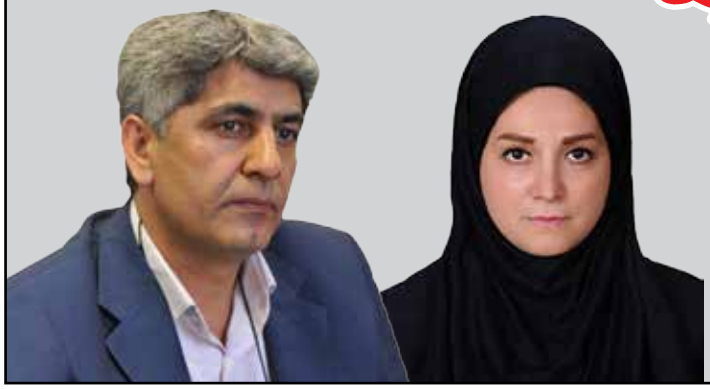
ملاحظات حسابرسی مربوط به رمزارزها و معاملات آن



مرتضی اسدی - آرشینا منتظری

مقدمه

رمزارزهـــا[1] به افراد و مشـــاغل اجازه می‌دهد بـــدون واســـطه‌ای مانند بانک یا مؤسســـات مالی دیگر بـــا یکدیگر و بـــدون دخالـــت هرگونه واســـطه‌ای در اینترنت معامله مســـتقیم داشته باشند. بیش‌تر رمزارزها برای بهرمند شـــدن از ویژگی‌های اساســـی مانند غیر متمرکز بودن، شـــفافیت و تغییر ناپذیر بودن، از بلاک‌چین اســـتفاده می‌کنند و بنابراین معاملات رمزارزها با فن‌آوری بلاک‌چین رابطه‌ی تنگاتنگی دارند. افزایش سریع و نوســـان رمزارزها منجر به افزایش علاقه و بررســـی جهانی توســـط ســـازمان‌ها، سرمایه‌گذاران، نهادهای نظارتی، دولت‌ها و دیگران شده اســـت. طی سال ۲۰۱۷ سرمایه بازار رمزارزها ۵۴۷ میلیارد دلار آمریکا یا ۳،۰۳۸ درصـــد افزایش یافت که ســـال موفقی را پشـــت سر گذاشت. محبوب تریـــن و پرکاربردترین رمزارز، بیت کوین اســـت. با ایـــن حال، بیش از ۹۰۰۰ رمزارز در گردش است. هر یک از این رمزارزها دارای ویژگی‌های منحصر به فرد خود است که درک، حسابداری و حسابرسی آن‌ها را به ویژه چالش‌برانگیز می‌کند. به‌طور معمول صورت‌های مالی، مانده رمزارزها و نتایج معاملات رمزارزها را منعکس می‌کنند. با این حال، بسیاری از حسابرســـان ممکن اســـت در زمینه رمزارزها تجربه کمی داشـــته باشند و یا هیچ تجربه‌ای نداشـــته باشند و بنابراین ممکن اســـت چالش‌هایی را که ممکن است حسابرسی در این موارد ایجاد کند، کاملاً ارزیابی نکننـــد. این مقاله در نظر دارد تا مواردی را برای بررسی در اختیار حسابرسان قرار دهد:

- تصمیم‌گیری در مورد پذیرش یا ادامه کار حسابرسی هنگامی که واحد تجاری در معاملات رمزارزها اقدام کرده است.
- شناســـایی و ارزیابی ریســـک‌های تحریف بااهمیـــت در صورت‌های مالی مربوط به معاملات و مانده رمزارزها.

رمزارزها چه هستند؟

رمزارزها یا دارایی‌های رمزنگاری شـــده شـــکل خاصی از پول دیجیتال اســـت که بر پایه علم رمزنگاری ایجاد شـــده اســـت. دارایی‌های رمزنگاری شده بر روی یک دفتر کل توزیع‌شده[2] ثبت می‌شوند، این دارایی‌ها نام خود را از سازوکارهای امنیتی رمزنگاری می‌گیرند که درون دفتر کل توزیع‌شـــده و بدون نیاز به مجوز بکار گرفته می‌شـــوند. دارایی‌های رمزنگاری شـــده همانند ریال و دلار پول‌هایی هســـتند که با سازوکارهای مختلفی ایجاد و توزیع می‌شـــوند. فرآیند خلـــق بعضی از این پول‌ها مانند بیت‌کوین با ماینینگ (اســـتخراج)[3] انجام می‌شود و برای تعدادی دیگر از آن‌ها، تمامی سکه‌ها از قبل بصورت اســـتخراج شـــده در شبکه قرار می‌گیرند. از دید بســـیاری بیت‌کوین اولین ارز دیجیتال حقیقی یا رمزارزی است که ایده آن در ســـال ۲۰۰۸ در وایپ پیپر بیت‌کوین منتشـــر و اولین سکه‌ها درسال ۲۰۰۹ استخراج گردید.

رمزارزها چـــه تفاوتی با پول‌های معمولی دارند؟

۱. تراکنش رمزارزها غیر قابل برگشـــت است.

۲. منحصر بـه فرد بـودن رمزارزها ناشـناس بودن یا نیمه ناشـناس بودن آن‌ها است.
۳. رمزارزها جهانی یا فرامرزی هستند.
۴. امنیـت رمزارزهـا در مبـادلات درون شـبکه‌ای توسـط قدرت هش به اشتراک گذاشته شـده توسط افراد (در سیستم‌های اثبات کار)[۴] تامین می‌شود.

نوآوری در سیستم‌های پرداخت

پروتکل رمزارزها تنها برای ارسال پول از نقطه الف به نقطه ب نیست. ویژگی‌ها و امکانـات بسـیاری دارد کـه جامعه هنوز در حال کشـف آن‌ها است. تمامی پرداخت‌ها در جهـان می‌توانند کاملاً با هم در ارتباط باشند. رمزارزها به بانک‌ها، کسـب و کارهـا و یا هر فـردی اجازه می‌دهـد در هر زمان و هـر مکان، چه حساب بانکی داشته و چه نداشته باشند، پرداخت‌های خود را بگونه‌ای امن، ارسال و یا دریافت نمایند. رمزارزها در بسیاری از کشورهایی که به دلیل محدودیتشان خارج از دسـترس بیش‌تر سیستم‌های پرداختی هسـتند، قابل دسترسی است. رمزارزها دسـتیابی جهانی به تجارت را افزایـش داده و می‌تواند به شـکوفایی تجارت بین‌المللی، کمـک کند. به‌طور پیش فرض، تمامـی تراکنش‌های بیت کوین عمومی و شـفاف بـوده و هویت کسـانی که در ورای پرداخت‌ها هستند، محرمانـه باقی می‌ماند. ایـن به افراد و سـازمان‌ها اجازه می‌دهد که با قوانین شـفاف و انعطاف‌پذیری کار کنند. مثلاً، یک کسب و کار می‌تواند انتخاب کند که تراکنش‌هـا و ترازها فقط برای کارکنان خاصـی قابل دیدن باشـند، درسـت همان‌طور که یک سـازمان غیرانتفاعی در نشـان دادن مقدار اعانـات دریافتی روزانـه و ماهانه خود به عمـوم مردم، مختار است.

