

# چالش‌های حسابرسی رمزارزها

در حال ظهور مربوط به رمزارزها سروکار دارند، چالشی اساسی برای حسابرسان است.

## حسابرسی رمزارزها

هدف حسابرس، افزایش میزان اطمینان استفاده‌کنندگان به صورت‌های مالی است. این هدف با اظهارنظر حسابرس نسبت به اینکه آیا صورت‌های مالی از تمام جنبه‌های بااهمیت، طبق چهارچوب گزارشگری مالی مربوط تهیه شده است یا خیر، تأمین می‌شود. انجام حسابرسی

اقبال روزافزون به رمزارزها و نوسان قابل توجه آنها منجر به عقب ماندن توجه جهانی و عدم توجه نظارت بیشتر توسط سازمان‌ها، سرمایه‌گذاران، نهادهای نظارتی، دولت‌ها و دیگران شده است. طی سنوات گذشته تنوع رمزارزها بسیار افزایش یافته است. هر یک از این رمزارزها دارای ویژگی‌های منحصر به فرد خود است که درک، حسابداری و حسابرسی آنها را چالش برانگیز می‌کند. لذا کمبود راهنمایی رسمی مربوط از تدوین‌کنندگان استاندارد که با مسائل

محمد رضا چهره‌نما

سید محمد توسلی طبائی



در بلاک‌چین و دنیای فیزیکی. این وظایف جدید می‌تواند چالش برانگیز باشد، به‌ویژه هنگامی که هیچ مرجع متمرکزی در فناوری بلاک‌چین وجود ندارد. علاوه بر این، رمزارزها از فرایند نمونه‌برداری حساب سنتی گذر کرده است. بنابراین، ثبت یک معامله در بستر بلاک‌چین ممکن است شواهد حسابرسی مناسب و کافی مربوط به ماهیت معامله را ارائه دهد یا ندهد.

به عبارت دیگر، یک معامله ثبت شده در بلاک‌چین ممکن است:

غیرمجاز، کلاهبرداری یا غیرقانونی باشد، مابین اشخاص وابسته صورت پذیرد، مرتبط با یک توافق‌نامه جانبی تحت عنوان «خارج از زنجیره» باشد، به اشتباه در صورت‌های مالی طبقه‌بندی شده باشد و به‌علاوه، بسیاری از معاملات ثبت شده در صورت‌های مالی، منعکس کننده ارزش‌هایی است که با بهای تاریخی متفاوت است.

همچنین، در بسیاری از مواقع حساب‌رسان نمی‌توانند به‌طور مستقیم معاملات رمزارزها را بیازمایند، بلکه در عوض به آزمون این کنترل‌ها پرداخته شود تا اطمینان معقولی در رابطه با صحت معاملات صورت گرفته حاصل شود (Manlu Liu, et al, 2019).

### چالش‌ها حسابرسی رمزارزها

حسابرسی باید حجم یا میزان مبلغ معاملات رمزارزها و ارزش موجود در حساب‌ها را در نظر بگیرد. خطرها برای دارایی رمزارزها یا معاملات بیشتر از اهمیت تخصیص یافته به مانده سایر حساب‌های دیگر است، ماهیت رمزارزها، کمبود شواهد معتبر برای حساب‌داری،

طبق استانداردهای حسابرسی و رعایت الزامات آیین رفتار حرفه‌ای، مبنای لازم را برای اظهارنظر حسابرس فراهم می‌کند (استانداردهای حسابرسی، ۱۴۰۰). حسابرس باید روش‌های ارزیابی خطر را به‌منظور فراهم کردن مبنایی برای تشخیص و ارزیابی خطرهای تحریف بااهمیت در سطح صورت‌های مالی و در سطح ادعاها اجرا کند.

