، دوباره آنها را خارج کنند.

همچنین تقریباً همان مفاهیمی که برای پولشویی پول فیات و پول نقد به کار می‌رود، در فضای رمز ارزها نیز کاربرد دارد.

به علت ویژگی مجهول و ناشناخته بودن که در شبکه بلاک چین تعبیه شده است، امکان پولشویی از طریق رمز ارزها به سادگی بیشتری نسبت به سایر طرق وجود دارد. در هر تراکنش، نشانی فرستنده و گیرنده ارز موزد نظر ثبت می‌شود. این نشانی مربوط یک شخص می‌باشد ولی برای بدست آوردن آن نیازی به ارائه هویت از سوی او نمی‌باشد؛ اگر چه اخیراً اکثر صرافی‌های رمز ارزها اقدام به احراز هویت کاربران خود می‌نمایند. هر شخص می‌تواند به کمک برنامه‌های کیف پول یک یا چندین آدرس مجزا بدست آورده و با آن‌ها اقدام به مبادله و جا به جایی رمز ارزها نماید. تنها در صورتی هویت فرد مشخص خواهد شد که در صرافی اقدام به مبادله رمز ارزها کرده یا یکی از طرف‌های معامله، هویت وی را درخواست کرده باشد، در غیر این صورت، فرد می‌تواند معامله یا تراکنشی را انجام داده، بدون آنکه هویت وی محرز شود. چنانچه صرافی یا ارز دیجیتال بر اساس

^۱ BET



قوانین و مقررات تعیین شده عمل نکنند، از این صرافی ها می توان برای تمیز کردن ارز های دیجیتال های کثیف که به همان پول شویی منتهی می شود، استفاده کرد. برخی دیگر از رمز ارزها از روش های پیچیده تری برای تامین گمنامی کامل استفاده می کنند، مانند مونرو، دَش و زیکش. در رمز ارز های مذکور حتی امکان ردگیری هویت افراد در معاملات نیز وجود نخواهد داشت. علاوه بر این ویژگی مجهول مذکور در رمز ارز ها که امکان پولشویی را فراهم می کند، سرویس های رد اثر در رمز ارز ها نیز شرایط ایجاد جرم مذکور را ایجاد و تحت شرایطی تشدید می کنند؛ این سرویس ها رمز ارز کثیف را از طریق انتقال بین نشانی های گوناگون، پیش از آنکه این مقدار به فرد دیگری منتقل شود، تمیز می کنند. این سرویس ها یک تا ۳ درصد از رمز ارزی را که رد اثر می کنند، شارژ می کنند که البته استفاده از این روش ریسک بالایی دارد. اصلی ترین راهکار مبارزه با پولشویی از طریق رمز ارز ها، اجرای مقررات شناسایی و احراز هویت مشتری در صرافی ها یا از سمت طرفین معامله است. هنگامی که هویت افراد در صرافی ها کاملاً ثبت شود، در آن صورت تا حد امکان مبارزه با پولشویی با استفاده از رمز ارز ها نیز فراهم می گردد. علاوه بر این روش های هوشمندی وجود دارد که امکان رد گیری زنجیره تراکنش ها را فراهم کرده و از رد پا های بدست آمده در جهت پیگرد مظنون های جرائم روی بستر رمز ارز ها استفاده می کنند.

امروزه در کشورمان دیده می شود که قوانین و مقرره های خاصی در این حوزه در کشورمان وجود ندارد و وب سایت های مختلفی ذیل عنوان صرافی های ارز های دیجیتال در کشورمان فعالیت می کنند، اگر چه آنها نیز برای ثبت نام احراز هویت می کنند، اما قطعاً وجود قوانین به آرامش خاطر مردم نیز کمک بسیار شایانی خواهد نمود، با این حال بانک مرکزی تا امروز مصوبه ای مبنی بر جواز یا عدم جواز فعالیت رمز ارز ها در کشورمان صادر نشده است.

