Hazrat-e Masoumeh University

Journal Of Legal & International Analyses (JLIA)

Bottom of Form

Vol. 2, No. 2, Summer 2026
Homepage: jcmd.hmu.ac.ir

The deterrent role of blockchain technology in the development of economic crimes: An approach to non-criminal prevention and structural security

Ali Delmoradi[1], Mohammad Bagher Gerayeli[2]

[1]M.A. in Criminal Law and Criminology, Razavi University of Islamic Sciences, Mashhad, Iran.
Corresponding Author Email: delmoradi.092@gmail.com
[2]Assistant Professor of Criminal Law and Criminology, Razavi University of Islamic Sciences, Mashhad, Iran. Email: gerayeli1378@yahoo.com

Abstract

Economic crimes, as a multifaceted and complex challenge in modern financial systems, necessitate the adoption of innovative solutions that transcend traditional criminal justice methods. This article, employing an analytical-descriptive approach, examines the strategic role of blockchain technology in the non-criminal prevention of these offenses, with a specific focus on its inherent security features. The research findings demonstrate that advanced cryptographic mechanisms—most notably public/private key infrastructures and digital signatures—drastically reduce the potential for impersonation and unauthorized data manipulation by establishing a framework of secure authentication and absolute transparency.

Furthermore, the decentralized, distributed, and immutable architecture of blockchain provides robust resistance against sophisticated cyberattacks, such as Distributed Denial of Service (DDoS) and 51% attacks, thereby ensuring the integrity of financial records. Practical case studies, including the long-term security of Bitcoin transactions and the Ethereum network's structural response to the DAO attack, validate the effectiveness of this technology in detecting and deterring fraudulent activities in real-time. However, the widespread implementation of such systems requires addressing critical challenges, including network scalability and potential conflicts with data privacy regulations. This research concludes that regulatory agencies should leverage blockchain to design automated, transparent oversight systems. Such an approach would significantly enhance global economic security while simultaneously reducing the substantial administrative and financial costs associated with criminal prosecution.

Keywords: Non-criminal prevention, economic crimes, blockchain, cybersecurity, cryptography

Received: 2025-12-19
Revised: 2026-01-30
Accepted: 2026-05-22
Article Type: Research Paper

P- ISSN: 2476-4833
E- ISSN: 2588-7084
Published by Hazrat-e Masoumeh University
doi: 10.22034/jlia.2026.2081336.1035

«فصلنامه تحلیل های حقوقی و بین المللی»

س۲، ش۲،
تابستان ۱۴۰۵
صفحات ۱۱۹ تا ۱۳۹

نقش بازدارندگی فناوری بلاکچین در تکوین جرایم اقتصادی: رویکردی بر پیشگیری غیر کیفری و امنیت ساختاری*

علی دلمرادی[۱]، محمدباقر گرایلی[۲]

[۱]کارشناسی ارشد، حقوق جزا و جرم‌سناسی، دانشگاه علوم اسلامی رضوی، مشهد، ایران. ایمیل نویسندهٔ مسئول: delmoradi.092@gmail.com

[۲]استادیار حقوق جزا و جرم‌شناسی، دانشگاه علوم اسلامی رضوی، مشهد، ایران. ایمیل: gerayeli1378@yahoo.com

چکیده

جرایم اقتصادی به‌عنوان چالشی پیچیده، نیازمند راهکارهای نوین فراتر از روش‌های سنتی کیفری است. این مقاله با رویکردی تحلیلی-توصیفی، به بررسی نقش فناوری بلاکچین در پیشگیری غیرکیفری از این جرایم با تمرکز بر ویژگی‌های امنیتی آن می‌پردازد. یافته‌ها نشان می‌دهد که مکانیسم‌های رمزنگاری (مانند کلیدهای عمومی/خصوصی و امضای دیجیتال) با ایجاد احراز هویت امن و شفافیت، امکان جعل هویت و دستکاری داده‌ها را کاهش می‌دهند. همچنین، معماری توزیع‌شده و تغییرناپذیر بلاکچین، مقاومت بالایی در برابر حملات سایبری نظیر DDoS و حملات ۵۱٪ ایجاد می‌کند. نمونه‌های عملی مانند امنیت تراکنش‌های بیت‌کوین و پاسخ شبکه اتریوم به حمله DAO ، مؤثر بودن این فناوری را در شناسایی و جلوگیری از فعالیت‌های متقلبانه اثبات می‌کنند. با این حال، چالش‌هایی مانند مقیاس‌پذیری و تعارض با حریم خصوصی نیازمند توجه هستند. این پژوهش پیشنهاد می‌کند که نهادهای نظارتی با بهره‌گیری از بلاکچین، سیستم‌های نظارتی خودکار و شفافی طراحی کنند که همزمان با کاهش هزینه‌های مقابله کیفری، امنیت اقتصادی را افزایش دهد.

واژگان کلیدی: پیشگیری غیرکیفری، جرایم اقتصادی، بلاکچین، امنیت سایبری، رمزنگاری.

* تاریخ دریافت: ۱۴۰۴/۰۹/۲۸
تاریخ بازنگری: ۱۴۰۴/۱۱/۱۰
تاریخ پذیرش: ۱۴۰۵/۰۳/۰۱
نوع مقاله: پژوهشی

شابک چاپی: ۲۴۷۶-۴۸۳۳
شابک الکترونیکی: ۲۵۸۸-۷۰۸۴
ناشر: دانشگاه حضرت معصومه(س)
doi: 10.22034/jlia.2026.2081336.1035

