Applied Criminology Research
پژوهش های جرم شناسی کاربردی
دوره ۱ / شماره ۱/ پاییز ۱۴۰۲
تاریخ دریافت: ۱۴۰۲/۰۴/۰۹
تاریخ پذیرش: ۱۴۰۲/۰۶/۱۵
صفحه: ۱ الی ۲۲

Volume 1, Issue 1, Autumn 2023
Received: 2023/06/30
Date of Acceptance: 2023/09/06
Pages: 1-22

Article Type: **Research**
نوع مقاله: پژوهشی

System: qacr.ir
doi: 10.22034/AQCR.2024.715538

The role of intelligentization of contracts in preventing the commission of crimes related to digital currencies

Ali Rafie[1], Mohammad Rezazadeh Soltan Abad[2]✉

Abstract

Field and Aims: With the growth of technology, the fields of using smart contracts have increased, however, there is a possibility of fraud and committing crimes through these contracts. Smart contracts have features such as transparency and the possibility of self-execution of smart contracts. But one of the concerns of Internet activities today is crimes that occur in modern spaces, and the capabilities of smart contracts show that it is possible to prevent these crimes.

Method: The present research was carried out with a descriptive and analytical method.

Findings and Conclusions: Prevention in two forms, punitive and non-punitive, aims to reduce the amount of delinquency, which is divided into two types of action and reaction, depending on the time of the intervention. Regarding prevention by smart contracts, although criminal prevention is necessary, but taking the necessary measures in non-criminal prevention (situational and social) is associated with better results. Smart contracts are currently vulnerable due to the technology that is used based on it. A smart contract vulnerability is an error or flaw in the smart contract code that can cause it to malfunction, change state, or move money. Finally, it should be said that smart contracts with current technology can prevent crime, but two categories of contracts, namely criminal and vulnerable contracts, may provide a platform for committing crimes. There are also basically two main types of intrusion detection systems: signature-based and anomaly-based. Therefore, it should be said that with the development of technology and identifying the vulnerable points of smart contracts, the defects of these contracts that provide the possibility and conditions for committing crimes can be resolved.

Keyword: Crime prevention, Smart contracts, Digital currencies, Information technology.

❋Citation (APA): Rafie, A.; Rezazadeh Soltan Abad, M. (2023). The role of intelligentization of contracts in preventing the commission of crimes related to digital currencies. *Applied criminology research*, 1(1), 1-22.
https://qacr.ir/article_715538.html?lang=en

1. Associate Assistant Professor, Department of Law, Faculty of Humanities, Fardis Branch, Islamic Azad University, Fardis, Iran. Email: rafie.barrister@gmail.com
2. Invited Assistant Professor, Department of Law, Faculty of Humanities, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran. (Author). Email: dr.mohamadrezadeh@gmail.com

دوره ۱ / شماره ۱/ پاییز ۱۴۰۲
تاریخ دریافت: ۱۴۰۲/۰۴/۰۹
تاریخ پذیرش: ۱۴۰۲/۰۶/۱۵
صفحه: ۱ الی ۲۲

پژوهش های جرم شناسی کاربردی
Applied Criminology Research

Volume 1, Issue 1, Autumn 2023
Received: 2023/06/30
Date of Acceptance: 2023/09/06
Pages: 1-22

نوع مقاله: پژوهشی
Article Type: **Research**

سامانه: qacr.ir
doi: 10.22034/AQCR.2024.715538

نقش هوشمندسازی قراردادها در پیشگیری از ارتکاب جرائم مرتبط با ارزهای دیجیتال

علی رفیعی[۱]، محمد رضازاده سلطان آباد[۲]✉

چکیده

زمینه و هدف: با رشد فناوری، زمینه‌های استفاده از قراردادهای هوشمند افزایش یافته است؛ با این حال، امکان تقلب و ارتکاب جرم از طریق این قراردادها وجود دارد. قراردادهای هوشمند دارای ویژگی‌هایی از جمله شفافیت و امکان خوداجرایی قراردادهای هوشمند می‌باشد. با این وجود، یکی از نگرانی‌های فعالیت‌های اینترنتی امروزه جرائمی است که در فضاهای نوین واقع می‌شود و قابلیت‌های قرارداد هوشمند نشان می‌دهد که امکان پیشگیری از این جرائم را دارد.

روش: پژوهش حاضر با روش توصیفی و تحلیلی انجام شده است.

یافته‌ها و نتایج: پیشگیری به دو شکل کیفری و غیرکیفری درصدد کاهش میزان بزهکاری است که برحسب زمان مداخله، به دو نوع کنشی و واکنشی تقسیم می‌شود. در خصوص پیشگیری توسط قراردادهای هوشمند، اگرچه پیشگیری کیفری ضرورت دارد، اما اتخاذ تدابیر لازم در پیشگیری غیرکیفری (وضعی و اجتماعی) با آثار بهتری همراه است. قراردادهای هوشمند در حال حاضر با توجه به فناوری که بر اساس آن بکار گرفته می‌شود، دارای آسیب‌پذیری می‌باشد. آسیب‌پذیری قراردادهای هوشمند، خطا یا نقصی در کد قرارداد هوشمند است که می‌تواند منجر به عملکرد نادرست، تغییر حالت یا جابجایی پول شود. در نهایت، باید گفت قراردادهای هوشمند با فناوری فعلی امکان پیشگیری از جرم را دارد، اما دو دسته از قراردادها، یعنی قراردادهای مجرمانه و آسیب‌پذیر، ممکن است بستر ارتکاب جرائم را فراهم آورد. همچنین، اساساً، دو نوع اصلی سیستم‌های تشخیص نفوذ وجود دارد: مبتنی بر امضا و مبتنی بر ناهنجاری. لذا، باید گفت با رشد فناوری و شناسایی نقاط آسیب‌پذیر قراردادهای هوشمند می‌توان ایرادات این قراردادها را که امکان و شرایط ارتکاب جرم را فراهم می‌کند، برطرف نمود.

کلیدواژه‌ها: پیشگیری از جرم، قراردادهای هوشمند، ارزهای دیجیتال، فناوری اطلاعات.

❋ استناددهی (APA): رفیعی، علی و رضازاده سلطان آباد، محمد. (۱۴۰۲). نقش هوشمندسازی قراردادها در پیشگیری از ارتکاب جرائم مرتبط با ارزهای دیجیتال. *پژوهش‌های جرم شناسی کاربردی*، ۱(۱)، ۲۲-۱.
https://qacr.ir/article_715538.html

۱. استادیار وابسته گروه حقوق دانشکده علوم انسانی، واحد پردیس، دانشگاه آزاد اسلامی، پردیس، ایران.
رایانامه: rafie.barrister@gmail.com
۲. استادیار مدعو گروه حقوق دانشکده علوم انسانی، واحد اسلامشهر، دانشگاه آزاد اسلامی، اسلامشهر، ایران.
(نویسنده مسئول). رایانامه: dr.mohamadrezazadeh@gmail.com

مقدمه

قراردادهای هوشمند، قراردادهای الکترونیکی هستند که در بستر بلاک‌چین منعقد شده و انعقاد آن‌ها تحت نظارت هوش مصنوعی و مراجع صلاحیت‌دار قانونی صورت می‌گیرد. قرارداد هوشمند با خصیصه تمرکززدایی «بلاک‌چین» امکان اجرای معاملات قابل‌اعتماد بدون دخالت اشخاص ثالث را فراهم کرده و با غیرعملی‌بودن حذف رکوردها و قابلیت دسترسی رکوردهای تائیدشده هر معامله برای مشارکت‌کنندگان، توانایی جستجو هرگونه فساد در اطلاعات را داراست که باعث افزایش اعتبار اطلاعات می‌شود (توکلی راد و طهماسبی، ۱۴۰۱). با این حال، گزارش‌های متعددی از ارتکاب جرم در قالب قراردادهای هوشمند وجود دارد که امنیت این قراردادها را با چالش مواجه می‌سازد.