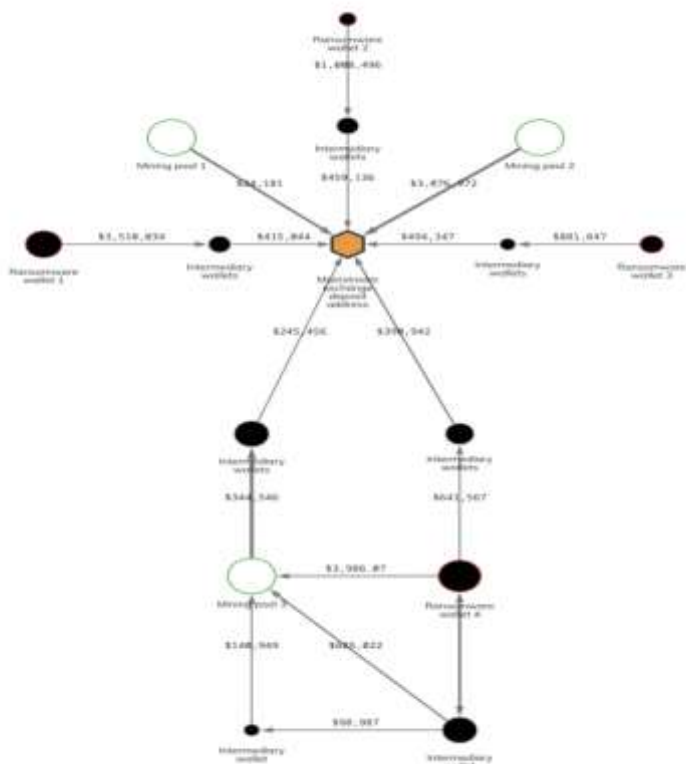
بخش چهارم: پولشویی با استفاده از استخر های ماینینگ:

استخراج یا ماینینگ یک بخش مهم و جدانشدنی از صنعت ارز دیجیتال است. استخراج کوین ها روشی برای کسب درآمد مستقیم از بلاک چین است و به همین دلیل، همیشه برای کلاهبرداران و مجرمان سایبری جذاب بوده است. برخی از این

مجرمان از استخرهای استخراج برای پولشویی و پاک کردن رد دارایی‌های مسروقه استفاده می‌کنند.

- واریز مقادیر کلان سود ماینینگ و باج‌افزارها به آدرس‌های فعال

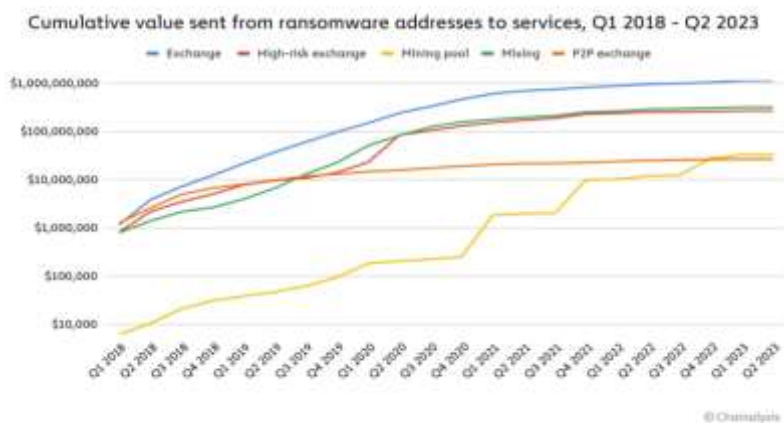
مثال اول مربوط به یک آدرس بسیار فعال در یکی از صرافی‌های ارز دیجیتال معمولی است که پول زیادی را از استخرهای استخراج و کیف پول‌های مربوط به باج‌افزارها دریافت کرده است. از ۹۴.۲ میلیون دلار ارز دیجیتالی که به این آدرس واریز شده، ۱۹.۱ میلیون دلار آن از آدرس‌های مربوط به باج‌افزارها و ۱۴.۱ میلیون دلار آن از استخرهای ماینینگ دریافت شده است. جزئیات فعالیت این آدرس در نمودار زیر قابل مشاهده است (دایره‌های سبز مربوط به استخرهای استخراج و دایره‌های مشکی مربوط به باج‌افزارها هستند):





با توجه به نمودار بالا، مجرمان برای ارسال وجوه به این آدرس از کیف پول‌های واسطه استفاده کرده‌اند. با این حال، تعامل بین کیف پول باج‌افزار ۴ و استخر ماینینگ ۳ که در پایین نمودار دیده می‌شود، بسیار جالب توجه است. هم کیف پول ۴ و هم استخر ۳ دارایی‌ها را از طریق کیف پول‌های واسطه به آدرس صرافی ارسال کرده‌اند؛ اما در برخی موارد مشاهده می‌کنیم که کیف پول باج‌افزار، پول‌ها را هم به صورت مستقیم و هم با واسطه به خود استخر استخراج واریز کرده است. این نوعی پولشویی پیچیده است و مجرم برای آن که هشدار دریافت نکند، پول‌ها را از طریق یک استخر استخراج به حساب صرافی دلخواه خود منتقل می‌کند. در این روش، استخر استخراج همانند یک میکسر (Mixer) عمل می‌کند و با پنهان کردن منشا دارایی‌ها، اینطور جلوه می‌دهد که دارایی‌ها از استخرهای دریافت شده‌اند نه از باج‌افزارها (می‌دانیم که ارزهای دیجیتال را نمی‌توان از طریق سرویس‌ها از جمله استخرهای استخراج ردیابی کرد).

