



تحلیل حقوقی مسئولیت استخراجگران و صرافی‌های رمزارز

اصغر خواجهی^۱
سیدمرتضی قاسم‌زاده^۲
کورش جعفرپور^۳

تاریخ دریافت مقاله: ۱۴۰۲/۰۴/۰۸ تاریخ پذیرش نهایی: ۱۴۰۲/۰۶/۲۵

چکیده

امروزه استفاده از فناوری بلاک چین و رمزارزها در معاملات تجاری، چالش‌های حقوقی بسیاری را مطرح نموده است و در کشور ما به رغم اینکه استخراج رمزارزها برابر مصوبه هیات وزیران با کسب مجوز از مراجع مربوطه مجاز بوده ولی هنوز موضع صریحی در خصوص رمزارزها اتخاذ نشده لذا شناسایی رابطین و قراردادهای رمزارزها و متعاقب آن تدوین قوانین مناسب، ضروری بنظر می‌رسد. برخلاف قوانین مالیاتی، که تعهدات و مسئولیت فردی که رمزارز دریافت می‌کند یا از تراکنش با رمزارزها سود کسب می‌کند تحت پوشش قوانین خاص در بسیاری از دولت‌هاست، در بحث دربارهٔ مسئولیت مدنی در زمینه روابط رمزارزی، مغایرت‌ها، ابهامات و سردرگمی‌های بسیاری به دلیل تازگی این پدیده مشاهده می‌شود. با توجه به بررسی ماهیت قراردادهای هوشمند، قراردادهای استخراج ابری و تجزیه و تحلیل توافقنامه‌های متعدد مصرف‌کنندگان که توسط سرویس‌دهندگان در فضای رمزینه ارزها ارائه می‌شود، نتایج این تحقیق نشان می‌دهد که قوانین پیش‌فرض در خصوص مسئولیت قراردادی در روابط قراردادی وافی به مقصود بوده و ماهیت منحصر بفرد و پیچیده رمزارزها که قرارداد آنها مورد بحث است نباید برای کاربردپذیری قوانین مدنی در خصوص اعتبار، الزام‌آوری و مسائل مسئولیت در موارد نقض حائز اهمیت باشد از سوی دیگر در خصوص مسئولیت خارج از قرارداد بیشتر

^۱ دانشجوی دکتری حقوق خصوصی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

Email: Kamran 481926@gmail.com

^۲ استاد گروه حقوق، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول).

Email: dr.qasem-zadeh@yahoo.com

^۳ استادیار گروه حقوق، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

ناشی از خطای بی‌احتیاطی و نقض وظیفه بوده و ضرورت داشته در زمینه حمایت از مصرف‌کننده، حفاظت حریم خصوصی داده‌ها و قانون حمایت از سرمایه‌گذار قوانینی مطلوب وضع گردد.

کلید واژه‌ها

استخراجگران رمزارز، صرافی، مسئولیت قراردادی، مسئولیت مدنی.

مقدمه

با توجه به تغییر و تحولات رخ داده در اقتصاد جهانی، فناوری جدید به خصوص بلاک چین و علم رمزنگاری و شبکه، تغییرات اساسی را در اقتصاد جهان ایجاد کرده اند. از جمله مهمترین این تحولات می‌توان به پدیده نوظهوری به نام رمزارزها اشاره کرد. در واقع پول مجازی یک سیستم خصوصی برای تسهیل انجام مبادلات بین افراد است بدون آنکه نیاز به حضور نهاد مرکزی واسط باشد. در حال حاضر ارزهای مجازی و فناوری بلاک چین به سرعت در حال فراگیر شدن هستند. (محمودی، ۱۳۹۸) امروزه استخراج و بیع رمزارزها در صرافی‌های متمرکز و غیرمتمرکز به شکل گسترده‌ای رواج یافته و بررسی و شناخت اعمال حقوقی قراردادهای منعقد فی مابین کاربران با رابطین رمزارزها همچون استخراجگران و صرافی‌های متمرکز و غیرمتمرکز که با قراردادهای عادی تفاوت بسیاری داشته جهت اعمال قواعد حاکم بر این معاملات ضروری بنظر می‌رسد. در یک قرارداد عادی، طرفین با امضای قرارداد، کالا یا خدماتی را در یک بازه کم و بیش مقرر دریافت می‌کنند. اما درباره قراردادهای استخراج اینگونه نیست. اولاً، شرکت‌های ماینینگ دعوتنامه برای مذاکره درباره شرایط قرارداد نمی‌فرستند. بلکه، توافقنامه‌های ضوابط و شرایط متعارف را روی وب سایت ارائه می‌دهند. ثانیاً، به دلیل دشواری فنی استخراج بلوک جدید، این قبیل روابط قراردادی عدم قطعیت بالایی دارند. مصرف‌کنندگان فقط امکان استخراج و مدیریت موفق خدمات را از شرکت‌های ماینینگ خریداری می‌کنند. نه مدیران استخراج متمرکز و نه استخراج‌های استخراج غیرمتمرکز ثبات را فراهم نمی‌کنند. زمانی که استخراج معینی بلوک جدید را می‌یابد و ماینرها درصدی از رمزارز استخراج شده را دریافت می‌کنند، نامعلوم است. مقدار رمزارزی که ماینر دریافت می‌کند متغیر است. براساس احتمال تئوریک، ممکن است ماینر همه پرداخت‌های ضروری جهت دریافت رمزارز را انجام دهد، اما در نهایت هیچ رمزارزی دریافت نکند (Antpool, 2020).

از سوی دیگر پیشرفت فناوری، باعث کاهش مشارکت انسان در بسیاری از فرایندها را می‌شود. همچنین، عامل رشد معاملات الگوریتمی بوده که اکنون پلتفرم صرافی‌های بسیاری آنها را اجرا می‌کنند. خودکار بودن این فرایند این سؤال جالب را به ذهن می‌آورد: آیا اشکال فنی در نرم‌افزار امکان تعدی از شرایط مقرر شده در قرارداد و بخشودگی فرد خاطی از مسئولیت قراردادی را فراهم می‌آورد؟ افزون بر این اگر در انعقاد قراردادهای هوشمند در صرافی‌های اشتباهی صورت گیرد مسئولیت نهایی آن بر عهده

کیست. در این پژوهش با توجه به تصویب نامه هیات وزیران مورخه ۹۸/۵/۱۳ که استخراج فرآورده‌های پردازشی رمزنگاری شده رمز ارزها (ماینینگ) با اخذ مجوز از وزارت صنعت و معدن و تجارت مجاز است و مراکز استخراج رمز ارزها به عنوان واحد تولیدی صنعتی شناخته شده در صدد است چالش‌های حقوقی قراردادهای استخراجگران و صرافی‌های متمرکز و غیر متمرکز مورد بررسی و تحلیل قرار می‌گیرد تا متناسب با آن قوانینی جهت حمایت مصرف کنندگان تدوین گردد.

۱- روابط قراردادی استخراج کنندگان

ماینینگ یا استخراج رمز ارزها را می‌توان به روش استخراج انفرادی، استخراج استخراج و استخراج ابری انجام داد. (Ershova and Trofimova, 2019, 77) استخراج استخراج، گروهی هم‌پیمان از ماینرها هستند که به‌طور مشترک و مستمر سعی می‌کنند بلوکی را استخراج کنند. واژه «ماینر» در این تعریف به اعضای استخراج استخراج اطلاق می‌شود. در بیشتر موارد، سازمان یا شرکتی وجود دارد که استخراج استخراج را مدیریت می‌کند و می‌تواند خدمات بیشتری ارائه دهد. بسته به موجودیت و نقش «مدیر استخراج»، وجهی که شرکت از ماینرها دریافت می‌کند، مشارکت ماینرها و پروتکلی که بر رمز ارز(های) استخراج شده حاکم است، می‌توان انواع متعددی از استخراج استخراج را از هم تفکیک کرد.

براساس پروتکل حاکم بر بلاک چین، استخراج استخراج دو نوع اصلی دارند:

(۱) استخراج استخراج فعال در حوزه استخراج رمز ارز که از پروتکل PoW استفاده می‌کنند؛

(۲) استخراج استخراجی که رمز ارزها از پروتکل PoS استفاده می‌کنند (sandler, 2018, 257)

این تفکیک مهم است زیرا پروتکلی که بر رمز ارزها حاکم است کنش‌های اعضای استخراج استخراج را مشخص می‌کند. تخصیص توان رایانشی برای افزایش امکان استخراج استخراج بلوک جدید و دریافت رمز ارز پاداش در بلاک چین‌های PoW ضروری است. پروتکل PoS گره اعتبارسنج را ملزم می‌کند تا مقداری از رمز ارز را در کیف پول دیجیتال ذخیره کند. هر چه رمز ارز ثبت شده در حساب اعتبارسنج‌ها بیشتر باشد، احتمال دریافت پاداش برای بلوک ایجاد شده جدید بیشتر است. بنابراین، فرض می‌شود اعضای توان رایانشی‌شان را در حالت اول به کار می‌گیرند؛ در سناریوی دوم، ارسال رمز ارز موجود به یک کیف پول مرکزی ضروری است.

استخراج استخراج براساس وجود یا نبود اپراتور مدیریت کننده:

(۱) استخراج استخراج متمرکز اپراتوری دارند که کار استخراج استخراج را مدیریت می‌کند. سروری که اپراتور مدیریت می‌کند فقط یک گره در بلاک چین است. این قبیل استخراج استخراج اغلب صفحات وب رسمی دارند که ضوابط و شرایط عمومی و شرایط پاداش در آن مشخص شده است (یا در سند مذکور قید شده و یا به‌صورت سندی مجزا ارسال می‌شود).