هیأت استانداردهای حسابداری

رمزارزها یک صنعـت رو به تکامل و به‌سرعت در حال پیشـرفت هستند. با این حال نهادهای حسـابداری هنوز در مورد آن نظر مشخصی اعلام نکرده اند. در دسـامبر ۲۰۱۶ هیأت استانداردهای حسابداری اسـترالیا (AASB) گزارشی با عنـوان «ارز دیجیتال مـوردی برای فعالیت تدوین اسـتاندارد» منتشر کرد کـه ارزهای دیجیتال به عنوان وجه نقد یـا معادل وجه نقد یا بـه عنوان دارایی مالـی (به غیـر از وجه نقد) یـا دارایی نامشـهود و یـا موجـودی طبقه‌بندی شـوند. در این گزاش نتیجه‌گیری شده است که براساس اسـتاندارد بین‌المللی حسـابداری۷ (IAS7) دارایی‌هـای رمزنگاری شـده وجه نقد و معادل وجه نقد نیسـتند، زیرا از پذیرش گسـترده به عنـوان ابزار معامله برخودار نیسـت و بانک‌هـای مرکـزی آن را منتشـر نمی‌کننـد. همچنین طبق اسـتاندارد بیـن المللی حسـابداری ۳۲ (IAS32) ابزارهـای مالی هم نیسـتند، زیرا فاقد رابطـه قراردادی هسـتند که برای یک طـرف دارایی مالی و بـرای طرف دیگر بدهی مالی لحاظ شـود. در این گزارش آمده اسـت تعریف رمزارزها با استاندارد بین‌المللـی حسـابداری ۳۸ (IAS38) مطابقت دارد زیرا دارایی رمزنگاری شده یک دارایی غیر پولی نامشـهود است که محتوای فیزیکی و ملمـوس ندارد. بند سه این اسـتاندارد یک اسـتثناء برای دارایی نامشـهود نگهداری شـده برای فروش در رونـد عادی فعالیت اشـاره دارد از ایـن منظر این قبیل دارایی‌های نامشـهود تابـع اسـتاندارد بین‌المللی حسابداری ۲(IAS2) هستند و به عنوان موجودی با روش اقل بهای تمام شده و خالص ارزش بازیافتنی و نه با استفاده از مدل بهای تمام شـده یا تجدید ارزیابی بر اسـاس IAS 38 شناسایی می‌شوند. همچنین هیأت استانداردهای بین‌المللی حسـابداری و هیـأت اسـتانداردهای حسـابداری مالی (آمریـکا) تاکنون به نتیجه جامع و کامل در مورد دارایی‌های رمزنگاری شـده نرسـیده‌اند و تحقیق، بحـث، گفتگو و پروژه‌های تحقیقاتی در این موضوع ادامه دارد.

ملاحظات پذیـرش و ادامه کار با صاحب‌کار[۵]

مؤسسه باید سیاست‌ها و روش‌هایی را برای پذیرش و ادامه کار طراحی و برقرار کند تا اطمینان معقول حاصل شـود که مؤسسه تنها پس از احراز شرایط زیر کار را قبول می‌کند یا ادامه می‌دهد:

الف- نبود اطلاعاتی حاکی از درستکار نبودن صاحبکار بـا توجه به ارزیابیهای انجام شده.

ب- برخورداری از صلاحیت، توانایی، زمان و منابع لازم برای انجام کار.

پ- امکان رعایت الزامات اخلاقی.

مؤسسـه باید این گونه اطلاعات را، تا آن‌جایی که با توجه به شرایط، ضروری بداند، پیش از پذیرش کار یک صاحبکار جدید، هنگام تصمیم‌گیری درباره ادامه یک کار موجود و هنگام بررسی پذیرش کار جدید صاحبکار موجود، کسب کند. در مواردی که مسـایلی مشخص شود و مؤسسـه بخواهد کار را بپذیرد یا ادامه دهد باید نحوه حل و فصل آن مسـایل را مستند کند.

صداقت صاحب‌کار از جمله هدف تجاری در ورود به معاملات رمزارزها

یک مثال از موضوعی که حسـابرس باید در مـورد صداقت صاحـب‌کار در نظر بگیرد این اسـت که آیا نشانه‌هایی وجود دارد که صاحـب‌کار می‌تواند در فعالیت‌های پولشـویی[۶] یا سایر اقدامات مجرمانـه نقش داشـته باشـد. دلایل مشروع تجاری برای استفاده از رمزارزها وجود دارد. با این حال، رمزارزها نیز برای پولشـویی درآمد حاصل از فعالیت‌های جنایی و تامین مالی تروریسـم و سایر اقدامات غیرقانونی نیز مورد استفاده قرار می‌گیرند. این نوع فعالیت‌ها با ناشناس مانـدن شـرکت‌کنندگان در معاملات

بلاک‌چین فعال می‌شوند. همچنین، در صرافی‌هایی که رمزارزها با ارزهای فیات معامله می‌شوند، تا حد زیادی کنترل نشده هستند (به عنوان مثال، برخی از آن‌ها تحت مقرراتی نیستند که برای بانک‌ها مانند قوانین مشتری یا مبارزه با پولشویی اعمال می‌شود.)

سطح شناخت صاحب‌کار از ریسک‌های رمزارزها و کنترل‌های داخلی مربوط به آن

برای تعیین وجود پیش شرط‌های قرارداد حسابرسی، حسابرس موافقت مدیریت را بدست می‌آورد که تصدیق می‌کند و مسئولیت خود را در مورد برخی موارد از جمله موارد زیر درک می‌کند:

• تهیه صورت‌های مالی مطابق با چارچوب گزارشگری مالی مربوط و قابل اعمال، شامل مربوط بودن و ارایه منصفانه

• کنترل‌های داخلی ضروری برای تهیه‌ی صورت‌های مالی عاری از تحریف با اهمیت چه به دلیل تقلب چه به دلیل اشتباه

در حالت ایده آل، صاحب‌کار می‌تواند درکی از مسائل مربوط به رمزارزها، از جمله مفاهیم گزارشگری مالی آن داشته باشد. صاحب‌کار همچنین می‌تواند کنترل‌های مربوط به معاملات رمزارزها را خود طراحی و اجرا کند. با این حال، یک حسابرس ممکن است با شرایطی روبرو شود که صاحب‌کار احتمالی حتی فرآیندی را برای ردیابی معاملات رمزارزها برای خود اجرا نکرده باشد. در این شرایط، ممکن است حسابرسی صورت‌های مالی واحد تجاری، بسیار دشوار باشد یا عملی نباشد.