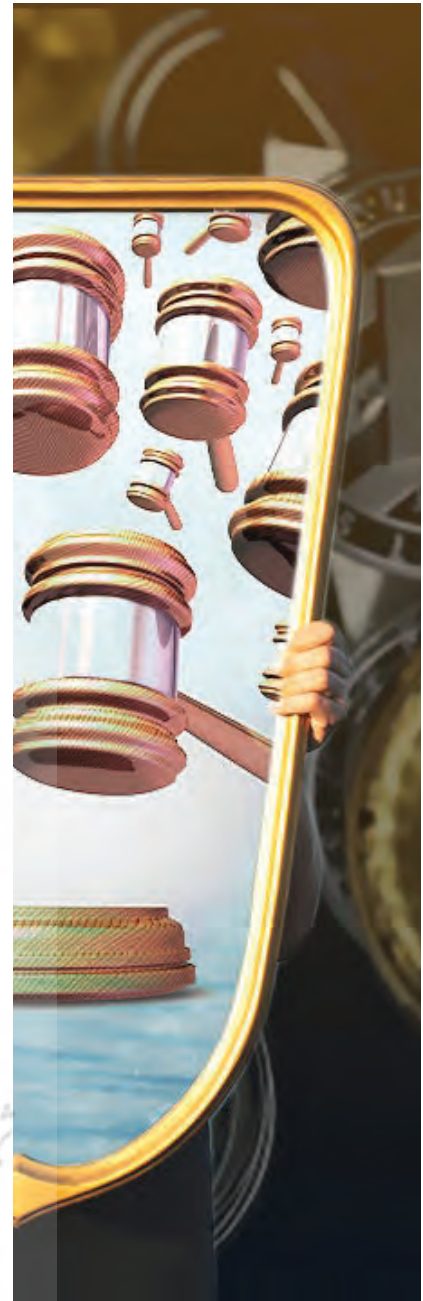
رمزارزها تجارت جدیدی را برای حساب‌رسان به ارمغان می‌آورد مانند بررسی معاملات خاص و اثبات وجود دارایی‌های دیجیتال و تأیید سازگاری بین اطلاعات موجود

گزارشگری، افشا، کمبود وجود قوانین و مقررات، ناشناس بودن نسبی طرفین معامله رمزارزها و اهمیت حجم یا مانده رمزارزها، خطر اظهارنظر نادرست را افزایش می‌دهد.

وقتی روش‌های حسابرسی در مرحله برنامه‌ریزی طراحی می‌شود، بایستی اهداف، دامنه، رویکرد و خطرهای حسابرسی را در نظر بگیرند (استانداردهای حسابرسی، ۱۴۰۰). خطرهای برنامه‌ریزی شده باید دربرگیرنده بررسی ادعاهای موجود در گزارشگری مالی مدیریت مانند حقوق و تعهدات، کامل بودن، آزمون صحت و ارزش‌گذاری، وقوع و کفایت افشا باشد.

### ادعای وجود

یکی از بزرگترین چالش‌ها در ارزیابی رمزارزها صحت تعداد رمز موجود در کیف پول الکترونیکی و مانده دارایی دیجیتال در ارزهای متنوع است. از زمانی که رمزارز، یک دارایی دیجیتال در نظر گرفته شده است، احتمالاً روش‌های قابل استفاده برای رسیدگی به موجودی‌های کالا و دارایی‌های ثابت مفید نیست. به‌طور سنتی تأییدیه‌ها نیز برای اثبات ادعای وجود، استفاده می‌شوند. برای مثال به‌طور معمول جهت اثبات موجودی نزد بانک از تأییدیه بانک استفاده می‌شود، لذا با توجه به اینکه رمزارزها بدون داشتن مرجع مرکزی در دفاتر نگهداری می‌شوند، حساب‌رسان ممکن است در دریافت تأییدیه از این بابت ناتوان باشند (Aquilio, 2018). اگر رمزارز از طریق صرافی معامله شود، فقدان مکانیسم‌های گزارشگری مناسب از کنترل‌های داخلی صرافی، ارزیابی و



است کنترل‌های داخلی مبتنی بر کیفیت پول را ارزیابی کنند. راه دیگر برای اثبات وجود، ارزیابی منبع یا مستندات قراردادهایی که دارایی را حمایت می‌کند، است. برخلاف قوانین موجود در صنعت بانکداری، ممکن است مستنداتی بین نگهدارنده‌ی دارایی ( صرافی) و مشتری موجود نباشد.