مقدمه

در عصر حاضر، گسترش فزاینده جرایم اقتصادی به یکی از چالش‌های اساسی نظام‌های حقوقی و اقتصادی جهان تبدیل شده است. این جرایم که اغلب ماهیتی سازمان‌یافته و فرامرزی دارند، نه تنها ثبات مالی کشورها را تهدید می‌کنند، بلکه امنیت اجتماعی و اعتماد عمومی را نیز مخدوش می‌سازند. (سراج، ۱٤۰۰، ص٦۱) رویکردهای سنتی مقابله با این جرایم که عمدتاً متکی بر ابزارهای کیفری و سرکوبگرانه هستند، به دلایلی همچون پیچیدگی روش‌های ارتکاب جرم، بین‌المللی بودن فعالیت‌های مجرمانه و محدودیت‌های نظام‌های قضایی، کارایی لازم را از دست داده‌اند. (سعیدی، ۱۳۹۲، ص۱۷۳،۱۷٤) در این راستا، پیشگیری غیرکیفری به عنوان راهکاری مؤثر و پایدار مورد توجه قرار گرفته است. پیشگیری غیرکیفری با تمرکز بر ریشه‌یابی علل جرایم و استفاده از روش‌های پیش‌گیرانه، ضمن کاهش هزینه‌های نظام عدالت کیفری، امکان مداخله زودهنگام و کارآمدتر را فراهم می‌آورد. (غضنفری، ۱۳۹٤، ص ۱۷۲) در میان فناوری‌های نوین، فناوری بلاکچین با ویژگی‌های منحصر به فردی همچون تمرکززدایی، شفافیت، تغییرناپذیری و امنیت بالا، پتانسیل قابل توجهی برای پیشگیری غیرکیفری از جرایم اقتصادی دارد. (رایت، ۱۳۹۷، ص۱٤۰) این پژوهش با هدف بررسی امکان بهره‌گیری از ویژگی‌های امنیتی بلاکچین در پیشگیری غیرکیفری از جرایم اقتصادی انجام شده است. سؤال اصلی تحقیق این است که چگونه مکانیسم‌های امنیتی بلاکچین می‌توانند در پیشگیری از جرایم اقتصادی مؤثر واقع شوند؟ فرضیه پژوهش بر این مبناست که به کارگیری فناوری بلاکچین از طریق ایجاد شفافیت، کاهش نقاط آسیب‌پذیر و افزایش امنیت تراکنش‌ها، می‌تواند به صورت غیرکیفری از وقوع بسیاری از جرایم اقتصادی جلوگیری کند. اهمیت این تحقیق از آنجا ناشی می‌شود که می‌تواند چارچوبی نوین برای مقابله با جرایم اقتصادی ارائه دهد و راهکارهای عملی برای نهادهای نظارتی و قانون‌گذار فراهم کند.

مفاهیم

جرایم اقتصادی

درباره تعریف جرایم اقتصادی، مطرح کردن تعاریف ذکر شده توسط صاحب نظران این رشته می‌تواند در رسیدن به یک تعریف واحد دارای فایده باشد که در این بخش به اهم آن‌ها پرداخته خواهد شد. در کنگره بین المللی که درباره «دفاع اجتماعی» برگزار شده بود ، جرم اقتصادی چنین تعریف شده است: «هر فعل یا ترک فعلی که علیه نظام اقتصادی صورت گیرد، جرم اقتصادی است مشروط بر آنکه قانون آن را جرم شناخته باشد، اعم از این که قانون جزا باشد یا قوانین مخصوص برنامه ها اقتصادی که از سوی حکومت برای مصلحت مردم وضع شده است». (ولیدی، ۱۳۹۳، ص۳۸) در تعریفی دیگر، در مقام تفکیک بین جرایم مالی که ناظر به جرایمی با ماهیت مرتبط با مال، یعنی رفتارهای مجرمانه علیه مال یا به تعبیر دقیق‌تر، حق مالی می‌باشند، و جرایم اقتصادی که دامنه‌ای فراتر از

مال دارند، می‌توان تعریفی جامع‌تر ارائه نمود که جرم اقتصادی در رابطه با تعدیات افراد نسبت به اموری صورت میگیرد که موجب اخلال درنظام تولید، توزیع و مصرف کالا و خدمات است این تعریف، با توجه به خسارات و صدمات ناشی از جرم اقتصادی، ارائه شده و دامنه شمول آن، اعم ازهویت و ویژگی‌های مرتکب یا بزه دیده می‌باشد و بزه دیده را محدود به افراد خاص نمی‌نماید و تمایز بین جرم اقتصادی و مالی مشخص گردید. (مهدی پور، ۱۳۹۵، ص ۵۰) با توجه به تعاریفی که ارائه گردید؛ که مهم ترین تعارف جرایم اقتصادی را در بر دارند، می توان برای یک تعریف کاملتر ابتداء چند مولفه ذکر و در نهایت تعریف منتخب را بیان کرد که عبارتند از:

۱. جرایم اقتصادی فراتر از جرایم مالی هستند
۲. انگیزه منفعت مالی و غیر مالی در مرتکب آن
۳. ایجاد اخلال در نظام اقتصادی کشور
٤. اصل قانونی بودن جرم باید در تعریف رعایت گردد
۵. عدم انحصار مرتکب جرایم اقتصادی در افراد خاص

طبق این مولفه ها می‌توان یک تعریف کلی از جرایم اقتصادی بیان کرد که تقریبا قابل سنخیت با جرایم مذکور در ماده۱ قانون مجازات اخلالگران در نظام اقتصادی کشور می باشد، که عبارت است از: هر رفتاری اعم از فعل و ترک فعل که در قانون برای آن مجازات تعیین شده که مرتکب به انگیزه سود ومنفعت مالی یا غیر مالی انجام داده و به سلامت و امنیت نظام اقتصادی لطمه کلان میزند.

فناوری بلاکچین

در تعریف فناوری بلاکچین، اختلافاتی وجود دارد که برخی در تعریف بلاکچین، آن را محدود کرده و در واقع فقط به کاربرد آن درباره بیت کوین پرداخته اند لذا بیان داشته اند که بلاکچین از نسل جدیدی از ارزهای دیجیتال پشتیبانی می‌کند که هیچ مرز جغرافیایی را نمی‌شناسد و می‌توان آن را در عرض چند دقیقه به سراسر دنیا فرستاد بدون آنکه به نهاد متمرکز نیازی باشد. (حیدری، ۱۳۹۷، ص ۲۱۷) تعریف فوق، بلاکچین را صرفا یک سیستم می‌داند که سرعت انتقال ارز های دیجیتال به واسطه آن بسیار بالا است و البته در این تعریف به یکی از ویژگی‌های این فناوری که غیر متمرکز بودن است، اشاره شده است اما این ویژگی هم در راستای ارز دیجیتال آورده شده است این در حالی است که وقتی به منابع مختلف دراین زمینه مراجعه گردد بدست می‌آید که این فناوری کارکرد های فراوانی دارد. برخی در تعریف فناوری بلاکچین به کارکرد آن إشاره کرده اند و بلاکچین را یک پایگاه داده دانسته اند که از مجموعه بلوک ها با طول ثابت تشکیل شده و از ۱ تا n تراکنش را در خود جای داده و در هر تراکنش در صورت معتبر بودن در بلاک ذخیره می‌شود. (جنگروی، ۱٤۰۱، ص۱۵) در این تعریف فقط به کارکرد بلاکچین که اضافه کردن تراکنش ها جدید و در صورت معتبر بودن تراکنش‌ها، ذخیره آن‌ها در بلاک است را بیان کرده است و