داده‌ها نشان می‌دهند که این نوع سوءاستفاده از استخرهای ماینینگ، روزبه‌روز در حال افزایش است. از زمان آغاز این کار (در سال ۲۰۱۸) تاکنون، ارزش دارایی‌های ارسال شده از کیف پول‌های باج‌افزاری به استخرهای استخراج به صورت مستمر رشد کرده است.

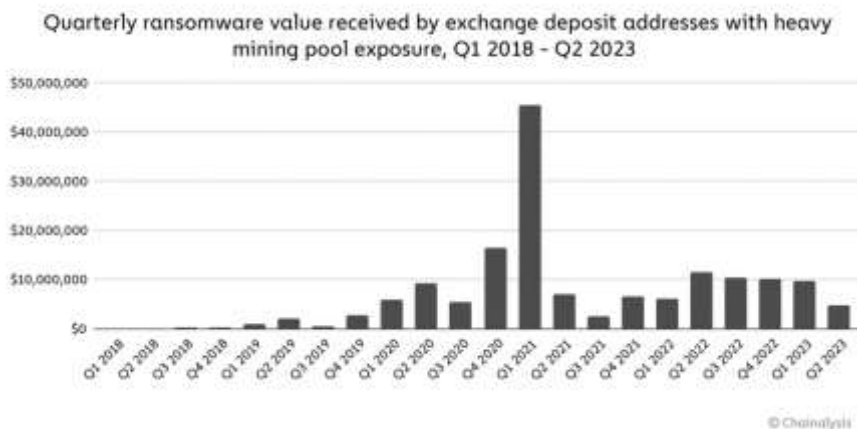


chainalysis^۱

^۱ chainalysis



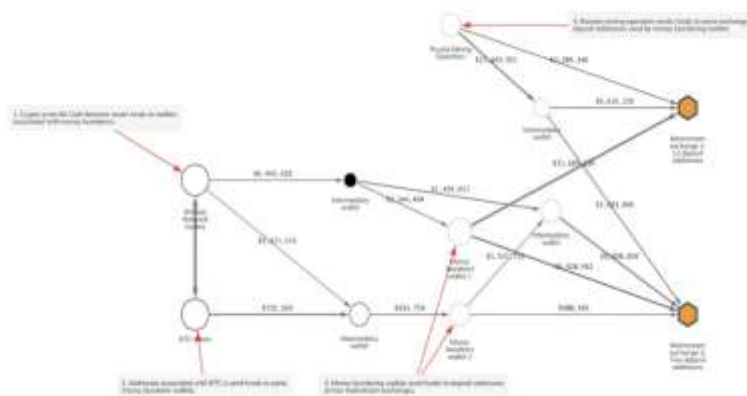
این رشد مستمر نشان می‌دهد که هر روز مجرمان بیشتری دارایی‌های غیرقانونی خود را از طریق استخرهای ماینینگ به صرافی‌ها ارسال می‌کنند. به‌طور کلی، در آدرس‌هایی که مقادیر زیادی ارز دیجیتال از استخرهای استخراج دریافت می‌کنند، میزان واریزی از طرف کیف پول‌های باج‌افزاری نیز زیاد است. اصولاً صرافی‌ها باید این نوع فعالیت‌ها را به‌راحتی تشخیص دهند؛ اما مجرمان سعی می‌کنند پول غیرقانونی خود را به‌عنوان درآمد حاصل از استخراج جلوه دهند (حتی اگر منشأ اولیه دارایی‌ها استخر استخراج نباشد). به‌طور کلی، ۳۷۲ آدرس در صرافی‌ها حداقل ۱ میلیون دلار ارز دیجیتال را از استخرهای ماینینگ و آدرس‌های باج‌افزاری دریافت کرده‌اند. نمودار زیر میزان سرمایه دریافت‌شده از آدرس‌های باج‌افزاری را از ماه ژانویه ۲۰۱۸ (اواسط دی ماه ۱۳۹۶) تاکنون نشان می‌دهد:



chainalysis ۱

از سال ۲۰۱۸، آدرس‌های واریز صرافی‌ها بیش از ۱۵۸.۳ میلیون دلار ارز دیجیتال را از آدرس‌های باج‌افزاری دریافت کرده‌اند. این عدد سهم قابل‌توجهی از مبلغ کل منتقل‌شده از کیف پول‌های باج‌افزاری به صرافی‌ها را تشکیل می‌دهد (توجه کنید که این آمار تقریبی است و با شناسایی آدرس‌های بیشتر رشد خواهد کرد). به‌طور کلی، داده‌ها نشان می‌دهند که استخرهای ماینینگ نقش مهمی در استراتژی پولشویی مجرمان ایفا می‌کنند.