### حقوق و تعهدات

به‌طور سنتی حسابرسان ادعای حقوق و تعهدات را از طریق بازرسی اسناد و مدارک از جمله موافقت‌های فی‌مابین با سایر اشخاص، تأییدیه‌ها و صورت‌جلسات هیأت مدیره ارزیابی می‌کنند. درحالی که هنگام مرور کردن اسناد مربوط به رمزارزها، حسابرسان متوجه خواهند شد که چه کسی مالک قانونی رمزارز نگهداری شده توسط خود مشتری است یا چه کسی مالک رمز نگهداری شده توسط صرافی است. اگر فعالیت صرافی تعطیل یا صرافی دارایی‌های رمزارز را از بین ببرد، برای دارایی‌های مشتری چه اتفاقی می‌افتد و چه کنترل‌های داخلی در جهت حفاظت از امنیت صرافی وجود دارد. فقدان اطمینان از گزارشگری شخص ثالث (صرافی) سختی ارزیابی، خطرهای مربوطه را افزایش می‌دهد.

حسابرس ممکن است نیاز به بررسی کنترل‌های داخلی مربوط به رمزارز نگهداری شده در شرکت را در اختیار داشته باشد و همچنین بررسی کند که دسترسی‌های عمومی یا خصوصی به این رمزارزها را محدود سازد.

منابع رمزارزها تقریباً ناشناخته هستند، زیرا آنها به صورت دیجیتالی ایجاد می‌شوند و به راحتی هویت با مالک خود

ارتباطی ندارند. علاوه بر این، آدرس‌های جدید به راحتی ساخته می‌شوند و نیازی به اطلاعات اشخاص نیست، برخلاف حساب‌های سرمایه‌گذاری جدید که نیاز به تأیید هویت مالک دارد. با توجه به ماهیت دیجیتال، مؤسسات حسابرسی نیاز داشته باشند برای شناسایی و تأیید حساب رمزارزهای متعلق به مشتریان خود، کارشناسی در این زمینه استخدام کنند یا نیاز به تهیه نرم‌افزار را در این زمینه داشته باشند (PWC، 2019) .

### کامل بودن

برای اثبات ادعا، کامل بودن نیاز است که تأیید شود تمامی معاملات رمزارزها تحت بلاک‌چین انجام شده است یا خیر، عموماً شواهد مربوط به به کامل بودن به وسیله اسناد و مدارک از پیش شمارش شده، ردیابی اسناد مالکیت به دفاتر و فهم و بررسی اثربخشی عملیاتی کنترل‌های داخلی مشتری مربوط به کامل بودن صورت می‌پذیرد. اگرچه معاملات انجام شده در فناوری بلاک‌چین در طول زمان بدون تغییر است، از لحاظ تئوری آنها می‌توانند معاملاتی یتیم باشند. بنابراین کنترل‌های مربوط به دسترسی مشتری یا صرافی نیاز به ارزیابی دارد. اگرچه موتورهای جستجوگر بلاک‌چین وجود دارد که می‌تواند برای ردیابی یا جمع‌آوری اطلاعات معاملات استفاده شود، با این حال حسابرسان احتیاج خواهند داشت تلاش حسابرسی خود را در جهت ردیابی اسناد اضافی افزایش دهند تا بتوانند اطمینان معقولی از کامل بودن به دست آورند.

مصالحه بین بلاک‌چین و سوابق حسابداری بایستی حفظ شود تا اندازه‌گیری کند

کنترل گزارش‌های صادره از صرافی و همچنین تأیید رمزارزها را با اطمینان بالا دشوار می‌سازد. بنابراین، رمزهای به سرقت رفته یا ناپدید شده، دارایی‌های بی‌ارزش را نشان می‌دهند.

حمله موفق به کیف پول دیجیتالی باعث از بین رفتن تمامی ارزها می‌شود (Young، 2019). لذا حسابرسان ممکن





کند.

