فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره دوم | تابستان ۱۴۰۲
ویگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN: 2821-126X

Civil Liability Incurred from Smart Contract Error

Seyed Mahdi Razavi
Department of Private Law, Faculty of Humanities, Azadshahr Branch, Islamic Azad University, Azadshahr, Iran (Corresponding Author)
l s.mahdi.razavi77@gmail.com
Mohammad Esmaeil Daemi
Department of Specialized Law, Faculty of Humanities, Azadshahr Branch, Islamic Azad University, Azadshahr, Iran

Keywords:
Artificial Intelligence, Blockchain, Civil Liability, Error, Smart Contract

Abstract

Smart contracts, as a new generation of electronic contracts, have been welcomed by many people to conclude contracts in cyberspace due to unique features, including transparency, self-execution, decentralization, and accuracy. Nevertheless, this technology will pose unknown legal challenges similar to what happened to the DAO smart contract in 2016. In this study, the causes of civil liability in case of occurrence of errors during the implementation of smart contracts were identified and studied. Utilizing library and internet resources with descriptive and analytical methods, with the underlying assumption that the terms of the contract were known to the parties, and mutual agreement on the contract's provisions was reached at. It was further posited that any errors that occur were not a result of a mistake by the will of the contracting parties. The results indicated that at least four cases can incur civil for the errors caused by implementing the smart contract, including (1) the blockchain on which the smart contract was implemented, but caused errors in the smart contract due to a security gap or programming problems, (2) artificial intelligence that is responsible for analyzing and executing smart contract codes and has not analyzed or executed the code correctly, (3) oracles connected to the smart contract that provide insecure or wrong information to the smart contract, and (4) the smart contract developer who did not write the security codes of the contract correctly or inadvertently put the wrong code in the smart contract, due to lack of skill or negligence.

فصلنامه علمی
مطالعات حقوقی فضای مجازی

صفحات مقاله ۱۵ الی ۲۸

مسئولیت مدنی ناشی از خطای قرارداد هوشمند

سید مهدی رضوی
گروه حقوق خصوصی، دانشکده علوم انسانی، واحد آزادشهر، دانشگاه آزاد اسلامی، آزادشهر، ایران
(نویسنده مسئول) s.mahdi.razavi77@gmail.com
محمد اسماعیل دائمی
گروه حقوق خصوصی، دانشکده علوم انسانی، واحد آزادشهر، دانشگاه آزاد اسلامی، آزادشهر، ایران

تاریخ دریافت: ۳ دی ۱۴۰۲ تاریخ پذیرش: ۴ مرداد ۱۴۰۳

چکیده
قراردادهای هوشمند به عنوان نسل نوین قراردادهای الکترونیکی، به علت ویژگی‌های منحصر به فردی همچون شفافیت، خوداجرایی، غیرمتمرکز بودن و دقیق بودن مورد استقبال بسیاری از اشخاص جهت انعقاد قرارداد در فضای سایبر قرار می‌گیرند اما بدیهی است این فناوری جدید، چالش‌های حقوقی ناشناخته‌ای همچون آنچه در سال ۲۰۱۶ برای قرارداد هوشمند The DAO به وقوع پیوست نیز به همراه خواهد داشت. فلذا در مقاله حاضر با استفاده از منابع کتابخانه‌ای و اینترنتی با روش توصیف و تحلیل تلاش می‌گردد به شناسایی و بررسی علل ایجاد مسئولیت مدنی در صورت بروز خطا در اجرای قرارداد هوشمند در فرضی که طرفین از مفاد قرارداد مطلع بوده و با یکدیگر وحدت قصد در مفاد قرارداد داشته‌اند و خطای رخ داده ناشی از اشتباه در اراده متعاقدین نبوده است، پرداخته شود. نتیجه پژوهش‌های انجام شده بیانگر این است که در فرض ذکر شده حداقل چهار مورد می‌تواند دارای مسئولیت مدنی خطاهای ناشی از اجرای قراردادهوشمند باشد که عبارت است از: بلاکچینی که قرارداد هوشمند بر روی آن اجرا شده است اما به علت خلأ امنیتی یا داشتن مشکلات برنامه نویسی سبب خطا در قرارداد هوشمند شده است؛ هوش مصنوعی‌ای که مسئول تحلیل و اجرای کدهای قراردادهای هوشمند بوده و به درستی کد را تحلیل یا اجرا نکرده است؛ اوراکل‌های متصل به قرارداد هوشمند که اطلاعات ناایمن یا اشتباه به قرارداد هوشمند ارائه می‌نمایند و توسعه دهنده قرارداد هوشمند که به سبب عدم مهارت کافی یا اهمال به درستی کدهای امنیتی قرارداد را ننوشته یا سهوا کد اشتباهی در قرارداد هوشمند قرار داده است.

واژگان کلیدی: بلاکچین، خطا، قرارداد هوشمند، مسئولیت مدنی، هوش مصنوعی

مقدمه

با گسترش تکنولوژی و فناوری‌های دیجیتال، قراردادها نیز از لحاظ شکل و ساختار دچار دگرگونی گردیده‌اند و از شکل سنتی و کاغذی آن، تبدیل به قراردادهای الکترونیکی شده‌اند و این دگرگونی همواره در طول زمان به شکل مستمر و همگام با تکنولوژی ادامه یافته است تا اینکه امروزه شاهد جدیدترین نسل قراردادها[۱] که «قرارداد هوشمند[۲]» نام دارند می‌باشیم. قراردادهای هوشمند از لحاظ فنی به یک برنامه رایانه‌ای گفته می‌شود که با کمک فناوری‌های نوینی مانند امضائات دیجیتالی[۳]، هوش مصنوعی[۴] و ارزهای دیجیتال[۵] و بر بستر فناوری دفاتر کل توزیع شده[۶] مانند زنجیره بلاک (بلاکچین[۷]) ایجاد شده و تحت شرایط خاص قراردادی، اقدامات از پیش تعیین شده را به طور خودکار اجرا می‌سازند (نجات زادگان و سلطانی، ۱۴۰۱: ۳۰۴). به مانند هر تکنولوژی دیگری، قراردادهای هوشمند نیز به سرعت میان عموم گسترش یافته است و مورد استفاده آنان در روابط میان خود، علی الخصوص روابط اقتصادی، قرار گرفته است. به طوری که از زمان شروع فعالیت بلاکچین اتریوم[۸] تا سال ۲۰۲۲، فقط در این بستر بیش از ۴۴ میلیون قرارداد هوشمند تشکیل شده است[۹] (Young, 2017). اما همواره هر تکنولوژی در کنار مزایای آن، دارای معایبی هم است که می‌تواند برای اشخاص چالش آفرین باشد. قراردادهای هوشمند مبتنی بر معماری نرم افزار هستند و شاید به همین دلیل است که آن‌ها را هوشمند می‌نامند، با این حال در بسیاری از موارد، آن‌ها نمی‌توانند عملکرد عالی و عاری از خطا و خطرات امنیتی را تضمین کنند (Roumpos, 2020:2). از جمله چالش‌های قرارداد هوشمند در مواردی است که طرفین قرارداد هوشمند در واقع پیرامون نوع عقد، موضوع عقد، مفاد قرارداد و آثار آن با یکدیگر وحدت قصد داشته و هیچ ابهام یا تردیدی در اراده و قصد طرفین درباره قرارداد وجود ندارد و به عبارتی متعاقدین دچار اشتباه نشده‌اند اما پس از انعقاد و اجرای قرارداد هوشمند، آثار قرارداد هوشمند به گونه‌ای اجرا می‌گردد که مقصود یا مطلوب متعاقدین نبوده یا حتی در مواردی قرارداد هوشمند علی رغم نهایی شدن کدنویسی، مفاد قرارداد را اجرا نمی‌کند، در این حالت‌ها قرارداد هوشمند دچار خطا[۱۰] گردیده است که طبیعتا به واسطه بروز این خطا ممکن است یکی از متعاقدین یا هردوی آن‌ها متحمل خسارت شوند، بنابراین لازم است تا بررسی شود و مشخص گردد در این حالت مسئولیت مدنی ناشی از خطای قرارداد هوشمند با چه شخص یا اشخاصی است. در ادامه جهت درک صحیح‌تر عملکرد قراردادهای هوشمند ضمن بررسی ویژگی‌های قراردادهای هوشمند و تبیین دقیق‌تر ماهیت خطا، به شناسایی و بررسی عواملی که می‌توانند مسئول جبران خسارت ناشی از خطای قرارداد هوشمند باشند، خواهیم پرداخت.

---

[۱] قراردادهای هوشمند به عنوان نسل سوم قراردادهای الکترونیکی شناخته می‌شوند (ناصر، ۱۳۹۷: ۳۸) زیرا این قراردادها نیز به مانند قراردادهای الکترونیکی در فضای سایبری منعقد می‌شوند اما دارای تفاوت‌هایی هم هستند، مهم‌ترین این تفاوت‌ها آن است که برخلاف نسل‌های قبلی قراردادهای الکترونیکی که به زبان انسانی منعقد می‌شدند (O'Shields, 2017: 181) و بدون این که نیاز به تجزیه و تحلیل مفاد قرارداد باشد، طبق دستورالعمل خود، در صورتی که طرف مقابل نیز مطابق دستورالعمل عمل نماید، اقدام به انعقاد قرارداد می‌نمودند و غالبا پس از انعقاد قرارداد، باید آثار آن در عالم واقع طرفین قرارداد جاری شود اما قراردادهای هوشمند می‌توانند به کمک هوش مصنوعی که وظیفه تحلیل کد رمزنگاری شده قرارداد هوشمند را دارد (ناصر، ۱۳۹۷: ۴۲) مفاد قرارداد را تجزیه و تحلیل نموده و سپس آن‌ها را به صورت خود به خود اجرا (Self-executing) می‌نمایند، بدون آن که نیاز به دخالت عوامل انسانی در ایجاد این آثار حقوقی باشد.