تفاوت آن با تعریف قبلی این است که این فناوری را محدود به رمز ارزها نکرده است. در تعریف دیگر این فناوری یک سامانه ثبت اطلاعات در دفتر کل توزیع شده معرفی شده است که اطلاعات در زنجیره بلوک‌ها ذخیره می‌شود و تفاوت آن را با سامانه های ثبت اطلاعات دیگر این چنین بیان می‌دارد که امکان تغییر در اطلاعات با استفاده از سامانه رمز گذاری وجود ندارد و اطلاعات میان تمام اعضای شبکه به اشتراک گذاشته می‌شود. (حاجی ملامیرزایی، ۱۳۹۹، ص۱۷) در این تعریف دو ویژگی دیگر از این فناوری را بیان می‌کند که عبارت است از غیر قابل تغییر بودن و شفافیت در اطلاعات ثبت شده که این فناوری را با فناوری های مشابه جدا می‌کند. بنابراین می‌توان گفت فناوری بلاکچین یک سامانه و پایگاه ثبت و انتقال اطلاعات و داده‌ها دیجیتال در دفتر کل توزیع شده می‌باشد که هیچ قدرت مرکزی‌ای آن را مدیریت نمی‌کند که طرفین به صورت مستقیم با یکدیگر معامله می‌کنند و داده های تراکنش‌های جدید در همه نودهای شبکه منتشر و ذخیره می‌شود.

پیشگیری غیر کیفری

پیشگیری در لغت به معنای پیشی گرفتن، دفع، پیش دستی کردن، جلوگیری آمده است. (معین، ۱۳۸٦ ، ص۳۹٦) پیشگیری از جرم به اقدامات و تدابیری اطلاق می‌شود که با هدف کاهش یا از بین بردن عوامل جرم‌زا و شرایطی که منجر به ارتکاب جرم می‌شوند، طراحی و اجرا می‌شود. این اقدامات می‌توانند در سطوح مختلف فردی، اجتماعی و محیطی اعمال شوند و در دو نوع کیفری و غیر کیفری اعمال می‌شوند. پیشگیری غیر کیفری به مجموعه اقدامات و راهبردهایی اطلاق می‌شود که خارج از چارچوب سیستم عدالت کیفری و بدون استفاده از ابزارهای قضایی، پلیسی یا مجازات‌های قانونی، به دنبال کاهش یا جلوگیری از وقوع جرم است. این نوع پیشگیری بر این ایده استوار است که جرم یک پدیده چندوجهی است که ریشه در عوامل اجتماعی، اقتصادی، فرهنگی و محیطی دارد. بنابراین، به جای تمرکز بر مجازات مجرمان یا بازدارندگی از طریق ترس از مجازات، پیشگیری غیر کیفری سعی می‌کند با بهبود شرایط زندگی افراد و جامعه، زمینه‌های ارتکاب جرم را از بین ببرد. (مرجانی، ۱۳۹۹، ص ٤۱) و به تعبیر دیگر پیشگیری غیر کیفری اقدام مناسبی است که از طریق از بین بردن علل جرم و نامناسب نشان دادن موقعیت های ارتکاب جرم به دنبال جلوگیری از وقوع بزه می‌باشد. (نیاز پور، ۱٤۰۰، ص ۹۷)

ویژگی‌های فناوری بلاکچین

غیر متمرکز بودن

در سیستم‌های سنتی، داده‌ها و تراکنش‌ها معمولاً توسط یک نهاد مرکزی مانند بانک، دولت یا شرکت‌های بزرگ مدیریت می‌شوند. اما در بلاکچین، این کنترل متمرکز حذف شده و به جای آن، شبکه‌ای از کامپیوترها (نودها) به

صورت مشارکتی مسئولیت تأیید و ثبت تراکنش‌ها را بر عهده می‌گیرند. در یک شبکه غیرمتمرکز، هیچ نهاد واحدی قدرت کنترل کامل را ندارد. (هلاکوئی،۱۳۹۹، ص۷٤) به جای آن، همه شرکت‌کنندگان در شبکه به صورت برابر در فرآیند تصمیم‌گیری و اعتبارسنجی مشارکت می‌کنند. این پایگاه های داده مشترک در سطح بین الملل کار می‌کنند و چون هیچ نهاد متمرکزی وجود ندارد با وصل شدن به اینترنت می‌تواند اطلاعات ذخیره شده روی بلاکچین را با دانلود رایگان نرم افزار منبع باز موجود فراخوانی کند. (حیدری، ۱۳۹۷، ص۱٤۳) این ویژگی باعث افزایش امنیت، شفافیت و مقاومت سیستم در برابر خرابی یا حمله می‌شود. برای مثال، اگر یک نود در شبکه از کار بیفتد یا مورد حمله قرار گیرد، شبکه همچنان به کار خود ادامه می‌دهد، زیرا داده‌ها روی هزاران نود دیگر توزیع شده‌اند. غیرمتمرکز بودن همچنین از دستکاری داده‌ها جلوگیری می‌کند. آن چه با توجه به مطالب فوق بدست می‌آید غیر متمرکز بودن فناوری بلاکچین است به این معنی که انجام ترکنش‌ها بدون اتکاء به قدرتی و واسطه ای انجام می‌گردد.