در ۱۱ جولای ۲۰۲۳، دفتر دادستان ایالات متحده در ناحیه جنوبی نیویورک اعلام کرد که شکیب احمد را دستگیر کرده و او را به کلاهبرداری و پولشویی در ارتباط با حمله او به یک صرافی غیرمتمرکز ارزهای دیجیتال (صرافی رمزارز) متهم کرده است. اگرچه این کیفرخواست صرافی را شناسایی نکرده است، اما بر اساس حقایقی که در کیفرخواست توضیح داده شده است، گزارش شده است که این هک علیه کریما فاینانس[1]، یک پلت فرم غیرمتمرکز ارز دیجیتال که بر روی بلاک‌چین سولانا[2] کار می‌کند، بوده است. در کیفرخواست توضیح داده شد که یک صرافی غیرمتمرکز به هیچ نوع نهاد یا شرکتی متکی نیست تا به عنوان واسطه بین خریداران و فروشندگان عمل کند. در عوض، به «قراردادهای هوشمند»، که اساساً، یک برنامه کامپیوتری است که بر روی بلاک‌چین اجرا می‌شود، تکیه می‌کند تا به‌عنوان «بازارساز خودکار» عمل کند.[3]

این امر بیانگر آن است که قراردادهای هوشمند در عین اینکه امکان ایجاد روابط حقوقی میان افراد را دارند، ممکن است زمینه‌ساز ارتکاب جرم باشند. از آنجا که قراردادهای هوشمند توافقات را اجرا می‌کنند، می‌توان از آنها برای اهداف مختلف استفاده کرد. یکی از ساده‌ترین کاربردها، اطمینان از انجام معاملات بین دو طرف مانند خرید و تحویل کالا است. با این حال، این فناوری دارای معایب و نواقصی است که اطمینان از این سیستم را زیر سؤال می‌برد. به علاوه، جرائمی که در قالب قراردادهای هوشمند امکان ارتکاب دارند نیز این چالش را نمایان‌تر می‌کند.

1. Crema Finance
2. Solana
3. https://blockchain.bakermckenzie.com/2023/07/17/first-u-s-criminal-case-involving-attack-on-a-smart-contract-operated-by-decentralized-exchange/

قراردادهای هوشمند بر بستر بلاک‌چین اجرا می‌شوند و فناوری بلاکچین اساساً، یک پایگاه داده توزیع‌شده از اسناد و یا دفترکل عمومی از همه تراکنش‌ها یا رویدادهای دیجیتال است که توسط اجزای تشکیل‌دهنده‌اش به شکل مشترک اجرا می‌شود. هر تراکنش در دفترکل عمومی با توافق اکثریت اجزای سیستم محقق می‌شود. اطلاعاتی که یک بار وارد سیستم شده باشد، هرگز پاک نمی‌شود. زنجیره بلوکی برای هر تراکنش منحصربه‌فردی که ایجاد شده باشد، اطلاعات قطعی و قابل‌بازبینی را ثبت می‌کند (برنگی، ۱۳۹۹: ٤٠). لذا، می‌توان گفت پلتفرم‌های محاسباتی توزیع‌شده با قابلیت قرارداد هوشمند تأثیرات فنی و اقتصادی قابل‌توجهی در آینده خواهند داشت. با این حال، اگر می‌خواهیم از خطر به همان اندازه مهم حوادث امنیتی اجتناب کنیم، باید اطمینان حاصل کنیم که قراردادهای هوشمند ایمن هستند.

با ظهور فناوری بلاکچین و ارزهای دیجیتال، دنیای مالی و اقتصادی با تحولات بنیادینی روبه‌رو شده است. ارزهای دیجیتال، به دلیل ویژگی‌های منحصربه‌فرد خود از جمله غیرمتمرکز بودن، شفافیت، و ناشناس بودن تراکنش‌ها، به سرعت به یکی از مهم‌ترین ابزارهای مالی جهان تبدیل شده‌اند. با این حال، این ویژگی‌ها باعث شده تا بستر مناسبی برای وقوع جرائم مالی و سایبری نیز فراهم شود. در این میان، هوشمندسازی قراردادها به‌عنوان یکی از نوآوری‌های کلیدی در فناوری بلاکچین، پتانسیل زیادی برای پیشگیری از ارتکاب جرائم مرتبط با ارزهای دیجیتال دارد.

قراردادهای هوشمند، برنامه‌های خوداجرا هستند که شرایط و مفاد قرارداد را به صورت خودکار و بدون نیاز به واسطه‌های انسانی اجرا می‌کنند. این فناوری، با ارائه راه‌حل‌های نوآورانه در حوزه‌های مختلف مالی و حقوقی، می‌تواند به کاهش ریسک‌های مرتبط با جرائم مالی، از جمله پولشویی، تقلب و سرقت دیجیتال کمک کند. مقاله حاضر به بررسی نقش هوشمندسازی قراردادها در پیشگیری از جرائم مرتبط با ارزهای دیجیتال می‌پردازد و تلاش می‌کند تا با تحلیل مزایا و محدودیت‌های این فناوری، دیدگاه جامعی در خصوص تأثیر آن بر امنیت مالی و حقوقی فضای دیجیتال ارائه دهد.

پیشینه پژوهش و ادبیات نظری

پیشینه پژوهش

کرامتی معز و بهاری غازانی (۱٤۰۱)، در پژوهشی با عنوان «**پیشگیری وضعی از جرائم در بستر رمزارزها**»، به این نتیجه رسیده‌اند که جهت اتخاذ سیاست پیشگیرانه وضعی، توجه به تئوری‌های جرم‌شناختی از اهمیت بسیاری برخوردار است و از تئوری‌های مرتبط در زمینه

بررسی‌های جرم‌شناختی رمزارزها، می‌توان به نظریه‌های انتخاب عقلانی، الگوی جرم و سبک زندگی برخط، گذار از فضا و جرم‌شناسی آبی اشاره نمود. همچنین، می‌توان نتیجه گرفت که راهکارهای پیشگیری وضعی از جرائم در بستر رمزارزها در دو محور: الف) تدابیر نظارتی (نصب و راه‌اندازی سیستم‌هایKYC، محدودیت دسترسی به رمزارزها و قرارگرفتن در لیست سیاه، نظارت بر صرافی‌های آنلاین و نظارت مؤثر در ارایه‌دهندگان خدمات رمز ارزها)؛ ب) تدابیر افزایش دشواری ارتکاب جرم (استفاده از داده‌های بلاک‌چین عمومی، طبقه‌بندی بازیگران حقیقی و حقوقی شبکه رمزارزها و حفاظت از داده‌های شخصی) قرار می‌گیرد.

جعفری و کوشا (۱۴۰۱)، در پژوهشی با عنوان «**هوشمندسازی پیشگیری از قاچاق کالا، جلوه‌ها و چالش‌ها**»، به این نتیجه رسیده‌اند که هرچند از حیث سیاست‌گذاری خطرمدارانه، رویکرد مناسبی به‌منظور ارتقای سطح شفافیت اطلاعات و مدیریت زنجیره تأمین اتخاذ شده و این راهبردها نقش مؤثری در کاهش قاچاق کالا داشته است، با این حال، در عمل شاهد اجرای مناسب راهبردها توسط نهادهای متولی امر نیستیم و هماهنگی لازم بین اجزای مختلف نظام عدالت کیفری وجود ندارد.

صادقی و مهدی (۱۳۹۷)، در پژوهشی با عنوان «**ملاحظاتی برای سیاستگذاری حقوقی قراردادهای هوشمند**»، به این نتیجه رسیده‌اند که این قراردادها با توجه به دارابودن ویژگی خوداجرایی نسبت به اجرای مفاد قرارداد بدون دخالت فرد سوم و اعمال ضمانت اجراهای عدم انجام تعهدات قراردادی اقدام و این ویژگی با توجه به دارابودن خصوصیت افزایش امنیت، کاهش هزینه و افزایش سرعت و دقت در انعقاد معاملات، منجر به توسعه نظام مبادلاتی می‌گردد.

ادبیات نظری

۱. ماهیت قرارداد هوشمند

قرارداد هوشمند یک برنامه خوداجرا است که اقدامات مورد نیاز در یک توافق‌نامه یا قرارداد را خودکار می‌کند و پس از تکمیل، تراکنش‌ها قابل‌پیگیری و برگشت‌ناپذیر هستند. بهترین راه برای تصور یک قرارداد هوشمند این است که به یک دستگاه فروش خودکار فکر کنید؛ وقتی مقدار صحیح پول را وارد می‌کنید و دکمه یک کالا را فشار می‌دهید، برنامه (قرارداد هوشمند) دستگاه را برای توزیع کالای انتخابی شما فعال می‌کند. قراردادهای هوشمند اجازه می‌دهند تا معاملات و توافقات قابل‌اعتماد بین طرف‌های ناهمگون و ناشناس بدون نیاز به یک مرجع

مرکزی، سیستم قانونی یا مکانیزم اجرایی خارجی انجام شود (کونیت و اندیایه[1]، ۲۰۲۳: ۱۱). به عبارت دیگر، قراردادهای هوشمند تحت نظارت هوش مصنوعی در بستر بلاک‌چین منعقد می‌شوند و عوض قراردادی در آن‌ها، دارایی‌های هوشمند یا ارزهای رمزنگاری‌شده دیجیتالی می‌باشد. عنصر قصد یکی از ارکان تشکیل هر قراردادی در نظامات حقوقی تلقی می‌گردد و ابراز و احراز آن شرط لازم برای تشکیل و اجرای هر قراردادی است. اعتبار این قراردادها نیز منوط به اثباتِ امکان احراز عنصر قصد به روشی مطمئن و اصیل است. ابراز قصد متعاملین در قراردادهای هوشمند از طریق مکانیسم‌های تخصیص مجوز استفاده از امضاهای دیجیتالی, مکانیسم‌های تخصیص مجوز استفاده از ارزهای مجازی و سازوکارهای برخورداری از سیستم‌های اطلاعاتی انجام می‌شود. همچنین، در قراردادهایی که به نمایندگی هوش مصنوعی انجام می‌گیرد، معامله از طریق نیابت که در سامانه‌های هوشمند ظهور یافته، انجام می‌گیرد. تأمین وصف محرمانگی و اصالت محتوا و امضای قرارداد هوشمند و اطمینان از اهلیت و قصد جدی طرفین و ملائت آنها دخالت گسترده مقامات عمومی و دولتی را موجب شده است که در قراردادهای سنتی سابقه ندارد، به گونه‌ای که می‌توان گفت اصل رضایی‌بودن کنار گذاشته شده و ابراز اراده معتبر در این قبیل معاملات رنگ و بوی خاصی به خود گرفته است (رشوند و ناصر، ۱۳۹۸: ۲۷۱).