[۲] Smart Contract

[۳] Electronic Signatures

[۴] Artificial Intelligence (AI)

[۵] Crypto Currencies

[۶] Distribute Ledgers

[۷] Blockchain

[۸] Ethereum

[۹] قراردادهای هوشمند به علت ویژگی‌های خود، مانند خوداجرایی، کدهای رمزنگاری شده، امنیت اطلاعات، حذف واسطه‌ها و...، در میان کاربران فضای سایبری محبوبیت یافته است چرا که این ویژگی‌ها سبب گردیده تا ضمن آن که مفاد قراردادی بین طرفین به صورت رمزنگاری است و شخص جز طرفین قرارداد نمی‌تواند از آن‌ها مطلع شود، امکان هک یا نفوذ به آن‌ها نیز ممکن نیست (ناصر، ۱۳۹۷: ۶۰) و علاوه بر آن هوش مصنوعی‌ای که وظیفه تحلیل و اجرای مفاد قرارداد هوشمند را دارد بدون دخالت طرفین و به طور خودکار مفاد قراردادی را مطابق با دستورالعمل‌های تعریف شده اجرا می‌نماید و همین امر سبب صرفه جویی در وقت و هزینه‌های طرفین قرارداد می‌شود و نیز در صورتی که به دلایلی مانند عدم وجود موجودی مالی کافی نزد یکی از طرفین قرارداد جهت اجرای تعهد، هوش مصنوعی می‌تواند این اطلاعات را تحلیل و از اجرای تعهدات طرف دیگر به نفع او جلوگیری و از تضرر طرفین قرارداد پیشگیری نماید.

[۱۰] Error

۱. قرارداد هوشمند

قراردادهای هوشمند را می‌توان چنین شرح داد که برنامه‌های کامپیوتری خوداجرایی که به ورودی‌های داده واکنش نشان می‌دهند و شرایط را مطابق دستورالعمل‌های کدگذاری شده خود برای تولید خروجی‌های مختلف اعمال می‌کنند (Giancaspro, 2022: 56). به علت نوآورانه بودن فناوری قراردادهای هوشمند هنوز تعریفی که بتواند به طور کامل و جامع وصف کننده قرارداد هوشمند باشند، ارائه نشده است اما از بررسی تعاریف بیان شده برای قراردادهای هوشمند می‌توان چنین یافت که مهم‌ترین ویژگی‌های قراردادهای هوشمند عبارت است از: ۱- قراردادهای هوشمند، قراردادهایی هستند که از تکنولوژی بلاکچین[۱] بهره‌مند می‌باشند (ناصر، ۱۳۹۷: ۴۳). با توجه به آن که اکثر بلاکچین‌ها به صورت غیرمتمرکز[۲] هستند به تبع آن قراردادهای هوشمند مبتنی بر آن‌ها نیز غیرمتمرکز می‌باشند (غیرمتمرکز بودن قراردادهای هوشمند). در بلاکچین، تمرکززدایی به انتقال کنترل و تصمیم گیری از یک نهاد متمرکز (فرد، سازمان یا گروه آن) به یک شبکه توزیع شده اشاره دارد، شبکه‌های غیرمتمرکز تلاش می‌کنند تا سطح اعتمادی را که شرکت‌کنندگان باید به یکدیگر داشته باشند، کاهش دهند و از توانایی آن‌ها برای اعمال قدرت یا کنترل بر یکدیگر به شیوه‌هایی که بازدهی شبکه را کاهش می‌دهند، جلوگیری کنند. ۲- در قراردادهای هوشمند به محض منعقد شدن قرارداد یا در زمانی که متعاقدین معین می‌نمایند قرارداد به اجرا درمی‌آید (خوداجرایی قراردادهای هوشمند) (ناصر، ۱۳۹۷: ۸۲). ۳- با عنایت به اینکه این قراردادها تحت نظر یک سیستم منعقد شده و این سیستم امکان بازخوانی قرارداد را دارد، امکان ذکر شروط باطل یا مبهم یا شروط باطل و مبطل در قرارداد در این نوع قراردادها توسط هر کدام از طرفین یا هردو، آگاهانه یا غیرآگاهانه ممکن نیست (شفافیت قراردادهای هوشمند) (ناصر، ۱۳۹۷: ۹۲). ۴- پس از تایید و ذخیره اطلاعات در بلاکچین، نمی‌توان آن‌ها را تغییر داد یا حذف کرد به همین دلیل بلاکچین ماهیتا محیطی غیرقابل تغییر و ایمن برای مبادله[۳]هاست که درجه بالایی از شفافیت را بین متعاقدین تضمین می‌کند (غیرقابل تغییربودن مفاد قرارداد هوشمند) (Roumpos, 2020: 11). این ویژگی قراردادهای هوشمند نیز به علت همتا به همتا (P2P[۴]) بودن سیستم بلاکچین می‌باشد.

برخلاف توسعه نرم افزارهای سنتی، کاربران نمی‌توانند هیچ ضرری را که در حین انجام مبادله‌ها در سیستم مالی مبتنی بر بلاکچین که با استفاده از قراردادهای هوشمند تجربه می‌کنند، جبران نمایند زیرا کد قرارداد هوشمند پس از استقرار در بلاکچین قابل تغییر نیست (Zou و همکاران، ۲۰۲۱: ۶). همین امر که به علت ویژگی‌های مطرح شده بلاکچین است نیز ضروری می‌سازد تا مسئولیت مدنی اشخاصی که ممکن در نتیجه اعمال آنان قرارداد هوشمند دچار خطایی در اجرای مفاد قراردادی شود مشخص و شناسایی شود تا بتوان از بروز این خطاها پیشگیری نمود.

۲. خطا

اشتباه، تصور خلاف واقعی است از چیزی مادی یا معنوی (جعفری لنگرودی، ۱۳۸۸: ۴۵). احتمال وقوع اشتباه در قراردادهای الکترونیکی و قراردادهای هوشمند غالبا هنگامی رخ می‌دهد که متعاقدین درباره مسائلی چون نوع عقد، موضوع عقد، جهت معامله، طرف معامله یا آثار عقد دارای تطابق اراده نیستند و هر یک از طرفین به اشتباه قصد متفاوتی دارند که بسته به نوع اشتباه صورت گرفته، کمااینکه در مواد ۱۹۹ الی ۲۰۱ قانون مدنی ایران نیز بیان شده، می‌تواند منجر به ایجاد حق فسخ یا بطلان قرارداد گردد. برخی از نویسندگان این نوع اشتباه در

---

[۱] بلاکچین یک پایگاه توزیع شده مشترک است که سوابق تمام مبادله‌های انجام شده توسط اعضای شبکه را ذخیره می‌کند. از نظر فنی، بلاکچین شامل مجموعه‌ای از بسته‌های داده (بلاک) است که در آن یک بلاک قطعات دیجیتالی اطلاعات مربوط به چندین مبادله را ذخیره می‌کند. داده‌های ذخیره شده در داخل بلاک به نوع بلاکچین بستگی دارد. هر بلاک به جز داده‌های مربوط به مبادله‌های ذخیره شده حاوی هش رمزنگاری شده است که همه بلاک‌ها فهرستی از آن را شناسایی و ذخیره می‌کنند و هش‌ها به طور خودکار توسط یک تابع الگوریتم محاسبه می‌شود که داده‌ها را به کدی از اعداد و حروف تبدیل می‌کند (Roumpos, 2020:9).

[۲] Decentralize

Transaction

[۴] سیستم همتا به همتا (Peer-to-Peer) یک پلتفرم غیرمتمرکز است که به موجب آن دو فرد مستقیما بدون واسطه شخص ثالث با یکدیگر تعامل دارند. در عوض، طرفین قرارداد مستقیما از طریق سیستم P۲P با یکدیگر معامله می‌کنند (Hayes, 2021).

قراردادهای الکترونیکی را به دو حالت «خطای وارداتی» و «خطای محض» تقسیم کرده‌اند (حبیب زاده، ۱۳۹۲: ۴۰) که البته با آنچه در این نوشتار به عنوان خطا دانسته شده، تفاوت دارد.