صلاحیت و توانایی‌های افرادی که در انجام کار حسابرسی نقش دارند

معاملات رمزارزها و مدیریت رمزارزها اغلب شامل استفاده از رمزنگاری و فن‌آوری اطلاعات بسیار پیچیده (IT) است. در برخی موارد، ممکن است حسابرسی دارایی‌ها و معاملات مربوط به رمز ارزها، بدون اتکا به عملکرد موثر کنترل‌های مربوط، عملی نباشد. علاوه بر این، مواردی مانند ارزشیابی رمزارزها برای اهداف گزارشگری مالی ممکن است نیاز به استفاده از کارشناسان ارزشیابی داشته باشد. بنابراین، هنگام تصمیم‌گیری در مورد پذیرش یا ادامه کار برای کار حسابرسی صورت‌های مالی که شامل موارد مهم و معاملات با اهمیت رمزارزها است، شریک باید تعیین کند که آیا افرادی که در انجام این کار مشارکت دارند (از جمله اعضای تیم منتخب و یا کارشناسان خارجی حسابرس) دارای شایستگی و توانایی‌های مناسب هستند یا خیر.

سیستم اطلاعاتی واحد تجاری برای معاملات رمزارزها

استانداردهای حسابرسی کانادا حسابرس را ملزم می‌کند که سیستم اطلاعاتی شرکت را درک و نسبت به آن شناخت کسب کنند. این شامل، به عنوان مثال، رویه‌های واحد تجاری، هم در سیستم اطلاعاتی و هم در سیستم دستی است که به موجب آن معاملات آغاز، ثبت، پردازش و در صورت لزوم اصلاح و به دفتر کل منتقل می‌شوند و در صورت‌های مالی آن گزارش می‌شوند.

رمز ارزهای اصلی از بلاک‌چین‌های[۷] شفاف استفاده می‌کنند. تمام معاملات به طور دائم در بلاک‌چین ثبت می‌شوند. هر کسی می‌تواند معاملات ثبت شده را بخواند. این معاملات را می‌توان برای مثال با استفاده از شماره شناسایی معامله یا آدرس، ردیابی کرد. گاهی ادعا می‌شود که فن‌آوری بلاک‌چین، نیاز به اعتماد را در بین مشارکت کنندگان در عمل از بین می‌برد. حتی اگر این تا حدی درست باشد، با این وجود استفاده از فن‌آوری بلاک‌چین و رمزارزها چالش‌ها و خطاهایی دارد.

برخی از جنبه‌های اقدامات واحد تجاری در مورد معاملات رمزارزها با ارزهای فیات تفاوت قابل توجهی خواهد داشت. به عنوان مثال، معاملات رمزارزها شامل استفاده از رمزنگاری، کیف پول رمزارزها و یک بلاک‌چین است. ممکن است (گرچه نادر) یک سازمان ارز رمزنگاری از یک سیستم رمزنگاری غیر از بلاک‌چین (به عنوان مثال Ripple) استفاده کند.

نمونه‌ای از خرید رمزارزها

نمونه ساده از معامله خرید رمزارزها

✓ مدیریت نوع رمزارز را برای خرید تعیین می‌کند

✓ یک کیف‌پول رمزارز[۸] از یک ارائه دهنده خدمات دانلود می‌شود. رمز عبور یا عبارت عبور و سایر اقدامات امنیتی مناسب در نظر گرفته شده برای محافظت از کیف پول در برابر دسترسی غیر مجاز استفاده می‌شود. (اطلاعات مربوط به انواع کیف پول‌ها را در بخش بعدی مقاله مشاهده کنید.)

✓ از نرم افزار کیف پول برای تولید کلید خصوصی رمزنگاری استفاده می‌شود. یک کلید عمومی با استفاده از کلید خصوصی تولید می‌شود و آدرس شرکت (شناسه یکبار مصرف) برای هر معامله خرید رمزارزها از کلید عمومی تولید می‌شود.

✓ مدیریت یک حساب کاربری با صرافی رمزارزها یا کارگزار ایجاد می‌کند

✓ مقدار دلخواه رمزارزها با استفاده از کیف پول داغ رمزارز شرکت خریداری می‌شود (به بخش بعدی مراجعه کنید).

✓ معاملات احراز هویت می‌شود و سپس به طور برگشت ناپذیر در بلاک‌چین ثبت می‌شود. معاملات را می‌توان با استفاده از blockchain یا block explorer مشاهده کرد.

✓ برای محافظت از کلید خصوصی واحد تجاری در برابر دسترسی غیرمجاز از طریق اینترنت، واحد تجاری ممکن

است از یک یا چند روش ذخیره سازی سرد (به عنوان مثال کیف‌پول سرد) برای ذخیره کلید خصوصی و اطلاعات مربوطه (به عنوان مثال آدرس‌هایی که کلید خصوصی به آن‌ها متصل است) استفاده کند.

✓ نسخه‌های پشتیبان از کلیدهای رمزنگاری واحد تجاری، به ویژه کلید خصوصی، و همچنین گذرواژه‌ها یا عبارات عبور مورد نیاز برای دسترسی به کیف‌پول، ساخته می‌شوند و با امنیت، ذخیره سازی و پشتیبان گیری را انجام می‌دهد.

✓ معامله‌ی رمزارزها در سیستم گزارشگری مالی شرکت ثبت می‌شود و سپس، در صورت لزوم، با نرخ ارز مناسب به ارز عملکردی واحد تجاری تبدیل می‌شود.

✓ در تهیه‌ی صورت‌های مالی واحد تجاری، هرگونه تعدیل لازم برای مقدار ثبت شده رمزارزها و معاملات مربوطه انجام می‌شود تا با چارچوب گزارشگری مالی قابل اجرا مطابقت داشته باشد (به عنوان مثال، استانداردهای IFRS). برای راهنمایی بیش‌تر در مورد پیامدهای حسابداری رمزارزها، به مقاله CPA Canada، مقدمه‌ای در حسابداری رمزارزها مراجعه کنید.

کیف‌پول رمزارزها

معاملات رمزارزها شامل استفاده از یک برنامه نرم افزاری است که به عنوان کیف رمزارزها شناخته می‌شود. برای مثال از کیف‌پول برای موارد زیر استفاده می‌شود:

✓ ذخیره‌ی کلیدهای عمومی و خصوصی رمزارزهای شرکت برای استفاده در معاملات رمز ارزها

✓ برای ارسال و دریافت رمزارزها، با یک یا چند بلاک‌چین ارتباط برقرار کنید.