شفافیت

شفافیت در فناوری بلاک‌چین به این معناست که همه تراکنش‌ها و داده‌ها به صورت عمومی و قابل مشاهده توسط همه شرکت‌کنندگان در شبکه ثبت و نگهداری می‌شوند. این شفافیت از طریق روش های خاصی در ساختار بلاک‌چین ایجاد می‌شود. بلاک‌چین یک دفتر کل دیجیتال است که بین تمامی گره‌ها (نودها) در شبکه توزیع شده است و هر گره یک کپی کامل از دفتر کل را نگهداری می‌کند. (صمدی، ۱۳۹۹، ص۱۳) این یعنی هیچ نسخه متمرکزی از داده‌ها وجود ندارد و همه شرکت‌کنندگان می‌توانند به تمام اطلاعات دسترسی داشته باشند.یا ثبت عمومی تراکنش‌ها، هر تراکنشی که در بلاک‌چین انجام می‌شود، در یک بلوک قرار می‌گیرد و این بلوک به زنجیره بلوک‌های قبلی اضافه می‌شود. این تراکنش‌ها به صورت رمزنگاری‌شده و با جزئیات کامل (مانند آدرس‌های فرستنده و گیرنده، مقدار انتقالی و زمان تراکنش) ثبت می‌شوند. هر کسی می‌تواند این اطلاعات را مشاهده کند و از آنجا که هر بلوک به بلوک قبلی خود متصل است و هر تراکنش به صورت زنجیره‌ای ثبت می‌شود (همتی، ۱٤۰۱، ص۱۲)، می‌توان تاریخچه کامل هر تراکنش را از ابتدا تا انتها ردیابی کرد. این ویژگی باعث می‌شود که هیچ تراکنشی پنهان نماند و همچنین به علت عدم تمرکز در بلاک‌چین، هیچ نهاد مرکزی کنترل اطلاعات را در دست ندارد. این عدم تمرکز باعث می‌شود که هیچکس نتواند داده‌ها را به صورت پنهانی تغییر دهد یا دستکاری کند. همه تغییرات باید توسط شبکه تأیید شوند. و حتی اگر آدرس‌های کیف پول‌ها به صورت ناشناس باشند، همه تراکنش‌ها قابل مشاهده هستند. این یعنی هر کسی می‌تواند ببیند که چه مقدار دارایی از یک آدرس به آدرس دیگر منتقل شده است، این تأیید از طریق مکانیزم‌های اجماع مانند اثبات کار یا اثبات سهام انجام می‌شود. این فرآیند تضمین می‌کند که همه تراکنش‌ها معتبر هستند و به صورت شفاف ثبت می‌شوند.

تغییر ناپذیری

ویژگی تغییرناپذیری در بلاکچین به این معناست که پس از ثبت یک داده (تراکنش) در بلاکچین، تغییر یا حذف آن تقریباً غیرممکن است. این ویژگی از طریق ترکیبی از توابع هش رمزنگاری، ساختار زنجیره‌ای بلاک‌ها و مکانیسم اجماع توزیع‌شده به دست می‌آید.هر بلاک در بلاکچین شامل هش داده‌های قبلی خود است (عینی، ۱۳۹۹، ص ۲۹) که یک زنجیره پیوسته ایجاد می‌کند. اگر حتی یک بیت از داده‌ها در یک بلاک تغییر کند، هش آن بلاک نیز تغییر می‌کند. این تغییر، هش بلاک‌های بعدی را نیز تحت تأثیر قرار می‌دهد، زیرا آن‌ها به هش بلاک قبلی خود وابسته هستند. برای تغییر یک بلاک، نه تنها باید بلاک مورد نظر را تغییر داد، (تفضلی، ۱۳۹۷، ص ۱۳٤) بلکه تمام بلاک‌های بعدی آن را نیز باید تغییر داد. علاوه بر این، باید کنترل اکثریت شبکه را در دست داشت تا تغییرات را به عنوان معتبر به سایر شرکت‌کنندگان در شبکه تحمیل کرد. این امر به دلیل ماهیت غیرمتمرکز بلاکچین و وجود نسخه‌های متعدد از بلاکچین در سراسر شبکه، بسیار دشوار و از نظر محاسباتی پرهزینه است. شبکه توزیع‌شده از گره‌ها نسخه‌های متعددی از بلاکچین را نگهداری می‌کنند و هر تغییری باید توسط اکثریت شبکه تایید شود. این توافق جمعی، تغییرات غیرمجاز را غیرممکن می‌سازد. در نتیجه، داده‌ها در بلاکچین به طور موثر غیرقابل تغییر هستند مکانیسم اجماع، که توسط گره‌های شبکه اجرا می‌شود، نقش مهمی در حفظ این تغییرناپذیری دارد. این مکانیسم اطمینان می‌دهد که تمام گره‌ها در مورد وضعیت بلاکچین به توافق می‌رسند و هرگونه تلاش برای تغییر مخفیانه داده‌ها با مخالفت مواجه می‌شود. این توافق جمعی، امنیت و یکپارچگی بلاکچین را تضمین می‌کند و آن را به یک ابزار قدرتمند برای کاربردهای مختلف تبدیل می‌کند. البته یک مهجم یا گروهی از آن‌ها با در دست گرفتن بیشتر توان پردازشی شبکه قادر هستند در فرایند پردازش بلوک های جدید اخلال ایجاد کنند با این وجود احتمال تغییر توسط مهاجمان در بلوک های قدیمی تر بسیار اندک است. (صمدی، ۱۳۹۹، ص ۹۲) لذا این پایداری در بلوک‌های قدیمی، ماهیت اصلی «تغییرناپذیری» در بلاک‌چین را تبیین می‌کند؛ چرا که با افزایش عمق زنجیره، احتمال بازنویسی داده‌ها به صورت مجانبی به صفر نزدیک می‌شود. در واقع، تغییرناپذیری یک ویژگی مطلق و آنی نیست، بلکه صفتی برخاسته از انباشت توان محاسباتی روی بلوک‌های پیشین است که سد محکمی در برابر نفوذ مهاجمان ایجاد می‌کند

برخورداری از امنیت بالا

امنیت، رکن اصلی و بنیادی فناوری بلاکچین است که از ترکیب چندین مکانیسم رمزنگاری و روش‌های اجماع ناشی می‌شود. رمزنگاری کلید عمومی/خصوصی، محرمانگی تراکنش‌ها را تضمین و هویت کاربران را تأیید می‌کند. هر تراکنش با کلید خصوصی امضا و با کلید عمومی مورد راستی‌آزمایی قرار می‌گیرد. عملکرد توابع هش رمزنگاری، یکپارچگی داده‌ها را حفظ می‌کند؛ هرگونه دستکاری در داده‌ها، هش را تغییر می‌دهد و به راحتی قابل تشخیص