۲) استخرهای غیرمتمرکز ماینرهای مستقل را تشکیل می‌دهند که هر ماینر نمایانگر یک گره در یک بلاک چین است، مانند P2Pool، بیت‌پنی، الیجیوس. استخرهای غیرمتمرکز از ایده اولیه زیربنایی رمزارزها (غیرمتمرکزسازی) حمایت می‌کنند، اما به اندازه استخرهای متمرکز موفق نیستند. بیت‌پنی سال ۲۰۱۱ فعالیتش را متوقف کرد. صفحه وب الیجیوس از سال ۲۰۱۷ قابل دسترس نیست به دلیل ماهیت غیرمتمرکز این استخرها، هیچ‌کسی در قبال هر گونه اختلال در شبکه، آسیب یا زیان پاسخگو نیست. (McCormick, 2020)

طبقه‌بندی‌های دیگری مانند تفکیک استخرهای استخراج براساس الگوی پرداخت پاداش (نسبتی، پرداخت در ازای N سهم آخر، پرداخت در ازای هر سهم و غیره)، و کوین‌های استخراجی گوناگون (استخر منفرد و استخر چندگانه) و غیره وجود دارد، اما در اینجا دو مورد از مهمترین‌ها ذکر شد. شرکت‌های استخر استخراج معمولاً در پاورقی قرارداد لینکی به توافقنامه خدمات کاربری در صفحه سایتشان در قالب ثبت نام به کاربر می‌دهند. معمولاً، فرم ثبت نام کادر انتخابی ندارد که کاربر مجبور می‌شود برای پذیرش توافقنامه اقداماتی انجام دهد (آنت‌پول) یا فیلد تیک‌زده‌ای دارد که نشانگر پذیرش کاربر است. این روش در این رابطه احتمال خواندن توافقنامه توسط کاربر را به شدت می‌کاهد. (Ibid, 35)

نقش مدیران استخر براساس شرایط و ضوابط متعدد استخر استخراج به ارائه نرم‌افزار لازم محدود می‌شود که به کاربران امکان دهد تا رمزارزها را استخراج کنند. (Slush Pool, 2020) خود نرم‌افزار قابلیت ایجاد حساب کاربری، اتصال به استخر استخراج، درخواست کوین‌های استخراج شده، پیگیری فعالیت گره‌های عامل و قابلیت‌های دیگری دارد. تعهد اصلی مدیران فقط پذیرش ورودی کاربران بر حسب توان رایانش سخت افزار آنها، استفاده از نرم‌افزار برای استخراج، پیگیری مقدار کار انجام شده توسط گره‌های معین و توزیع پاداش براساس قوانین پاداش و پرداخت است.

شرکت‌های ماینینگ سعی می‌کنند مسئولیتشان در حوزه کاربری را تا حد امکان محدود کنند. تحلیل ضوابط و شرایط عمومی یکی از بزرگترین استخرهای استخراج (آنت‌پول) که براساس توزیع هش ریت یا قدرت محاسباتی به روش اثبات کار مشغول فعالیت می‌باشد سه شرط اصلی را نشان داد که قابل بررسی بودند. این شروط به کاهش مسئولیت شرکت در قبال کاربر یا محدودسازی حقوق کاربر اختصاص داشتند.

۱-۱- شرط حوادث قهری

شرکت آنت‌پول در شرط حوادث قهری این حوادث را قید کرده است: هک، ویروس‌های رایانه‌ای، «فروپاشی یا عدم استفاده از سیستم تحت مدیریت آنت‌پول به دلیل هر گونه حوادث قهری یا هر علتی خارج از اراده شرکت» و سایر حوادث. (Antpool, 2020)

رویدادهای سایبری که از جمله حوادث قهری محسوب می‌شوند قابل‌بحث‌اند. حملات سایبری جزئی، متوسط و حتی اساسی ممکن است توسط سرویس‌دهندگان پیشگیری شوند، مخصوصاً وقتی شرکت‌ها دارایی مردم را مدیریت می‌کنند. برای این منظور، سیاست‌های امنیت آی‌تی، پیروی از استانداردهای صنعت (مانند ISO 27000)، برنامه ریزی تداوم یک کسب و کار هنگام وقوع حادثه جهت برگشت به حالت عادی، الزامات بیمه رمز ارز و پیروی از دستورالعمل‌های نجات از بلایای فناوری اطلاعات (IT) باید توسط این قبیل شرکت‌ها انجام شود. (Rogers et al., 2020) این استانداردها به کاهش احتمال نفوذ و اختلال شبکه در اثر بدافزارها و هک کمک می‌کنند. شاید شرکت‌ها به دلیل نبود مراجع ویژه سرپرستی و نظارت، به انجام چنین کاری تمایل نداشته باشند. بنابراین، سیاست‌گذاران باید اتخاذ مقررات الزامی در ارتباط با این شرایط را در نظر داشته باشند که منجر به حفظ توازن بین حقوق و تعهدات طرفین در قراردادهای مصرف‌کننده می‌شود.

برخی شرکت‌ها ممکن است در قراردادهای از ادبیات گسترده‌تری استفاده کنند و به‌طور خاص به رویدادهای سایبری که از جمله حوادث قهری محسوب می‌شوند اشاره نکنند، مانند سایت 2miners این مورد، شرکت در قبال نقض قرارداد و خسارات وارده مسئول است. پرونده شرکت کلاسیک مری‌تایم در مقابل شرکت لیم‌بانگان ماکمور اس‌دی‌ان بی‌اچ‌دی ممکن است برای مسئولیت قراردادی سرویس‌دهندگان صادق باشد. در این مورد، «دادگاه استیناف پس از وقوع حادثه قهری، پرداخت خسارت قابل توجه به شخص بی‌گناه را مقرر کرد در شرایطی که طرفی که برای فرار از مسئولیت به دنبال استفاده از حوادث قهری بود نمی‌توانست به تعهدات پیمانی‌اش عمل کند (حتی اگر حادثه قهری رخ نمی‌داد)». این بدین معناست که فقط اثبات وقوع حادثه قهری برای طرفین کفایت نمی‌کند، بلکه طرف دعوی باید این موضوع را نیز ثابت کند که اگر رویداد مانع رخ نمی‌داد، به تعهدش عمل می‌کرد. اگر دادگاه‌های حوزه‌های قضایی مختلف چنین رویکردی را اتخاذ کنند، سرویس‌دهندگان نیز باید توانایی عمل به تعهداتشان را در زمان عدم وقوع رویداد سایبری اثبات کنند. (Goodrich & Tung, 2019)

۱-۲- سلب مسئولیت درستی و اعتبار محتوا

شرکت آنت‌پول توضیح داده است که «دقت، جامعیت یا قابلیت اطمینان هیچ محتوا یا اطلاعاتی که به طرق دیگر توسط کاربر در سایت درج شده، به آن منتقل شده، به آن لینک شده، از آن دانلود شده یا از آن تهیه شده است، تضمین نمی‌کند. همچنین، این شرکت در قبال هیچ‌گونه محصول، خدمات، اطلاعات یا محتوایی که کاربر به دلیل محتوا یا اطلاعات بر روی سایت خریداری یا استحصالی کرده است مسئولیتی ندارد. مسئولیت ریسک‌های ناشی از استفاده از اطلاعات روی سایت فقط بر عهده کاربر است» (Antpool, 2020).

با توجه به اینکه وب سایت رسمی یک شرکت استخراج تنها منبع اطلاعات حیاتی و قطعی درباره خدمات و محصولات ارائه شده است، درج اظهار سلب مسئولیت در قرارداد مصرف کننده، توازن روابط پیمانی را تا حد زیادی به نفع سرویس دهنده تغییر می دهد. هر گونه اطلاعات غیردقیق و گمراه کننده درج شده در وبسایت رسمی که منجر به خسارت شود، به لحاظ تئوریک منجر به تعقیب قانونی شرکت مربوطه بابت این موضوع نمی شود.

نه تنها ادبیات به کار رفته در اظهار سلب مسئولیت برای محدودسازی مسئولیت شرکت مهم است، بلکه درج این اظهارنامه در وب سایت نقش مهمی دارد. وب سایت ها تمایل دارند که بخش های ضروری توافقنامه کاربران را پنهان کنند و به شکلی آنها را در بین سایر محتویات وب سایت از دید خارج کنند، در نتیجه، احتمال نادیده گرفته شدن این اطلاعات از سوی کاربر بیشتر می شود. چنین رفتاری از جانب سرویس دهندگان از نظر دادگاه ها قصد مبهم سازی اطلاعات ضروری برای کاربران و ایجاد شرایط نامطلوب برای کاربران ارزیابی و تفسیر می شود. «این رفتار توافقنامه ای را که شرکت قصد افشای کامل آن را داشته است تضعیف می کند یا هر آنچه موضوع اظهار سلب مسئولیت وب سایت بوده است تکذیب می کند. ممکن است چنین رفتاری هدف استفاده از اظهار سلب مسئولیت را به طور کلی در نظر دادگاه نقض کند.» اظهار سلب مسئولیت، معافیت از مسئولیت را تضمین نمی کند. «دادگاه، حقایق و شرایط مختص موقعیت یا ادعای اظهار شده را در هر تعیین مسئولیتی می سنجد.» (Nicolosi, 2020)