✓ مانده واحد تجاری را در هر رمزارز نشان می‌دهد که از معاملات مختلف حاصل می‌شود.

✓ اگر شرکت کلید خصوصی را گم کند و امکان بازیابی آن دیگر وجود ندارد، شرکت دیگر نمی‌تواند به رمزارزها مرتبط با آن کلید دسترسی پیدا کند. بنابراین، در واقع رمزارزها از بین می‌رود. همچنین، اگر کلید خصوصی موجود توسط شخص خارجی بدست آمده باشد، می‌توانند از آن برای انجام معاملات غیر مجاز رمزارزها استفاده کرد که قابل برگشت نیست. کیف پول

شرکت معاملات غیر مجاز توسط شرکت را نشان می‌دهد. رمز ارزهای سرقت شده ممکن است هرگز بازیابی نشود.

انواع کیف پول رمز ارزها

کیف‌پول داغ

«کیف‌پول داغ» در دستگاهی متصل به اینترنت (اعم از میزبان یا تحت کنترل واحد تجاری) قرار دارد. برای ارسال رمزارزها به آدرس دیگر و به دست‌آوردن یک تصویر فوری به روز از کلیه معاملات و مانده‌های اخیر رمز ارزها، یک کیف‌پول داغ مورد نیاز است.

کیف پول سرد

«کیف‌پول سرد» (یا «کیف‌پول سرد ذخیره‌سازی») به اینترنت متصل نیست. موارد زیر نمونه کیف‌پول سرد است:

کیف پول سخت افزار

«کیف‌پول سخت‌افزاری» روی یا دستگاه دیگری قرار دارد. کلیدهای خصوصی و عمومی شرکت با استفاده از یک مولد اعداد تصادفی در حالت آفلاین در دستگاه تولید می‌شود. وقتی کیف‌پول به اینترنت متصل نیست، مطمئناً کلید خصوصی شرکت توسط اشخاص خارجی از طریق اینترنت قابل دسترسی نیست.

کیف پول کاغذی

«کیف‌پول کاغذی» یک پرونده کاغذی از کلید خصوصی و اطلاعات

مربوط به آن است. هنگامی که رایانه یا سایر دستگاه‌ها و چاپگر آنلاین نیستند، از نرم‌افزار برای تولید مجموعه‌ای از کلیدهای خصوصی و عمومی و آدرس‌های مربوط به کیف پول سرد استفاده می‌شود. کلیدهای عمومی و خصوصی کیف‌پول روی کاغذ چاپ می‌شوند.

کیف‌پول میزبان صرافی

یک «کیف‌پول میزبان صرافی» توسط یک صرافی رمز ارز در سرور خود میزبانی می‌شود.

✓ در زیر ۹ نمونه از اتفاقات یا شرایطی وجود دارد که حسابرسان احتمالاً آن‌ها را به‌عنوان بخشی از مراحل انجام کار برای تشخیص و ارزیابی ریسک‌های تحریف بااهمیت موجود در معاملات ارز و رمزارزها در نظر می‌گیرند، چه به دلیل تقلب یا اشتباه. اطلاعات ارائه شده برای هر مثال شامل:

• شرح مختصری از شرایط یا رویداد

• ادعاهای مرتبط

• نمونه‌هایی از جنبه‌های کنترل داخلی‌های که می‌تواند به جلوگیری یا کشف و اصلاح یک تحریف با اهمیت کمک کند. این مثالها لیست کاملی از ملاحظات کنترل‌های داخلی نیستند.

این لیست قصد ندارد جامع و کامل باشد. سایر شرایط و رویدادها ممکن

است منجر به افزایش ریسک تحریف با اهمیت در معاملات یا مانده‌های رمزارزها شود.

۱- واحد تجاری، صرافی را که روی آن کنترل‌های موثری ندارد انتخاب می‌کند و صرافی از طرف واحد تجاری به مانده و معاملات رمزارزها وارد می‌شود.

ادعاهای مرتبط: این احتمال وجود دارد که هر یک از ادعاها تحت تأثیر قرار گیرد

معمولاً یک واحد تجاری برای مبادله رمزارزها ازصرافی آنلاین استفاده می‌کند. همچنین، در برخی موارد، شرکت ممکن است از کیف‌پول رمز ارز میزبانی شده توسط صرافی استفاده کند.

ویژگی‌های صرافی انتخاب شده ممکن است پیامدهای مهمی در تمام ادعاهای مربوط به رمز ارزهای ذکر شده در بالا داشته باشد. ملاحظات در انتخاب صرافی آنلاین ممکن است شامل موارد زیر باشد:

• صاحبان و کارمندان صرافی (به عنوان مثال، برخی صرافی‌ها با طرح‌ها «بالا ببر و بفروش»[۱۰] همراه بوده‌اند (به عنوان مثال، قیمت اوراق بهادار را از طریق داستان‌های دروغ بالا می‌برند و سپس به سرمایه‌گذاران جدید می‌فروشند) که اثر غیر واقعی (مصنوعی) بر قیمت‌ها دارد.

• کشوری که صرافی در آن واقع شده است. ممکن است، به عنوان مثال، قوانین و مقررات دیگری را که تبادلات تحت آن است تعیین کند و می‌تواند شامل مقررات پولشویی باشد که نیاز دارد صرافی از آن قوانین پیروی کند که پروتکل‌های «مشتری خود را بشناسید» باشند.

• حجم نقدینگی و حجم معاملات

• کنترل‌های انجام شده توسط صرافی در واقع مهم است، به عنوان مثال، امنیت کیف‌پول‌های میزبان برای مبادلات.

• این‌که آیا صرافی گزارش حسابرس را در مورد تأثیر کنترل خود بر معاملات رمزارزها ,و مانده‌های انجام شده از طرف مشتریان خود ارائه می‌دهد.

ملاحظات کنترل‌های داخلی

شرکت ممکن است مسئولیت انتخاب رمزارزها برای خرید و مبادله را به پرسنل آگاه و مطلع از ریسک‌های موجود و چگونگی کاهش ریسک آن‌ها اختصاص دهد.