- پولشویی بیت کوین‌های مسروقه از طریق درآمد حاصل از استخراج
- مثال دوم درباره کلاهبرداری بیت کلاب نتورک^۱ و دو کیف پول مربوط به آن است. کلاهبرداران این پروژه توانستند میلیون‌ها دلار بیت کوین را به صرافی‌های معروف واریز کنند. شبکه بیت کلاب یک پروژه کلاهبرداری در سال‌های ۲۰۱۴ تا ۲۰۱۹ بود که با وعده‌های دریافت سود کلان از استخراج بیت کوین، کاربران زیادی را فریب داد. این پروژه صدها میلیون دلار از کاربران دزدی کرد و در نهایت، مدیران آن توسط وزارت دادگستری ایالات متحده دستگیر و متهم شدند. اوایل سال ۲۰۱۹ (اواخر ۱۳۹۷) و قبل از اعلام جرم، پروژه بیت کلاب میلیون‌ها دلار بیت کوین را به کیف پول‌های مرتبط با سرویس‌های پولشویی زیرزمینی (که ظاهراً در روسیه مستقر هستند) منتقل کرد. در سه سال بعدی، بیت کوین‌های مسروقه از این کیف پول‌های پولشویی به صرافی‌های معروف واریز شدند. در همین برهه و مخصوصاً از اکتبر ۲۰۲۱ (اواسط مهر ماه ۱۴۰۰) تا آگوست ۲۰۲۲ (اواسط مرداد ماه ۱۴۰۱)، یک سرویس استخراج بیت کوین در روسیه نیز میلیون‌ها دلار بیت کوین را به همان آدرس‌ها واریز کرد. نمودار زیر طرح کلی فعالیت پولشویی این کلاهبرداران را نشان می‌دهد:



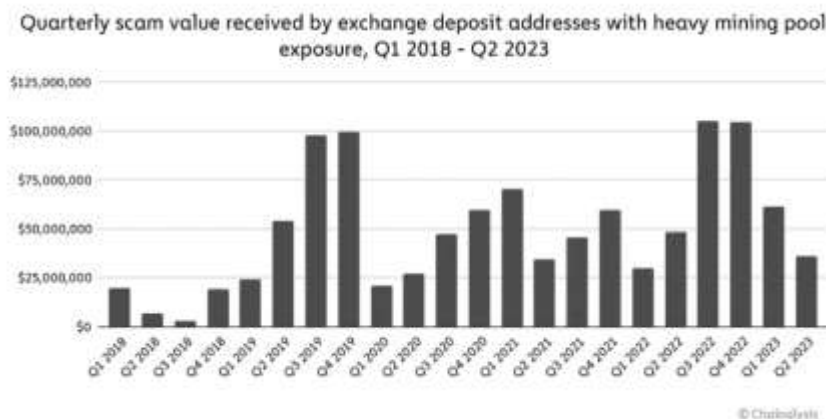
Chainalysis

¹ Bitclub Network



به طرز جالبی بین مارس ۲۰۱۷ (اواسط اسفند ماه ۱۳۹۵) تا نوامبر ۲۰۱۸ (اواسط آبان ماه ۱۳۹۷)، وجوهی که از صرافی بیت ای^۱ به یکی از کیف پول‌های پولشویی ارسال شده بود، به همان آدرس‌هایی که برای پولشویی توسط بیت کلاب استفاده می‌شد، منتقل شده است. در سال ۲۰۱۷ بیت کلاب و بیت ای پول‌هایی را بین خود رد و بدل کردند. بیت ای یک صرافی روسیه‌ای بود که در سال ۲۰۱۷ با اتهام کمک به پولشویی (از جمله پولشویی دارایی‌های مسروقه در هک ام تی جاکس^۲) تعطیل شد.