در واقع، قرارداد هوشمند، قراردادی است که در جایی که شرایط بین دو طرف به صورت کد (روی زنجیره بلوک) ایجاد و نوشته شود، به‌طور خودکار اجرا می‌شود. البته، این قراردادها زمانی اجرا می‌شوند که یک تابع فراخوانی می‌شود و زمانی که شرایط آن تابع برآورده می‌شود، می‌توان از آنها برای خودکارسازی اجرای توافقات بدون هیچ واسطه‌ای استفاده کرد (بویسن[2]، ۲۰۲۲: ۹۶۱). پس، این قراردادها زمانی اجرا می‌شوند که یک تابع فراخوانی می‌شود و شرایط آن تابع برآورده می‌شود و می‌توان از آنها برای خودکارسازی اجرای توافقات بدون هیچ واسطه‌ای استفاده کرد و در ساده‌ترین شکل آن، قرارداد فقط مجموعه‌ای از کارکردها است. قراردادهای هوشمند در خود زنجیره بلوکی (بلاکچین) ذخیره می‌شوند؛ بنابراین، با طراحی قابل‌ردیابی، قطعی و غیرقابل‌برگشت هستند. در این زمینه باید گفت که پلتفرم بلاکچین اتریوم یکی از رایج‌ترین پلتفرم‌های بلاکچینی مورد استفاده برای ایجاد قراردادهای هوشمند است که از زبان برنامه‌نویسی سالیدیتی برای این کار استفاده می‌کند. یکی از اجزای مهمی که به غیر از قراردادهای هوشمند، سایر قراردادها آن را ندارند، زبان برنامه‌نویسی است. یک قرارداد

1. Ndiaye
2. Boison

هوشمند از کدهای رمزنگاری‌شده برای ثبت در شبکه بلاکچین استفاده می‌کند و لازمه پدیدآمدنِ این کدها، یک زبان برنامه‌نویسی است.

در تعریف دیگر، قرارداد هوشمند، که به عنوان یک پروتکل تراکنش رایانه‌ای تعریف می‌شود، می‌تواند به طور جزئی یا کامل بر اساس شرایط یک قرارداد ازپیش‌تعریف‌شده بدون تعامل انسانی اجرا شود. به طور خاص، قرارداد هوشمند یک پروتکل رایانه‌ای را بین شرکت کنندگان غیرقابل‌اعتماد ایجاد می‌کند. پس از برآورده‌شدن پیش‌شرط‌های کتبی، قرارداد به طور خودکار اجرا می‌شود و قابل‌فسخ نیست (ناماسودرو[1]، ۲۰۲۳: ٤). البته، فناوری بلاکچین یکی از رایج‌ترین مشکلات در سال‌های اخیر است. قرن بیست‌ویکم، انقلاب صنعتی چهارم را معرفی کرده است و یک تغییر پارادایم صنعتی را توصیف می‌کند که محیط‌های اجتماعی، اقتصادی و سیاسی را به‌طور هم‌زمان تغییر می‌دهد. فناوری‌های نوآورانه مانند بلاکچین، هوش مصنوعی و شبکه‌های پیشرفته تلفن همراه، این انقلاب دیجیتالی را تقویت می‌کنند؛ برای مثال، فناوری بلاکچین این پتانسیل را دارد که زیرساختی برای عناصر دیجیتال، بیولوژیکی و فیزیکی برای همگرایی در انقلاب صنعتی چهارم فراهم کند. الگوریتم‌های هوش مصنوعی با پتانسیل خود برای تجزیه‌وتحلیل سریع انواع مختلف و مقادیر زیاد داده، می‌توانند فرآیندهای تصمیم‌گیری پیچیده را تسهیل و خودکار کنند. همچنین، هوش مصنوعی می‌تواند از فناوری‌های بلاکچین با تجزیه‌وتحلیل الگوهای ورودی بزرگ‌تر و پیچیده‌تر پشتیبانی کند (مهربانی، ۱٤۰۱: ۱۸۵). در واقع، بلاکچین، فناوری جدیدی است که در بخشهای مختلف باعث افزایش بهره‌وری و جهانی‌سازی می‌شود. در سالهای اخیر، با توسعه فن‌آوری، تصمیمات کلان در جهت بکارگیری فن‌آوری‌های نوین در تمامی دستگاههای دولتی و خصوصی و تجارت جهانی و بین‌الملل اتخاذ شده است که ضرورت این موضوع را بیش‌ازپیش نمایان می‌کند. با این حال، با چالش‌هایی مانند ظرفیت ذخیره‌سازی پیام الکترونیکی، تغییرناپذیری بلاکچین، خطرات ابزارهای الکترونیک، اعتبارسنجی ارزهای مجازی و توکن‌های دیجیتالی مواجه است. همچنین، بلاکچین در توسعه خدمات بیمه و بانکی و همچنین، زنجیره تأمین و بازارهای مالی تاثیرگذار بوده است. قراردادهای هوشمند براساس توسعه زیرساخت‌ها امکان‌پذیر است (صفری، ۱٤۰۱: ۱۱۰۹).

اگرچه فناوری بلاکچین از رفتارهای تقلبی جلوگیری می‌کند، اما به تنهایی نمی‌تواند تقلب را تشخیص دهد. استفاده از برنامه‌های بلاکچین، مانند بیت‌کوین، مجرمان سایبری را تشویق

1. Namasudra

می‌کند تا در جرائم سایبری شرکت کنند. در نتیجه، فناوری قراردادهای هوشمند برای جلوگیری از این مجرمان به کار گرفته شده است. آن‌ها با ارائه تراکنش‌های غیرقابل‌برگشت، ارزش سهام پرداخت را در تجارت تسهیل می‌کنند و همچنین، برای فعالیت‌های غیرقانونی یا مخرب مانند پولشویی و باج‌افزار استفاده می‌شوند.

۲. ویژگی‌های قراردادهای هوشمند

شناخت ویژگیهای قراردادهای هوشمند از این نظر دارای اهمیت دارد که به نقش و جایگاه قراردادهای هوشمند در پیشگیری از جرم کمک می‌نماید. قراردادهای هوشمند دارای ویژگی‌های خاصی می‌باشد که آنها را از سایر قراردادهای الکترونیکی متمایز می‌نماید.

۲-۱. شفافیت در قراردادهای هوشمند

ماهیت قراردادهای هوشمند بدین صورت است که برای اجرا باید از طریق امضای دیجیتالی تأیید گردند. این امضاء بیان‌کننده قصد و رضایت طرف معامله از انعقاد معامله می‌باشد. بر این مبنا، فردی که از طریق قرارداد هوشمند مبادرت به انعقاد قرارداد هوشمند می‌نماید، در حقیقت به انتقال املاک خود از طریق عقود تملیکی اقدام می‌کند.

بر این اساس، آنچه که به عنوان عوض قراردادی مورد معامله صورت می‌گیرد، ملک وی بوده و وی امکان انعقاد عقد نسبت به املاک دیگران را ندارد؛ مگر اینکه به عنوان وکالت این امر را انجام دهد که در این صورت، وکیل نیز باید از قوه حاکمه مجوز انعقاد این عقود را گرفته و پس از تأیید قرارداد وی، ضامن صحت مفاد قرارداد خواهد بود (کازانو[1]، ۲۰۱۶: ۳۰). بنابراین، در هر حال، امکان انعقاد عقود فضولی توسط این مکانیسم ممکن نمی‌باشد که ثمره این امر حفظ حق مالکانه مالک حقیقی و جلوگیری از ورود وی در فرآیند طولانی‌مدت رسیدگی‌های قضایی می‌باشد. پس از قطعیت معامله، نمونه‌ای از آن به تمامی سیستم‌های متصل به بلاکچین ارسال شده و تمامی افراد از از طریق کلیدهای عمومی قادر به مشاهده مفاد قراردادهای منعقده می‌باشند.