اما آنچه در این پژوهش مورد بررسی قرار می‌گیرد خطاهای قرارداد هوشمند است. خطا مقابل عمد است و آن عبارت است از وصف عملی که فاعل آن دارای قوه تمیز نبوده و به علت غفلت یا نسیان یا جهل یا بی مبالاتی و عدم احتیاط عملی را که مخالف موازین اخلاق یا قانون است مرتکب شده شده است (جعفری لنگرودی، ۱۳۸۸: ۲۶۳). خطا ناشی از عملکرد نادرست یک سیستم الکترونیکی، خراب بودن، نقص فنی و غیره است ولی اشتباه به امور ذهنی مربوط می‌شود (آهنگران و احمدی، ۱۳۹۸: ۴). علی رغم آن که قانون مدنی ایران درباره وقوع اشتباه در روابط قراردادی قاعده‌ای را بیان نموده که قابل اعمال در قراردادهای هوشمند نیز است اما در قوانین ایران، من جمله قانون تجارت الکترونیکی مصوب ۱۳۸۲ در خصوص خطا در انعقاد قراردادهای الکترونیکی و به تبع آن قراردادهای هوشمند ساکت است. بنابراین لازم است تا ابتدائا تعریفی از خطا در قراردادهای هوشمند ارائه شود. یک خطا، اتفاقی است که به دلایلی مثل نقص فنی در کدگذاری قرارداد هوشمند باعث می‌شود که قرارداد هوشمند فراتر از دستورالعمل‌های برنامه ریزی شده خود عمل کند، این خطا به این معناست که به هیچ وجه مقصود متعاقدین نبوده یا از وقوع آن مطلع نبوده‌اند زیرا طرف‌های انسانی قرارداد از قبل نمی‌توانستند وقوع این خطا در قرارداد را پیش بینی کنند (Giancaspro, 2022: 72). برخی نویسندگان این نوع خطا را «خطای سامانه خودکار» نامیده‌اند (حبیب زاده، ۱۳۹۲: ۴۰). خطاهای قرارداد هوشمند دارای سه ویژگی می‌باشند: اگرچه متحمل هستند اما شایع و منطقی نیستند. به طور غیرعمدی بروز می‌یابند و هرگز ارادی نیستند. نامطلوب هستند و هیچ انسان منطقی‌ای چنین تصمیمی نمی‌گیرد (Giancaspro, 2022: 72). بنابراین آنچه به عنوان خطا در این پژوهش مدنظر است حالتی است که قرارداد هوشمند، به عنوان یک سیستم خوداجرا، اقدام به تحلیل و اجرای کدهای قرارداد هوشمند می‌نماید اما به عللی مثل ایرادات فنی در برنامه نویسی، اختلال در بلاکچین، عدم دریافت اطلاعات معتبر و... نتیجه‌ای را به اجرا می‌گذارد که متعاقدین به هیچ عنوان قصد آن را نداشته‌اند و همچنین انتظار وقوع چنین اثری را از قرارداد نداشته‌اند یا گاها بنا به علل بیان شده قرارداد هوشمند هیچ اثری از کدهای قرارداد را به اجرا نمی‌گذارد؛ که این تعریف با آنچه به عنوان خطا در ادبیات حقوقی ایران دانسته می‌شود تطابق نزدیک‌تری دارد. به عنوان مثالی برای خطای قرارداد هوشمند می‌توان به خطای قرارداد هوشمند The DAO در سال ۲۰۱۶ اشاره نمود که برای حمایت از پروژه‌های بلاکچینی نوشته شده بود و در آن خطایی منطقی وجود داشت که این خطا باعث شد هکری بتواند ۵۰ میلیون دلار اتر از شبکه اتریوم را به حساب خود منتقل کند[۱]. یا در مثالی دیگر، در ۱۴ سپتامبر ۲۰۲۱ بلاکچین سولانا[۲] به علت اضافه بار به وجود آمده که سبب ایجاد اختلال در بیشتر نودهای اعتبارسنج[۳] سولانا شده بود منجر به قفل شدن شبکه و ایجاد اختلال در کلیه قراردادهای هوشمند مبتنی بر بلاکچین سولانا به مدت حدود ۱۷ ساعت شده بود[۴].

قانون تجارت الکترونیک مصوب ۱۳۸۲ درباره خطا قراردادهای الکترونیکی و به تبع آن، قراردادهای هوشمند سکوت نموده و هیچ حکمی پیرامون مسئولیت مدنی ناشی از خطاهای قراردادهای هوشمند نیز بیان ننموده بنابراین لاجرم برای دست یافتن به حکم این مسائل باید به قواعد عام مسئولیت مدنی در حقوق ایران رجوع نماییم. مسئولیت مدنی در حقوق ایران چنین تعریف گردیده است:«هر کس به دیگری ضرر بزند باید آن را جبران کند، مگر در مواردی که اضرار به غیر به حکم قانون باشد یا ضرری که به شخص وارد آمده است ناروا و نامتعارف جلوه نکند» (کاتوزیان، ۱۳۸۸: ۱۳). یکی از وجوهی، که به عنوان هدف مسئولیت مدنی ابراز شده، ارضاء خاطر یا جذب رضایت زیان دیده است بنابراین، ورود ضرر شرط موضوعی مسئولیت مدنی است (باریکلو، ۱۳۹۲: ۴۰) و یکی از شرایط این ضرر آن است که بر طبق مسیر طبیعی و متعارف امور، احتمال ورود آن به مراتب بیشتر باشد (کاتوزیان، ۱۳۸۸: ۴۸) و به طور متعارف قابل پیش بینی باشد. به نظر می‌رسد در خصوص شرط قابل پیش بینی بودن ضرر در فضای مجازی (و به تبع آن خطاهای قرارداد هوشمند)، باید دایره لزوم شرط ضررهای قابل پیش بینی را محذوف یا حتی الامکان مضیق‌تر از فضای واقعی تلقی نمود زیرا ماهیت این فضا به گونه‌ای است که ممکن است نه تنها نوع، مقدار و گستره

[۱] برای مطالعه بیشتر پیرامون ابعاد فنی و حقوقی هک قرارداد هوشمند The DAO رجوع کنید به:
Kolber, Adam. (2018). Not-So-Smart Blockchain Contracts and Artificial Responsibility. Stanford Technology Law Review, Vol 21.

[۲] Solana

[۳] Validator

[۴] امیریان، آرن. (به روزرسانی ۲۵ اردیبهشت ۱۴۰۲). وقوع اختلال در شبکه سولانا؛ هفته قبل چه اتفاقی برای این شبکه افتاد؟.
https://mihanblockchain.com/disruption-of-the-solana-network/

ضرر برای آن عامل قابل پیش بینی نباشد بلکه شخص یا اشخاص زیان‌دیده نیز به طور مشخص مورد هدف و شناخت زیان‌رسان نیستند (ملکوتی، ۱۴۰۱: ۷۲). به عنوان مثال در هک The DAO طبیعتا هکر هدف مشخصی از برداشت اترهای شخص خاصی از اعضای این قرارداد هوشمند را نداشته است و پس از هک قرارداد، تا جایی که میسر بود اقدام به برداشت اترهای موجود در ولت[۱]های متصل به این قرارداد هوشمند نمود.

رکن دیگر در تحقق مسئولیت مدنی، فعل زیانباری است که در نظر اجتماع ناهنجار باشد و اخلاق عمومی ورود ضرر را ناشایسته بداند (کاتوزیان، ۱۳۸۸: ۵۷) کمااینکه در ماده ۱ قانون مسئولیت مدنی[۲] مصوب ۱۳۳۹ نیز به این مورد تصریح شده است. به طور کلی در حقوق ایران می‌توان گفت که ملاک تشخیص فعل زیان‌بار در فضای مجازی همانند ملاک‌های دنیای واقعی است. در جهان واقعی فعل زیان‌بار در قالب چهارگانه ماده ۳۰۷ قانون مدنی[۳] و در سایر موارد تحت عنوان ماده ۱ قانون مسئولیت مدنی مصوب ۱۳۳۹ و قاعده لاضرر تبیین می‌شوند، همین ملاک‌ها و منابع در فضای مجازی نیز قابلیت استفاده دارند (ملکوتی، ۱۴۰۱: ۷۶) بنابراین هر فعالیتی که ناشی از خطای قرارداد هوشمند باشند و به نوعی بتوان در محدوده‌ی یکی از قالب‌های بیان شده تعریف کرد، می‌تواند مصداق فعل زیان‌بار باشد، به عنوان مثال در مورد قفل شدن قراردادهای هوشمند مبتنی بر سولانا به مدت ۱۷ ساعت در سال ۲۰۲۱، سبب ورود ضرر به طرفین قراردادهای هوشمند گردیده و در نتیجه توقف اجرای قراردادهای هوشمند ممکن است طرفین آن دچار ضررهای مالی یا ضررهای شغلی در مشاغل مبتنی بر بلاکچین سولانا شده باشند که این فعل‌های زیان‌بار در قالب قاعده لاضرر قابل توجیه است.

در نهایت سومین رکن ایجاد مسئولیت مدنی وجود رابطه سببیت میان ضرر و فعل زیان‌بار است. باید احراز شود که بین دو عامل ضرر و فعل زیان‌بار رابطه سببیت وجود دارد، یعنی ضرر از آن فعل ناشی شده است (کاتوزیان، ۱۳۸۸: ۷۹) و آنچه در استناد ضرر به فعل زیان‌بار در حقوق ایران مورد قبول است استناد عرفی است. مطابق این نظریه، همین که عرف ضرر وارده به زیان‌دیده را مستند به زیان‌رسان بداند، جبران خسارت بر عهده زیان‌رساننده می‌باشد و استناد عرفی عمل زیان‌بار به زیان‌رساننده برای مسئول شناختن وی کافی است. در این دیدگاه، تقصیر تنها یکی از راه‌هایی است که نشان دهنده استناد ضرر به زیان‌رساننده می‌باشد اما حتی در صورت عدم تقصیر زیان‌رساننده نیز اگر عمل زیان‌بار مستند به او فعل او باشد باید خسارت را جبران نماید (هوشمند فیروزآبادی، ۱۳۹۸: ۲۹۹). بنابراین بدیهی است اگر نتوان ضرر را به فعل زیان‌بار شخصی نسبت داد نمی‌توان از وی تقاضای جبران خسارت نمود و این رکن در مسئولیت مدنی ناشی از خطاهای قرارداد هوشمند نیز وجود دارد اما به مانند ارکان پیشین مسئولیت مدنی، این رکن در مسئولیت مدنی فضای سایبر نیز تفاوت‌هایی با مسئولیت مدنی در دنیای واقعی دارد. برای احراز ارتباط میان فعل زیان‌بار و خسارت وارده باید ملاک را سببیت فنی قرار داد که مفهومی اعم از سببیت عرفی در مسئولیت مدنی سنتی است. مفهوم سبب فنی این است که با عنایت به اقتضائات و خصوصیات فضای مجازی (که قراردادهای هوشمند نیز در همین فضا هستند)، اگر از نظر فنی بتوان عمل ارتکابی را به عامل زیان منتسب کرد، مسئولیت مدنی برای او محقق شده است، هرچند نتوان خسارت حاصله را به طور کامل مربوط به آن عمل دانست (ملکوتی، ۱۴۰۱: ۷۷). در فضای مجازی برای تحقق سببیت، اثبات ارتباط میان فعل زیان‌بار و عامل ارتکاب آن کافی می‌باشد، یعنی همین که اثبات شد که عمل موجب زیان را، خوانده مرتکب شده است سببیت در ارتباط با او محقق شده است و نیازی به اثبات زیان برای تحقق سببیت نیست، اگرچه در پایان برای تحقق مسئولیت مدنی نیاز به اثبات ورود ضرر ضروری است و علت حذف ارتباط ضرر و فعل ارتکابی در فضای مجازی این است که ضرر و فعل زیان‌بار در فضای مجازی در بسیاری از موارد قابل اندازه گیری و رهگیری نیست (ملکوتی، ۱۴۰۱: ۷۷). به عنوان مثال در ۱۰ اوت ۲۰۲۱ دومین سرقت و هک بزرگ تاریخ ارز دیجیتال در پلتفرم پالی