۱-۳- شرط داوری

این شرط معمولاً در توافقنامه های ضوابط و شرایط وجود دارد. شرکت آنت پول این شرط را بدین صورت آورده است: «هر گونه اختلاف بین کاربر و شرکت ابتدا باید از طریق مذاکره مسالمت آمیز برطرف شود. در مواردی که توافق به واسطه مذاکره حاصل نشود، این نوع اختلافات باید به حکمیت ارجاع داده شده و در نهایت توسط حکمیت حل و فصل شود...». این جمله بندی نشانگر حکمیت الزام آور است. این شرط به عنوان آخرین شرط در توافقنامه درج شده و فقط الزامات فرایند حاکمیت را بیان می کند. کاربران عادی تشخیص نمی دهند که حق و حقوق تعقیب قانونی شرکت در دادگاه های ملی، پیوستن به دعوی های گروهی و درخواست استیناف را از دست می دهند. شرایط انصراف نیز در متن این سند نیامده است. کاربر مجبور است توافقنامه را همانگونه که هست بپذیرد. همین مسئله در این شرط که همراه با اظهار سلب مسئولیت (درج اطلاعات) است دیده می شود. افزون بر این، ادبیات و گستره جمله بندی شرط به طور کامل کاربر را از حقوق در دست رفته مطلع نمی کند. اهمیت درج و ادبیات به کار رفته در پرونده شرکت لانگ در مقابل شرکت پروواید کامرس نشان داده شده است. «در این مورد، وب سایت شرایط استفاده را از طریق هایپرلینک (Hyperlink) - ارتباطی از یک سند به سند دیگر یا در یک سند یکسان، از نقطه ای به نقطه دیگر که با کلیک بر روی آن توسط ماوس فعال می شود- مشخصی در هر یک از صفحات وب سایتش در

دسترس قرار می‌دهد، اما نه به کاربران اطلاع می‌دهد و نه آنها را ملزم می‌کند که برای اثبات موافقت، اقدام مثبتی را انجام دهند، حتی مجاورت هایپرلینک با دکمه‌های مرتبط که کاربران باید روی آنها کلیک کنند (بدون هیچ اقدام دیگری) برای اطلاع‌رسانی سازنده کفایت نمی‌کند.» این بدین معناست که شرط داوری کاربر را ملزم نکرده است، زیرا اطلاعیه مناسب در خصوص وجود چنین شرطی به او داده نشده است. (Find law, 2016)

علاوه بر اینها، توافقنامه‌های ضوابط و شرایط که نوعی قرارداد مصرف‌کننده محسوب می‌شوند ممکن است به صورت کلی از نظر انصاف در شرایط توافقنامه توسط دادگاه بررسی شوند. در حوزه‌های قضایی مختلف قانونی وجود دارد که به این مسئله می‌پردازد: بخشنامه شورا 93/13/EEC در خصوص شرایط نامنصفانه در قراردادهای مصرف‌کننده در اتحادیه اروپا، (EUR-lex, 2020) قانون حقوق مصرف‌کننده مصوبه سال ۲۰۱۵ (legislation.gov.uk, 2020) شرایط نامنصفانه در مقررات قراردادهای مصرف‌کننده مصوبه سال ۱۹۹۹ (Ibid, 2020) در بریتانیا، و تا حدی قانون کمیسیون تجارت فدرال و قانون ایالتی مربوطه در ایالات متحده و قوانین مدنی و سایر قوانین موضوعه کشورهای دارای نظام قانون مدنی.

این قبیل اسناد به دنبال حمایت از مصرف‌کننده در مقابل رفتارهای نامنصفانه متخصصینی است که از شرایط متعارف استفاده می‌کنند. شرایط متعارف مذاکره‌نشده و طویل علیه مصرف‌کننده استفاده می‌شوند که معمولاً یک کلمه از توافقنامه‌ای را که می‌پذیرند، نمی‌خوانند. این اتفاقات منجر به عدم توازن قابل توجه در حقوق و تعهدات طرفین می‌شود. در این موارد، ممکن است رفتار سرویس‌دهندگان با قانون فوق‌الذکر و آداب رایج‌تر حس نیت در معاملات تناقض داشته باشد (Feria & vogenauer, 2011, 247).

۱-۴- استخراج ابری

واژه «استخراج ابری» برای انجام عملیات استخراج ابداع شده و مربوط به رمزارزهای مختلفی مانند بیت کوین و اتریوم است. این واژه را می‌توان اینگونه نیز تعریف کرد «نوعی تمهید اقتصادی که در آن فرد مبلغی را به فرد یا نهادی دیگر می‌پردازد تا از جانب آنها رمزارز استخراج کند و در عوض، کارمزدهای تراکنش، رمزارز یا درصدی از آن را که از طریق این فعالیت‌های استخراجی تولید شده است دریافت کند.» (Krishnan et al., 2015, 115)

استخراج ابری پرریسک است زیرا شرکت‌هایی که فرصت چنین فعالیتی را فراهم می‌کنند، پیشنهادشان را در اینترنت آگهی می‌کنند و اگر در حوزه قضایی خاصی فعالیت کنند، از الزامات قانونی پیروی نمی‌کنند. ممکن است تسهیلات و فناوری‌های آنها خارج از محل شرکت باشد که به همین دلیل

سخت‌تر می‌توان کنترل کرد که ادعاها و وعده‌هایشان پشتوانه دارد یا خیر. بدین ترتیب، حوزه استخراج ابری به واسطه کلاهبرداری و استیفاء ناعادلانه از ثروت دیگران اشباع شده است.

د.ج. ساندلر، قراردادهای استخراج ابری را قراردادهای سرمایه‌گذاری مانند اوراق بهادار تلقی می‌کند. او چارچوب‌های قانونی ایالات متحده را که برای قراردادهای استخراج قابل اجرا هستند را تجزیه و تحلیل می‌کند (Sandler, 2018, 3) استان کیوبک در کانادا نیز مشارکت در استخراج ابری را نوعی اوراق بهادار تلقی می‌کند. (Tassev, 2020) ممکن است سایر حوزه‌های قضایی نیز همین رویکرد را داشته باشند. در اینصورت، سرمایه‌گذاران در حوزه استخراج ابری شروط دیگری اضافه و شرکت‌ها مجبور می‌شوند از مقررات دولت در این زمینه پیروی کنند.

د.ج. ساندلر از تشابه بین تمهیدات استخراج ابری و قراردادهای سرمایه‌گذاری با بکارگیری آزمون هووی-تست (Howey test) هوی در پرونده شرکت دلبیوج. هووی که از سوی دادگاه عالی ارائه شده است برای تعیین اینکه آیا یک معامله واجد شرایط "قرارداد سرمایه‌گذاری" است یا خیر، بهره می‌گیرد. «قراردادی یک قرارداد سرمایه‌گذاری تلقی می‌شود که با تعریف اوراق بهادار مطابقت کند، مشروط بر اینکه موارد زیر نیز وجود داشته باشد:

۱- سرمایه‌گذاری پولی

۲- در شرکتی مشترک

۳- با انتظار سوددهی

۴- سود تنها از طریق اقدام سایرین (مانند تبلیغ‌کننده یا شخص ثالث) تأمین شود، «صرفنظر از اینکه گواهی‌های رسمی یا سهام اسمی در دارایی‌های فیزیکی که شرکت از آنها استفاده می‌کند دال بر وجود سهام در شرکت باشند یا نباشند.» (Sandler, 2018, 269)

در پرونده هووی، شرکت دلبیوج. هووی و سرویس هووی ایند هیلز، قراردادهای هوشمند زمین را ارائه می‌کردند. اراضی موجود به باغستان‌های مرکبات اختصاص می‌یافت. براساس این قرارداد، خریداران اراضی را با قیمت یکنواختی در ازای هر جریب یا درصدی از آن خریداری می‌کردند و پس از آنکه مطلع می‌شدند امکان سرمایه‌گذاری در درختستان‌ها وجود ندارد مگر اینکه تمهیدات خدمات اتخاذ شده باشد برای همین مجبور بودند «قرارداد خدمات» را هم امضا کنند. دادگاه دریافت که خریداری امکان دسترسی به اراضی را نداشته‌اند و به دلیل وسعت محدود اراضی (باریکه‌های کم‌عرضی که پهنایشان تنها به اندازه یک درخت بود) خودشان فعالیت کشاورزی را انجام می‌دادند، کاملاً به سرویس نامبرده متکی بودند و استحقاق دریافت بخشی از سود حاصل از فعالیت‌های کشاورزی تحت رهبری شرکت را داشته‌اند. ازین‌رو، دادگاه عالی تصدیق کرد که چیزی به جز قراردادهای فروش اراضی همراه با خدمات مدیریتی به خواننده‌ها عرضه شده است.

آن‌ها فرصتی برای مشارکت مالی و سهام‌شدن در سود یک شرکت بزرگ مرکبات که توسط پاسخ‌دهندگان مدیریت می‌شد و بخشی از آن به آنها تعلق داشت، فراهم می‌کردند. این شرکت‌ها این فرصت را در اختیار افرادی می‌گذاشتند که ساکن مناطق دوردست بودند و تجهیزات و تجربه لازم برای زراعت، برداشت و بازاریابی محصولات باغ مرکبات نداشتند. چنین افرادی هیچ تمایلی به سکونت در اراضی یا توسعه مستقل آن ندارند؛ فقط سود بالقوه سرمایه‌گذاری آنها را جذب می‌کند. در پایان، دادگاه عالی به این نتیجه رسید که ظاهرالفاظ قراردادهای سرمایه‌گذاری نمی‌توان ماهیت واقعی این قراردادها را پنهان کند (Ibid, 270)

بدین ترتیب، د.ج. ساندلر خصوصیات قراردادهای استخراج ابری را براساس آزمون هووی با هم مقایسه کرد و به این نتیجه رسید که شاید دادگاه‌های ایالات متحده چنین قراردادهایی را قراردادهای سرمایه‌گذاری تلقی کنند. با این حال، این وضعیت عمدتاً به دو عامل بستگی دارد: ارزیابی وجود یا عدم وجود شرکت مشترک‌المنافع (دادگاه‌های مختلف در ایالات متحده رویکرد متفاوتی در این باره دارند) و مشارکت شرکت ماینینگ در استخراج PoW یا PoS.