نمونه‌هایی از شرایط یا رویدادها «چه چیزی ممکن است اشتباه باشد»	نمونه‌هایی از ادعاها که ممکن است اظهار نظر نادرست در این رابطه باشد					
	صحت، ارزشیابی و تخصیص	کامل بودن	آزمون انقطاع زمانی	وجود	رخداد و وقوع	حقوق و مالکیت
۱- واحد تجاری، صرافی را که روی آن کنترل‌های موثری ندارد انتخاب می‌کند و صرافی از طرف واحد تجاری به مانده و معاملات دارایی رمز ارزها وارد می‌شود.	✓	✓	✓	✓	✓	✓
۲- واحد تجاری کیف پول رمز ارزی دارد که آن را ثبت نکرده است.		✓				
۳- واحد تجاری یک کلید خصوصی را از دست می‌دهد و بنابراین دیگر نمی‌تواند به رمز ارز مربوط دسترسی پیدا کند.						✓
۴- یک شخص غیر مجاز به کلید خصوصی دسترسی پیدا می‌کند و رمز ارزهای موجود را می‌دزدد.				✓		✓
۵- واحد تجاری کلید خصوصی و رمز ارزهای مربوط را اشتباه نشان می‌دهد.				✓	✓	✓
۶- واحد تجاری رمز ارزها را به آدرس غیر مستقیم می‌فرستد و رمز ارزها قابل بازیابی نیستند.						✓
۷- واحد تجاری وارد معاملات رمز ارزها با یک شخص وابسته می‌شود که به دلیل ناشناس بودن افراد در معاملات بلاک‌چین نمی‌تواند شناسایی کند.	✓	✓				
۸- در پایان دوره تاخیر قابل توجهی در پردازش معاملات رمز ارزها وجود دارد.			✓			
۹- رویدادها و شرایط برای تشخیص ارزش رمز ارزهایی که باید برای هدف گزارشگری مالی ثبت شوند را دشوار می‌کند.	✓					

• مدیریت ارشد می‌تواند انتخاب‌های انجام شده را بررسی و در صورت لزوم آن‌ها را تأیید کند.

• شرکت ممکن است تصمیم بگیرد حداقل از احراز هویت دو عاملی برای دسترسی به حساب خود استفاده کند. این امر تا حدودی خطر دسترسی غیر قانونی به کیف پول میزبان در مبادلات شرکتی را کاهش می‌دهد.

۲- واحد تجاری کیف‌پول رمزارزی دارد که آن را ثبت نکرده است.

ادعاهای مرتبط: کامل بودن در ثبت دارایی رمزارزها و معاملات مرتبط

یک واحد تجاری حسابرسی شده ممکن است یک یا چند کیف پول رمز ارز خود را شناسایی نکند. در واقع رمز ارزهای واحد تجاری و معاملات مربوطه به طور کامل ثبت نشده باشند.

ارزیابی ریسک تحریف با اهمیت در مورد کامل بودن دارایی‌ها و معاملات رمزارزها ممکن است دشوار باشد. کلیدهای عمومی و آدرس‌های مربوط به آن در بلاک چین، هویت طرف‌های شرکت‌کننده در معاملات را شفاف نمی‌کند. به‌علاوه، ممکن است واحد تجاری سابقه طولانی در معاملات رمزارزها نداشته باشد. در نتیجه، حسابرس ممکن است در به‌دست آوردن اطلاعات مفیدی که می‌تواند انتظارات خود مبنی بر عدم ثبت معاملات قابل توجه رمزارزها وجود داشته باشد را دشوار کند.

اگر در طول حسابرسی وجود کیف پول که قبلاً به حساب گرفته نشده بود مورد توجه حسابرس قرار گیرد، ممکن است نشانه‌هایی وجود داشته باشد که عمداً پنهان شده است. این ممکن است نشان دهنده یک ریسک تقلب باشد، از جمله خطر نادیده گرفتن کنترل‌های مدیریت در مورد کیف رمز ارز.

ملاحظات کنترل‌های داخلی

عدم شناسایی کیف‌پول متعلق به واحد تجاری ممکن است سهوی باشد.

یک شرکت می‌تواند تعداد زیادی کیف‌پول داشته باشد، از جمله ممکن است کنترل‌های مربوط به مجوز ایجاد کیف پول و پیگیری بعدی کیف‌پول به طور موثر انجام نشده باشد. بنابراین شرکت ممکن است یک یا چند کیف‌پول را از دست داده باشد. ایجاد خطوط مشخص مسئولیت مربوط به ایجاد و پیگیری کیف‌پول‌ها ممکن است چنین خطری را کاهش دهد.

۳- واحد تجاری یک کلید خصوصی را از دست می‌دهد و بنابراین دیگر نمی تواند به رمزارز مربوط دسترسی پیدا کند.

ادعاهای مرتبط: حقوق (مالکیت) دارایی رمزارزها

اگر واحد تجاری یک کلید خصوصی را از دست بدهد، یا خراب شود و نتوان آن را بازیابی کرد، واحد تجاری دیگر نمی تواند به رمزارزهای مرتبط با آن کلید دسترسی داشته باشد و بنابراین دیگر نمی‌تواند حقوق مالکیت خود را بازیابی کند. رمزارزهای متصل به آن کلید خصوصی، در بلاک چین مربوط همچنان وجود خواهد داشت. با این وجود، رمزارزهای متصل به کلید خصوصی دیگر به عنوان دارایی شرکت وجود ندارد.

اگر اثر ضرر به درستی محاسبه نشود، از دست دادن کلید خصوصی منجر به سوء استفاده و تحریف با اهمیت می‌شود. به عنوان مثال، افرادی که مسئولیت کنترل کلید خصوصی را بر عهده دارند، هنگام تهیه صورت‌های مالی، ممکن است از ضرر آن مطلع و آگاه نباشند، زیرا آن‌ها تجربه زیادی در معاملات رمزارزها ندارند. به عنوان مثال دیگر، افرادی که در از دست دادن کلید خصوصی مقصر هستند، ممکن است انگیزه قوی برای تلاش برای پنهان کردن ضرر یا گزارش نکردن به موقع آن را نیز داشته باشند.

ملاحظات کنترل‌های داخلی

کنترل‌هایی برای کاهش ریسک دسترسی به کلید خصوصی:

به عنوان مثال، سیاست‌ها و رویه‌هایی ممکن است به منظور پشتیبان گیری از کلید خصوصی (و شاید از کلیدها و آدرس‌های عمومی مرتبط) استفاده شودپشتیبان گیری ممکن است در دستگاه‌های الکترونیکی جداگانه باشد. روش دیگر استفاده از کیف‌پول کاغذی است. از کلیدهای خصوصی و رمزهای عبور یا عبارات عبور ذخیره شده در دستگاه پشتیبان یا کیف‌پول کاغذی ممکن است به نوبه خود نسخه پشتیبان تهیه شود تا به شما کمک کند اطمینان منطقی ایجاد کنید که واحد تجاری رمز ارزهای خود را از دست نخواهد داد. علاوه بر این، محل دستگاه پشتیبان یا کیف‌پول کاغذی باید توسط چندین فرد مناسب شناخته شود (یعنی فقط محدود به یک شخص نباشد)

کنترل‌هایی برای کاهش خطر عدم انتقال کلید خصوصی و عدم ثبت ضرر ناشی از آن:

سیاست‌ها و رویه‌های اجرا شده توسط یک واحد تجاری ممکن است شامل تعیین تفکیک وظایف مناسب باشد (به عنوان مثال، مسئولیت نظارت بر دارایی‌های رمزارزها از نقطه نظر گزارشگری مالی توسط افرادی انجام می‌شود که در انجام معاملات ارز رمزنگاری واحد تجاری مشارکت ندارند). همچنین سیاست‌ها و رویه‌ها ممکن است ایجاب کنند که چنین نظارتی مداوم باشد (به عنوان مثال، از طریق بررسی کیف‌پول یا استفاده از جستجو گر بلاک‌چین در صورت وجود).