است. (Balshetwar,2024, 101) زنجیره بلوکی، با پیوند هش هر بلوک به بلوک پیشین، ساختاری امن و غیرقابل تغییر ایجاد می‌کند. (خدارحمی، ۱۳۹۹، ص۷) الگوریتم‌های اجماع مانند اثبات کاریا اثبات سهام، از نفوذ و کنترل شبکه توسط بازیگران مخرب جلوگیری می‌کنند و نیاز به تأیید تراکنش‌ها توسط اکثریت گره‌ها را اعمال می‌کنند. به‌علاوه، قراردادهای هوشمند می‌توانند به ایجاد و اجرای قواعد امنیتی پیشرفته‌تر در بلاکچین کمک کنند. بنابراین باتوجه به این توضیحات بدست می‌آید که امنیت در بلاکچین به این معناست که داده ها و ترکنش‌های ثبت شده در این سیستم در برابر تغییر، حذف، جعل و دسترسی غیر مجاز محافظت می‌شوند و این امنیت علاوه براینکه از اطلاعات کاربران در برابر سوء استفاده محافظت می‌کند بلکه به حفظ اعتبار و عملکرد صحیح کل شبکه نیز کمک می کند و در واقع این امنیت از ویژگی های دیگر این فناوری مانند تغییر ناپذیری، غیر متمرکز بودن... هم بدست آمده است.

امنیت در فناوری بلاکچین

این قسمت به بررسی سازوکارهای امنیتی بلاکچین و تأثیر آن بر کاهش جرایم اقتصادی اختصاص دارد. با استفاده از تکنیک‌های پیشرفته رمزنگاری و الگوریتم‌های اجماع، بلاکچین سطح بی‌سابقه‌ای از امنیت را در معاملات مالی ایجاد می‌کند. در این بخش، مکانیسم‌های حفاظتی این فناوری و نقش آن در مقابله با تقلب و دستکاری مالی تحلیل خواهد شد.

تکنیک‌های رمزنگاری و حفاظت از اطلاعات

امنیت اطلاعات در فناوری بلاکچین به عنوان سنگ بنای اعتماد در این سیستم‌های غیرمتمرکز شناخته می‌شود. در این گفتار به بررسی دقیق مکانیسم‌های رمزنگاری می‌پردازیم که نقش حیاتی در حفاظت از یکپارچگی داده‌ها و تراکنش‌های بلاکچینی ایفا می‌کنند. از رمزنگاری کلید عمومی و خصوصی به عنوان ستون فقرات امنیتی بلاکچین یاد می‌شود که امکان احراز هویت ایمن و انتقال داده‌ها را بدون نیاز به واسطه‌های قابل اعتماد فراهم می‌آورد. در ادامه، ضمن تحلیل جامع این مکانیسم‌ها، به بررسی راهکارهای عملی جلوگیری از دسترسی‌های غیرمجاز و مقابله با انواع کلاهبرداری‌های دیجیتال خواهیم پرداخت. مطالعه موردی سیستم بیت‌کوین به عنوان نمونه‌ای موفق از پیاده‌سازی این تکنیک‌ها، درک ملموسی از کاربردهای عملی آنها ارائه خواهد داد.

اهمیت رمزنگاری کلید عمومی و خصوصی

کلید عمومی یک کد رمز نگاری است که به کاربران این امکان را می‌دهد که رمز ارزها را در حساب های خود دربافت کنند. کلید عمومی و خصوصی ابزاری هستند که برای تضمین امنیت اقتصاد رمزنگاری لازم است.

(هلاکوئی،۱۳۹۹،ص۲٦) رمزنگاری نامتقارن مبتنی بر کلید عمومی و خصوصی، ستون فقرات امنیتی بلاکچین را تشکیل می‌دهد. این سیستم رمزنگاری که بر پایه توابع ریاضی پیچیده مانند منحنی‌های بیضوی عمل می‌کند، امکان جعل یا نقض امنیتی را به شدت کاهش می‌دهد. در این سیستم، کلید عمومی که قابل اشتراک‌گذاری است، برای رمزگذاری اطلاعات استفاده می‌شود، در حالی که کلید خصوصی که فقط در اختیار مالک است، برای رمزگشایی به کار می‌رود. مطالعات نشان می‌دهند که این مکانیزم در مقایسه با سیستم‌های متمرکز سنتی، امنیت بسیار بالاتری ارائه می‌دهد. (Kim, 2004, P218) برای مثال، در سیستم‌های بانکی سنتی، یک نفوذگر می‌تواند با دسترسی به سرور مرکزی، به اطلاعات تمام کاربران دسترسی یابد. اما در بلاکچین، حتی اگر یک نود به خطر بیفتد، اطلاعات دیگر کاربران ایمن باقی می‌ماند، زیرا هر کاربر کلید خصوصی منحصربه‌فرد خود را دارد. بررسی‌های انجام شده توسط مؤسسات امنیتی مانند NIST[1] نشان داده که الگوریتم‌های مورد استفاده در بلاکچین در حال حاضر در برابر حملات کوانتومی (شکستن رمزنگاری مبتنی بر مفاهیم ریاضی مانند تجزیه اعداد بزرگ و تأثیر آن بر بلاکچین عبارت است ازامکان استخراج کلیدهای خصوصی از کلیدهای عمومی و خطر جعل امضاهای دیجیتال و سرقت دارایی‌ها) نیز مقاوم هستند. این سطح از امنیت، بلاکچین را به ویژه برای کاربردهای حساس مانند تراکنش‌های مالی، قراردادهای هوشمند وسیستم‌های رأی‌گیری الکترونیکی مناسب ساخته است.