تعریف قراردادهای استخراج ابری به‌عنوان اوراق بهادار پیامدهای قابل توجهی برای موضوع سرمایه‌گذاری و سرمایه‌گذاران دارد. دولت‌ها قوانین اوراق بهادار را اتخاذ می‌کنند که اقدامی برای بهبود افشاجری به سرمایه‌گذاران، به‌طور مستقیم یا به واسطه آثار بازدارنده عام و خاص راهکارهای مدنی، کیفری و اداری است. نه تنها این قوانین، ثبت اوراق بهاداری را که به‌صورت خصوصی عرضه شده‌اند الزام می‌کند، بلکه راهکارهای مدنی برای موارد کلاهبرداری نیز دارد. علاوه بر این، دارای فوایدی مانند مانند مسئولیت سخت‌گیرانه قلب واقعیت یا بی‌احتیاطی در توضیحات ثبت اوراق بهادار، تحمیل مسئولیت بی‌احتیاطی و تحمیل مسئولیت اثبات موضوع بر خواننده و غیره می‌باشد (Gordon, 2011, 63) هرچند قراردادهای استخراج ابری روابط پیمانی بین سرمایه‌گذاران و موضوع سرمایه‌گذاری ایجاد می‌کنند، وضعیت اوراق بهادار به راهکارهای مدنی قابل دسترس برای سرمایه‌گذاران منتج می‌شود که برپایه حقوق مسولیت مدنی (law of torts) است.

۲- صرافی‌های متمرکز و غیرمتمرکز

کلیه اطلاعات بخش قبلی درباره قراردادهای مصرف‌کننده برای قراردادهای کاربر که در وب سایت پلتفرم‌های تبادلات رمزارز به نمایش در می‌آیند نیز صدق می‌کنند. اما، نظارت دولت بر صرافی‌های رمزارزها در مقایسه با نظارت‌های موجود در خصوص استخراج پیشرفته‌تر است. صرافی‌های رمزارزها با روند فزاینده‌ای مسئولیت هک را می‌پذیرند. کمیسیون معاملات منصفانه (FTC) بیان کرد که ۵ صرافی رمزارز کره‌ای ضوابط خدماتشان را تغییر داده‌اند و اکنون در قبال خسارات ناشی از حملات سایبری یا نقایص فنی سیستم، صرفنظر از بی‌احتیاطی، مسئولیت می‌پذیرند. این اتفاق پس از ارائه

توصیه اصلاحی از سوی FTC به صرافی‌های رمزارز در آوریل ۲۰۱۸ رخ داد (Yonhap News Agency, 2020). افزون بر این، این قبیل صرافی‌ها به هدف حسابرسی‌های امنیتی ارگان‌های دولتی مبدل می‌شوند (Chan, 2020) با توجه به این موضوعات، صرافی‌های رمزارزها از شروط حوادث قهری یا سلب مسئولیتی که استخرهای استخراج برای اجتناب از مسئولیت‌ها بهره می‌گیرند استفاده نمی‌کنند. به‌عنوان مثال، یکی از بزرگترین صرافی‌های رمزارز در بازار کره، که قربانی هک شده بود، پیش‌تر اعلام کرد که کاربران خسارت‌دیده سرمایه از دست‌رفته‌شان را پس می‌گیرند. همچنین، این صرافی دستورالعمل‌های نجات از حوادث را که جایش در استخرهای استخراج خالی‌ست، اتخاذ کرده است (Jamie, 2020).

پیشرفت فناوری، باعث کاهش مشارکت انسان در بسیاری از فرایندها را می‌شود. همچنین، عامل رشد معاملات الگوریتمی - این معاملات فرایندی برای اجرای سفارش‌ها با استفاده از دستورات معامله خودکار یا از قبل برنامه‌نویسی شده با در نظر گرفتن متغیرهایی نظیر قیمت، زمانبندی و حجم است - بوده که اکنون پلتفرم صرافی‌های بسیاری آنها را اجرا می‌کنند. خودکار بودن این فرایند این سؤال جالب را به ذهن می‌آورد: آیا اشکال فنی در نرم‌افزار امکان تعدی از شرایط مقرر شده در قرارداد و بخشودگی فرد خاطی از مسئولیت قراردادی را فراهم می‌آورد؟

یکی از اولین پرونده‌هایی که به این موضوع پرداخت؛ پرونده شرکت با مسئولیت محدود B2C2 در مقابل شرکت با مسئولیت محدود کوآین پی‌تی‌ای (Quoine Pte Ltd) بود که حکم نهایی توسط س. تورلی، قاضی دادگاه تجاری بین‌المللی سنگاپور، صادر شد. در این پرونده، اصول قراردادی و تراست-نهادی در نظام حقوقی کامن لا است که در آن شخصی به عنوان تشکیل دهنده تراست اموالی را به یک یا چند شخص دیگر موسوم به تراستی سپرده و شرط می‌کند که این اموال به نفع یک یا چند شخص دیگر اداره شود - برای معاملات رمزارزها اعمال شد.

خواهان این پرونده شرکت با مسئولیت محدود B2C2، یک شرکت بازاریاب الکترونیکی ثبت شده در انگلیس و ویلز بود که در خصوص نقض قرارداد و نهاد تراست از سوی شرکت کوآین، که یک صرافی رمزارز سنگاپوری است، به دادگاه ارجاع شده بود. موضوع دعوی تراکنش‌هایی بود که در پلتفرم صرافی کیوئین (Quoine) در ۱۹ آوریل ۲۰۱۷ صورت گرفته بود که شرکت B2C2 همان موقع سفارش‌هایی را برای فروش اتریوم در قبال بیت کوین در این صرافی گذاشته بود. به دلیل رفتار غلط پلتفرم کوآین، معاملات فوق با نرخ معادل ۲۵ برابر نرخ تبادل بازار اتریوم و بیت کوین به نفع شرکت B2C2 انجام شده بود. این تراکنش‌ها از طریق برنامه‌های رایانه‌ای و بدون دخالت انسان انجام می‌شدند. وقتی CTO شرکت کوآین به نرخ تبادل غیرعادی پی می‌برد، متوجه خطا می‌شود و تراکنش‌های بدهی و بستانکاری موردبخت را بازگردانی می‌کند. (Singapore court's cryptocurrency decision, 2019, 28)

در این پرونده خاص، چهار حقیقت مهم توسط قاضی پرونده تصدیق شد:

۱) بازگشت یکطرفه تراکنش‌ها صرفنظر از خطای فنی که سبب نرخ تبادل غیرعادی تراکنش‌ها شده است، نقض قرارداد محسوب می‌شود.

۲) زمانی که قرارداد فعلی به شرکت امکان ارائه ضوابط به‌روزشده یا جدید توافقنامه فعلی یا آپلود توافقنامه جدید را بدون نیاز به ابلاغ قبلی به طرف مقابل می‌دهد، نحوه ارائه ضوابط به‌روزشده یا جدید یا آپلود توافقنامه کاملاً جدید، مهم است.

۳) در مواردی که تراکنش‌ها از طریق برنامه‌های رایانه‌ای و بدون هر گونه دخالت انسان انجام می‌شوند، دانش و نیت سازنده برنامه یا برنامه‌نویس واجد شرایط، نه یک فرد عادی و محتاط، در نظر گرفته می‌شود.

۴) هولد کردن (Hold) (نگه داشتن و نفروختن رمز ارز) رمز ارز توسط صرافی‌های رمز ارز یا هر گونه پلتفرم رمز ارز دیگر به منزله تراس است. دادگاه تصدیق کرد که این روابط در واقعیت بین شرکت B2C2 و کوآین بنا به دلایل زیر وجود داشته است: دادگاه و طرفین پرونده ارز مجازی را نوعی دارایی می‌دانستند که به صورت امانی قابل نگهداری است (قطعیت موضوع) (Ibid, 101-102). شرکت کوآین مالکیت، کنترل و مدیریت تنها کیف پول سرد رمز ارزی که سپرده کلیه معامله‌گران را در آن نگهداری می‌کند برعهده دارد. دارایی‌های طرفین مقابل کوآین جدا از دارایی‌های کوآین مدیریت می‌شوند. بنابراین، «ذینفع‌ها از حساب‌های مجزای هر یک از اعضاء قابل تشخیص‌اند (قطعیت اهداف) (Ibid, 102). کلمات بیان شده برای ایجاد یک تراس الزامی نیستند. تعیین رفتار ارائه‌دهنده پیشنهادی، ادبیات بکار رفته در مستندات مربوط به روابط قانونی بین طرفین و شرایط مربوطه جهت تعیین مقصود ایجاد تراس کفایت می‌کند. شواهد روشن دال بر اینکه شرکت کوآین برای نگهداری دارایی‌های هر یک از اعضا در تراس تعیین شده است این است که «این شرکت هیچ عنوانی را برای این دارایی‌ها مطالبه نکرده است و تصدیق می‌کند که در حال نگهداری آنها به سفارش اعضاء و جدا از دارایی‌های خود است که اعضا می‌توانند هر زمانی تقاضای برداشت دهند» (Ibid, 57-58). قاضی اثبات کرد که تراس ایجاد شده است. علاوه بر نقض قرارداد از جانب کوآین و این حقیقت که این شرکت برای بازگردانی تراکنش‌ها محق نبوده است، بازگردانی مورد بحث به منزله نقض وظیفه کوآین و نقض تراس است.