احتمال می‌رود که کلاهبرداران عمداً دارایی‌های بیت ای و بیت کلاب را با دارایی‌های به دست آمده از استخراج ترکیب کرده باشند تا این‌طور به نظر بیاید که کل دارایی‌های واریز شده به صرافی‌ها از استخراج حاصل شده است. داده‌ها نشان می‌دهد که کلاهبرداران و مجرمان ارز دیجیتال از استخرهای ماینینگ به‌عنوان بخشی از فرایند پولشویی استفاده می‌کنند. نمودار زیر میزان کل ارزهای دیجیتال واریز شده به آدرس‌هایی را نشان می‌دهد که از سال ۲۰۱۸ به بعد، حداقل ۱ میلیون دلار از استخرهای ماینینگ دریافت کرده‌اند:



از سال ۲۰۱۸ تاکنون، میزان کل سرمایه‌ای که از آدرس‌های مرتبط با کلاهبرداری به آدرس‌های صرافی واریز شده، کمتر از ۱.۱ میلیارد دلار است.

^۱ BTC-E

^۲ Mt.Gox

• راهکار جلوگیری از پولشویی به روش ماینینگ

بررسی‌ها نشان می‌دهد کلاهبرداران ارز دیجیتال گاهی از فرایند استخراج رمزارز و استخرهای ماینینگ برای پولشویی و پاک کردن رد دارایی‌های مسروقه استفاده می‌کنند. در واقع اگر همان استراتژی شناسایی باج‌افزار و پولشویی با استخرهای ماینینگ را در پیش بگیریم و آن را برای تمام جرائم ارز دیجیتال به کار ببریم، به این نتیجه می‌رسیم که ۱.۸ میلیارد دلار ارز دیجیتال به‌صورت غیرقانونی و به کمک استخرهای استخراج به صرافی‌ها واریز شده است.

اما این مشکل حل‌شدنی است. اولین و مهم‌ترین راه‌حل این است که سرویس‌های هش و استخرهای ماینینگ در کنار احراز هویت، کیف پول‌ها را با اقدامات سخت‌گیرانه غربالگری کنند. همچنین به کمک تکنولوژی بلاکچین، منشا دارایی‌های کاربر را شناسایی کرده و دارایی‌های ارسال شده از آدرس‌های غیرقانونی را مسدود کنند. در قدم بعدی، صرافی‌های ارز دیجیتال باید کیف پول‌های واریزکننده ارز دیجیتال را به‌دقت بررسی و بازبینی کنند (ابزارهای مختلفی برای این کار وجود دارد که صرافی‌ها می‌توانند از آن‌ها استفاده کنند). با چنین اقداماتی، کلاهبرداران دیگر نمی‌توانند از استخرهای استخراج ارز دیجیتال برای پولشویی استفاده کنند و فرایند استخراج رمزارز را بدنام کنند.

• پولشویی در بزرگترین صرافی رمزارز جهان و پردازش مالی ایران^۱

در پی توافق میان بایننس، بزرگترین پلتفرم مبادلات رمزارز در جهان، با مقام‌های آمریکایی، چانگ‌پنگ ژائو بنیانگذار و مدیر میلیاردر این صرافی از مقام خود کناره‌گیری می‌کند. ژائو پذیرفته که به نقض قوانین ضد پولشویی آمریکا اعتراف کند و در پی این توافق، بایننس حدود ۴.۳ میلیارد دلار جریمه خواهد پرداخت تا پرونده علیه خود را مختومه کند. مقامات آمریکایی حداقل از سال ۲۰۱۸ در حال بررسی این صرافی بوده‌اند، اما تاکنون به‌طور رسمی اقدام قانونی انجام نداده بودند. ژائو یکی از بنیانگذاران، رئیس و سهامدار عمده بایننس، شهروند کانادایی متولد چین است که به مشهورترین چهره در دنیای رمزارزها تبدیل شده

^۱ <https://www.reuters.com/>



است. تحقیقات مقامات آمریکا در این زمینه که به طور گسترده در مطبوعات بازتاب داشته، برای چندین سال تهدیدی برای بایننس بوده و چندین مدیر اجرایی آن در ماه‌های اخیر استعفا داده‌اند. علاوه بر این، این صرافی امسال توسط دو آژانس اصلی تنظیم کننده بازار مالی، اس‌ای‌سی و اس‌اف‌تی‌سی به دادگاه کشیده شد. اس‌اف‌تی‌سی اعلام کرده که این صرافی اقدامات کافی برای جلوگیری از پولشویی انجام نداده و مشتریان می‌توانند بدون اینکه هویت آنها قبلاً تأیید شده باشد، به پلتفرم صرافی دسترسی داشته باشند.