این امر موجب می‌گردد تا افراد در عرصه مبادلات الکترونیکی از معاملات دیگران آگاه بوده و به نوعی، با آگاهی کامل از دارایی افراد نسبت به انعقاد معامله با آنان اقدام نمایند. این قراردادها پس از انعقاد بصورت کد بهینه‌سازی‌شده در بستر بلاکچین ثبت گردیده و با توجه به مشخص‌بودن مشخصات عوضین معامله دیگر امکان انعقاد عقود دیگر نسبت به این عوضین

1. Cassano

امکان‌پذیر نمی‌باشد که ثمره این امر در عدم امکان انجام معاملات متعدد بر روی اموال مورد معامله قرار گرفته می‌باشد (مظفری، ۱٤۰۰: ۲٦۲). این ویژگی کمک می‌نماید تا اطمینان بیشتری به این قراردادها شکل بگیرد.

۲-۲. امکان خوداجرایی قراردادهای هوشمند

برای انعقاد قراردادهای هوشمند، افراد باید دارای امضاء الکترونیکی باشند و افراد در صورتی می‌توانند دارای امضای الکترونیکی باشند که از طرف مراجع صلاحیتدار قانونی به آنها یک کلید خصوصی جهت امکان امضای معامله داده شود. یکی از تشریفات دریافت این مجوز، احراز هویت افراد و تعیین میزان دقیق دارایی‌های وی می‌باشد (سینگ[1]، ۲۰۱۸: ۲۲).

موضوع احراز هویت در خصوص قراردادها اهمیت دارد و اولین مرحله از انعقاد یک قرارداد می‌باشد؛ زیرا در صورتی که طرفین قرارداد مشخص نباشند، قرارداد دارای ایراد می‌باشد و البته، این امر در قراردادهای هوشمند که ممکن است حتی یک رباط در آنسوی رایانه در حال انعقاد یک قرارداد باشد، دارای اهمیت بسیاری می‌باشد.

یکی از زیرساخت‌های به‌کارگیری چنین فرآیندی، انجام کامل تشریفات ثبت اموال غیرمنقول افراد جهت شناسایی دقیق میزان دارایی غیرمنقول آن‌ها می‌باشد. در صورتی که چنین هدفی محقق گردد، زمینه برقراری چنین قراردادهایی در نظام حقوقی فراهم می‌گردد. این قراردادها در یک سیستم پیوسته نامتمرکز منعقد می‌گردند؛ پس از تأیید و ثبت در بلاکچین دیگر نیازی به ثبت مجدد در مراجعی مانند اداره ثبت نداشته و تمامی اسناد آنها رسمی تلقی شده و بصورت الکترونیکی می‌باشند، چرا که با توجه به پیوسته‌بودن سیستم، به محض انعقاد و انتقال مالکیت، این انتقال در سیستم ثبت نیز مشخص می‌گردد (لوی[2]، ۲۰۱۷: ٤).

این قراردادها به دو صورت کنترل می‌گردند: اول، توسط مراجع صلاحیتدار و سپس، توسط رایانه که از طریق دستورالعمل‌های پیش‌فرض بر نحوه قراردادن شروط و توافقات برای آنکه خلاف قانون نباشد، نظارت دارد؛ بدین صورت که این دستورالعمل‌های پیش‌نویس‌شده الکترونیکی به رایانه امکان بازخوانی قرارداد را داده و در صورتی که امری برخلاف قانون در قرارداد هرچند با توافق طرفین ذکر شده باشد، موجب عدم امکان انعقاد قرارداد می‌گردد.

1. Singh
2. Levy

یافته‌ها

۱. اهداف و کارکرد پیشگیری از جرائم مرتبط با ارزهای دیجیتال

یکی از نگرانی‌های فعالیت‌های اینترنتی امروزه، جرائمی است که در فضا واقع می‌شود و قابلیت‌های قرارداد هوشمند نشان می‌دهد که امکان پیشگیری از این جرائم را دارد. پیشگیری به مجموعه تدابیر و سیاستهایی گفته می‌شود که یک دولت با مداخله سعی در کاهش خسارت‌های ناشی از اعمال بزهکارانه و رفتارهای مرتبط با آن دارد. این اقدامات پیشگیرانه نه تنها می‌توانند از وقوع جرم جلوگیری کنند، بلکه راه‌حل‌های مقرون‌به‌صرفه‌ای هستند که موجب صرفه‌جویی در منابع عمومی می‌شوند (کرولی[1]، ۲۰۱۳: ٤).

در خصوص پیشگیری کیفری باید گفت که مبنای نظری این نوع پیشگیری، اصرار بر تأیید بازدارندگی مقررات کیفری و روشهای رسمی یا قانونی برخورد با جرم، یعنی اعمال مجازات و اقدامات موثرتر برای دستگیری مرتکبین، از جمله تقویت پلیس و دستگاه قضایی، است.

در حقیقت، پیشگیری کیفری با تهدید تابعان حقوق کیفری، از یک سو و به اجرا گذاشتن این تهدید از طریق مجازات کسانی که ممنوعیت‌های کیفری را نقض کرده‌اند از سوی دیگر، در مقام پیشگیری عام و خاص از جرم و تکرار آن است (خدائیان، ۱۳۹۱: ٤).

در خصوص مفهوم پیشگیری غیرکیفری و خصوصیات آن، تعاریف متعددی ارائه گردیده است. در یک تعریف، موریس کوسن، جرم‌شناس کانادایی، پیشگیری غیرکیفری را چنین تعریف کرده است: «مجموعه اقدامها و تدابیر غیرقهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم و کاهش وخامت جرم پیرامون علل جرائم اتخاذ می‌شود.»

پیشگیری به دو شکل کیفری و غیرکیفری درصدد کاهش میزان بزهکاری است که برحسب زمان مداخله، به دو نوع کنشی و واکنشی تقسیم می‌شود. پیشگیری کنشی به تدابیر پیشگیرانه‌ای گفته می‌شود که قبل از وقوع جرم با هدف جلوگیری از ارتکاب جرم و یا کاهش ضرر و زیان ناشی از آن اتخاذ می‌شود و دو نوع است: یکی، پیشگیری اجتماعی از جرم به روش اصلاح جامعه و نظام اجتماعی مانند خانواده، آموزش‌وپرورش، اقتصاد و پرورش افراد در فرآیند جامعه‌پذیری آنها و دیگری، پیشگیری وضعی است که از گذر زمان، فرصت و موقعیت‌هایی که ارتکاب جرم را تسهیل می‌کند، تحقق می‌یابد (روستایی، ۱۳۸۸: ۲۱۷).

در خصوص پیشگیری کیفری باید گفت که مبنای نظری این نوع پیشگیری، اصرار بر تأیید بازدارندگی مقررات کیفری و روشهای رسمی یا قانونی برخورد با جرم، یعنی اعمال مجازات

1. Crowley

و اقدامات موثرتر برای دستگیری مرتکبین از جمله تقویت پلیس و دستگاه قضایی است (صفاری، ۱۳۸۱: ۲۷۷). در حقیقت، پیشگیری کیفری با تهدید تابعان حقوق کیفری، از یک سو و به اجرا گذاشتن این تهدید از طریق مجازات کسانی که ممنوعیت‌های کیفری را نقض کرده‌اند از سوی دیگر، در مقام پیشگیری عام و خاص از جرم و تکرار آن است.

در خصوص مفهوم پیشگیری غیرکیفری و خصوصیات آن تعاریف متعددی ارائه گردیده است. در یک تعریف، موریس کوسن، جرم‌شناس کانادایی، پیشگیری غیرکیفری را چنین تعریف کرده است: «مجموعه اقدامها و تدابیر غیرقهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم و کاهش وخامت جرم پیرامون علل جرائم اتخاذ می‌شود.» (ابراهیمی، ۱۳۹۰: ۳۸).

با توجه به تعاریف متعددی که از پیشگیری غیرکیفری صورت گرفته است، به طور کلی می‌توان چند ویژگی عمده برای پیشگیری احصاء نمود: ۱. غیرقهرآمیزبودن تدابیر ۲. اختصاصی‌بودن اقدامات ۳. کاستن آثار جرم و ٤. درنظرگرفتن عوامل خطر و محیط اجتماعی (اکرمی، ۱۳۹۵: ۲). از میان تقسیم‌بندیهای مختلفی که در خصوص تدابیر پیشگیرانه صورت گرفته است، دو نوع پیشگیری اجتماعی و پیشگیری وضعی بیشترین مقبولیت را دارد.