هرچند کشورهای دارای قانون مدنی با مفهوم تراس و نیز اشتباه چندجانبه در نظام کامن لا و در قاعده انصاف ناآشنا هستند، قوانین کمی مشابه در خصوص قراردادهای فسخ‌پذیر، که در نتیجه نقایص فرایند انعقاد قرارداد منعقد می‌شوند، در حوزه‌های قضایی قوانین مدنی وجود دارد. قانون مدنی اراده آزاد طرفین قرارداد را تصدیق می‌کند. چنانچه با نقض اراده مواجه باشند، منجر به فسخ قرارداد می‌شود، یعنی به دلیل مفاد این قانون این قرارداد قابل اجرا نخواهد بود یا تصدیق فسخ‌پذیری قرارداد این امکان را به

طرفین می‌دهد تا از انعقاد آن اجتناب کنند. خطاهای گوناگونی در قوانین مدنی ملی بیان شده و معمولاً به خطا در مذاکرات، خطای فردی، خطای شرکت‌ها و خطا در اساس قرارداد محدود می‌شوند (Markesinis et al., 2006, 276-277) قانون اساسی ملی نه تنها این قبیل خطاها را تعیین کرده، بلکه برخی مستندات منطقه‌ای مانند ماده‌های ۴۱۰۳-۴۱۰۳ در (Principles of European Contract Law) نیز به این موضوع می‌پردازند. (Peter Berger, 2020). در خصوص تعمیم نتایج این پرونده باید گفت:

- از آنجایی که نرم‌افزار تسهیل‌کننده معاملات رمزارزها تابع قوانین برنامه‌نویسی است، تراکنش‌ها را بدون هیچ تأثیر مستقیم انسان انجام می‌دهد و عمدتاً منبع‌باز است، یعنی مهندسیین زیادی در توسعه آن نقش دارند، بنابراین استدلال قاضی در پرونده این دو شرکت برای اختلافات مربوط به رمزارزها بسیار ارزشمند خواهد بود.
- تراکنش‌های بلاک چین براساس طراحی آنها بازگشت‌ناپذیرند و اگر فردی تراکنشی را بازگردانی کند، قرارداد را نقض می‌کند یا در قبال خطا و تحمیل خسارت به اشخاص ثالث مسئول خواهد بود. در ابتدای تاریخچه شکل‌گیری بیت کوین، وقتی تراکنشی لغو شد و زمانی که توسعه‌دهنده در آگوست ۲۰۱۰ به اشکالی در سیستم پی برد، حادثه‌ای به وقوع پیوست. در حقیقت، تراکنشی بازگردانی نشده بود؛ بلکه توسعه‌دهندگان فقط کد را تصحیح که اشکال را رفع کنند و این اشکال به تاریخچه تراکنش‌ها بازگشت، به همین دلیل به نظر می‌آمد که تراکنش هرگز انجام نشده است (Sedgwick, 2020) گرچه جامعه بیت کوین در آن زمان نسبتاً کوچک بود و این مسئله سریعاً حل شد، این رویداد نشان می‌دهد که دستکاری برنامه‌نویسی که در تراکنش‌های بلاک چین به‌کار می‌رود ممکن است سبب مسائل احتمالی در ارتباط با مسئولیت شود.
- افراد در پس نرم‌افزارها هستند که ممکن است در قبال شیوه طراحی برنامه مسئول باشند.
- شرکت‌ها در قبال اشکالات جزئی برنامه‌هایشان پاسخگو هستند؛ افرادی که رمزارزها را هولد می‌کنند به عنوان امانت‌گذار و شخصی که اموال امانی را منتقل می‌کند شناخته می‌شوند.

۳- قراردادهای هوشمند رمز ارزها

۳-۱- تعریف قراردادهای هوشمند

مفهوم قراردادهای هوشمند چندان جدید نیست این مفهوم نخستین بار توسط نیک سابو در سال ۱۹۹۴ به صورت فرمول‌بندی دیجیتالی یک رابطه تجاری معرفی شد. سابو قراردادهای هوشمند را به صورت قرارداد رمزنگاری شده تعریف کرد که در آن تایید و تعهدات قراردادی از طریق کد رایانه‌ای خودکار اجرا می‌شود (سابو، ۱۹۹۶) هر چند تعریفی واحد در مورد قراردادهای هوشمند وجود ندارد برخی از مهمترین تعاریف ارائه شده عبارتند از:

- قراردادهای برنامه‌ریزی شده که هنگام برقراری شرایط از پیش تعیین شده به صورت خودکار اجرا می‌شود. (Capegemini, 2016, 4)

- قراردادهایی که به شکل کد به طور خودکار تعهدات مورد توافق طرفین قرارداد را اجرا می‌کند. (Iif, 2016, 2)
- قراردادهای الکترونیکی که مطابق با ایجاب و قبول طرفین در بستر بلاک چین متعقد می‌شود (Böhme, 2015, 25)

ابزاری مستقل که بدون مداخله مستقیم عامل انسانی و یا دیگر وسایل عمل کرده و نسبت به اقدام‌ها و اعضای سازنده اش، دارای نوعی کنترل است (weitzenboeck, 2001, 205).

در تعاریف ذکر شده برای قراردادهای هوشمند، ویژگی‌هایی همچون خودکار بودن، استفاده از فناوری بلاک چین و کدهای برنامه نویسی مورد توجه قرار گرفته است در واقع برای اجرا و انجام قراردادهای هوشمند نه تنها به مداخله و کلا نیاز دارد، بلکه مشارکت کدنویس‌ها نیز ضروری است. امروزه، پرفرودارترین پلتفرمی که انعقاد قراردادهای هوشمند را تسهیل می‌کند اتریوم است.

۳-۲- چالش‌های قرارداد هوشمند

اشتباه در انعقاد قراردادهای هوشمند علاوه بر مفهوم رایج اشتباه در حقوق قراردادها، وارد کردن اطلاعات غلط در زمان انعقاد قرارداد است. اگر برنامه نویسی عامل نرم افزار هوشمند مرتکب خطا شده باشد و به جهت خطای صورت گرفته خسارتی ایجاد شود، مسئولیت نهایی بر عهده برنامه نویسی مستقر بوده اما اعتقاد رایج در تجارت الکترونیک این است که هر کاری که عامل نرم افزار انجام می‌دهد منتسب به اصل ساز است مگر اینکه وقوع اشتباه به افراد دیگری مثل هکرها یا برنامه نویسی یا علل غیر قابل پیش بینی دیگر قابل انتساب باشد. مبنای این اعتقاد مرسوم در این است که واسط الکترونیکی به عنوان یک عامل نرم افزاری در واقع کاری را انجام می‌دهد که از ناحیه اصل ساز به او دستور داده شده است و خود عامل نرم افزار اراده و اختیاری ندارد و موضوع حق و تکلیف نمی‌باشد. (پناهی و دیگران، ۱۴۰۱، ۵۱۲-۵۱۳)

از سوی دیگر تخلف از انجام تعهدات قراردادی مانند زمانی که طرفین قرارداد فروش کالا را آغاز کرده باشد که در آن پرداخت معمولاً از پیش و با کمک قرارداد هوشمند انجام می‌گیرد و خریدار ضوابط قرارداد را رعایت کرده باشد، اما فروشنده کالا را به موقع را تحویل نداده است، در اینصورت باید شروط مربوطه در قرارداد قید شود که هر زمان نقض قابل پیش‌بینی رخ داد این شروط اجرا شوند. اما زمانی که در متن قرارداد شرطی درباره مسائل احتمالی قید نشود، طرف متضرر استحقاق جبران دارد و باید از طریق دادگاه پیگیری کند. زمانی که یک طرف قرارداد به قرارداد عمل نمی‌کند یا در مواردی که اختلاف به دادگاه کشیده می‌شود، ممکن است مشکلاتی همچون عدم عمل به قرارداد عدم مشروعیت حادث شود. این قبیل معذوریت‌ها را می‌توان در قرارداد ذکر کرد. هرچند، ارزیابی این رویدادها به مداخله یک

اوراکل (oracle) یا رابط بین دنیای هوشمند و واقعی مانند اوراکل کارشناس نیاز دارد (Tjing Tai, 2018, 15).