گزارش جدید شرکت خدمات مالی رمزارز «بلوک چین» حاکی از تراکنش ۷.۸ میلیارد دلار منابع مالی برای ایران توسط صرافی بین‌المللی رمزارز «بایننس» از سال ۲۰۱۸ است. خبرگزاری رویترز روز جمعه ۱۳ آبان ۱۴۰۲ با پوشش این گزارش چنین بیان کرد: این تراکنش‌های مالی نقض تحریم‌های آمریکاست و می‌تواند بایننس، از صرافی‌های پیشرو صنعت ۱ تریلیون دلاری رمزارز با ۱۲۰ میلیون کاربر، را با چالش مواجه سازد. کل تراکنش‌های مالی با بزرگترین صرافی رمزارز ایرانی، نوبیتکس، انجام شده و سه چهارم تراکنش‌ها با رمزارز «ترون» که اجازه مخفی کردن هویت کاربران را می‌دهد، انجام شده است. در سال گذشته نیز صرافی نوبیتکس در سایت رسمی خود از کاربران و مشتریان درخواست کرد که برای مخفی نگاه داشتن هویت خود و دور زدن تحریم‌های آمریکا از رمزارز ترون استفاده کنند. رویترز ژوئیه امسال نیز طی گزارشی به ادامه ارائه خدمات توسط بایننس به مشتریان ایرانی خبر داده و نوشته بود خود این صرافی به محبوبیت در جمهوری اسلامی واقف است. همان زمان بایننس در واکنش به این گزارش گفته بود از قوانین تحریم‌های بین‌المللی علیه ایران پیروی می‌کند و طبق تحریم‌ها، دسترسی افراد به این پلتفرم را مسدود می‌کند. چانگ پنگ ژائو شهروند چین و بنیانگذار میلیاردی صرافی بایننس در توییتی اعلام کرده بود: «بایننس پس از تحریم‌ها، کاربران ایرانی را از دریافت خدمات ممنوع کرد؛ ۷ ایرانی از چشم دور مانده بودند که دریافت خدمات برای آنها نیز بعداً ممنوع شد.» در واکنش به گزارش جدید شرکت بلوک چین، سخنگوی بایننس اعلام کرد اگرچه این صرافی یک شرکت آمریکایی نیست، اما اقدامات پیشگیرانه برای محدود کردن ورود ایرانی‌ها را انجام داده است.

بایننس در اوت پارسال اعلام کرد که مشتریان دیگر قادر به افتتاح حساب و

استفاده از خدمات آن بدون ثبت هویت نیستند، اما بر اساس داده‌های «بلوک چین» از آن زمان تا نوامبر سال جاری این صرافی بین‌المللی بیش از یک میلیارد دلار معاملات را مستقیماً از نوبیتکس و سایر صرافی‌های ایران پردازش کرده است و از زمان توییت آقای ژائو در ماه ژوئیه، بایننس حدود ۸۰ میلیون دلار در معاملات ایران پردازش کرده است. آمارهای ترون نیز نشان می‌دهد از آوریل ۲۰۲۰ تاکنون به تعداد یک میلیون و ۱۵۰ هزار تراکنش میان بایننس و نوبیتکس انجام شده است.

داده‌های بررسی شده نشان می‌دهد که در مجموع ۲.۹۵ میلیارد دلار رمز ارز از سال ۲۰۱۸ به طور مستقیم بین صرافی‌های ایرانی و بایننس جابجا شده. همچنین ۵ میلیارد دلار رمز ارز دیگر نیز بین صرافی‌های ایرانی و بایننس از طریق لایه‌هایی از واسطه‌ها جابجا شده است.

قانون‌گذاران می‌گویند که چنین نقل و انتقالات «غیر مستقیمی» باید هشدار پولشویی و نقض تحریم‌ها برای صرافی‌های رمزارز باشد.

• مراقب پولشویی رمزارزی با ترفند «کار در منزل» باشید:^۱

هشدار انجمن بلاک‌چین ایران: بر اساس اطلاعیه این انجمن، روش‌های تبلیغاتی مانند «کار در منزل، اجاره کارت بانکی، کار پاره‌وقت با درآمد بالا و غیره»، از ترفندهای جدید کلاه‌برداران هستند که تمامی آنها به یک چیز ختم می‌شوند: با هویت خودتان (کارت ملی و کارت بانکی) در یک پلتفرم عضو شوید و با پول واریزشده توسط فرد سودجو، اقدام به خرید رمزارز کنید و سود خود را هم بردارید. این سودها اغلب وسوسه‌کننده هستند و فرد قربانی تصویری از مسوولیت کامل مالی این کار ندارد. در واقع، وی تصور می‌کند از آنجاکه کارت ملی و کارت بانکی هزینه‌ای برایش ندارد و پولی را از خودش مصرف نمی‌کند، می‌تواند سود کسب کند. این در حالی است که پول‌های دزدی، باج‌گیری، قمار، فیشینگ و هک، از این طریق تبدیل به یک دارایی شده و فرد سودجو سپس متواری می‌شود. و در نهایت، این فرد قربانی است که مسوولیت کامل این کار را بر عهده دارد و باید

^۱ انجمن بلاکچین ایران

پاسخگو باشد. به همین دلیل، انجمن بلاکچین ایران به کاربران توصیه می‌کند که «هرگز هویت (کارت ملی) و حساب بانکی خود را در اختیار دیگران قرار ندهید.»