---

[۱] ولت (کیف پول رمزنگاری شده Wallet) اپلیکیشنی است که به عنوان کیف پول برای ارز دیجیتال عمل می‌کند و به این دلیل ولت نامیده می‌شود زیرا مانند کیف پولی که پول نقد و کارت را در آن قرار می‌دهید می‌باشد، با این تفاوت که به جای نگه داشتن پول فیزیکی، کلیدهای عبوری را که برای امضای مبادله-های ارز دیجیتال استفاده می‌شود، در آن ذخیره می‌گردد و پل ارتباطی است که امکان دسترسی به ارزهای دیجیتال موجود در آن را می‌دهد (Frankenfield, 2023).

[۲] ماده ۱ قانون مسئولیت مدنی مصوب ۱۳۳۹:«هر کس بدون مجوز قانونی عمدا یا در نتیجه بی احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود مسئول جبران خسارت ناشی از عمل خود می‌باشد.»

[۳] ماده ۳۰۷ قانون مدنی:«امور ذیل موجب ضمان قهری است: ۱- غصب و آنچه که در حکم غصب است؛ ۲- اتلاف؛ ۳- تسبیب؛ ۴- استیفاء»

نتورک، که پلتفرم قراردادهوشمند برای تبادل توکن‌ها بین بلاکچین‌های مجزا نظیر بیت کوین و اتریوم بود، رخ داد و مبلغی معادل ۶۱۱ میلیون دلار از توکن‌های پالی نتورک به سرقت رفت و علی رغم بازگشت کل توکن‌های به سرقت رفته توسط هکر به علت عدم توانایی در نقدسازی آن‌ها (Behnke, 2023)، هیچ گاه هویت حقیقی هکر مشخص نگردید تا بتوان در دنیای واقعی، او را مسئول جبران خسارات وارده به کاربران این پلتفرم دانست.

۳. عوامل موجب مسئولیت مدنی ناشی از خطای قرارداد هوشمند

قراردادهای هوشمند فناوری جدیدی هستند که هنوز بسیاری از ابعاد حقوقی آن‌ها ناشناخته مانده یا مورد بررسی قرار نگرفته است. همان طور که بیان شد ابعاد مرتبط با مسئولیت مدنی ناشی از خطای قراردادهای هوشمند نیز ناشناخته است و در این پژوهش تلاش گردیده تا به این بعد از قراردادهای هوشمند بپردازیم و به مانند آنچه پیش‌تر بیان شد مسائل حقوقی مرتبط با آن را شناسایی نماییم. در قراردادهای هوشمند، عواملی که می‌تواند منجر به بروز خطا در عملکرد آن‌ها گردد و مسئولیت مدنی ایجاد کند نیز از قاعده اخیر مستثنی نیست و به علت نوآورانه بودن این فناوری و تازگی ابعاد گوناگون آن نمی‌توان به طور کامل و قاطع کلیه عواملی که سبب بروز مسئولیت مدنی در هنگام خطای قراردادهای هوشمند می‌شوند را بیان نمود اما می‌توان با بررسی عوامل رایجی که در سال‌های اخیر سبب بروز خطاهای مختلف در قراردادهای هوشمند شده‌اند را شناسایی و مسئولیت مدنی در فرض وقوع آن خطاها را تعیین نمود.

طبق بررسی‌های عینی انجام شده، رایج‌ترین خطاهای قرارداد هوشمند را می‌توان به این موارد تقسیم نمود: وجود خطا در کدها، ناسازگاری با پروتکل بلاکچین، فراموش کردن تابع Selfdestruct[۱]، استفاده نادرست از Delegatecall[۲]، حملات بازگشت ناپذیر[۳]، حملات اوراکل، حملات Underflow/Overflow[۴]، حملات[۵] Front Running (توایی، ۱۴۰۲) خطاهای منطقی[۶] و تعیین سطح دسترسی[۷] (Yatchenko, 2022). که با بررسی هر یک از این خطاها، می‌توان حداقل چهار عامل بلاکچین، هوش مصنوعی، اوراکل یا توسعه دهنده قراردادهوشمند را مسئول خطاهای قرارداد هوشمند دانست که در ادامه مسئولیت هر یک از آن‌ها را به تفکیک مورد بررسی قرار خواهیم داد.

[۱] زمانی رخ می‌دهد که قرارداد هوشمند فاقد تابع Selfdestruct باشد؛ تابع Selfdestruct به طور پیش‌فرض در زبان برنامه‌نویسی Solidity موجود است و به قرارداد هوشمند اجازه می‌دهد خود را حذف کرده و دارایی‌های خود را به آدرسی دلخواه منتقل کند (توایی، ۱۴۰۲).

[۲] استفاده نادرست از Delegatecall ، زمانی رخ می‌دهد که قرارداد هوشمند از تابع Delegatecall به صورت نادرست یا بدون احتیاط استفاده کند؛ در برنامه‌نویسی قراردادهای هوشمند، تابع Delegatecall ، اپ‌کدی است که به قرارداد امکان می‌دهد تا تابعی را از قرارداد دیگری فراخوانی کند؛ این بدان معنا است که قرارداد می‌تواند کد قرارداد دیگری را بدون اینکه آن قرارداد را به طور مستقیم فراخوانی کند، اجرا کند (توایی، ۱۴۰۲).

[۳] حملات بازگشت‌پذیر (Reentrance) نوعی حمله امنیتی به قراردادهای هوشمند به حساب می‌آیند که که در آن هکر با استفاده از تابعی به نام Fallback ، برای فراخوانی مجدد استفاده می‌کند. این امر می‌تواند منجر به از دست دادن دارایی‌ها، سرقت اطلاعات، یا اختلال در عملکرد قراردادهای هوشمند شود (Yatchenko, 2022).

[۴] حملات Underflow/Overflow زمانی رخ می‌دهد که قرارداد هوشمند در حین انجام عملیات ریاضی، با مقادیری خارج از محدوده متغیرهای خود روبه‌رو شود که مسئله، ممکن است باعث شود تا قرارداد هوشمند به صورت ناخواسته، پول را افزایش یا کاهش دهد (توایی، ۱۴۰۲).

[۵] استفاده نادرست از Delegatecall ، زمانی رخ می‌دهد که قرارداد هوشمند از تابع Delegatecall به صورت نادرست یا بدون احتیاط استفاده کند؛ در برنامه‌نویسی قراردادهای هوشمند، تابع Delegatecall ، اپ‌کدی است که به قرارداد امکان می‌دهد تا تابعی را از قرارداد دیگری فراخوانی کند؛ این بدان معنا است که قرارداد می‌تواند کد قرارداد دیگری را بدون اینکه آن قرارداد را به طور مستقیم فراخوانی کند، اجرا کند (توایی، ۱۴۰۲).

[۶] خطاهای منطقی ممکن است شامل خطاهای تایپی، تفسیر نادرست مشخصات و خطاهای برنامه‌نویسی جدی‌تر باشد که امنیت قراردادهای هوشمند را کاهش می‌دهد (Yatchenko, 2022).

[۷] سطح دسترسی پیش فرض (Default visibility) مشخص می‌کند که آیا یک تابع می‌تواند به صورت داخلی یا خارجی توسط کاربران فراخوانی شود. زمانی که توسعه دهندگان قراردادهای هوشمند سطح دسترسی عملکردهایی را که باید خصوصی یا فقط در خود قرارداد قابل فراخوانی باشند، مشخص نمی کنند، مشکل ساز می‌شود (Yatchenko, 2022).