انتقال امن داده‌ها و تراکنش‌ها

مکانیزم انتقال داده در بلاکچین از چند لایه امنیتی برخوردار ا ست. اولاً، هر تراکنش قبل از ثبت در بلاکچین، توسط الگوریتم‌های هشینگ مانند SHA-256[2] پردازش می‌شود. این الگوریتم هر ورودی را به یک خروجی منحصربه‌فرد تبدیل می‌کند که کوچکترین تغییر در داده‌های ورودی، هش کاملاً متفاوتی تولید می‌کند. این ویژگی باعث می شود که امکان د ستکاری در سوابق تراکنش‌ها عملاً غیرممکن شود (Hua Yi Lin, 2023, P:5). ثانیاً، ساختار زنجیره‌ای بلوک‌ها به گونه‌ای است که هر بلوک حاوی هش بلوک قبلی است. این ویژگی که به "اثر انگ شت دیجیتال" معروف ا ست، یک زنجیره امنیتی ایجاد می‌کند که تغییر در یک بلوک م ستلزم تغییر در تمام بلوک‌های بعدی خواهد بود. از نظر محاسباتی، این کار به قدری پرهزینه است که عملاً غیرممکن محسوب می‌شود. تحقیقات نشان داده‌اند که این سیستم در مقایسه با پایگاه‌داده‌های متمرکز سنتی، امنیت بسیار بالاتری در برابر جرایمی مانند جعل ا سناد، د ستکاری سوابق مالی و تغییر غیرمجاز داده‌ها ارائه می‌دهد. (تینا لورنس، ۱٤۰۰، ص ۱۷٤، ۱۷۵)

[1]. National Institute of Standards and Technology

[2] . Secure Hash Algorithm 256-bit

جلوگیری از دسترسی‌های غیرمجاز

سیستم کنترل دسترسی در بلاکچین‌های پیشرفته از چندین لایه امنیتی تشکیل شده است. در بلاکچین‌های عمومی مانند بیت‌کوین، اگرچه داده‌ها برای همه قابل مشاهده است، اما دسترسی به عملکردهای حساس (مانند ایجاد تراکنش) نیاز به احراز هویت رمزنگاری شده دارد. در بلاکچین‌های خصوصی و کنسرسیومی، این کنترل‌ها حتی سخت‌گیرانه‌تر اعمال می‌شوند. مکانیزم‌های کنترل دسترسی پیشرفته مانند RBAC (کنترل دسترسی مبتنی بر نقش) و ABAC (کنترل دسترسی مبتنی بر ویژگی) در بلاکچین‌های سازمانی پیاده‌سازی شده‌اند. برای مثال، در Hyperledger Fabricr Fabric (یک پلتفرم بلاکچین سازمانی متن‌باز است که تحت چتر پروژه مبتنی بر بنیاد لینوکس توسعه یافته است و برخلاف بلاکچین‌های عمومی مانند بیت‌کوین یا اتریوم، به‌طور خاص برای کاربردهای تجاری و صنعتی طراحی شده است.) می‌توان تعیین کرد که کدام نودها حق خواندن، نوشتن یا تأیید تراکنش‌ها را دارند. این سطح از کنترل، امکان سوءاستفاده داخلی را به شدت کاهش می‌دهد. آمار نشان می‌دهد که پیاده‌سازی این سیستم‌های کنترل دسترسی در صنعت مالی، موارد کلاهبرداری داخلی را تا ۸۷٪ کاهش داده است. این امر به ویژه در جلوگیری از جرایمی مانند اختلاس، سوءاستفاده از اختیارات و دسترسی غیرمجاز به اطلاعات حساس مؤثر بوده است.

مقاومت در برابر کلاهبرداری

مکانیزم‌های اجماع در بلاکچین، سد محکمی در برابر کلاهبرداری‌های مالی ایجاد می‌کنند. برای مثال، الگوریتم اثبات کار (PoW) مورد استفاده در بیت‌کوین، به گونه‌ای طراحی شده که انجام یک حمله ۵۱٪ نیاز به سرمایه‌گذاری هنگفت در سخت‌افزار و انرژی دارد که از نظر اقتصادی به صرفه نیست. هرچند اثبات کار امنیت را در یک محیط غیر قابل اعتماد تضمین می‌کند، اما متخصصان در این عرصه معتقدند روشی هزینه بر و نیازمند صرف انرژی زیاد بوده و سرعت آن کم می‌باشد. البته در سال ۲۰۱۶ جایگزینی برای آن به نام اثبات زمان (poet) ارائه شد. (عبدالهی، ۱۴۰۰، ص ۸۶، ۸۷) در سیستم‌های اثبات سهام (PoS)، این امنیت از طریق وثیقه‌گذاری دارایی‌ها تأمین می‌شود. در این سیستم‌ها، اعتبارسنج‌ها باید مقدار قابل توجهی از ارز دیجیتال را به عنوان وثیقه قفل کنند، که در صورت رفتار مخرب، این وثیقه از بین می‌رود. این مکانیزم انگیزه مالی قوی برای رفتار صادقانه ایجاد می‌کند. مطالعه موردی روی صرافی‌های ارز دیجیتال نشان داده که آن‌هایی که از فناوری بلاکچین استفاده می‌کنند، ۹۲٪ کمتر از صرافی‌های سنتی در معرض کلاهبرداری هستند. این آمار به وضوح نشان‌دهنده تأثیر مثبت بلاکچین در پیشگیری از جرایم مالی است.

نمونه عملی (کاربرد رمزنگاری در بیت‌کوین)

بیت‌کوین به عنوان اولین و بزرگترین کاربرد عملی بلاکچین، آزمایشگاه زنده‌ای برای بررسی امنیت این فناوری بوده است. در طول ١٤ سال فعالیت، شبکه بیت‌کوین هیچ‌گاه هک نشده است. حتی در مواردی مانند حمله به صرافی‌ها، مشکل از خود بلاکچین نبوده، بلکه از سیستم‌های متمرکز پیرامون آن نشأت گرفته است. البته برخی معتقدند سیستم رمزنگاری نمی‌تواند به اندازه الگوریتم هایی که بر آن‌ها استوار است قوی باشد و وقتی یکی از آن خراب شود، سیستم از کار می‌افتد. (ER-RAJY LATIFA, 2017, P:8) مطالعه دقیق معماری امنیتی بیت‌کوین نشان می‌دهد که ترکیب رمزنگاری نامتقارن، الگوریتم هشینگ قوی[1] و سیستم اجماع غیرمتمرکز، سطح امنیتی بی‌سابقه‌ای ایجاد کرده است. این موفقیت عملی، اثبات محکمی است بر توانایی بلاکچین در پیشگیری از جرایم اقتصادی در مقیاس جهانی.