پیشگیری اجتماعی مجموعه اقدام‌های پیشگیرانه است که بر کلیه محیط‌های پیرامون فرد که در فرایند جامعه‌پذیری نقش داشته و دارای کارکرد اجتماعی هستند، تأثیر می‌گذارد. این روش پیشگیری از جرم با تمرکز بر برنامه‌های تکمیلی، سعی در بهبود بهداشت زندگی خانوادگی، آموزش، مسکن، فرصت‌های شغلی و اوقات فراغت دارد تا محیطی سالم و امن ایجاد نماید. در حقیقت، پیشگیری اجتماعی به طور مستقیم یا غیرمستقیم هدف تأثیرگذاری بر شخصیت افراد است تا از سازماندهی فعالیت خود، حول محور انگیزه‌های بزهکارانه پرهیز کنند (کی نیا، ۱۳۷٦: ۹۷). کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. به عبارت دیگر، این نوع پیشگیری دربرگیرنده مجموعه تدابیر غیرکیفری است که از طریق ازبین‌بردن یا کاهش فرصتهای مناسب، از ارتکاب بزه جلوگیری می‌کند.

پیشگیری وضعی برخلاف پیشگیری اجتماعی، مبتنی بر تقویت ارزش‌های جامعه، متعالی‌کردن نهادهای آن، بررسی ریشه‌های بزهکاری و قطع آن نیست، بلکه به طور ساده بر کاهش فرصتها و موقعیت‌های ارتکاب جرم تکیه دارد. این امر از یک سو، از طریق کاهش وضعیت‌های ماقبل بزهکاری، یعنی وضعیت‌های پیش‌جنایی که وقوع جرم را مساعد و تسهیل

می‌کند و از سوی دیگر، با افزایش خطر شناسایی و احتمال دستگیری بزهکاران انجام می‌شود (خسرو شاهی و قدمی، ۱۳۹۸: ۲۸۹). رکن اصلی پیشگیری وضعی، حفظ آماج‌ها و بزه دیدگان از تعرض مجرمان است. آنچه در این نوع پیشگیری دنبال می‌شود، این است که با جاذبه‌زدایی از جرم، بالابردن هزینه و کاهش احتمال نتیجه‌گیری از جرم، زمینه ارتکاب آن را از بین ببریم یا تا حد قابل‌قبولی پایین بیاوریم. در خصوص ارتکاب جرم تأمین مالی تروریسم از طریق رایانه باید گفت که مخاطبان اصلی پیشگیری وضعی از جرائم رایانه‌ای کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای تبادل اطلاعات در اختیار آنها قرار می‌دهد، مرتکب جرم شوند؛ نه این که خود دست به ابتکار عمل بزنند.

با این وصف، پیشگیری از جرائم مرتبط با ارزهای دیجیتال اهمیت زیادی دارد؛ زیرا با توجه به ماهیت دیجیتال و بین‌المللی این ارزها، امکان سوءاستفاده‌های مالی و جرائم سایبری افزایش می‌یابد. یکی از اهداف اصلی پیشگیری از جرائم دیجیتال، حفاظت از سرمایه‌های افراد در برابر سرقت، تقلب و کلاهبرداری‌های مرتبط با ارزهای دیجیتال است. با ایجاد تدابیر پیشگیرانه و حفاظت از کاربران، اعتماد عمومی به ارزهای دیجیتال افزایش یافته و از نفوذ بازارهای غیررسمی جلوگیری می‌شود.

با توجه به جهانی‌بودن ارزهای دیجیتال، همکاری بین‌المللی میان کشورها برای مقابله با جرائم فرامرزی مرتبط با این ارزها ضروری است. تشکیل نهادها و تیم‌های تخصصی برای مبارزه با جرائم سایبری و مرتبط با ارزهای دیجیتال می‌تواند به کنترل و پیشگیری از این جرائم کمک کند. به طور کلی، با توجه به گسترش روزافزون ارزهای دیجیتال، پیشگیری از جرائم مرتبط با آن‌ها از اهمیت زیادی برخوردار است و نیازمند رویکردهای چندجانبه و همگانی است.

۲. پیشگیری از جرم در پرتو قراردادهای هوشمند

قراردادهای هوشمند تحت نظارت سیستم رایانه‌ای که بر مبنای دستورالعمل داده‌شده عمل نموده و نسبت به انعقاد عقد نظارت داشته و جهت تأیید قرارداد برای ثبت در بستر بلاکچین قرارداد را مورد باز بینی قرار می‌دهد، منعقد می‌گردند. در خصوص پیشگیری از قراردادهای هوشمند، اگرچه پیشگیری کیفری ضرورت دارد، اما اتخاذ تدابیر لازم در پیشگیری غیر کیفری (وضعی و اجتماعی) با آثار بهتری همراه است.

در این نوع قراردادها، صرف‌نظر از انگیزه مرتکب بر نحوه انعقاد عقد، رکن مادی جرم محقق نشده؛ چرا که در صورتی که در قرارداد هر گونه امر خلاف واقعی اتفاق افتاده باشد، هوش مصنوعی از انعقاد عقد خودداری نموده و در هیچ صورتی عقد منعقد نمی‌گردد. بنابراین، انعقاد این قراردادها بیشتر رویکردی پیشگیرانه نسبت به تحقق جرائم دارد (ریکا[1]، ۲۰۱۶: ۵۵). به نظر می‌رسد اصلی‌ترین کاربرد قراردادهای هوشمند در پیشگیری از وقوع جرائم مالی مرتبط با عقود و معاملات باشد که جرائمی همچون فروش مال غیر، کلاهبرداری، تحصیل مال نامشروع، پولشویی، جعل و غیره را شامل می‌گردد.

با توجه به ناشناس‌بودن و حذف واسطه‌های مورد اعتماد، ارزهای دیجیتال مانند بیت‌کوین باعث ایجاد یا رشد در بسیاری از مشاغل و جوامع شده است که برخی از این موارد مجرمانه هستند؛ به عنوان مثال، پولشویی، بازارهای غیرقانونی و باج‌افزار. ارزهای دیجیتال نسل بعدی مانند اتریوم شامل زبان‌های برنامه‌نویسی غنی برای پشتیبانی از قراردادهای هوشمند خواهند بود، برنامه‌هایی که به طور مستقل تراکنش‌های میانی را انجام می‌دهند.

در این خصوص، خطر قراردادهای هوشمند که به اکوسیستم‌های جنایی جدید دامن می‌زنند، به عنوان یک چالش مد نظر می‌باشد. به طور خاص، این امر مهم است که چگونه قراردادهای هوشمند می‌تواند نشت اطلاعات محرمانه، سرقت کلیدهای رمزنگاری و جنایات مختلف در دنیای واقعی را تسهیل کنند.

قراردادهای هوشمند برای نشت اسرار در زبان‌های اسکریپت‌نویسی موجود مانند زبان اتریوم به‌طور مؤثر قابل‌تحقق هستند. همچنین، از قراردادهای هوشمند برای سرقت کلیدهای رمزنگاری می‌توان با استفاده از موارد ابتدایی که قبلاً در این زبان‌ها قابل‌بیان هستند و برای آن‌ها پسوندهای زبان پشتیبانی کارآمد پیش‌بینی می‌شود، استفاده نمود. به علاوه، فیدهای داده تأییدشده، یکی از ویژگی‌های نوظهور سیستم‌های قرارداد هوشمند است که می‌توانند برای جرائم دنیای واقعی (مانند جرائم دارایی) تسهیل‌کننده باشند.

ویژگی سازگاری در قراردادهای هوشمند تضمین می‌کند که تمام گره‌های همتا در شبکه بلاکچین پس از فراخوانی، در یک دفترکل جهانی ثابت باقی می‌مانند و ویژگی پاسخگویی به افراد امکان می‌دهد تا در صورت انجام فعالیت‌های مخرب، برخی اقدامات مربوطه مانند مجازات‌های پولی انجام گیرد. ویژگی منشأ نشان می‌دهد که بلاکچین اطلاعاتی را در مورد منشاء رکوردهای داده ارائه می‌دهد (منور[2]، ۲۰۲۲: ۲۶۹).

1. Riikka
2. Munawar

چندین مطالعه، عملکردهای اصلی یک بلاک‌چین را استخراج کرده و مدل بلاکچین رمزنگاری را رسمیت می‌بخشد. با ساخت این عملکرد ایده‌آل، مدل بلاک‌چین رمزنگاری‌شده در چارچوب ترکیب‌پذیری جهانی تعمیم‌یافته ساخته می‌شود که هدف آن، مشخص‌کردن و استدلال جامع در مورد امنیت، پروتکل‌های توانمند بلاک‌چین و تسهیل طراحی برنامه‌های غیرمتمرکز در بلاک‌چین است (آئوبله[1]، ۲۰۲۲: ۱۵).