۱،۳. بلاکچین

قراردادهای هوشمند مبتنی بر بلاکچین هستند[۱] و بنابراین کلیه اطلاعات در بلاکچین و قراردادهای مبتنی بر آن به صورت داده‌هایی رمزنگاری شده کدنویسی و ذخیره می‌گردد که این امر دارای مزایای فراوانی از جمله کاهش احتمال هک و دستکاری اطلاعات موجود در بستر بلاکچین است. در این بستر، مشکلی که یک هکر با آن مواجه می‌باشد این است که به جهت وجود فرآیند رمزنگاری اطلاعات ذخیره شده، در وهله اول هکر از محل اصلی و بلاک اصلی که داده پیام‌های مدنظر او در آن ذخیره شده است، اطلاعی ندارد، بر فرض هم که بتواند بر آن دسترسی پیدا کند، تغییر هش بلاک آن بلاک منجر به بهم خوردن نظم موجود در آن زنجیره شده و دسترسی وی به آن زنجیره قطع می‌شود (ناصر، ۱۳۹۷: ۶۰). اما با این وجود نوع خاص برنامه نویسی بلاکچین و عدم مطابقت کد نرم افزارهای مبتنی بر بلاکچین با آن یا وجود نقص-هایی در برنامه نویسی بلاکچین که می‌تواند منجر به ضعف در اجرای بلاکچین یا نرم افزارهای مبتنی بر آن شود باعث می‌گردد خطاهایی برای نرم افزارهای مبتنی بر بلاکچین مثل قراردادهای هوشمند رخ دهد. برای مثال در سال ۲۰۱۷، قرارداد هوشمند Parity Multisig Wallet که برای نگهداری و انتقال اتر بود، به دلیل ناسازگاری با پروتکل اتریوم باعث شد تا قرارداد دچار خطا گردد و حدود ۵۱۴ میلیون دلار، ارز دیجیتال قفل شده و دسترسی به آن غیرممکن شود (توایی، ۱۴۰۲) که علت این امر ناسازگاری این قرارداد هوشمند با پروتکل بلاکچین مبتنی بر آن بود. پیش از بررسی مسئولیت مدنی ناشی از خطای قرارداد هوشمند که عامل بلاکچین در آن دخیل است، باید توجه داشت درست است که در فرض اخیر به علت ناسازگاری بلاکچین، قرارداد هوشمند دچار خطا گردیده اما اگر این خطا در حالتی رخ داده که توسعه دهندگان قرارداد هوشمند نسبت به بررسی کدها و پروتکل بلاکچین مربوطه کوتاهی کرده‌اند و بدون بررسی قرارداد هوشمند را بر روی آن اجرا نموده‌اند باید آن‌ها را مسئول جبران خسارات وارده دانست، که این موضوع در مباحث آینده مورد بررسی قرار خواهد گرفت، اما اگر این خطا در فرضی به وقوع پیوسته که قرارداد هوشمند ابتدائا با بلاکچین سازگار بوده اما به علت ایجاد تغییرات در پروتکل توسط توسعه دهندگان بلاکچین، دچار خطا شده است، به نظر می‌رسد باید در دو فرض تمایز قائل شد: اگر توسعه دهندگان بلاکچین پیش از تغییرات، به نحوی از انحاء نسبت به اطلاع رسانی تغییرات و زمان اعمال تغییرات اقدام کرده باشند، در این صورت نمی‌توان فعل زیان‌بار ناشی از خطای قرارداد هوشمند را به آن‌ها نسبت داد چرا که هشدار لازم و ضرورت همگام سازی نرم افزارهای مبتنی بر بلاکچین با تغییرات آتی را اطلاع رسانی کرده‌اند و در صورت بروز خطا باید توسعه دهندگان قرارداد هوشمند که نسبت به همگام سازی قرارداد هوشمند با تغییرات آتی بلاکچین کوتاهی نموده‌اند مسئول جبران خسارات وارده دانست. اما در فرضی که تغییرات در پروتکل بلاکچین بدون اطلاع رسانی بوده یا بدون رعایت استانداردهای حرفه‌ای[۲] اقدام به توسعه بلاکچین نموده‌اند و سبب خطا در قراردادهای هوشمند مبتنی بر آن شده‌اند، به نظر می‌رسد باید توسعه دهندگان بلاکچین را مسئول جبران خسارات وارده دانست. متخصصین فضای مجازی، ملاک را در خلق برنامه‌ها و تولیدات فضای مجازی بر پایه معیارها و استانداردهای معقولی پایه گذاری کرده‌اند و عدول از ورود زیان در نتیجه عدول از استانداردهای حرفه‌ای و معقول در تولید یک نرم افزار است که فعل تقصیر محسوب و در نتیجه محقق عنصر مادی فعل زیان‌بار خواهد شد (ملکوتی، ۱۴۰۱: ۷۴). بنابر آنچه بیان شد به نظر می‌رسد می-توان با وحدت ملاک از نظر اخیر آن را به توسعه دهندگان بلاکچین و قراردادهای هوشمند نیز تعمیم داد و نتایج بیان شده را به دست آورد. گرچه برخی نویسندگان معتقدند احتمال عملکرد نادرست قراردادهای هوشمند در اثر بلاکچین آن کم است زیرا احتمال نقص یا هک شدن بلاکچین کم است، بنابراین مسئولیت سازندگان بلاکچین در این موارد بسیار مورد تردید است (Kirill, 2018: 12) اما بنابر آنچه بیان شد و مثال‌های ذکر شده مشاهده می‌شود که هر چند میزان خطای قراردادهوشمند در اثر بلاکچین آن کم است، اما بعید نیست و لازم است تا این خطاها در موارد مختلف بررسی و مسئول جبران کننده خسارات مشخص شود.

در پاره‌ای از موارد مانند قفل شدن بلاکچین سولانا در سال ۲۰۲۱ تعیین مسئول جبران خسارات وارده می‌تواند با سهولت بیشتری انجام گیرد چرا که در مورد اخیر قفل شدن و ایجاد اختلال در قراردادهای هوشمند مبتنی بر آن به علت عدم پیش بینی جهت توسعه به موقع بلاکچین

---

[۱] از آنجا که بلاکچین یک بستر غیرمتمرکز است که جهت ثبت اطلاعات مبادلات کاربرد دارد و علاوه بر آن داده‌ها در آن به صورت رمزنگاری شده وجود دارند و هوش مصنوعی اطلاعات ثبت شده تحلیل، اجرا و ثبت می‌کند (ناصر، ۱۳۹۷: ۵۹)، سبب می‌شود تا مناسب‌ترین و تنهاترین بستری باشد که امکان اجرای قراردادهای هوشمند با ویژگی‌های بیان شده در آن وجود داشته باشد، به همین علت بیان می‌شود که قراردادهای هوشمند مبتنی بر بلاکچین هستند.

[۲] Professional Value

سولانا و عدم رفع نقص‌های برنامه نویسی آن بوده است و می‌توان توسعه دهندگان این بلاکچین را مسئول جبران خسارات وارده دانست. همچنین لازم به ذکر است بلاکچین‌ها بر دو نوع‌اند: بلاکچین عمومی (بدون مجوز) که بدون هیچ کنترل متمرکزی در شبکه کامپیوتری به رایگان وجود دارد مانند بلاکچین بیت کوین و بلاکچین خصوصی (با مجوز) که توسط سازندگان آن راه اندازی شده و در شبکه بلاکچین سازندگان مذکور نیز حضور دارند (Kirill, 2018: 10) مانند بلاکچین Hyperledger Fabric IBM که بررسی نحوه شناسایی و مسئول دانستن اشخاص در فرضی که بلاکچین عمومی است و سازنده یا توسعه دهندگان آن نامعلوم هستند جای تأمل و بررسی دارد که از حوصله این نوشتار خارج است.

۲،۳. هوش مصنوعی

قراردادهای هوشمند، نوعی پیشرفته از قراردادهای الکترونیکی هستند که از زمان انعقاد تا نهایی شدن توسط هوش مصنوعی[۱] مورد نظارت قرار می‌گیرند (ناصر، ۱۳۹۷: ۴۵). این سیستم وظیفه بازخوانی مفاد قرارداد، ثبت، عرضه قرارداد در بستر بلاکچین، تایید نهایی، تطبیق قرارداد با دستورالعمل داده شده به آن و مواردی مانند استخراج اطلاعات از پایگاه‌های داده اوراکل را برعهده دارد (ناصر، ۱۳۹۷: ۴۶). پیشرفته‌ترین نوع هوش مصنوعی، سیستم خبره[۲] است که در قراردادهای هوشمند مورد استفاده قرار می‌گیرد. این سیستم‌ها به عنوان سیستم‌های هوشمند کامپیوتری از دانش و روش استنتاج برای حل مسائلی که نیاز به مهارت و صرف وقت فراوان توسط عامل انسانی دارند، استفاده می‌نمایند (ناصر، ۱۳۹۷: ۶۸). استفاده از هوش مصنوعی در کنار کلیه مزایا و برتری‌هایی که برای قراردادهوشمند ایجاد کرده، مانند فراهم کردن ویژگی خوداجرایی قراردادهوشمد و عدم امکان درج شروط باطل و مبهم در قرارداد هوشمند یا حتی شناسایی و رفع باگ‌های قراردادهوشمند[۳]، اما ممکن است در مواردی سبب ایجاد خطا در اجرای قراردادهوشمند نیز گردد. غالبا سیستم هوش مصنوعی، سیستمی متمرکز است[۴] و متمرکز بودن این سیستم می‌تواند منجر به نفوذ به آن و دستکاری اطلاعات یا ورود اطلاعات تغییریافته به سیستم هوش مصنوعی شود و در نتیجه این عمل، هوش مصنوعی اقدام به تحلیل کدهای قراردادی برخلاف آنچه مورد انتظار متعاقدین است می‌نماید که نهایتا قراردادهوشمند با خطا مواجه می‌شود یا ممکن است کدهای برنامه نویسی خود هوش مصنوعی به علت نقص یا ابهام، سبب خطا در تحلیل و تصمیم گیری هوش مصنوعی ناظر بر قراردادهوشمند شود.