۴- یک شخص غیر مجاز به کلید خصوصی دسترسی پیدا می‌کند و رمزارزهای موجود را می‌دزدد.

ادعاهای مرتبط: حقوق (مالکیت) دارایی‌های رمزارزها و وجود دارایی‌ها برای واحد تجاری

موارد مربوط به سرقت یک کلید خصوصی مشابه مواردی است که برای از دست دادن کلید خصوصی ذکر شده در مثال ۳ در بالا ذکر شده است.

ملاحظات کنترل‌های داخلی

خطرات دسترسی غیر مجاز به کیف پول داغ ممکن است با استفاده از احراز هویت دو عاملی یا چند عاملی برای دستیابی به کیف پول کاهش یابد. رمزگذاری در محتویات کیف پول ممکن است سطح دیگری از امنیت را ایجاد کند. همچنین، استفاده از کیف پول داغ فقط هنگام انجام معاملات رمزارزها واستفاده از کیف پول سرد برای ذخیره کلید خصوصی و اطلاعات مربوط به آن، ممکن است خطر دسترسی غیرمجاز به کلید خصوصی از طریق اینترنت را کاهش دهد. به‌علاوه، یک واحد تجاری ممکن است تصمیم بگیرد که فقط قسمت کوچکی از رمزارزهای خود را از یک کیف پول داغ در دسترس داشته باشد، و بیش‌تر رمزارزهای خود را در یک کیف‌پول سرد نگهداری کند.

۵- واحد تجاری کلید خصوصی و رمزارزهای مربوط را اشتباه نشان می‌دهد.

ادعاهای مرتبط: حقوق (مالکیت) رمزارزها، وقوع (یعنی واقعه یا معامله مربوط به ایجاد مالکیت رخ نداده است)

پرداختن به ریسک مالکیت دشوار است، زیرا مالکیت رمزارزها به دلیل ناشناس بودن طرف‌های معامله گر از بلاک‌چین به آسانی مشخص نیست. داشتن یک کلید خصوصی به روشنی نشانگر مالکیت رمزارزها است که با استفاده از آن کلید قابل دسترسی هستند.

با این حال، مالکیت یک کلید خصوصی همیشه قابل انتساب به یک واحد تجاری نیست. ممکن است شرایطی وجود داشته باشد، به عنوان مثال، هنگامی که کلید خصوصی (و

مالکیت رمزارز مربـــوط) به طور قانونی بین طرفین تقسیم شده باشد. همچنین ممکن است تعیین این‌که کلید خصوصی (و در نتیجه رمزارز مربوط به آن) متعلق به واحد تجاری است یا شخصاً متعلق به یک یا چند فرد است دشوار باشد.

علاوه بر این، یک حسابرس همچنین ممکن اســت با شــرایطی روبرو شــود که نشــان می‌دهد یک واحــد تجاری حسابرسی شــده با تقلب نشان می‌دهد که به تنهایــی کلید خصوصی را کنترل می‌کند و رمزارزهای مربوط را در اختیار دارد. حســابرس موظف اســت در تمام مدت حسابرسی، تردید حرفه‌ای را حفظ کنــد و این احتمال را که یک تحریف با اهمیت به دلیل تقلب وجود داشته باشد را درنظر بگیرد، بــدون توجه به تجربه گذشته حسابرسان از درستی و صداقت مدیریت واحد تجاری، این کنترل‌ها باید انجام شوند.

ملاحظات کنترل‌های داخلی

سیستم اطلاعات شرکت و کنترل‌های مربــوط به ایجــاد کیــف پول‌های آن ممکن است مســتنداتی در مورد ایجاد کلیدهای خصوصی و اســتفاده از آن‌ها در انجام معامــلات رمزارزها ارائه دهد. محیط کنترلی واحد تجاری، از جمله با سیاست‌ها و رویه‌های شرکت نیز ممکن است مرتبط باشد.

۶- واحد تجــاری رمزارزها را به آدرس غیر مســتقیم می‌فرستد و رمزارزها قابل بازیابی نیستند.

ادعــای مرتبــط: حقــوق (مالکیت) رمزارزها

هر بلاک‌چین فرآینــد خاص خود را دارد تــا تأیید کند که اقدامات معاملات رمزارزها معتبر هســتند و کپی نیستند (یعنی الگوریتم کلــی آن‌ها یا الگوریتم اجماع[۱۱]). با این حال، ویژگی مشــترک همــه بلاک چین‌هــا این اســت که به محــض تأییــد معاملــه در بلاک‌چین، غیرقابل برگشت است. اگر این ویژگی به نشانی نادرستی ارسال شود، ممکن است این ویژگی باعث از دســت رفتن رمزارز شود. پرســنل واحد تجاری حسابرسی شده ممکن است هنگام ارسال رمزارزها، آدرس نادرســتی را وارد کننــد. طرف پذیرنده ممکن است به صورت داوطلبانه رمزارزهــا را در معاملــه جدید به واحد جاری حسابرســی شــده بازگرداند اما همچنیــن ممکن اســت تصمیم بگیرد که ایــن کار را انجام ندهــد. بنابراین، رمزارزهــا از بیــن خواهد رفــت. اگر از دســت دادن رمزارزها به طور مناســب ثبت نشــود، تحریــف اشــتباه صورت می‌گیرد. به عنــوان مثال، وقتی افرادی که مسئولیت مدیریت رمزارزها را دارند، انگیزه‌ی زیادی جهت پنهان کردن ضرر یا گزارش نکردن به موقع آن دارند.