یکی از چالش‌ها و خطرات کلیدی در امنیت بلاکچین، عدم وجود استانداردها و مقررات تعیین‌شده است. در مطالعه‌ای که توسط جولز و همکاران صورت گرفت، مفهوم قراردادهای هوشمند مجرمانه[2] معرفی شد که چندین نمونه معمولی از این قراردادها را برجسته می‌کند؛ مانند افشای داده‌های محرمانه، سرقت کلیدهای رمزنگاری و مشارکت در فعالیت‌های مجرمانه در دنیای واقعی مانند قتل، آتش‌سوزی و تروریسم. فقدان مکانیسم‌های نظارتی مؤثر، نظارت و رسیدگی به این فعالیت‌های مخرب در قراردادهای هوشمند را چالش‌برانگیز می‌کند (جین[3]، ۲۰۲۲: ۱). قراردادهای هوشمند مجرمانه، قراردادهای هوشمندی هستند که اقدامات قراردادی را برای فریب یا آسیب‌رساندن به کاربران بلاکچین به منظور سرقت ارزهای دیجیتال، ترویج تراکنش‌های غیرقانونی و غیره اجرا می‌کنند.

قرارگرفتن در معرض داده نیز موضوع دیگری است که در این حوزه باید به آن توجه نمود. قرارگرفتن در معرض داده، به قرارگرفتن در معرض داده‌های حساس و نشت اطلاعات حریم خصوصی اشاره دارد که می‌تواند زمانی رخ دهد که داده‌های خصوصی با رمزگذاری ضعیف در بلاک‌چین ذخیره می‌شوند. علاوه بر این، از آنجایی که تراکنش‌های بلاکچین قابل‌ردیابی هستند، برخی از فعالیت‌های یک فرد را می‌توان شناسایی کرد (سینگ، کوشواها، جوشی و سینگ[4]، ۲۰۲۳: ٤). همچنین، قراردادهای هوشمند بدون مجوز دارای محدودیت‌هایی مانند عدم نظارت، مقیاس‌پذیری و قابلیت همکاری است که در راه‌اندازی، بهره‌برداری و نگهداری این قراردادها برای همه شرکت‌کنندگان در تجارت بین‌المللی مشکل ایجاد می‌کند.

علاوه بر این، قراردادهای هوشمند همچنین با تسهیل نشت اطلاعات محرمانه، سرقت کلیدهای رمزنگاری و سایر جرائم مانند قتل و تروریسم، خطر سوختن اکوسیستم جنایی را به همراه دارند. در مقابل، بلاکچین مجاز می‌تواند با اطمینان از اعتبار همه نهادهای درگیر، حفظ

1. Ahubele
2. criminal smart contracts (CSCs)
3. Jin
4. Singh, Kushwaha & Joshi

نظم تراکنش و تأیید صحت اسناد ارائه‌شده و نمایش‌های مرتبط در مبارزه با چنین رفتار متقلبانه‌ای مؤثر باشد.

البته، پلتفرم‌های قرارداد هوشمند دارای ضعف‌های نرم‌افزاری ذاتی هستند که آنها را در برابر تقلب آسیب‌پذیر می‌کند. انجام اقدامات مجرمانه با کمک قراردادهای هوشمند امکان‌پذیر است. ورود مجدد، تعداد صحیح بیش از حد زیر جریان و اتریوم قفل‌شده[1] شایع‌ترین نقص قراردادهای هوشمند هستند (جورج[2]، ۲۰۲۳: ۳۷). اتریوم در مسیر تبدیل‌شدن به بستر مالی غیرمتمرکز، منسجم‌تر و قوی‌تر می‌شود و تاکنون تقریباً یک‌چهارم موجودی اتریوم در قراردادهای هوشمند قفل شده است. با این وصف، باید گفت که نتایج بدست‌آمده بر ضرورت ایجاد سیاست و حفاظت فنی در خصوص قراردادهای هوشمند تأکید دارد. با این حال، دو ویژگی مهم باعث می‌شود تا قراردادهای هوشمند از ارتکاب جرائم مرتبط جلوگیری کنند. این دو ویژگی شامل شفافیت و امنیت است. در قراردادهای هوشمند، در دفترکل توزیع‌شده‌ای ذخیره می‌شوند و قابل‌پیگیری هستند؛ این امر باعث افزایش شفافیت و اعتماد می‌شود. همچنین، قراردادهای هوشمند از فناوری‌های رمزنگاری برای ایمن‌سازی اطلاعات استفاده می‌کنند و عموماً، در برابر دستکاری و کلاهبرداری مقاوم هستند.

کاربران پلتفرم اتریوم «شبه‌ناشناس» هستند و یک کاربر می‌تواند چندین حساب تحت چندین هویت رمزنگاری داشته باشد. این امر بیانگر آن است که چگونه قراردادهای هوشمند می‌توانند نشت اطلاعات محرمانه، سرقت کلیدهای رمزنگاری و جرائم مختلف در دنیای واقعی را تسهیل کنند. آتزی و همکاران[3] رده‌بندی از آسیب‌پذیری‌های قراردادهای هوشمند در اتریوم از جمله آسیب‌پذیری‌هایی مانند اختلال و وضعیت‌های غیرقابل‌پیش‌بینی را ارائه کرده‌اند (جیانگ[4]، ۲۰۲۳: ۲۸۳).

قراردادهای هوشمند در حال حاضر با توجه به فناوری که بر اساس آن بکار گرفته می‌شود، دارای آسیب‌پذیری می‌باشد. آسیب‌پذیری قراردادهای هوشمند، خطا یا نقصی در کد قرارداد هوشمند است که می‌تواند منجر به عملکرد نادرست، تغییر حالت یا جابجایی پول شود (لیفنگ[5]، ۲۰۲۹: ۱۴۹). این آسیب‌پذیری‌ها شامل وجود خطا در کدها، ناسازگاری با پروتکل بلاک‌چین، فراموش‌کردن تابع، حملات اوراکل و حملات مختلف دیگر مانند فرانت رانینگ

1. Locked Ether
2. George
3. Atzei et al
4. Jiang
5. Lifeng

می‌باشد. در این راستا، قراردادهای هوشمند توسط برخی از محققان مورد مطالعه قرار گرفته، اما همچنان نمونه اپلیکیشن‌هایی وجود دارد که با وجود استفاده از قرارداد هوشمند، همچنان برای تأیید برخی رویه‌های امنیتی نیاز به واسطه دارند (یلی، آندریا، تائو لی، زینچون و مینگهائو[1]، ۲۰۱۹: ۲۹۳). سیستم‌های تشخیص نفوذ کارآمدترین راه برای دفاع در برابر حملاتی هستند که سیستم‌های رایانه‌ای را هدف می‌گیرند. این سیستم‌ها تقریباً در تمام زیرساخت‌های فناوری اطلاعات در مقیاس بزرگ استفاده می‌شوند. اساساً، دو نوع اصلی سیستم‌های تشخیص نفوذ وجود دارد: مبتنی بر امضا و مبتنی بر ناهنجاری. سیستم‌های مبتنی بر ناهنجاری یک مدل آماری ایجاد می‌کنند که رفتار عادی را توصیف می‌کند و هر رفتار غیرعادی که از مدل منحرف شود، شناسایی می‌شود. در نهایت، باید گفت قراردادهای هوشمند با فناوری فعلی امکان پیشگیری از جرم را دارد؛ اما دو دسته از قراردادها، یعنی قراردادهای مجرمانه و آسیب‌پذیر، ممکن است بستر ارتکاب جرائم را فراهم آورد. با رشد فناوری و شناسایی نقاط آسیب‌پذیر قراردادهای هوشمند می‌توان ایرادات این قراردادها را که امکان و شرایط ارتکاب جرم را فراهم می‌کند، برطرف نمود.

بحث و نتیجه‌گیری

قرارداد هوشمند یک برنامه خوداجرا است که اقدامات مورد نیاز در یک توافق‌نامه یا قرارداد را خودکار می‌کند و پس از تکمیل، تراکنش‌ها قابل‌پیگیری و برگشت‌ناپذیر هستند. به عبارت دیگر، این قراردادها به عنوان یک پروتکل تراکنش رایانه‌ای تعریف می‌شود که می‌تواند به طور جزئی یا کامل بر اساس شرایط یک قرارداد ازپیش‌تعریف‌شده بدون تعامل انسانی اجرا شود. به طور خاص، قرارداد هوشمند یک پروتکل رایانه‌ای را بین شرکت کنندگان غیرقابل‌اعتماد ایجاد می‌کند. پس از برآورده‌شدن پیش‌شرط‌های کتبی، قرارداد به طور خودکار اجرا می‌شود و قابل‌فسخ نیست.