در این موارد بیان اینکه چون خطا توسط یک رایانه هوشمند یا یک الگوریتم صورت گرفته پس هیچ کس مسئول نیست نمی‌تواند صحیح باشد چرا که در صورت وقوع همین خطا توسط عامل انسانی، او را مسئول جبران خسارات می‌دانستیم (Soyer & Tettenborn, 2022: 387). به عقیده برخی از نویسندگان، مسئول شناختن هوش مصنوعی به سه عامل بستگی دارد: ۱- توجه به ظرفیت‌های هوش مصنوعی و تشریح این ظرفیت برای متعاقدین قراردادهوشمند. ۲- سیستم هوش مصنوعی به عنوان ارائه‌دهنده خدمت باشد. ۳- این عمل هوش مصنوعی مسئولیت آور باشد (Kingston, 2016: 7) و نیز اگر سیستم هوش مصنوعی از نوع سیستم خبره باشد، استانداردهای فنی آن باید توسط حداقل یک متخصص نظارت شود (Kingston, 2016: 5). اما نویسنده‌ای دیگر راه حل مسئول شناختن هوش مصنوعی را ساده‌تر ترسیم می‌نماید و معتقد است به جای تمرکز بر ابزاری که تصمیم گیری از طریق آن انجام شده، باید بر خود تصمیم تمرکز نمود و اگر چنین تصمیمی توسط شخصی در شرایط مشابه مصداق سهل انگاری یا خطا محسوب می‌شد بنابراین باید هوش مصنوعی تصمیم گیرنده این تصمیم را نیز مسئول دانست (Soyer & Tettenborn, 2022: 391). در مواردی که متعاقدین منشا خطای قراردادهوشمند را معیوب بودن هوش مصنوعی می‌دانند باید

---

[۱] اصطلاح هوش مصنوعی (Artificial Intelligence) برای تشریح عملکرد ابرکامپیوترهایی اطلاق می‌گردد که رفتار انسانی را مورد تقلید و شبیه سازی قرارداده و عملکرد خود را بر اساس آن شکل می‌دهند (ناصر، ۱۳۹۷: ۶۲).

[۲] Expert System

[۳] هوش مصنوعی ChatGPT با بررسی کدهای قرارداد هوشمند اتریوم، موفق به شناسایی چندین راه آسیب پذیری این قرارداد که سابقا باعث هک این قرارداد نیز شده بود و برای توسعه دهندگان ناشناخته مانده بود، شد (Lindrea, 2023).

[۴] سیستم هوش مصنوعی هم می‌تواند به صورت متمرکز باشد و هم به صورت غیرمتمرکز (Decentralized AI). هوش مصنوعی غیرمتمرکز یک حوزه نوظهور هوش مصنوعی است که بلاکچین و سایر فناوری‌های دفتر کل توزیع شده را در خود جای داده است اما همچنین این فناوری نوظهور دارای مشکلاتی است (Keary, 2023) که هنوز به میزان کافی آن را اطمینان بخش نساخته است.

بتوانند دو موضوع را جهت معیوب دانستن هوش مصنوعی ثابت نمایند: ۱- هوش مصنوعی عملکردی را که منطقا انتظار می‌رود کلا یا به درستی انجام ندهد و ۲- در نتیجه این عیب، احتمال وقوع و افزایش خسارات وارده بیشتر شود (Soyer & Tettenborn, 2022: 393). با بررسی نظریات اخیر و مطابقت با قواعد مسئولیت مدنی در حقوق ایران می‌توان به این جمع بندی رسید که هوش مصنوعی را در صورتی می‌توان مسئول جبران خسارات ناشی از خطای قرارداد هوشمند دانست که اولا بتوان خطای رخ داده را زیان تلقی کرد و آن را منتسب به هوش مصنوعی دانست و بنابراین در فرضی که خطا در اثر اطلاعات نادرست فرستاده شده توسط اوراکل به هوش مصنوعی باشد، هوش مصنوعی را نمی‌توان مسئول دانست. دوما اگر متعاقدین با ظرفیت‌های هوش مصنوعی جهت تحلیل و اجرای مفاد قراردادی آشنا باشند و بدانند این هوش مصنوعی توانایی تحلیل یا اجرای دقیق قراردادهوشمند آنان را ندارد و باز هم آن هوش مصنوعی را ناظر و مجری قرارداد خود قرار دهند، به نظر می‌رسد که هوش مصنوعی مسئول جبران خسارات وارده نیست و متعاقدین طبق قاعده اقدام باید متحمل زیان‌های وارده شوند و سوما اگر متعاقدین معتقدند خطای قراردادهوشمند و خسارت وارده ناشی از معیوب بودن هوش مصنوعی است باید بتوانند نقص عملکردی آن را ثابت کرده و خسارت وارده را به آن نقص منتسب کنند.

پیرامون نحوه مسئول دانستن هوش مصنوعی باید بیان داشت، برخی از نویسندگان (شریفی و بیرمی، ۱۳۹۷: ۵۲) ضمن بررسی خصوصیات اساسی و مشترک نمایندگان هوشمند[۱] (مانند هوش مصنوعی) و ارائه و بررسی ماهیت‌های حقوقی گوناگون از نمایندگان هوشمند، نهایتا تئوری شخص حقوقی دانستن نماینده هوشمند را با وجود ایراداتی، نسبت به باقی تئوری‌ها بهتر می‌دانند و نیز عده‌ای دیگر (دهقانی و همکاران، ۱۴۰۱: ۴۰) تئوری نمایندگان ذهنی و نمایندگان عینی را ارائه می‌دهند. اما در حال حاضر از لحاظ فقهی، تایید شخصیت حقوقی مستقل برای این نوع سامانه‌های هوشمند تایید شده و پذیرفته نیست و تنها چیزی که می‌توان بیان داشت آن است که همانند قراردادهای الکترونیکی، چناچه خطایی در قرارداد هوشمند وجود داشته باشد که منجر به ایجاد زیان‌های احتمالی برای طرفین شود، جبران آن بر عهده اصیل و سازنده آن است (خوانساری و قلیچ، ۱۳۹۹: ۱۹). لذا بحث نمایندگی از طریق سامانه هوشمند منتفی است زیرا سامانه هوشمند، نماینده شخص در قصد و اراده انشاء نیست و یک هوش مصنوعی است که جایگزین شخص می‌شود (آهنگران و احمدی، ۱۳۹۸: ۱۹) بنابراین در کلیه موارد اخیر که هوش مصنوعی مسئول جبران خسارات وارده دانسته شد، در واقع برای جبران خسارات وارده باید به سازندگان هوش مصنوعی مراجعه نمود زیرا بر اساس آنچه بیان شد، فعل زیان‌بار را فقط می‌توان به سازندگان هوش مصنوعی نسبت داد، نه خود هوش مصنوعی.

۳،۳. اوراکل

قراردادهای هوشمند از سیستم اطلاعاتی به نام اوراکل[۲] بهره‌مند هستند. اوراکل‌ها سیستم‌های اطلاعاتی خارج از بلاکچین می‌باشند که به عنوان منبع داده جهت دریافت اطلاعات خارجی به کار گرفته می‌شوند. این سیستم‌ها ارتباطی آنلاین با بلاکچین و کامپیوتری که عقد در شمول دستورالعمل آن انجام می‌شود داشته و در کسری از ثانیه تمامی اطلاعات جدید طرفین را به آن منتقل می‌نماید (ناصر، ۱۳۹۷: ۹۵). قراردادهای هوشمند جهت استعلام موارد مختلف نظیر قیمت لحظه‌ای کالاها یا خدمات مرتبط با موضوع قرارداد، هویت و اهلیت متعاقدین، بررسی وضعیت معامله در عالم واقع و... نیازمند اتصال به اوراکل‌های مرتبط با موضوع عقد است. سیستم اوراکل برای استعلام اطلاعات مزبور از پایگاه‌های اطلاعات تعریف شده برای آن نیز نیازمند برخورداری از سیستم مرکزی است که عملکرد آن را کنترل کند، چنین مکانیسمی می‌تواند سیستم‌های اطلاعاتی اوراکل را در برابر حملات سایبری آسیب پذیر نماید (ناصر، ۱۳۹۷: ۱۲۰) و اگر هکر بتواند به سیستم اوراکل نفوذ کند و اطلاعات آن را دستکاری نماید منجر به این خواهد شد که قراردادهوشمند بر اساس اطلاعات هک شده دریافتی از اوراکل، اثری متفاوت با آنچه که مقصود متعاقدین بوده بر جا گذارد یا آن که به علت تعارض اطلاعات هک شده اوراکل با اطلاعات ثبت شده در قرارداد هوشمند، اجرای مفاد قرارداد متوقف گردد و هیچ اثری بر جا نگذارد. برای مثال، در سال ۲۰۱۹، حمله اوراکل به قرارداد هوشمند Synthetix باعث شد تا کاربری بتواند حدود ۳۷ میلیون دلار از ارز دیجیتالی را با قیمتی نادرست خریداری کند (توایی، ۱۴۰۲). حداقل اثر نقص نرم افزاری یا سخت افزاری در یک سامانه، ایراد خسارت یا تشدید آسیب پذیری محصولات یا سامانه‌های دیگری است که با یک یا چند سامانه هوشمند هماهنگ

[۱] در نظریه نماینده دانستن قرارداد هوشمند (یا هوش مصنوعی ناظر بر آن) نرم افزارهای الکترونیکی که به صورت هوشمند و با قابلیت تصمیم گیری نسبت به انعقاد قرارداد اقدام می‌کنند مانند یک نماینده انسانی در نظر گرفته می‌شود (شیروی و محمدی، ۱۳۸۸: ۳۱).