• هشدار پلیس فتا نسبت به پولشویی و کلاهبرداری در پوشش رمزارز^۱

اخیرا پرونده‌های کلاهبرداری و پولشویی از طریق سایت دیوار با ترفند تبدیل وجه سرقتی به رمز ارز رواج زیادی پیدا کرده است. در این روش کلاهبرداران با ترفند درآمد هفتگی در منزل با آموزش رمز ارز و به بهانه داشتن درآمد دو میلیون تومانی، دام خود را در فضای مجازی پهن کرده و افراد نا آشنا نیز با برقراری ارتباط با این افراد نهایتا به شبکه اجتماعی تلگرام هدایت می‌شوند. کلاهبرداران در ادامه شگرد فریبکارانه خود به افراد پیشنهاد می‌کنند با نصب برخی صرافی‌های دیجیتال مرتبط با رمز ارزها و... به افتتاح یک حساب بانکی اقدام کنند و در نهایت عکس کارت بانکی و شماره تماس خودشان را از طریق تلگرام برای وی ارسال کنند. افراد کلاهبردار با سرقت موجودی حساب بانکی افراد غیر، وجه را مستقیما به حساب قربانی واریز و بعد آن به فرد واسط اعلام می‌کنند تا بابت ارسال وجه مذکور اقدام به شارژ کیف پول دیجیتال خود کرده و با آن رمز ارز خریداری کند و سپس وجه مذکور را به آدرس کیف پولی که به وی اعلام شده، انتقال دهند. از آنجایی که آدرس‌های کیف پول مقصد در رمز ارزها قابل شناسایی نیست، عملا کلاهبرداران اقدام به پولشویی کرده و تمام مسئولیت عواقب تعقیب قانونی از قبیل مسدودی حساب و... متوجه فرد قربانی است که حساب خودش را در اختیار کلاهبرداران قرار داده است. در این شگرد کلاهبرداران از خودشان اثری باقی نمی‌گذارند.

• انتقاد سازمان ملل از پولشویی در صرافی‌های رمزارز^۲

سازمان ملل متحد، در گزارشی هکرهای کره شمالی را به فعالیت در شبکه‌های پولشویی در جنوب شرقی آسیا متهم کرد. رویترز مدعی شده است که هکرهای

^۱ وبسایت پلیس فتا

^۲ <https://www.reuters.com/>



کره شمالی در حال به اشتراک گذاشتن داده‌های خود با شبکه‌های پولشویی و بانکی زیرزمینی، کلاهبرداران و قاچاقچیان مواد مخدر در جنوب شرقی آسیا هستند. این شبکه‌ها شامل کازینوها و صرافی‌های رمزارزها به عنوان مکان‌های کلیدی سازماندهی شده برای ارتکاب به جرم هستند. دفتر مبارزه با مواد مخدر و جرایم سازمان ملل متحد بدون اشاره به جزئیات اعلام کرد که چند نمونه از چنین همکاری‌هایی در منطقه مکنونگ (که شامل بخش‌هایی از میانمار، تایلند، لائوس و کامبوج است) توسط هکرها از جمله گروه لازاروس در کره شمالی مشاهده شده است. این نهاد سازمان ملل گفت: این فعالیت‌ها از طریق تجزیه و تحلیل اطلاعات پرونده و داده‌های بلاک چین شناسایی شده است. در تماس تلفنی درباره این گزارش، یک فرد در نمایندگی کره شمالی در سازمان ملل در ژنو، بدون ذکر نام خود، گفت اطلاعاتی از این موضوع ندارد و گزارش‌های قبلی درباره لازاروس و همه گمانه زنی و اطلاعات نادرست بوده است. آمریکا مدعی است توسط دفتر اطلاعات اولیه کره شمالی کنترل می‌شود، به دست داشتن در یک رشته حملات سایبری و باج افزارهای معروف متهم شده است. آمریکا مدعی است وجوه دزدیده شده از صرافی‌های رمزارز توسط هکرها کره شمالی منبع اصلی تامین مالی برای پیونگ یانگ و برنامه‌های تسلیحاتی آن است. گزارش دفتر مبارزه با مواد مخدر و جرایم سازمان ملل متحد می‌گوید: کازینوها و مراکز قمار در آسیای جنوب شرقی از طریق بازیگران ثروتمند، مبادلات غیرقانونی رمزارزها را تسهیل می‌کنند و به «مراکز اساسی» بانکداری مورد استفاده جرایم سازمان‌یافته در منطقه تبدیل شده‌اند. ازی‌نوها ثابت کرده‌اند که برای جابه‌جایی و شستشوی حجم عظیمی از پول‌های رمزنگاری‌شده و سنتی، غیرقابل شناسایی هستند و توانایی خود را برای ایجاد کانال‌هایی برای ترکیب کردن میلیاردها دلار عواید اعمال مجرمانه در سیستم مالی رسمی ثابت کرده‌اند. جرمی داگلاس، نماینده منطقه ای دفتر مبارزه با مواد مخدر و جرایم سازمان ملل متحد در آسیای جنوب شرقی و اقیانوس آرام، به رویترز گفت: افزایش کازینوها و رمزارزها، به تعداد گروه‌های جرایم سازمان یافته در جنوب شرقی آسیا اضافه کرده است.