اگرچه قراردادهای هوشمند بر بستر بلاکچین اجرا می‌شوند، با این حال، با آنکه فناوری بلاکچین از رفتارهای تقلبی جلوگیری می‌کند، اما به تنهایی نمی‌تواند تقلب را تشخیص دهد. در نتیجه، فناوری قراردادهای هوشمند برای جلوگیری از این مجرمان به کار گرفته شده است. آن‌ها با ارائه تراکنش‌های غیرقابل‌برگشت، ارزش سهام پرداخت را در تجارت تسهیل می‌کنند و همچنین، برای فعالیت‌های غیرقانونی یا مخرب مانند پولشویی و باج‌افزار استفاده می‌شوند. قراردادهای هوشمند دارای ویژگی‌هایی از جمله شفافیت و امکان خوداجرایی قراردادهای

1. Yilei, Andrea, Tao Li, Xinchun& Minghao

هوشمند می‌باشند. با این حال، یکی از نگرانی‌های فعالیت‌های اینترنتی امروزه، جرائمی است که در فضا واقع می‌شود و قابلیت‌های قرارداد هوشمند نشان می‌دهد که امکان پیشگیری از این جرائم را دارد. پیشگیری به مجموعه تدابیر و سیاستهایی گفته می‌شود که یک دولت با مداخله سعی در کاهش خسارت‌های ناشی از اعمال بزهکارانه و رفتارهای مرتبط با آن دارد. این اقدامات پیشگیرانه نه تنها می‌توانند از وقوع جرم جلوگیری کنند، بلکه راه‌حل‌های مقرون‌به‌صرفه‌ای هستند که موجب صرفه‌جویی در منابع عمومی می‌شوند.

در خصوص پیشگیری از قراردادهای هوشمند، اگرچه پیشگیری کیفری ضرورت دارد، اما اتخاذ تدابیر لازم در پیشگیری غیرکیفری (وضعی و اجتماعی) با آثار بهتری همراه است. قراردادهای هوشمند تحت نظارت سیستم رایانه‌ای که بر مبنای دستورالعمل داده‌شده عمل نموده و نسبت به انعقاد عقد نظارت داشته و جهت تأیید قرارداد برای ثبت در بستر بلاکچین قرارداد را مورد بازبینی قرار می‌دهد، منعقد می‌گردند. با توجه به ناشناس‌بودن و حذف واسطه‌های مورد اعتماد، ارزهای دیجیتال مانند بیت‌کوین باعث ایجاد یا رشد در بسیاری از مشاغل و جوامع شده است که برخی از این موارد مجرمانه هستند؛ به عنوان مثال، پولشویی، بازارهای غیرقانونی و باج‌افزار. ارزهای دیجیتال نسل بعدی مانند اتریوم شامل زبان‌های برنامه‌نویسی غنی برای پشتیبانی از قراردادهای هوشمند خواهند بود، برنامه‌هایی که به طور مستقل تراکنش‌های میانی را انجام می‌دهند.

قرارگرفتن در معرض داده نیز موضوع دیگری است که در این حوزه باید به آن توجه نمود. قرارگرفتن در معرض داده، به قرارگرفتن در معرض داده‌های حساس و نشت اطلاعات حریم خصوصی اشاره دارد که می‌تواند زمانی رخ دهد که داده‌های خصوصی با رمزگذاری ضعیف در بلاک‌چین ذخیره می‌شوند. علاوه بر این، قراردادهای هوشمند همچنین با تسهیل نشت اطلاعات محرمانه، سرقت کلیدهای رمزنگاری و سایر جرائم مانند قتل و تروریسم، خطر سوختن اکوسیستم جنایی را به همراه دارند. با این وصف، باید گفت که نتایج بدست‌آمده بر ضرورت ایجاد سیاست و حفاظت فنی در خصوص قراردادهای هوشمند تأکید دارد. با این حال، دو ویژگی مهم باعث می‌شود تا قراردادهای هوشمند از ارتکاب جرائم مرتبط جلوگیری کنند. این دو ویژگی شامل شفافیت و امنیت است. قراردادهای هوشمند در دفترکل توزیع‌شده‌ای ذخیره می‌شوند و قابل‌پیگیری هستند؛ این امر باعث افزایش شفافیت و اعتماد می‌شود. همچنین، قراردادهای هوشمند از فناوری‌های رمزنگاری برای ایمن‌سازی اطلاعات استفاده می‌کنند و عموماً، در برابر دستکاری و کلاهبرداری مقاوم هستند. قراردادهای هوشمند

در حال حاضر، با توجه به فناوری که بر اساس آن بکار گرفته می‌شوند، دارای آسیب‌پذیری می‌باشند.

آسیب‌پذیری قراردادهای هوشمند، خطا یا نقصی در کد قرارداد هوشمند است که می‌تواند منجر به عملکرد نادرست، تغییر حالت یا جابجایی پول شود. در نهایت، باید گفت قراردادهای هوشمند با فناوری فعلی امکان پیشگیری از جرم را دارد؛ اما دو دسته از قراردادها، یعنی قراردادهای مجرمانه و آسیب‌پذیر، ممکن است بستر ارتکاب جرائم را فراهم آورد. همچنین، اساساً، دو نوع اصلی سیستم‌های تشخیص نفوذ وجود دارد: مبتنی بر امضا و مبتنی بر ناهنجاری. لذا، باید گفت با رشد فناوری و شناسایی نقاط آسیب‌پذیر قراردادهای هوشمند می‌توان ایرادات این قراردادها را که امکان و شرایط ارتکاب جرم را فراهم می‌کند، برطرف نمود. برای پیاده‌سازی تحول دیجیتال در سایه قراردادهای هوشمند، به تحول و توسعه زیرساخت‌های فنی و فرهنگی و همچنین، تحول ساختاری نیاز داریم؛ به‌طوری‌که از چالش‌هایی همچون هک و تهدید سایبری در امان باشیم.

از سوی دیگر، هوشمندسازی قراردادها شفافیت و ردیابی‌پذیری تراکنش‌ها را افزایش می‌دهد و از این طریق، امکان شناسایی و جلوگیری از فعالیت‌های مجرمانه نظیر پول‌شویی و تأمین مالی تروریسم را فراهم می‌سازد. همچنین، با حذف واسطه‌ها و کاهش تعاملات انسانی، امکان اشتباهات عمدی یا غیرعمدی کاهش یافته و سرعت و دقت در اجرای قراردادها افزایش می‌یابد.

بنابراین، با توجه به مزایای متعدد قراردادهای هوشمند، این فناوری می‌تواند به عنوان ابزاری کارآمد برای پیشگیری از جرائم مرتبط با ارزهای دیجیتال مورد استفاده قرار گیرد و نقشی کلیدی در بهبود امنیت و اعتماد در فضای دیجیتال ایفا کند. استفاده از این فناوری، همراه با تدوین قوانین مناسب و همکاری‌های بین‌المللی، می‌تواند به کاهش جرائم و ترویج استفاده قانونی و امن از ارزهای دیجیتال کمک شایانی کند.

پیشنهادها

۱) ایجاد استانداردهای حقوقی برای قراردادهای هوشمند: تدوین استانداردهای حقوقی شفاف و جامع برای قراردادهای هوشمند می‌تواند از سوءاستفاده‌ها و جرائم مرتبط با ارزهای دیجیتال جلوگیری کند. این استانداردها باید به‌گونه‌ای طراحی شوند که تمامی طرفین قرارداد از حقوق و وظایف خود آگاه باشند.

۲) آموزش و آگاهی‌رسانی: برگزاری دوره‌های آموزشی و کارگاه‌های تخصصی برای فعالان حوزه ارزهای دیجیتال و کاربران عمومی به‌منظور آشنایی با مزایا و ریسک‌های قراردادهای هوشمند. افزایش آگاهی می‌تواند از ارتکاب جرائم به دلیل ناآگاهی یا سوءاستفاده از دانش ناکافی پیشگیری کند.

۳) همکاری بین‌المللی در تنظیم قوانین: با توجه به جهانی‌بودن ارزهای دیجیتال، همکاری بین‌المللی در تدوین قوانین و مقررات مرتبط با قراردادهای هوشمند ضروری است. این همکاری می‌تواند به‌ویژه در زمینه تبادل اطلاعات و پیشگیری از پول‌شویی و تأمین مالی تروریسم مؤثر باشد.

٤) استفاده از الگوریتم‌های پیش‌بینی‌کننده برای شناسایی رفتارهای مشکوک: پیاده‌سازی الگوریتم‌های هوش مصنوعی در قراردادهای هوشمند که توانایی شناسایی و پیش‌بینی رفتارهای مشکوک و جرائم احتمالی را دارند. این الگوریتم‌ها می‌توانند به‌صورت خودکار تراکنش‌های مشکوک را مسدود و به مراجع ذی‌صلاح گزارش کنند.

۵) توسعه قراردادهای هوشمند قابل‌بازنگری: ایجاد قراردادهای هوشمندی که امکان بازنگری و اصلاح در صورت بروز اختلاف یا مشکلات غیرمنتظره را فراهم می‌کنند. این قابلیت می‌تواند از تبدیل‌شدن اختلافات به جرائم پیشگیری کند.

سپاسگزاری

پژوهشگران از عزیزانی که در فرآیند ویراستاری ادبی و صفحه‌آرایی این مقاله همکاری و راهنمایی داشتند، کمال تشکر و امتنان را دارند.