[۲] Oracle

شده‌اند (السان، ۱۴۰۰: ۴۵)، بنابراین در این حالات چون نقص فنی یا امنیتی در سیستم اوراکل یا ارسال اطلاعات خلاف واقع توسط اوراکل متصل به قراردادهوشمند سبب بروز خطا در قراردادهوشمند می‌گردد پس فعل زیان‌بار مستند به سازندگان و توسعه دهندگان اوراکل است و رابطه سببیت میان ضرر وارده و فعل زیان‌بار سازندگان اوراکل نیز قابل توجیه است و می‌توان در این فروض، سازندگان یا توسعه دهندگان اوراکل را مسئول جبران خسارات وارده به کاربران و توسعه دهندگان قراردادهوشمند متصل به آن دانست. البته باید توجه داشت اگر اطلاعات اوراکل مرتبط با شرایط اساسی صحت معامله[1] یا شرایطی که مستقیما بر صحت یا بطلان قرارداد تاثیر می‌گذارد باشد و به سبب ارسال اطلاعات نادرست به قرارداد هوشمند، این شرایط در انعقاد قرارداد رعایت نشود، منجر به باطل شدن قرارداد هوشمند و بی اثر شدن آثار آن از نظر حقوقی خواهد شد که طبیعتا مسئولیت مدنی بیشتری برای توسعه دهندگان اوراکل به همراه خواهد داشت.

۴،۳. توسعه دهنده

قراردادهای هوشمند بر پایه الگوریتم طراحی می‌شود که مبتنی بر کدهای برنامه نویسی است؛ بنابراین طراحی این قراردادها تا حدی مستلزم درک زبان برنامه نویسی است که ممکن است برای متعاقدین چندان آسان نباشد. در حال حاضر شکلی استاندارد برای قرارداد هوشمند و برنامه نویسی آن وجود ندارد و هنوز هم کدنویسی الگوریتم به عامل انسانی اتکا دارد که در معرض خطاست؛ بنابراین نمی‌توان گفت قرارداد هوشمند عاری از خطاست (خوانساری و قلیچ، ۱۳۹۹: ۱۰). خطاهای فنی در قرارداد هوشمند ممکن است به روش‌های متعددی مانند ناتوانی توسعه دهنده در درک زبان پیچیده برنامه نویسی، عدم اقدام یا سهل انگاری در ایجاد الگوریتم ایمن یا عجله در کدگذاری رخ دهد و سبب معیوب شدن قرارداد و بروز خطا گردد (Roumpos, 2020: 38). خطاهایی مثل فراموش کردن تابع Selfdestruct یا استفاده نادرست از Delegatecall یا حملات بازگشت ناپذیر، خطاهایی ناشی از اشکال در برنامه نویسی هستند. اگر توسعه دهنده‌ای که قراردادهوشمند را توسعه می‌دهد، سهل انگارانه عمل کند یا وظایف خود را به درستی انجام ندهد و در نتیجه آن خساراتی وارد شود مسئول زیان‌های وارده است که ممکن است شامل خسارات ناشی از نقص فنی، نقض امنیت یا سایر فعالیت‌های غیرقانونی باشد (Roumpos, 2020: 47). علاوه بر آن در بسیاری از موارد شکاف بین قصد متعاقدین و توسعه قرارداد ممکن است خطر ایجاد کد نادرست را افزایش دهد و منجر به خروجی نامطلوبی شود (Roumpos, 2020: 20) البته در مواردی که توسعه دهنده هیچ اطلاعی نسبت به قصد واقعی طرفین ندارد و کدنویسی را انجام می‌دهد می توان مسئولیت خطا را برعهده متعاقدین دانست که قصد خویش را به صورت شفاف و دقیق برای توسعه دهنده توضیح نداده‌اند (Harsimar, 2021: 114). از سویی چون قراردادهای هوشمند خوداجرا بوده و به علت غیرمتمرکز بودن آن‌ها نمی‌توان عملکرد آن‌ها را اصلاح یا متوقف کرد (Roumpos, 2020: 36) ضروری است تا در توسعه قرارداد هوشمند از توسعه دهندگان متخصصی استفاده شود که کاملا به برنامه نویسی بلاکچین تسلط داشته و کلیه اقدامات امنیتی جهت جلوگیری از بروز خطا یا هک قرارداد، مانند اعمال کدهای محدودکننده برای هوش مصنوعی ناظر بر قرارداد جهت جلوگیری از ایجاد آثاری که مقصود متعاقدین نیست یا اعمال کدهایی جهت اخذ تایید از متعاقدین پیش از اجرای برخی از مفاد قرارداد هوشمند، را رعایت نمایند و نیز در کنار آن‌ها از متخصصین حقوقی آشنا به علم بلاکچین و قراردادهای هوشمند، جهت بررسی انطباق کد برنامه نویسی شده با آثار حقوقی مدنظر متعاقدین، بهره ببرند. در غیر این صورت در صورت وقوع خطا در فروض مطرح شده، توسعه دهندگان قراردادهوشمند مسئول جبران خسارات وارده خواهند بود چرا که آسیب پذیری‌های کد ممکن است راه ورودی برای حملات یا دستکاری مخرب محتوای قراردادهای هوشمند باقی گذارد. بنابراین پیشنهاد می‌شود متعاقدین به مسئولیت مدنی ناشی از خطای قرارداد هوشمند بر اثر اقدامات یا سهل انگاری توسعه دهندگان اکتفا ننماید و ضمن مکتوب کردن میزان تخصص و تعهدات توسعه دهنده در توسعه قراردادهای هوشمند، حدود مسئولیت وی در حالت‌های مختلف بروز خطا در قراردادهوشمند زا معین نموده و ضمانت اجراهای متناسب لحاظ نمایند.

[1] ماده ۱۹۰ قانون مدنی:«برای صحت هر معامله شرایط ذیل اساسی است: ۱- قصد طرفین و رضای آن‌ها؛ ۲- اهلیت طرفین؛ ۳- موضوع معین که مورد معامله باشد؛ ۴- مشروعیت جهت معامله.»

نتیجه گیری

قراردادهای هوشمند به عنوان پیشرفته‌ترین نسل قراردادها، علی رغم آن کـه مبتنـی بـر فنـاوری بلاکچـین هسـتند و از ویژگـی‌هـایی نظیـر غیرمتمرکز بودن، خوداجرایی و شفافیت برخوردارند اما از بروز خطا در اجرای مفاد قراردادی خود مصون نیستند. منظور از خطا حالتی است کـه قرارداد هوشمند، به عنوان یک سیستم خوداجرا، اقدام به تحلیل و اجرای کدهای قرارداد هوشمند می‌نماید اما به عللی مثـل ایـرادات فنـی در برنامه نویسی، اختلال در بلاکچین، عدم دریافت اطلاعات معتبر و... نتیجه‌ای را به اجرا می‌گذارد کـه متعاقـدین بـه هـیچ عنـوان قصـد آن را نداشته‌اند و همچنین انتظار وقوع چنین اثری را از قرارداد نداشته‌اند یا گاها بنا به علل بیان شده قرارداد هوشمند هیچ اثری از کدهای قرارداد را به اجرا نمی‌گذارد. به علت بدیع بودن فناوری قراردادهای هوشمند به طور کامل و قـاطع نمـی‌تـوان کلیـه مـواردی کـه سـبب بـروز خطـا در قراردادهای هوشمند می‌شود را مشخص نمود اما با بررسی شایع‌ترین خطاهای رخ داده در ایـن قراردادهـا، مـی‌تـوان حـداقل چهـار عامـل را شناسایی کرد که در بروز خطا در قراردادهوشمند موثر هستند که عبارت است از: بلاکچین، هوش مصنوعی، اوراکل و توسعه دهنده.

اگر خطای قراردادهوشمند در اثر اشکالات فنی رخ داده در بلاکچین مبتنی بر آن باشد یا بر اثر تغییر پروتکـل‌هـای بلاکچـین توسـط توسـعه دهندگان آن بدون رعایت استانداردهای لازم و معقول باشد، باید توسعه دهندگان بلاکچین را مسئول زیان‌هـای وارده دانسـت و اگـر خطـای قراردادهوشمند در اثر هک هوش مصنوعی قراردادهای هوشمند باشد (با توجه به آن که قراردادهای هوشمند برای اجرا خودکار مفاد قراردادی از فناوری هوش مصنوعی برای تحلیل و اجرای مفاد خود استفاده می‌نمایند) یا بر اثر عدم تحلیل و اجرای صحیح مفاد قراردادی توسط هـوش مصنوعی به علت ضعف در برنامه نویسی آن باشد، باید سازندگان آن هوش مصنوعی را مسـئول جبـران خسـارت ناشـی از خطاهـای رخ داده دانست، البته در این مورد اگر کدهای قراردادهوشمند دارای ابهام یا نقص باشد می‌توان توسعه دهندگان قرارداد هوشمند را مسئول شناخت. در مواردی که خطای رخ داده ناشی از اطلاعات هک شده یا اطلاعات نادرست یا متعارض اوراکل باشد و قرلردادهوشمند بدین جهت مفاد قرارداد را اجرا ننموده یا برخلاف آنچه که تعیین شده اجرا نماید، مسئول جبران خسارات وارده به توسعه دهنـدگان اوراکـل منتسـب خواهـد بـود و در نهایت، هنگامی که توسعه دهندگان قراردادهوشمند به علت ضعف در مهارت کدنویسی بلاکچین یا عدم درک صحیح مقصود حقوقی متعاقدین از انعقاد عقد و عدم کدنویسی صحیح آن یا عدم رعایت مسائل امنیتی مرتبط با قراردادهای هوشمند منجر به بروز خطا یا حمـلات هکـری در اجرای قراردادهوشمند می‌شوند می‌توان جهت جبران خسارات وارده به توسعه دهندگان قراردادهوشمندرجوع نمود.