به مجرد پیشامد علت عدم عمل به قرارداد که از طریق اوراکل‌های خودکار یا TTP شناسایی شده است، مداخله اجتناب‌ناپذیر قاضی با توجه به شرایط مختلف صورت می‌پذیرد که نیازمند ارزیابی معذوریت عدم عمل به قرارداد است. اگر حوادث قهری رخ داده باشد، «می‌توان پیامدهای آن را به‌سادگی برنامه‌نویسی کرد. حوادث قهری مانع مطالبه جبران عدم عمل به قرارداد می‌شوند، زیرا هیچ نقض قراردادی وجود ندارد. با این حال، بستانکار می‌تواند قرارداد را فسخ کند. فسخ نیز به‌سادگی برنامه‌نویسی می‌شود (اگرچه ممکن است تهیه پیش‌نویسی مناسب برای اتخاذ تمهیدات لازم پیرامون و پس از فسخ قرارداد مانند بازگشت مبالغ پیش‌پرداخت، ارزش‌گذاری اقدامات انجام شده در طی قرارداد به فراست حقوقی قابل توجهی نیاز دارد)» (Ibid, 16)

در مورد قراردادهای بی‌اعتبار، بازگشت‌ناپذیری تراکنش‌ها در بلاک چین نباید مسئله‌ای اجرایی تلقی شود زیرا طرف دیگر قرارداد همواره می‌تواند تراکنش ثانویه‌ای را صورت دهد که پرداخت طرف دیگر را بازگردانی کند. از طرفی دیگر، زمانی که دادگاه قراردادی را از اعتبار ساقط می‌کند، شرایطی ایجاد می‌شود که گویی قرارداد هرگز وجود نداشته است. در این مورد، می‌توان بازگشت‌ناپذیری را یک مانع دانست زیرا تراکنش برای همیشه در بلاک‌چین باقی می‌ماند. از دیدگاه ما، این همچنان یک مسئله محسوب نمی‌شود. حتی اگر تراکنش در دفتر توزیع شده باقی بماند، مادامی که طرفین بتوانند در زمان جبران تراکنش‌های نظیر را انجام دهند، بازگشت‌ناپذیری تراکنش‌های اولیه نباید یک مانع تلقی شود. بالاخره، زمانی که فرد تقاضای استرداد وجه می‌کند، فرد (طرف دیگر قرارداد یا بانک) باید همچنان یک تراکنش بیشتر انجام دهد تا پول به حساب طرف متقاضی مسترد شود. (Arkhyphenko, 2020)

قراردادهای هوشمند همچنان محدود به توافق‌هایی هستند که اتکای زیادی به رویدادهای خارج از زنجیره ندارند. قراردادهای هوشمند باید از طریق زیرساخت توسعه‌یافته و مناسب پشتیبانی شوند که توسط نهادها و پلتفرم‌های گوناگون، اوراکل‌های سخت‌افزاری مانند حسگرهای درون اشیای فیزیکی، شبکه‌های کافی اوراکل‌هایی که کارآمدی داده‌ها را تضمین می‌کنند و غیره عرضه تا بدین طریق مزایای وعده داده‌شده محقق شوند. حتی در صورت بهبود زیرساخت، قراردادهای هوشمند کاملاً مداخله انسانی را از بین نمی‌برند، مخصوصاً زمانی که برای احراز حقایق مربوطه مانند علیت، رخداد حوادث قهری، عدم امکان عمل به قرارداد، سوءتشخیص ضوابط از سوی طرفین و غیره، تحلیل الزامی است. با این حال، محققین همچنان اطمینان دارند که قراردادهای هوشمند می‌توانند ابزاری کافی، ساده و مناسب در آینده باشند، یعنی زمانی که فناوری‌ها موانع فعلی آن را از سر راه بر می‌دارند.

۴- مسولیت رابطین رمز ارزها

در نظام کامن لا، خواهان می‌تواند خواننده‌ای را که وظیفه ناشی از قانون را نقض کرده است، برای جبران خسارت خود تحت تعقیب قانونی قرار دهد. بدین معنا که، خواننده تکلیفی را نقض کرده است که تحت قانون موضوعه (برای بریتانیا قانون پارلمان)، برعهده دارد. (McBride & Bagshaw, 2018) این حقیقت در بازار رمز ارزها موضوعیت خاصی پیدا می‌کند، زیرا با رشد این صنعت، قوانین رمز ارزها نیز رشد پیدا می‌کنند. به‌طور خاص، زمانی که دارایی رمز ارزی در دسته ابزارهای مالی قرار می‌گیرد، شرکت‌هایی که با آن سروکار دارند باید از مقررات زیرساخت بازار اروپا ("EMIR")، مقررات بازارها در ابزارهای مالی ("MiFIR") و بخشنامه بازارها در ابزارهای مالی (MiFID II) پیروی کنند. (Eflow, 2019) به‌طور مثال، این موضوع به فعالان بازار معاملات مشتقه (derivatives trading) رمز ارز (فیوچرز، سوآپ، قراردادهای فوروارد و قراردادهای مابه‌التفاوت رمز ارزها و غیره) ارتباط پیدا می‌کند. رمز ارزها معمولاً دارایی مالی شناخته می‌شوند، لذا، صرافی‌های رمز ارز و شرکت‌های دارای کیف پول رمز ارز در حیطه چارچوب‌های FATCA و CRS قرار می‌گیرند (Szkudlarek, 2020) همچنین فعالان رمز ارزها در حیطه قانون ضد پولشویی و مقررات مالی ضد تروریسم قرار می‌گیرند که مؤسسات و شرکت‌های مالی را که با تراکنش‌های پولی در ارتباط هستند به پایش تراکنش‌های صورت گرفته در پلتفرم‌های بر بستر وب خود از روش‌های ویژه (ردیابی مبالغی که از مبلغ مقرر تجاوز می‌کنند، گزارش تراکنش‌های مشابه به مراجع ذیربط، سیاست‌های شناسایی مشتریان و غیره) ملزم می‌کنند. انتظار می‌رود که سایر اسنادی که به‌طور ویژه به نظارت بر رمز ارزها اختصاص می‌یابند به‌زودی تدوین شوند؛ به‌عنوان مثال، قانون رمز ارزها مصوب سال ۲۰۲۰، لایحه‌ای که اخیراً در ایالات متحده معرفی شده است (Helms, 2020). هر نقض وظیفه قانونی به لحاظ مدنی قابل پیگرد قانونی نیست، زیرا افراد حقیقی اغلب وظایف ناشی از قانون را اجرا نمی‌کنند. اغلب دعوی‌ها توسط مراجع دولتی به دادگاه مطرح می‌شوند تا رفتار غیرقانونی متوقف یا پیامدهای منفی رفتار مذکور رفع شود.

می‌توان سه گروه قوانین مرتبط با رمز ارزها در سطوح ملی، منطقه‌ای و بین‌المللی را نام برد که برای حراست از منافع گروه‌های خاصی از افراد طراحی شده‌اند:

- ۱- قوانینی که از سرمایه‌گذاران رمز ارزها حمایت می‌کنند؛
- ۲- مقرراتی که برای حمایت از کاربران (مصرف‌کنندگان) خدمات ارائه‌شده در اینترنت طراحی شده‌اند؛
- ۳- مقررات حریم خصوصی داده‌ها که قوانین در خصوص حفاظت داده‌های شخصی و جابجایی آزاد اطلاعات شخصی وضع می‌کند. قانون حمایت از مصرف‌کننده با قانون قراردادهای و مسؤلیت قراردادی ارتباط زیادی دارد. لذا، مقررات طراحی شده توسط سیاست‌گذاران را می‌توان براساس روابط قراردادی به پیش از عقد و بعد از عقد تقسیم کرد:

- مرحله پیش از عقد قرارداد: شرکت‌ها از مقررات پیروی می‌کنند که مصرف‌کننده را پیش از ورود به روابط قراردادی از اطلاعات مرتبط، کافی و موردنیاز مطلع می‌کند؛ الف. منع گمراه‌سازی یا تبلیغات جعلی؛
- ب. «عنوان‌گذاری محتوا و هشدارها و نیز شروط پیشین دال بر «رضایت مصرف‌کننده برای عقد قرارداد» (توانایی عقد قرارداد، اختیار آزاد و غیره)»
- ث. محدودیت «آزادی عقد قرارداد با منع یا تعهد فروشندگان به استفاده از شروط خاص در قراردادها» مانند وضع استانداردهای کیفی، کنترل قیمت، مقررات تعیین سقف نرخ بهره»
- د. منع ضوابط یا رویه‌های پیمانی نامنصفانه (Solli, 2011, 10)

- مرحله پس از عقد قرارداد
- الف. شروط نامنصفانه و قابل استطاعت برای دسترسی به مکانیزم‌های جبران خسارت؛
- ب. قواعدی که مسئول اثبات را (به نفع مصرف‌کننده) تغییر دهند. (Ibid, 11)
- ث. قوانین مسئولیت محصول

قانون حفاظت داده‌ها نیز یکی از دغدغه‌های شرکت‌هایی است که در تراکنش‌های رمزارزی دخالت دارند. اولین دغدغه احتمال نشت داده‌ها در پی حملات هکرها یا آسیب‌پذیری نرم‌افزار است. مسئله دیگر ممکن است معماری خود بلاک چین باشد (تغییرناپذیری داده‌ها در بلاک چین). براساس مقرراتی که برای حفاظت از داده‌های کاربران طراحی شده است، مانند GDPR، سوژه‌های داده‌ها از حقوق اصلی در خصوص اطلاعات شخصی برخوردارند مانند حقوق دسترسی، اصلاح، «فراموش‌شدگی» و غیره احقاق دو مورد اخیرالذکر در فضای رمزارزها ناممکن است. بعد از اینکه داده‌ها در DLT قرار می‌گیرند، کسی نمی‌تواند آنها را تغییر دهد یا حذف کند. لذا، شرکت‌های دخیل در تراکنش‌های رمزارزها باید به چنین خصوصیتی توجه داشته باشند و سازوکارهای مدیریت داده‌ها را ایجاد کنند که از شکایات مربوط به حریم خصوصی و حفاظت داده‌ها جلوگیری شود. در خصوص کشورهای تابع نظام حقوقی رومی ژرمنی، از زیرفصل پیش درباره خطای بی‌احتیاطی مشخص شد که خواهان می‌تواند در مواردی که کلیه عناصر جرم وجود دارد طرح دعوی کند. هرچند نقض وظیفه ناشی از قانون برخلاف قانون بریتانیا نه تنها نقض قوانین مجلس نیست، بلکه نقض سایر مقررات دولتی نیز است. زمانی که تنها قوانین موضوعه ملی نقض می‌شوند، این در حیطه قانون اداری است و مقامات ایالتی خاطیان را در دادگاه مسئول می‌دانند، اما زمانی که در پی نقض وظیفه ناشی از قانون به شخص حقیقی خسارت وارد می‌شود، این می‌تواند در حیطه مسئولیت خارج از قرارداد باشد. ممکن است بین مسئولیت قراردادی و خارج از قرارداد تداخلی وجود داشته باشد: وجود خطای می‌تواند نقض قرارداد تلقی شود و شبه‌جرم می‌تواند باعث ابطال قرارداد شود یا خطا تنها به این دلیل وجود دارد که نقض قرارداد صورت گرفته است، و غیره (vonbar et al., 2004, 15-16)

این حال، می‌توان خطاهایی را استخراج که احتمالاً در حوزه رمزارزها رخ می‌دهند (خطای بی‌احتیاطی و نقض وظیفه) و آن را جدا از مسئولیت قراردادی تجزیه و تحلیل کرد برای تلقی خطای بی‌احتیاطی، خواهان باید وجود عناصر الزامی شبه‌جرم را اثبات کند. ازین‌رو، قضات ایالات متحده و بریتانیا از استانداردهای قانونی (آزمون‌ها) استانداردهای قانونی (آزمون) موجود در رویه قضایی خود استفاده می‌کنند. نقض وظیفه ممکن است در خصوص نقض قوانین محفوظ در سه پیکره قانون رخ دهد: حمایت از مصرف‌کننده، حفاظت حریم خصوصی داده‌ها و قانون حمایت از سرمایه‌گذار. در قانون موضوعه مربوطه باید نیت امکان تعقیب این نوع نقض وظیفه در قانون مدنی لحاظ شود.