منابع

– ابراهیمی، شهرام. (۱۳۹۰). *جرم‌شناسی پیشگیری*. جلد اول. انتشارات میزان.

– اکرمی، سام؛ اکرمی، سعیده. (۱۳۹۵). پیشگیری غیرکیفری در جرائم اینترنتی. *کنفرانس ملی چارسوی علوم انسانی*.

https://civilica.com/doc/721009/certificate/print/

– برنگی، حامد؛ راجی، فاطمه و خاصه، علی اکبر. (۱۳۹۹). تحلیل تحقیقات امنیت و حریم خصوصی حوزه بلاک‌چین: یک مطالعه علم سنجی. *محاسبات نرم*، ۹ (۱۷)، ۵۵ – ۴۰.

https://scj.kashanu.ac.ir/article_111451.html

– توکلی راد، رضا و طهماسبی، معصومه. (۱۴۰۱). بررسی چالش‌ها و مزایای پیاده‌سازی قراردادهای هوشمند مبتنی بر تکنولوژی بلاک‌چین. *کنفرانس بین‌المللی پژوهش‌های مدیریت و علوم انسانی در ایران رتبه بین‌المللی*، ۱۱.

https://civilica.com/doc/1673159/

– خدائیان چگنی، ذبیح اله. (۱۳۹۱). بررسی تطبیقی نهادهای نظام عدالت کیفری فرانسه و ایران در مقابله با جرائم اقتصادی. *مطالعات حقوقی*، ٤(۲)، ۵۸-۳۱.

https://jls.shirazu.ac.ir/article_1130.html

– خسروشاهی، قدرت الله و قدمی، نسرین. (۱۳۹۸). تبیین محیط اجتماعی به عنوان یکی از عوامل جرم‌زا و تأثیر آن بر سبک زندگی (با تأکید بر شبکه‌های اجتماعی مجازی). *پژوهش‌های حقوقی*، ۱۸(٤۰)، ٤۱۰ – ۳۸۹.

https://jlr.sdil.ac.ir/article_104283.html

– جعفری، سهیل و کوشا، جعفر. (۱۴۰۱). هوشمندسازی پیشگیری از قاچاق کالا، جلوه‌ها و چالش‌ها. *دیدگاه‌های حقوق قضایی*، ۲۷(۹۸)، ۲۶۳-۱۹۳.

https://jlviews.ujsas.ac.ir/article_703725.html

– رشوندبوکانی، مهدی و ناصر، مهدی. (۱۳۹۸). قصد متعاملین در قراردادهای هوشمند: شرایط اعتبار و شیوه احراز آن. *پژوهشنامه حقوق اسلامی*، ۲۰(٤۹)، ۳۰۰ – ۲۷۱.

https://ensani.ir/fa/article/408819/

– روستایی، مهرانگیز. (۱۳۸۸). ارزیابی مداخله کیفری در حوزه جرائم اقتصادی. *کارگاه*، ۲(۷)، ۳۱-۶.

http://det.jrl.police.ir/article_10610.html

– صادقی، حسین و مهدی، ناصر. (۱۳۹۷). ملاحظاتی برای سیاستگذاری حقوقی قراردادهای هوشمند. *سیاستگذاری عمومی*، ٤(۲)، ۱۶۳-۱٤۳.

https://jppolicy.ut.ac.ir/article_67873.html

– صفاری، علی. (۱۳۸۱)، انتقادات وارده بر پیشگیری وضعی از جرم. *تحقیقات حقوقی*، ۵(۳۵ و ۳۶)، ۲۳۳ – ۱۹٤.

https://lawresearchmagazine.sbu.ac.ir/article_56556.html

– صفری ورزرد، امیرحسین. (۱٤۰۱). بلاکچین و قراردادهای هوشمند: سازوکارها و کاربردها. *کنفرانس بین‌المللی مدیریت، گردشگری و تکنولوژی*، ٤.

https://civilica.com/doc/1461078/
– کرامتی معز، هادی و بهاری غازانی، مجید. (۱٤۰۱). پیشگیری وضعی از جرائم در بستر رمز ارزها. *مطالعات پیشگیری از جرم*، ۱۷ (٦۳)، ۱٦۷–۱۸۹.
http://cps.jrl.police.ir/article_98908.html
– کی نیا، مهدی. (۱۳۷٦). *مبانی جرم‌شناسی*. چاپ پنجم. نشر دانشگاه تهران.
– مصطفی مظفری، مهدی ناصر. (۱٤۰۰). نقش قراردادهای هوشمند در تثبیت حقوق مالکانه افراد. *فصلنامه تحقیقات حقوقی*، ۲٤(۹٥)، ۲۸۲–۲٥۹.
https://lawresearchmagazine.sbu.ac.ir/article_87133.html
– مهربانی، قربانعلی. (۱٤۰۱). چهارمین انقلاب صنعتی: ادغام هوش مصنوعی، بلاکچین و G٥. *کنفرانس ملی پژوهش‌های سازمان و مدیریت*، ٤.
https://civilica.com/doc/1572379/

-Ahubele, B. (2022). On-Blockchain Validation Smart Contract Model on Ethereum Distributed Ledger System for Pharmaceutical Products Distribution. *Journal of Computer Engineering*, 23(2), 10-22.
DOI:10.9790/0661-2302021022
-Boison, D. (2022). A Framework for the Evaluation of Factors Affecting Smart Contract Adoption and Enforceability in Port Supply Chain Industry in Ghana. *Theories and Applications*, 13, 957-969.
https://vbn.aau.dk/en/publications/a-framework-for-the-evaluation-of-factors-affecting-smart-contrac
- Cassano, J. (2016). *What are Smart Contracts? Crypto currency 's Killer App*. Fast Company. Online website accessible from,
https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app
-Chishti, M. S., Sufyan, F., Amit, B. (2021). Decentralized On-Chain Data Access via Smart Contracts in Ethereum Blockchain. *IEEE Transactions on Network and Service Management*, 9(1), 174 - 187.
https://doi.org/10.1109/TNSM.2021.3120912
-Crowley, D. Max. (2013). Building Efficient Crime Prevention Strategies Considering the Economics of Investing in Human Development. *Criminology & Public Policy*, 12(2), 353–366.
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4137908/
-George, W., Tareq, A. (2023). Review of Blockchain Applications in Food Supply Chains. *Blockchains*, 1(1), 34-57;
https://doi.org/10.3390/blockchains1010004
-Jin, L., , Yinzhi, C., Yan, C., Simone, C. (2022). EXGEN: Cross-platform, Automated Exploit Generation for Smart Contract Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, 20(1), 650-664.
https://doi.org/10.1109/TDSC.2022.3141396
-Jiang, Z.T. (2023). A Practical Detection and Defense Scheme Against Smart Contract Attacks Based on Transaction Features. *Mobile Internet Security*, 280-291. http://dx.doi.org/10.1007/978-981-99-4430-9_21
-Konate, K., Ndiaye, M. (2023). Anomaly Detection Algorithm Based on Smart Contracts Behaviours in Ethereum Ecosystem. *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*.
https://ieeexplore.ieee.org/abstract/document/10252520

-Lifeng, Z., Yilei, W., Fengyin, L., Yuemei, H., and Man, H. A. (2019). A game-theoretic method based on q-learning to invalidate criminal smartcontracts. *Information Sciences*, 498, 144-153.
https://doi.org/10.1016/j.ins.2019.05.061
-Levy, Karen, E. C. (2017). Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science Technology and Society*, 3 (2017), 1-15. DOI: https://doi.org/10.17351/ests2017.107
-Singh, A. (2018). *What is an oracle, How Oracles connect Smart contracts to the real world?*. Online website accessible from,
https://www.blockchainsemantics.com/blog/oracle-connects-smart-contracts- to-real-world
-Munawar, M. (2022). The Legality of Smart Contract in the Perspectives of Indonesian Law and Islamic Law. *Al-ISTINBATH Jurnal Hukum Islam*, 7(1).
http://dx.doi.org/10.29240/jhi.v7i1.4140
-Namasudra, S., Akkaya, K. (2023). Introduction to Blockchain Technology. *Journal Studies in Big Data Blockchain and its Applications in Industry*, 4,1-28.
https://doi.org/10.1007/978-981-19-8730-4_1
-Riikka, K. (2016). Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement. *Scripted*, 13(1), 40.
https://script-ed.org/?p=2669
-Singh, A., Kushwaha, S., Joshi, D., Singh, H.N. L. (2022). Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access*, (99), 1-16.
DOI:10.1109/ACCESS.2021.3140091
-Yilei, W., Andrea, B., Tao, L., Fengyin, L., Xinchun, C., and Minghao, Z. (2019). Randomness invalidates criminal smart contracts. *Information Sciences*, 477, 291-301.
https://doi.org/10.1016/j.ins.2018.10.057