ملاحظات کنترل‌های داخلی

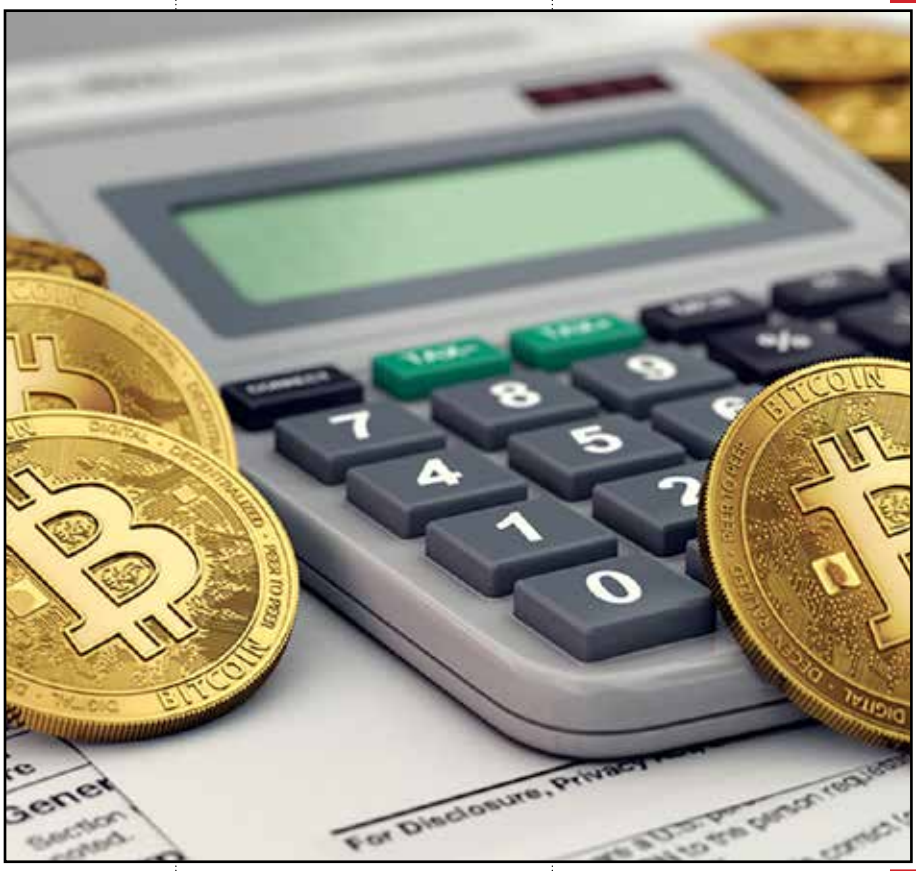
• کنترل‌ها برای جلوگیری از استفاده از آدرس‌های نادرســت: سیاســت‌ها و رویه‌های واحد تجــاری می‌تواند هم به بررسی دقیق هر آدرس قبل از ارسال و هم استفاده از یک مجموعه از کنترل‌ها برای جلوگیری از خطاهای تایپی هنگام ورود به آدرس نیاز داشــته باشد.به طور مثــال چهار شــماره اول و آخر آدرس، کنترل مجدد گردد.

علاوه بــر این، واحد تجــاری ممکن اســت در ابتدا ارسال مقدار بسیار کمی از رمزارزهــا را برای گیرنــده مورد نظر در نظر بگیرد. بنابرایــن آدرس گیرنده می‌توانــد قبل از ارســال، تأیید شــود. اســتفاده از کــد QR (در مقابــل تایپ آدرس یا کپــی و جایگذاری آدرس) نیز می‌تواند به جلوگیری از خطا کمک کند.

• کنترل‌هایــی برای کمک به کاهش خطر ریســک عدم ارتباط و از دســت دادن رمزارزها: نمونه‌های کنترل همان مواردی است که در مثال ۳ در بالا ذکر شده است.

۷- واحد تجـــاری وارد معاملات رمزارزها با یک شـــخص وابســـته می‌شـــود که بـــه دلیل ناشـــناس بودن افـــراد در معاملات بلاک‌چین نمی‌تواند تشخیص دهد.

ادعاهـــای مرتبـــط: صحت (شـــامل ارزشـــیابی و تخصیص) برای دارایی‌ها و کامل بودن برای افشای اطلاعات از هویـــت خریـــداران و فروشـــندگان رمزارزهـــا بعضـــا به عنوان ناشـــناس یاد می‌شود. اطلاعاتی مانند نام آن‌ها را نمی توان از طریق مشاهده آدرس در بلاک‌چین تعیین کرد. بـــا این وجود، ارتباطاتی بین آدرس‌هـــای بلاک‌چین و هویت معاملات شـــرکت کننـــدگان در پرونده ســـوابق مبادلات و کارگزاران مورد استفاده طرفین وجـــود دارد. بنابراین ممکن اســـت یک قانـــون گذار یا طرف دیگر بتواند هویت را کسب کند. با این حال، در بیش‌تر موارد، نام شرکت کنندگان در معاملات مشهود نخواهد بود. بنابراین، ممکن است مشخص نباشـــد که آیا واحد تجاری حسابرســـی شـــده در حال انجام معاملات رمزارزها با اشخاص وابســـته است که مدیریت آن‌ها را مشخص نکرده است یا شخص دیگری. در نتیجه، اشخاص وابسته، در معاملات با اشخاص مرتبط دیگر، ممکن است مطابق با چارچوب گزارشگری مالی مناسب ثبت و افشا نشوند.



ملاحظات کنترل‌های داخلی

این یک بررســـی کلی اســـت که آیا محیط کنترلـــی و فعالیت‌های کنترلی واحد تجاری در مورد شناسایی اشخاص وابســـته و تأیید مجوز معاملات مربوط با اشـــخاص وابســـته در رمزارزها اعمال می‌شود یا خیر. به عنوان مثال:

• سیاســـت‌ها و روش‌های به دســـت آوردن آگاهـــی مناســـب از طرف‌هایی که واحد تجاری بـــا آن‌ها وارد معاملات رمزارزها می‌شود.

• اختصاص مسئولیت‌هایی در شرکت برای شناســـایی، ضبـــط، جمع بندی و افشـــای معاملات مربوط به اشـــخاص وابسته، از جمله معاملات رمزارزها.

۸- در پایـــان دوره تاخیر قابل توجهـــی در پـــردازش معاملات رمزارزها وجود دارد.

ادعاهای مرتبط: آزمون انقطاع زمانی

بلاک‌چین‌های رمزارزها ممکن اســـت به طور قابل توجهی در ســـرعت پردازش و تأییـــد معاملات متفاوت باشـــند. اغلب معاملات طی چند دقیقه انجام می‌شوند. با این حال، در برخی موارد، ممکن اســـت معامله‌ای به مدت چند روز به تاخیر بیفتد.