با توجه به غیرمتمرکز بودن قراردادهای هوشمند، غالبا امکان تصحیح خطاهای رخ داده امری سخت و غیرممکن مـی‌شـود، البتـه در مـواردی مانند خطا در اثر اوراکل یا خطا در اثر هوش مصنوعی که متصل به سیستم متمرکز هستند می‌توان با رفع اشکالات، از تکرار یا گسترش خطاها جلوگیری کرد اما برای پیشگیری از بروز این خطاها مطلوب است توسعه دهندگان قراردادهوشمند ابتدائا از امنیت و سازگاری بلاکچین مبتنـی بر آن اطمینان حاصل نموده و هوش مصنوعی و اوراکلی را به قراردادهوشمند خود متصل نمایند که کلیه اقدامات امنیتـی جهـت جلـوگیری از بروز خطا و نفوذ هکرها رو به عمل آورده باشد و علاوه بر اعمال کدهای محدودکننده یا نیازمند تایید متعاقدین جهـت اجـرای برخـی از مفـاد قراردادی در برنامه نویسی قراردادهوشمند یا هوش مصنوعی ناظر بر آن از وقوع خطا در اثر تفسیرهای خلاف مقصود متعاقدین پیشگیری کنند. همچنین متعاقدین باید از توسعه دهندگان متخصص در زبان کدنویسی بلاکچین در کنار متخصص حقوقی آشنا به فناوری بلاکچین اسـتفاده نمایند تا از صحت کدهای نوشته شده از منظر فنـی و آثـار حقـوقی آن اطمینـان یابنـد و نیـز مـی‌تـوان بـا اشـخاص دخیـل در امـر توسـعه قراردادهوشمند، قرارداد مسئولیت منعقد و حدود مسئولیت هر یک از طرفین در فرض وقوع خطاهای قراردادهوشـمند را بـه صـورت قـراردادی تعیین نمود و ضمانت اجرای متناسب قرار داد.

منابع

۱.السان، مصطفی. (۱۴۰۰). حقوق فضای مجازی، چاپ هفدهم، تهران، شهر دانش.

۲.آهنگران، محمدرسول؛ احمدی، امیر. (۱۳۹۸). آثار و احکام فقهی و حقوقی اشتباه و خطا در قراردادهای الکترونیکی، فصلنامه پژوهش¬های فقهی، بهار، دوره ۱۵، شماره ۱.

۳.باریکلو، علیرضا. (۱۳۹۲). مسئولیت مدنی. چاپ چهارم، میزان.

۴.جعفری لنگرودی، محمدجعفر. (۱۳۸۸). ترمینولوژی حقوق، چاپ بیست و دوم، تهران، گنج دانش.

۵.حبیب زاده، طاهر. (۱۳۹۲). وضعیت حقوقی نماینده الکترونیکی در انعقاد قراردادهای الکترونیکی (مطالعه تطبیقی)، فصلنامه پژوهش حقوق خصوصی، زمستان، دوره ۲، شماره ۵.

۶.خوانساری، رسول؛ قلیچ، وهاب. (۱۳۹۹). گزارش سیاستی بررسی ابعاد فقهی و حقوقی به¬کارگیری قراردادهای هوشمند در نظام مالی ایران، پژوهشکده پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، بهمن.

۷.دهقانی تفتی، مجتبی؛ افضلی مهر، مرضیه؛ اسکینی، ربیعا. (۱۴۰۱). مطالعه تطبیقی الزامات حقوقی طراحی قراردادهای هوشمند دیجیتالی در حقوق ایران و فرانسه، پژوهشنامه حقوق تطبیقی، پاییز، دوره ۶، شماره ۱۰.

۸.شریفی، سید الهام الدین؛ بیرمی، گلناز. (۱۳۹۷). ماهیت حقوقی نمایندگان هوشمند در عرصه قراردادهای الکترونیکی، پژوهش¬های حقوقی، بهار، دوره ۱۷، شماره ۳۳.

۹.شیروی، عبدالحسین؛ محمدی، مرتضی. (۱۳۸۸). تشکیل قراردادها از طریق نمایندگی سامانه هوشمند، فصلنامه حقوقی، شماره ۱.

۱۰.کاتوزیان، ناصر. (۱۳۸۸) دوره مقدماتی حقوق مدنی: وقایع حقوقی، چاپ شانزدهم، تهران، انتشار.

۱۱.ملکوتی، رسول. (۱۴۰۱). بررسی ارکان تحقق مسئولیت مدنی در فضای سایبر، فصلنامه مطالعات حقوقی فضای مجازی»، پاییز، دوره ۱، شماره ۳.

۱۲.ناصر، مهدی. (۱۳۹۷). قراردادهای هوشمند (مطالعه تطبیقی حقوق ایران و آمریکا)، چاپ اول، تهران، مجد.

۱۳.نجات زادگان، سعید؛ سلطانی، محمد. (۱۴۰۱). ارزیابی شرایط عمومی صحت قراردادهای هوشمند از منظر حقوق ایران و آمریکا، فصلنامه تحقیقات حقوقی ویژه نامه حقوق و فناوری، بهمن، دوره ۲۵.

۱۴.هوشمند فیروزآبادی، حسین. (۱۳۹۸). ارزیابی مبانی فقهی مسئولیت مدنی، فصلنامه آموزه¬های فقه مدنی، بهار، دوره ۱۱، شماره۱۹.

۱۵.توایی، شبنم. (۴ شهریور ۱۴۰۲). آسیب‌پذیری‌های قراردادهای هوشمند؛ علت، عواقب و راهکارها.

.۱۶Giancaspro, Mark. (2022). I,Contranct: Evaluating the Mistake Doctrine’s Application Where Autonomous Smart Contracts Make Bad Decisions. Campbell Law Review, Vol 45, No 2.

.۱۷Giuffrida, Iria. (2019). Liability for AI Decision-Making: Some Legal and Ethical Considerations. William & Mary Law School Scholarship Respository, Vol 88.

.۱۸Harsimar, Dhanoa. (2021). Making Mistakes with Machines. Santa Clara High Technology Law Journal, Vol 37, No 1.

.۱۹Kirill, Khotulev. (2018). Civil Liability for Damaging of Goods Following the Application of the Smart Contracts in the Context of International Sale and Carriage of Goods Industry: The UK and German Perspective. Master's Thesis, Tilburg University.

.۲۰Kingston, John. (2016). Artificial Intelligence and Legal Liability. International Conference on Innovative Techniques and Applications of Artificial Intelligence.

.۲۱Kolber, Adam. (2018). Not-So-Smart Blockchain Contracts and Artificial Responsibility. Stanford Technology Law Review, Vol 21.

.۲۲O'Shields, Reggie. (2017). Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute. Vol 21, No 1.

.۲۳Roumpos, Dimitrios. (2020). Liability of the Smart Contract Developer. Master's Thesis, Tilburg University.

.۲٤Soyer, Baris, & Tettenborn, Andrew. (2022). Artificial Intelligence and Civil Liability – Do We Need a New Regime?. International Journal of Law and Information Technology, Vol 30, No 4.

.۵۵Zou, Weiqin, & Lo, David, & Xia, Xin. (2021). Smart Contract Development: Challenges and Opportunities. IEEE Transactions on Software Engineering, Vol 47, No 10.

.٦٦Behnke, Rob. (4 July 2023). Explained: the Poly Network Hack. https://www.halborn.com/blog/post/explained-the-poly-network-hack-july-2023

.۲۷Cobb, Michael. (25 May 2023).9 Smart Contract Vulnerabilities and How to Mitigate Them. https://www.techtarget.com/searchsecurity/tip/Smart-contract-vulnerabilities-and-how-to-mitigate-them.

.۲۸Frankenfield, Jake. (29 August 2023). Cryptocurrency Wallet: What It Is, How It Works, Types, Security. https://www.investopedia.com/terms/b/bitcoin-wallet.asp#:~:text=A%20cryptocurrency%20wallet%20is%20a,needed%20to%20sign%20cryptocurrency%20transactions.

.۲۹Hayes, Adam. (Updated 31 October 2021). Peer-to-Peer (P2P) Service: Definition, Facts, and Examples. https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp#:~:text=A%20peer%2Dto%2Dpeer%20(P2P)%20service%20is%20a,other%20via%20the%20P2P%20service.

.۳۰Keary, Tim. (Updated 5 December 2023). Decentralized Artificial Intelligence (DAI). https://www.techopedia.com/definition/decentralized-ai-dai.

.۳۱Lindrea, Brayden. (15 March 2023). ChatGPT v4 Aces the Bar, SATs and Can Identify Exploits in ETH Contracts. https://cointelegraph.com/news/chatgpt-v4-aces-the-bar-sats-and-can-identify-exploits-in-eth-contracts#:~:text=Mar%2015%2C%202023-,ChatGPT%20v4%20aces%20the%20bar%2C%20SATs%20and%20can%20identify%20exploits,up%20in%20the%20bottom%2010%25.

.۳۲Yatchenko, Darya. (16 December 2022). 7 Most Common Smart Contract Vulnerabilities. https://pixelplex.io/blog/smart-contract-vulnerabilities.

.۳۳Young, Martin. (Updated 4 Aug 2022). Over 44 Million Contracts Deployed to Ethereum Since Genesis: Research. https://cryptopotato.com/over-44-million-contracts-deployed-to-ethereum-since-genesis-research.