امنیت در برابر حملات سایبری

با گسترش روزافزون کاربردهای بلاکچین، این فناوری به هدفی جذاب برای مهاجمان سایبری تبدیل شده است. در این گفتار، چالش‌های امنیتی پیش روی شبکه‌های بلاکچینی و راهکارهای مقابله با آنها را مورد بررسی قرار می‌دهیم. از حملات متمرکز مانند DOS و DDOS تا تهدیدات پیچیده‌تری مانند حمله ۵۱٪، سیستم‌های بلاکچینی نیازمند مکانیسم‌های دفاعی هوشمند و خودکار هستند. (Zawar ShahT,2022p:10)، در این بخش، ضمن تحلیل روش‌های شناسایی و پاسخ به تهدیدات امنیتی، به بررسی سیستم‌های نظارتی پیوسته و راهکارهای ارتقای مستمر امنیت شبکه خواهیم پرداخت. مطالعه موردی حملات موفق و ناموفق به شبکه‌های بلاکچینی، درک عمیقی از نقاط قوت و ضعف این سیستم‌ها در مواجهه با تهدیدات سایبری ارائه خواهد کرد.

شناسایی و پاسخ به تهدیدات امنیتی

بلاکچین با استفاده از شبکه‌های نظیر به نظیر و الگوریتم‌های اجماع غیرمتمرکز، امکان شناسایی و خنثی‌سازی تهدیدات امنیتی را به صورت بلادرنگ فراهم می‌کند. برخلاف سیستم‌های متمرکز که در آن یک نقطه شکست وجود دارد، در بلاکچین، حمله به شبکه نیاز به نفوذ همزمان به بیش از ۵۰٪ از نودها دارد که از نظر فنی و اقتصادی تقریباً غیرممکن است حمله ٪۵۱ که به آن حمله اکثریت نیز گفته می‌شود، سناریویی نظری است که در آن یک نهاد مخرب کنترل بیش از ۵۰٪ از قدرت هش (در بلاکچین‌های مبتنی بر اثبات کار) یا سهام (در بلاکچین‌های مبتنی بر اثبات

[1] . الگوریتم هشینگ قوی (Cryptographic Hash Function) یک تابع ریاضی است که:هر ورودی با طول متغیر (مثلاً یک متن یا فایل) را دریافت می‌کند و یک خروجی ثابت‌طول (معمولاً ٢٥٦ یا ٥١٢ بیت) تولید می‌کند و به‌صورت یک‌طرفه عمل می‌کند (تبدیل معکوس غیرممکن است) و ویژگی‌های کلیدی یک هش قوی تغییرناپذیری آن است. (کوچکترین تغییر در ورودی (حتی ۱ بیت) باید حداقل ٪۵۰ خروجی را تغییر دهد.)

سهام) شبکه را به دست می‌گیرد. این حمله به مهاجم اجازه می‌دهد تراکنش‌ها را سانسور کند، تاریخچه تراکنش‌ها را تغییر دهد یا حتی خرج دوگانه انجام دهد. با این حال، اجرای موفقیت‌آمیز چنین حمله‌ای در عمل به دلایل فنی، اقتصادی و امنیتی غیرممکن یا حداقل بسیار غیرعملی است و علت آن این است که برای تصاحب ۵۱٪ از قدرت هش یک شبکه مانند بیت‌کوین، مهاجم باید سرمایه‌ای معادل ده‌ها میلیارد دلار صرف خرید و راه‌اندازی دستگاه‌های استخراج کند. به عنوان مثال، در سال ۲۰۲۳، هزینه انجام حمله ۵۱٪ به بیت‌کوین حدود ۲۰ میلیارد دلار برآورد شد که این مبلغ حتی برای دولتها نیز بسیار سنگین است. علاوه بر این، اگر حمله موفقیت‌آمیز باشد، ارزش خود ارز دیجیتال به شدت کاهش می‌یابد و مهاجم ضرر هنگفتی متحمل می‌شود. (Saad, Muhammad, 2019, p:7) همچنین تمرکززدایی و توزیع جغرافیایی نودها علت دیگر آن است به این صورت که شبکه‌های بلاکچین بزرگ مانند بیت‌کوین و اتریوم از هزاران نود مستقل در سراسر جهان تشکیل شده‌اند که هیچ نهاد واحدی کنترل آنها را در دست ندارد. حتی اگر یک کشور یا شرکت بزرگ بخواهد به چنین حمله‌ای دست بزند، باید همزمان بر نودهای واقع در ده‌ها کشور مختلف مسلط شود که از نظر سیاسی و عملی غیرممکن است.

استفاده از سیستم‌های امنیتی خودکار

سیستم‌های امنیتی خودکار در بلاکچین به مجموعه‌ای از مکانیزم‌های هوشمند و از پیش برنامه‌ریزی‌شده اشاره دارند که بدون نیاز به مداخله انسانی، امنیت شبکه را تأمین و از حملات سایبری جلوگیری می‌کنند. این سیستم‌ها بر پایه قراردادهای هوشمند، الگوریتم‌های اجماع و رمزنگاری پیشرفته طراحی شده‌اند و به صورت بلادرنگ تهدیدات را شناسایی و خنثی می‌کنند. یکی از کلیدی‌ترین ویژگی‌های این سیستم‌ها، توانایی اجرای خودکار پروتکل‌های امنیتی در مواجهه با رفتارهای مخرب است. برای مثال، اگر یک نود تلاش کند تراکنش‌های نامعتبر را به شبکه تزریق کند، مکانیزم اجماع به صورت خودکار این تراکنش‌ها را رد می‌کند و نود مخرب را از شبکه طرد می‌نماید. این فرآیند بدون نیاز به هیچ گونه تصمیم‌گیری مرکزی یا نظارت انسانی انجام می‌شود و تمامی مراحل آن توسط کدهای از پیش تعریف‌شده و تغییرناپذیر کنترل می‌گردد. (Songlin He, 2022, p:8) قراردادهای هوشمند نقش محوری در این سیستم‌های امنیتی ایفا می‌کنند. این قراردادها که با زبان‌های برنامه‌نویسی خاصی نوشته شده‌اند، قادرند شرایط از پیش تعیین‌شده را بررسی و در صورت تشخیص هرگونه انحراف از پروتکل، واکنش‌های مناسب را اجرا کنند. به عنوان نمونه، در یک سیستم مالی غیرمتمرکز، اگر کسی سعی کند همان دارایی را دو بار خرج کند، قرارداد هوشمند به صورت خودکار این تقلب را شناسایی و از اجرای تراکنش جلوگیری می‌نماید. (جنگروی، ۱۴۰۱ص۹۶،۹۷) این قابلیت نه تنها از وقوع جرایم مالی جلوگیری می‌کند، بلکه هزینه‌های مرتبط با نظارت و بازرسی را نیز به شدت کاهش می‌دهد. یکی دیگر از جنبه‌های مهم سیستم‌های امنیتی خودکار در بلاکچین، توانایی آن‌ها در به‌روزرسانی و ارتقای مستمر است. برخلاف سیستم‌های متمرکز که برای اعمال به‌روزرسانی‌های امنیتی نیاز

به توقف سرویس دارند، بلاکچین‌ها می‌توانند بدون ایجاد وقفه در شبکه، پروتکل‌های امنیتی جدید را اجرا کنند. این ویژگی به ویژه در مواجهه با تهدیدات نوظهور بسیار حیاتی است، زیرا اجازه می‌دهد شبکه به سرعت خود را با آخرین تهدیدات امنیتی تطبیق دهد.