نتیجه‌گیری

این پژوهش چالش‌های حقوقی قراردادهای استخراجگران و صرافی‌های متمرکز و غیر متمرکز مورد بررسی و تحلیل قرار گرفته است. امروزه استخراج و بیع رمز ارزها در صرافی‌های متمرکز و غیرمتمرکز به شکل گسترده‌ای رواج یافته و بررسی و شناخت اعمال حقوقی قراردادهای منعقد فی مابین کاربران با رابطین رمز ارزها همچون استخراجگران و صرافی‌های متمرکز و غیرمتمرکز که با قراردادهای عادی تفاوت بسیاری داشته جهت اعمال قواعد حاکم بر این معاملات ضروری بنظر می‌رسد. در یک قرارداد عادی، طرفین با امضای قرارداد، کالا یا خدماتی را در یک بازه کم و بیش مقرر دریافت می‌کنند. اما درباره قراردادهای استخراج اینگونه نیست. اولاً، شرکت‌های ماینینگ دعوتنامه برای مذاکره درباره شرایط قرارداد نمی‌فرستند. بلکه، توافقنامه‌های ضوابط و شرایط متعارف را روی وب سایت ارائه می‌دهند. ثانیاً، به دلیل دشواری فنی استخراج بلوک جدید، این قبیل روابط قراردادی عدم قطعیت بالایی دارند. مصرف‌کنندگان فقط امکان استخراج و مدیریت موفق خدمات را از شرکت‌های ماینینگ خریداری می‌کنند. نه مدیران استخراج متمرکز و نه استخراج‌های غیرمتمرکز ثبات را فراهم نمی‌کنند. زمانی که استخراج معینی بلوک جدید را می‌یابد و ماینرها درصدی از رمزارز استخراج شده را دریافت می‌کنند، نامعلوم است. مقدار رمزارزی که ماینر دریافت می‌کند متغیر است. براساس احتمال تئوریک، ممکن است ماینر همه پرداخت‌های ضروری جهت دریافت رمزارز را انجام دهد، اما در نهایت هیچ رمزارزی دریافت نکند. از سوی دیگر پیشرفت فناوری، باعث کاهش مشارکت انسان در بسیاری از فرایندها را می‌شود. همچنین، عامل رشد معاملات الگوریتمی بوده که اکنون پلتفرم صرافی‌های بسیاری آنها را اجرا می‌کنند. شرکت‌های ماینینگ سعی می‌کنند مسئولیتشان در حوزه کاربری را تا حد امکان محدود کنند. تحلیل ضوابط و شرایط عمومی یکی از بزرگترین استخراج‌های استخراج (آنت‌پول) که براساس توزیع هش ریت یا قدرت محاسباتی به روش اثبات کار مشغول فعالیت می‌باشد سه شرط اصلی را نشان داد و این شروط به کاهش مسئولیت شرکت در قبال کاربر یا محدودسازی حقوق کاربر اختصاص داشتند. استخراج ابری پرریسک است زیرا شرکت‌هایی که فرصت چنین فعالیتی را فراهم

می‌کنند، پیشنهادشان را در اینترنت آگهی می‌کنند و اگر در حوزه قضایی خاصی فعالیت کنند، از الزامات قانونی پیروی نمی‌کنند. ممکن است تسهیلات و فناوری‌های آنها خارج از محل شرکت باشد که به همین دلیل سخت‌تر می‌توان کنترل کرد که ادعاها و وعده‌هایشان پشتوانه دارد یا خیر. بدین ترتیب، حوزه استخراج ابری به واسطه کلاهبرداری و استیفاء ناعادلانه از ثروت دیگران اشباع شده است. تعریف قراردادهای استخراج ابری به عنوان اوراق بهادار پیامدهای قابل توجهی برای موضوع سرمایه‌گذاری و سرمایه‌گذاران دارد. دولت‌ها قوانین اوراق بهادار را اتخاذ می‌کنند که اقدامی برای بهبود افشاگری به سرمایه‌گذاران، به‌طور مستقیم یا به واسطه آثار بازدارنده عام و خاص راهکارهای مدنی، کیفری و اداری است. اشتباه در انعقاد قراردادهای هوشمند علاوه بر مفهوم رایج اشتباه در حقوق قراردادها، وارد کردن اطلاعات غلط در زمان انعقاد قرارداد است. اگر برنامه نویس عامل نرم افزار هوشمند مرتکب خطا شده باشد و به جهت خطای صورت گرفته خسارتی ایجاد شود، مسئولیت نهایی بر عهده برنامه نویس مستقر بوده اما اعتقاد رایج در تجارت الکترونیک این است که هر کاری که عامل نرم افزار انجام می‌دهد منتسب به اصل ساز است مگر اینکه وقوع اشتباه به افراد دیگری مثل هکرها یا برنامه نویس یا علل غیر قابل پیش‌بینی دیگر قابل انتساب باشد. با توجه به بررسی ماهیت قراردادهای هوشمند، قراردادهای استخراج ابری و تجزیه و تحلیل توافقنامه‌های متعدد مصرف‌کنندگان که توسط سرویس‌دهندگان در فضای رمزینۀ ارزها ارائه می‌شود، نتایج این تحقیق نشان می‌دهد که قوانین پیش‌فرض در خصوص مسئولیت قراردادی در روابط قراردادی وافی به مقصود بوده و ماهیت منحصر بفرد و پیچیده رمزارزها که قرارداد آنها مورد بحث است نباید برای کاربردپذیری قوانین مدنی در خصوص اعتبار، الزام‌آوری و مسائل مسئولیت در موارد نقض حائز اهمیت باشد از سوی دیگر در خصوص مسئولیت خارج از قرارداد بیشتر ناشی از خطای بی‌احتیاطی و نقض وظیفه بوده و ضرورت داشته در زمینه حمایت از مصرف‌کننده، حفاظت حریم خصوصی داده‌ها و قانون حمایت از سرمایه‌گذار قوانینی مطلوب وضع گردد.

منابع

پناهی، هادی، علی غریبه، حسن پاشا زاده (۱۴۰۱) امکان سنجی مسولیت نرم افزار الکترونیکی هوشمند در فرض وقوع و اشتباه در حقوق ایران و کامن لا، تحقیقات حقوقی بین المللی، شماره ۱۵، ص ۴۹۵-۵۱۵.

صفایی، سید حسین، محمود کاظمی، مرتضی عادل، اکبر میرزائزاد (۱۳۹۹) حقوق بیع بین‌المللی، چاپ نهم، تهران، موسسه انتشارات دانشگاه تهران.

محمودی، اصغر (۱۳۹۸)، «تحلیل ارزشهای مجازی در پرتو فقه، حقوق خصوصی و مطالعات تطبیقی»، مطالعات حقوق خصوصی، دوره چهل و نهم، ش ۳، ص ۵۰۳-۵۲۲.

Boehm, Franziska and Paulina Pesch. "Bitcoin: A First Legal Analysis - With Reference to German and US-American Law." Financial Cryptography

- Workshops (2014).
https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf
- Basil S. Markesinis, Hannes Unberath, and Angus Johnston, *The German Law of Contract: A Comparative Treatise* (Oxford: Hart Publishing, 2006), 276-277.
- Böhme, Rainer; Christin, Nicolas; Edelman, Benjamin; & Moore, Tyler (2015). "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives*, 29(2), 213–238. doi:10.1257/jep.29.2.213
- Capegemini Consulting. (2016). *Smart Contracts in Financial Services: Getting from Hype to Reality*. Retrieved from <https://scihub.tw/https://www.capegemini.com>
- Singapore International Commercial Court of the Republic of Singapore. *B2C2 Ltd v. Quoine Pte Ltd*. SGHC(I) 03 (2019). https://www.sicc.gov.sg/docs/default-source/modulesdocument/judgments/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d7b
- Ershova, Inna, and Elena Trofimova. (July 2019): 73-82. <https://cyberleninka.ru/article/n/mayning-i-predprinimatelskaya-deyatelnost-vpoiska>
- Eric Tjong Tjing Tai, "Force Majeure and Excuses in Smart Contracts" *European Review of Private Law* 6, 26 (2018): 15, https://pure.uvt.nl/ws/portalfiles/portal/28903834/Smart_contracts_excuses_ERP_L_1_postprint.pdf
- Feria, Rita de la, Stefan Vogenauer. *Prohibition of Abuse of Law: A New General Principle of EU Law?* Oxford : Hart Publishing, 2011
- Gordon, James D., "Defining a Common Enterprise in Investment Contracts" *Ohio State Law Journal* 72, 1 (2011): 59-94, https://kb.osu.edu/bitstream/handle/1811/71438/OSLJ_V72N1_0059.pdf
- German Civil Code, Bundesministerium der Justiz und für Verbraucherschutz, Accessed 14 March 2020, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html
- Solli, Jami, Arthur Goujon, and Michael Gaweseb, "A guide to developing consumer protection law." London: Consumers International, 2011. <http://www.fao.org/3/a-at346e.pdf>
- IIF (2016). "Getting Smart: Contracts on the Blockchain," Institute Of International Finance, https://www.iif.com/portals/0/Files/private/32370132_smartcontracts_report_may_2016_vf.pdf
- German Civil Code, Bundesministerium der Justiz und für Verbraucherschutz, Accessed 14 March 2020, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html
- Idjeri, Anaëlle, "Reform of French contract law – Ratification Law published on April 21, 2018: Main changes impacting business law," *Soulier Avocats*, Accessed 14 March 2020, <https://www.soulier-avocats.com/en/reform-of-french-contract-law-ratification-law-published-on-april-21-2018-main-changes-impacting-bu>