نتیجه گیری

بازار رمز ارزها و فضای بلاکچین علاوه بر روی مثبت خود که سود ها و سرمایه گذاری ها هستند روی منفی ای دارند که استفاده نامشروع به حساب می آید. همان طور که در مطالب مقاله بررسی کردیم بیشترین مورد پولشویی از حساب، اکانت اشخاص حقیقی که رو حشان از پولشویی خبر ندارد صورت گرفته است در واقع این افراد با کرایه دادن اکانت خود به سودجویان مبلغی نا چیز به طور ماهیانه یا سالیانه دریافت کرده اند که با همین طمع قربانی یک جرم پولشویی شده اند. رمزارزها به دلیل ذات گمنام و بدون هویت خود بیشتر از سایر حوزه های دیگر در معرض پولشویی قرار دارد یا می توان گفت که پولشویی در این بازار به راحتی آب خوردن انجام می شود و هیچ کسی هم متوجه این کار نمی شود اما حداقل صرافی های متمرکز در ایران می توانند نظارت بیشتری برروی تراکنش هایی که در صرافی انجام می دهند داشته باشند تا پول های کثیف وارد این بازار نشود که موجب بد نامی بازار رمز ارزها شود. در نهایت هم باید گفت که پولشویی و آثار آن متأسفانه به وضوح در وبسایت های خرید اموال منقول و غیر منقول مشاهده می شود که کار این افراد را اسان می کند. به این شکل که پولی کثیف به دنیای رمز ارزها ورود کرده و تبدیل به بیتکوین یا هر ارزی شده است و باید تبدیل به پول فیات شود اینجا افراد به دنبال اگهی تهاتر ملک یا خودرو با رمز ارز هستند وبا این تهاتر پول کثیف به همین راحتی شسته شد و وارد پول های فیات شد.

تشکر و قدردانی:

اول از خداوند سپاسگذارم، چون زیباست، زیبایی را دوست دارد و زیبایی هایی مثل ما را آفرید

دوم از اساتید محترم دانشگاه آزاد اسلامی واحد تهران شمال سپاسگذارم بابت راهنمایی ها و نقشه راهی که در اختیار دانشجویان قرار می دهند

و آخرین تشکر هم میرسد به کسی که در همه سختی ها کنارم بود و در تک تک لحظات زندگی همراه و هم قدمم



منابع و مآخذ

الف) منابع فارسی

- انجمن بلاکچین ایران
- آزمون دکتری ۱۳۹۸
- آزمون وکالت ۱۳۸۹
- بلاگ پلیس فتا
- شرح جزای اختصاصی دکتر بهزاد ستاری/۱۴۰۰
- قانون اصلاح قانون مبارزه با پولشویی
- قانون مجازات اسلامی ایران
- لغت نامه معین
- مقاله پولشویی بانک تجارت ایران
- وبسایت میهن بلاکچین
- <https://rc.majlis.ir/fa/law/show/۱۳۳۴۰۰>

ب) منابع انگلیسی

- Clean Coin, Dirty Money: Understanding the Risks of Crypto Laundering
- <https://www.reuters.com>
- Money Laundering: A Guide for Criminal Investigators, Third Edition
- The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond Hardcover