### وقوع

وقوع برای حساب‌های درآمدی شامل به‌دست آوردن شواهد حسابرسی مبتنی بر معتبر بودن معاملات مندرج در صورت‌های مالی است که این امر فقط هنگامی اتفاق می‌افتد که درآمدی

مانند سکه به‌عنوان یک واحد قابل اندازه‌گیری هستند و آزمون کاهش ارزش برای هر واحد حساب انجام می‌شود. سوابق حسابداری بایستی برای ردیابی هزینه‌های رمزارزها جهت آزمون کاهش ارزش، نگهداری شوند (FASB, 2014)؛ به‌علاوه، سیاست‌های حسابداری استفاده شده برای ارزشگذاری رمزارز مانند بازار مورد استفاده برای ارزیابی بایستی شناسایی و افشا شود تا بتوان شواهدی از دستکاری در بازار و اینکه بازار، حجم کافی از اطلاعات قیمت‌گذاری جهت ارزیابی قابلیت اطمینان و مربوط بودن ارائه می‌کند. به‌علاوه نوسان بازار دارایی و ثبات ارزشگذاری نیز بایستی در نظر گرفته شود.

به‌طور عمومی مرور کنترل‌های اصلاحی، محاسبه مجدد، بازرسی اسناد و مدارک و فهم و آزمون کنترل‌های داخلی شواهدی از صحت اطلاعات ارائه می‌کند. از آنجا که معاملات رمزارزها با مراجعه به آدرس مبدأ یا گیرنده دشوار است، ممکن است خطر عدم شناسایی معاملات با اشخاص وابسته یا توانایی در مشخص کردن گیرنده و فرستنده ثبت شده را افزایش دهد. اشتباهاتی مانند ارسال رمزارز به آدرس اشتباه یا خطاهای تایپی در معاملات ورودی که قابل لغو نیستند زیرا معاملات بلاک‌چین دائمی هستند، بنابراین مشتری ممکن است رمز خود را از طریق خطاهای ورودی داده از دست بدهد و از این رو خطر تحریف بااهمیت افزایش یابد. بنابراین حسابرس نیاز خواهد داشت کنترل‌های صحت ورود اطلاعات مشتری، دسترسی و کنترل‌های مربوط به ذخیره‌سازی را جهت مطمئن شدن از صحت معاملات رمزارزها را آزمون

که آیا هنوز معامله‌ای وجود دارد که بلاک‌چین اضافه شده است یا خیر. در واقع، بعضی اوقات بین تاریخ معاملات انجام شده و تاریخ معامله نشان داده شده در بلاک‌چین تفاوت وجود دارد که این امر ناشی از محدودیت‌های تکنولوژی، کنترل‌ها و نوسان در صرافی است. به‌علاوه حساب‌برسان بایستی بررسی کنند که حساب‌های کیف پولی که غیرفعال هستند در دفاتر حذف یا غیر فعال شده‌اند. در واقع کیف پول‌هایی که بسته شده است معاملات مربوط به این کیف پول‌ها برای شناسایی دشوارند. از آنجا که هویت طرف‌های معامله به‌صورت دیجیتالی پوشانده شده است، تأیید ارتباط یک یا چند مورد از طرفین مبادلات دشوار است. در آخر حساب‌برسان باید در نظر بگیرند که مشتری ممکن است با زبان‌های بالقوه‌ای ناشی از دعوی حقوقی و جرائم از سوی دولت‌ها به دلیل استفاده از رمزارز مواجه شوند.

### صحت و ارزش‌گذاری

از ادعای صحت و ارزشیابی صورت مالی برای جمع‌آوری شواهدی استفاده می‌شود که معاملات را در صورت‌های مالی با مانده صحیح، طرفین واقعی مبادله، طبقه‌بندی و تخصیص صحیح نشان می‌دهد. ارزشگذاری رمزارز به دلیل عدم وجود معاملات قابل مقایسه، تفاوت در قیمت‌گذاری سفارشات خرید و فروش و تفاوت در قیمت‌گذاری یک رمزارز خاص توسط صرافی خاص دارای چالش‌های بسیاری است. در تعیین ارزش منصفانه دارایی رمزارز، اندازه‌گیری جداگانه هر رمزارز نسبت به اندازه‌گیری پرتفوی آنها مهمتر است. در بیشتر موارد، رمزارزها

- 6) PwC. 2019. PwC launches solution supporting audit of cryptocurrency. Available at: <https://www.pwc.com/gx/en/news-room/press-releases/2019/cryptocurrenc-audit.html>.
- 7) Young, J. 2019. Round-up of crypto exchange hacks so far in 2019: How can they be stopped? Available at: <https://cointelegraph.com/news/round-up-of-crypto-exchanges-hack-so-far-in-2019-how-can-it-be-stopped>.