به عنوان مثال:

• اســـتخراج کنندگان بلاک‌چین در صورت پرداخت هزینه‌ای که فرســـتنده موافقت می‌کند بـــه ماینرها بپردازد اگر نســـبت به ســـایر تراکنش‌ها به میزان قابل توجهی کم‌تر باشد، معاملات واحد تجـــاری اولویت کم‌تـــری دارند و حجم معاملات با کارمـــزد بالاتر نیز بیش‌تر و زودتر انجام می‌شود.

• تعلیـــق معامـــلات توســـط صرافی میزبـــان در کیف پـــول رمزارزها انجام می‌گیرد.

ملاحظات کنترل‌های داخلی

واحد تجاری ممکن است روش‌هایی را بـــرای نظارت بر معاملات رمزارزها در روزهای قبل و بعد از تاریخ گزارشـــگری مالـــی برای تعیین این‌کـــه معاملات در دوره مناسب ثبت شده است، اجرا کند.

۹-رویدادهـــا و شـــرایط برای تشخیص ارزش رمزارزهایی که باید برای هدف گزارشـــگری مالی ثبت شوند را دشوار می‌کند.

ادعاهـــای مرتبـــط: صحت (شـــامل ارزشیابی و تخصیص)

چارچوب‌های گزارشگری مالی مانند اســـتانداردهای IFRS در حـــال حاضر

حاوی اشاره‌های صریح به رمزارزها نیست. مقاله CPA کانادا «مقدمه‌ای در حسابداری رمزارزها» خاطرنشان می‌کند که نگرانی‌هایی مبنی بر استفاده از دارایی‌های نامشهود IAS 38 و اندازه‌گیری رمزارزها با قیمت منعکس‌کننده اقتصادی نیست و اطلاعات مربوط را به کاربران مالی ارائه نمی‌دهد.

بیانیه: در برخی موارد، ارزش منصفانه‌ی رمزارزها ممکن است در صورت‌های مالی به حساب منظور و یا افشا شود.

موارد خاصی که باید در مورد ارزشیابی رمزارزها در نظر گرفت شامل موارد زیر است:

• بسیاری از رمزارزها بی ثبات هستند و بازار رمزارزها ۲۴ ساعته و ۷ روز هفته می‌باشد باشد. ممکن است زمانی که یک واحد گزارشگری رمزارزها را ارزشیابی می‌کند مهم باشد. به عنوان مثال، آیا ارزشیابی در ساعت ۱۱:۵۹ بعد از ظهر است. (منطقه زمانی) در آخرین روز دوره‌ی گزارش یا در پایان کار در آن روز؟ این ممکن است نشان‌دهنده‌ی یک سیاست حسابداری قابل توجه باشد. سازگاری در استفاده از این سیاست لازم است.

• همانند سهام یا کالاها، سفارشات «خرید» و «فروش» نیز وجود دارد که غالباً بین قیمت‌های مربوطه فاصله زیادی دارند و همچنین در هر زمان ممکن، مبادله مقدار قابل توجهی رمزارزها با ارز فیات با قیمتی که دارنده آن را عادلانه می‌داند، در یک بازه زمانی معقول دشوار می‌باشد.

• برخی از رمزارزها کم معامله می‌شوند.

• ممکن است در قیمتی که رمزارزها هم‌زمان در صرافی‌های مختلف معامله می‌شود تغییرات قابل توجهی وجود داشته باشد. (آربیتراژ)

• ماهیت و میزان نظارت بر بازار رمزارزها در حوزه‌های قضایی بسیار متفاوت است. غالباً شفافیت در مورد نحوه گزارش قیمت‌ها، نظم کمی است که از جمله موارد دیگر می‌تواند باشد.

اگر اخیرا حجم قابل توجهی از رمزارزها مبادله شده باشند، قیمت‌های معاملاتی ممکن است شواهدی از ارزش منصفانه را ارائه دهند اگر معاملات اخیر کمی انجام شده باشد یا هیچ معامله‌ای انجام نشده باشد، ورودی‌های قابل مشاهده مربوط ممکن است شواهد درستی از ارزش نباشد.

ملاحظات کنترل‌های داخلی

واحد تجاری می‌تواند سیاست‌ها و رویه‌های مربوط به ارزشیابی رمزارزها را برای گزارشگری مالی اجرا کند. برای مثال، ممکن است این سیاست‌ها ایجاب کند که روش ارزشیابی و پیش فرض‌ها توسط پرسنل ذی صلاح یا شخصی انجام شود و توسط پرسنلی که مسئولیت مجاز به معاملات رمزارزها را نیز ندارند، مورد بازبینی و تأیید قرار گیرند.

نتیجه

این مقاله با هدف آگاهی اولیه حسابرسان، در سطح بالا، از موضوعات مختلف مربوط به پذیرش صاحب‌کار و تداوم آن و ارزیابی ریسک تحریف بااهمیت مربوط به رمزارزها در صورت‌های مالی است. همان‌طور که اشاره شد، یک موضوع اساسی که حسابرسان باید در نظر بگیرند این است که آیا تیم کاری دارای توانایی‌های لازم برای رسیدگی مناسب به فرآیندهای پیچیده فن‌آوری اطلاعات را دارد. حسابرسان همچنین ممکن است مایل باشند به منابع دیگر مراجعه کنند تا در مواردی که در این مقاله ذکر شده است، عمیقاً کاوش کنند تا با آمادگی مناسب برای انجام حسابرسی‌های مربوط به مقادیر قابل توجه رمزارزها، آماده شوند. ■

منابع:

1. Audit Considerations Related to Cryptocurrency Assets and Transactions, Charted Professional Accountants Of Canada ,CPA, 2018
2. Accounting for and auditing of digital assets , Association Of Internatinal Certified Professional Accountants ,AICPA & CIMA, 2019
۳. حسابداری دارایی‌های رمزنگاری شده، محسن ژاله آزاد زنجانی و علی اصغر صالحی، نشریه ۳۲۶ و ۳۲۷ حسابدار،۱۳۹۸
۴. کمیته تدوین استانداردهای حسابرسی، «استانداردهای حسابرسی، سایر خدمات اطمینان بخشی و خدمات مرتبط»، تهران، سازمان حسابرسی، چاپ شانزدهم، ۱۳۹۷
۵. راهنمای ارزهای دیجیتال، سامان کریمی شاد و کسری رفالیان،انتشارات کلید آموزش،۱۳۹۸
۶. استاندارد حسابرسی ایران شماره ۱
۷. www.bitcoin.org

پی‌نوشت‌ها:

1. Cryptocurrencies
2. distributed ledger
3. Mining
4. Proof of work
5. Client Acceptance and Continuance Considerations
6. Money laundering activities
7. blockchains
8. Cryptocurrency Wallets
9. Exchange-Hosted Wallet
10. pump and dump
11. consensus algorithm