- Helms, Kevin. "US Lawmaker Introduces Crypto-Currency Act of 2020 While Under Coronavirus Quarantine." Bitcoin.com. Accessed 6 April 2020. <https://news.bitcoin.com/cryptocurrency-act-of-2020/>
- Miklos Kiraly, "The Vienna Convention on International Sales of Goods and the Bitcoin," US-Chine Law Review 16, 5 (2019): 181, <https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf>
- McCormick, Jamie. "Eligius Bitcoin Mining Pool Review." Bitcoins In Ireland. Accessed 7 March 2020. <https://bitcoinsinireland.com/eligius-bitcoin-mining-pool-review/>
- "MiFID II, Crypto Assets and the Cryptocurrency Market," eflow, Accessed 4 April 2020, <https://eflowglobal.com/2019/06/17/mifid-ii-crypto-assets-and-the-cryptocurrency-market/>
- McBride Nicholas J, Roderick Bagshaw, "Breach of Statutory Duty," Tort Law (Harlow: Pearson Education Limited, 2018), <https://books.google.com.ua/books?id=171dDwAAQBAJ>
- Szabo Nick (1996). "Smart Contracts: Building Blocks for Digital Markets," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/sza_bo.best.vwh.net/smart_contracts_2.html
- Szkudlarek, Anna. "Cryptocurrency taxes – CRS/FATA: Do you need to disclose your cryptocurrencies?" KENDRIS. Accessed 4 April 2020. <https://www.kendris.com/en/blog/crsfata-do-y>
- UNIDROIT International Institute for the Unification of Private Law (Rome: International Institute for the Unification of Private Law, 2016), 218, <https://www.unidroit.org/english/principles/contracts/principles2016/principles2016-e.pdf>
- Von Bar Christian, Ulrich Drobnig, and Guido Alpa, The Interaction of Contract Law and Tort and Property Law in Europe: A Comparative Study (Munich: Sellier European Law Publishers, 2004), 15-16
- Weitzenboeck, Emily M. (2001). Electronic Agents and the Formation of Contracts. International Journal of Law and Information Technology, 9(3), 204 – 234. <https://academic.oup.com/ijlit/article-abstract/9/3/204/732909>
- لوبومیر تأسف، «در دیلی: قانون کوین لیبرستاد و قراردادهای هوشمند لوگزامبورگ»، Bitcoin.com، دسترسی ۹ مارس ۲۰۲۲، <https://news.bitcoin.com/in-the-daily-liberstad-coin-mining-contracts-luxembourg-law/>
- کای سدویک، «تاریخچه بیت کوین بخش ۱۰: باگ ۱۸۴ میلیاردی بیت کوین»، Bitcoin.com، دسترسی ۱۴ مارس ۲۰۲۲، <https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/>
- «شرکت با مسئولیت محدود B2C2 در مقابل شرکت با مسئولیت محدود کوآین پی تی ای»، SGHC(I) ۰۳ (۲۰۱۹): ۱-۲، ۲۷-۲۸، https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoise-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf

- هری کریشنان ر، سای ساکت وای و ونکاتا تج وایباف م، «استخراج رمز ارز - ورود به فضای ابری»، ژورنال بین‌المللی علوم و کاربردهای پیشرفته رایانه ۶، ۹ (۲۰۱۵): ۱۱۵، https://www.researchgate.net/publication/283810104_Cryptocurrency_Mining_-_Transition_to_Cloud
- ماین، آنت پول، دسترسی ۸ مارس ۲۰۲۲، <https://v3.آنت پول.com/home>
- جیسون چان، «صرافی‌های رمز ارز کره‌ای مسئولیت زیان ناشی از هک را می‌پذیرند»، ایژیا کریپتو تودی، دسترسی ۹ مارس ۲۰۲۲، <https://www.asiacryptotoday.com/s-korean-cryptocurrency-exchanges-take-responsibility-for-losses-from-hacks>
- الیزابت جیمی، «جای نگرانی وجود دارد: بای‌تامب دارایی از دست‌رفته کاربرانش را پس می‌دهد»، BTCNN.com، دسترسی ۹ مارس ۲۰۲۰، <https://www.btcnn.com/no-worries-bithumb-will-reimburse-lost-money-of-users/>
- «صرافی‌های رمز ارز ضوابط خدمات خود را تغییر می‌دهند: FTC»، آژانس خبری یون‌هپ نیوز، دسترسی ۹ مارس ۲۰۲۲، <https://en.yna.co.kr/view/AEN20190617005300320?section=search>
- کلوس پیتر برگر، «قوانین فراملی بازرگانی (قدیمی و جدید) و اصول ترنس‌لکس»، ترنس‌لکس، دسترسی ۱۴ مارس ۲۰۲۲، <https://www.trans-lex.org/400200>
- دارن ج. ساندلر، «درختستان‌های مرکبات در فضای ابری: آیا استخراج ابری رمز ارزها مطمئن است؟»، ژورنال حقوق فناوری پیشرفته سانتا کلارا ۳۴، ۳ (۲۰۱۸)، <https://digitalcommons.law.scu.edu/chtlj/vol34/iss3/1>
- فیل نیکولوسی، «چه زمانی اظهار سلب مسئولیت وبسایت مؤثر است؟» قانون فیل نیکولوسی، پی.سی. (بلاگ)، دسترسی ۹ مارس ۲۰۲۲، <https://www.internetlegalattorney.com/when-is-a-website-disclaimer-effective/>
- مارک گودریج، هیرا تونگ، «حوادث قهری: خسارات هنگفت حتی در صورت عدم اقدام» (نیویورک: وایت‌اند کیت ال‌ال‌پی، جولای ۲۰۱۹): ۱، <https://www.whitecase.com/sites/default/files/2019-07/force-majeure-substantial-damages-even-if-you-cannot-perform.pdf>

کرایگ راجرز، وندی بوکروت، مایکل باهار، «آیا حملات سایبری «حوادث قهری» محسوب می‌شوند؟
Je ne crois pas!» لکسولوژی، دسترسی ۸ مارس ۲۰۲۰،

<https://www.lexology.com/library/detail.aspx?g=9f8784de-aa99-4eed-ab92-79a3353582bf>

ضوابط و شرایط عمومی»، اسلاش پول، دسترسی ۸ مارس ۲۰۲۲،

<https://slushpool.com/about/tos/>

شرکت تعاونی لانگ وی پروواید کامرس. B257910 (۱۷ مارس ۲۰۱۶)، فاین‌دلا، دسترس ۹ مارس

<https://caselaw.findlaw.com/ca-court-of-appeal/1729412.html>، ۲۰۲۲



Legal analysis of the responsibility of cryptocurrency miners and exchanges

Asghar khajavi *
Syed Morteza Ghasem Zadeh **
Kourosh jafarpour ***

Abstract

Today, the use of blockchain technology and cryptocurrencies in commercial transactions has raised many legal challenges, and in our country, despite the fact that the mining of cryptocurrencies is permitted by the approval of the Cabinet of Ministers, with the permission of the relevant authorities, an explicit position regarding cryptocurrencies has not yet been taken. Therefore, it seems necessary to identify the contacts and contracts of cryptocurrencies and subsequently formulate appropriate laws. Unlike tax laws, where the obligations and responsibilities of a person who receives cryptocurrencies or profits from transactions with cryptocurrencies are covered by specific laws in many states, in the discussion of civil liability in the field of cryptocurrency relations, there are many contradictions, ambiguities and confusions due to the newness of this The phenomenon is observed. According to the investigation of the nature of smart contracts, cloud mining contracts and the analysis of numerous consumer agreements provided by service providers in the space of cryptocurrencies, the results of this research show that the default rules regarding contractual responsibility in contractual relationships are appropriate and unique in nature. And the complexity of cryptocurrencies whose contract is discussed should not be important for the applicability of civil laws regarding validity, binding and liability issues in cases of violations. In the field of consumer protection, data privacy protection and investor protection law, favorable laws should be enacted.

Keywords

Cryptocurrency miners, exchange, contractual liability, civil liability.

* Faculty of Law, South Tehran Branch, Islamic Azad University, Tehrn, Iran. Kamran 481926@gmail.com

** Department of Law, South Tehran Branch, Islamic Azad University, Tehrn, Iran. (Corresponding author): dr.qasem-zadeh@yahoo.com

*** Department of Law, South Tehran Branch, Islamic Azad University, Tehrn, Iran.