سید محمد توسلی طبائی: حسابدار رسمی، دانشجوی دکتری حسابداری دانشگاه تربیت مدرس  
محمد رضا چهره‌نما: دانشجوی کارشناسی ارشد حسابداری دانشگاه علامه طباطبائی



مالی که شامل رمزارزها ارائه نشده است، حسابرسان بایستی کفایت افشا را براساس اصول حسابرسی یا مقالات سفید مورد بررسی قرار دهند. حداقل افشاهای مورد نیاز از قبیل ماهیت دارایی، سیاست‌ها و روش‌های حسابداری، ارزش منصفانه، خطرهای مرتبط با رمزارزها و ارزشگذاری‌های انجام شده در صورت‌های مالی است. ■

منابع:

- 1) Nishani Edirisinghe Vincent and Anne M. Wilkins, 2020, Challenges when Auditing Cryptocurrencies, CURRENT ISSUES IN AUDITING, Vol. 14, No. 1, Spring 2020.

۲) کمیته فنی سازمان حسابرسی (۱۴۰۰)، اصول و ضوابط حسابداری و حسابرسی، استانداردهای حسابرسی، انتشارات سازمان حسابرسی.

- 3) Aquilio, M. 2018. Court grants IRS summons of coinbase records. Available at: <https://www.journalofaccountancy.com/issues/2018/mar/irs-summons-of-coinbase-records.html>.

- 4) Financial Accounting Standards Board (FASB). 2014. Intangibles—Goodwill and Other. Accounting Standards Codification (ASC) 850. Washington, DC: FASB.

- 5) Manlu Liu, Kean WuTT and Jennifer Jie Xu .2019. How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permitted Blockchain. CURRENT ISSUES IN AUDITING,

کسب شده باشد. خطرهای شامل معاملات ساختگی و شناسایی معاملات قبل از رخ دادن است. روش‌های حسابرسی شامل تأییدیه، شناخت کنترل‌های داخلی، بازرسی اسناد و مدارک و مغایرت‌گیری شواهد حسابرسی را جهت اثبات وقوع فراهم می‌کند. در حسابرسی رمزارزها، حسابرسان باید شواهد مربوط با تأیید مالکیت رمزارزها و طرفین معامله رمز را شناسایی کنند. حسابرسان بایستی از کنترل‌های داخلی مربوط به ادعای وقوع که در سطح صرافی یا سطح مشتری وجود دارد، شناخت کسب کنند. تفکیک وظایف بین حفاظت، ثبت و اختیار معاملات رمزارز بایستی بخشی از کنترل‌های داخلی مشتری حسابرسی باشد. به علاوه کنترل‌های فیزیکی مربوط به اطلاعات تکنولوژی مورد استفاده برای معاملات رمزارزها نیز بایستی بخشی از کنترل‌های داخلی مشتری حسابرسی باشد. کنترل‌ها در سطح صرافی در نظر گرفته شود. حسابرس باید کنترل‌های برنامه‌ها (نرم‌افزارها) که خطرهای عدم شناسایی طرف معامله یا میزان معامله را جلوگیری می‌کند یا حداقل می‌سازد، مورد بررسی قرار دهد.

#### افشا

اظهار نظر حسابرس در مورد منصفانه بودن صورت‌های مالی شامل ارزیابی افشائات صورت پذیرفته، است. به‌طور معمول، چک لیست افشا جهت اینکه صورت‌های مالی طبق اصول و مبانی پذیرفته شده است یا خیر، تکمیل می‌شود. لذا از آنجایی که هیچگونه رهنمودی از طرف تدوین‌کنندگان استاندارد مربوط به افشا صورت‌های