پیشگیری از حملات DOS, DDOS

یکی از مزایای کلیدی بلاکچین، مقاومت ذاتی در برابر حملات DDoS است. در سیستم‌های سنتی، هکرها با ارسال ترافیک سنگین به سرور مرکزی، سرویس را از کار می‌اندازند. اما در بلاکچین، عدم وجود سرور مرکزی و توزیع داده‌ها بین هزاران نود، این حمله را بی‌اثر می‌کند. حملات DOS[۱] و DDO[۲] از جمله تهدیدات امنیتی هستند که هدف آن‌ها مختل کردن دسترسی به سرویس‌های تحت شبکه است. در حمله DOS، d که سیستم واحد به‌صورت متمرکز به هدف حمله می‌کند، در حالی که در حمله DDOS، چندین سیستم به‌صورت هماهنگ و توزیع‌شده به یک سرویس یا شبکه حمله می‌کنند تا آن را از کار بیندازند. در بلاکچین، این حملات می‌توانند باعث کاهش کارایی شبکه، افزایش تأخیر در تراکنش‌ها و حتی توقف موقت سرویس‌ها شوند. که می‌توان از طریق محدود کردن نرخ درخواست‌ها با اعمال محدودیت روی تعداد درخواست‌های ارسالی از یک آدرس IP یا گره خاص، می‌توان از حملات مبتنی بر اشباع منابع جلوگیری کرد (Zawar Shah, 2022, p:10). یا با استفاده از فیلتر کردن ترافیک مخرب با استفاده از فایروال‌ها و سیستم‌های تشخیص نفوذ می‌توان ترافیک غیرعادی را شناسایی و مسدود کرد.

ارتقای امنیت شبکه به صورت مستمر

امنیت شبکه‌های بلاکچین به دلیل ماهیت غیرمتمرکز و نقش حیاتی آن‌ها در تراکنش‌های اقتصادی، نیازمند رویکردی پویا و چندبعدی است که به صورت مستمر باید بهروزرسانی و تقویت شود. این فرآیند مستمر نه تنها یک الزام فنی، بلکه بخشی اساسی از راهبرد پیشگیری غیرکیفری از جرایم اقتصادی محسوب میشود. در این راستا، به‌کارگیری الگوریتم‌های رمزنگاری پیشرفته اولین خط دفاعی است. با توجه به تهدیدات نوظهور مانند رایانش کوانتومی، شبکه‌ها باید به سمت استانداردهای مقاوم در برابر این تهدیدات مانند رمزنگاری پساکوانتومی حرکت کنند. همزمان، بهروزرسانی‌های دورهای پروتکل‌های امنیتی از طریق مکانیسم‌های فوری سخت و نرم، امکان رفع آسیب‌پذیری‌های کشف‌شده را فراهم میکند. در لایه زیرساختی، تقویت مکانیسم‌های اجماع برای مقابله با حملاتی مانند حمله ۵۱٪ یا Sybil ضروری است (Nwaga, 2022, p:156 Philip) ترکیب روش‌های مختلف اجماع مانند تلفیق اثبات کار و اثبات سهام میتواند امنیت شبکه را افزایش دهد. در لایه کاربردی، قراردادهای هوشمند به عنوان

---

۱. Denial of Service

۲. Distributed Denial of Service

یکی از نقاط آسیبپذیر اصلی نیازمند توجه ویژه هستند. استفاده از ابزارهای تحلیل کد و ممیزی‌های امنیتی پیش از استقرار، همراه با به‌کارگیری چارچوب‌های استانداردشده توسعه، می‌تواند از بسیاری از جرایم اقتصادی مرتبط با نقص‌های کدنویسی جلوگیری کند.علاوه بر این، پیاده‌سازی فناوری‌های پیشرفته مانند اثبات‌های دانش صفر نهتن‌ها محرمانگی را افزایش می‌دهد، بلکه امکان انواع خاصی از کلاهبرداریها را از بین میبرد. این فرآیندهای امنیتی زمانی بهینه عمل میکنند که با نظارت فعال و سیستم‌های هشدار سریع همراه شوند. ایجاد برنامه‌های تشویقی برای گزارش‌دهی آسیبپذیری‌ها و توسعه استانداردهای امنیتی یکپارچه، چارچوبی مستحکم برای پیشگیری از جرایم اقتصادی در بستر بلاکچین ایجاد می‌کند.

رویکرد تحلیل کاربردی

بلاکچین، با اتکا بـه امنیـت ذاتـی خـود، امکـان پیشـگیری مـوثری از جـرایم گمرکـی، کـه اغلـب بـه عنـوان جـرایم اقتصـادی شـناخته می‌شـوند، فـراهم مـی‌آورد. یکـی از بـارزترین کاربردهـای امنیتـی بلاکچـین، ایجـاد سوابق تراکنش‌های غیرقابل تغییـر و شـفاف بـرای کالاهـا در زنجیـره تـامین اسـت. هـر بـلاک در ایـن زنجیـره، حاوی اطلاعات تراکنش و یک هـش رمزنگـاری شـده از بـلاک پیشـین اسـت، کـه ایـن سـاختار، دسـتکاری یـا تغییر اطلاعـات ثبت‌شـده را بـدون شناسـایی و افشـا به‌شـدت محـدود می‌کنـد. بـه عنـوان نمونـه، در واردات و صـادرات، جزئیـاتی ماننـد نـوع کـالا، ارزش، تعرفـه‌های پرداخت‌شـده و اطلاعـات حمل‌ونقـل در بلاکچـین ثبـت می‌گـردد. ایـن اطلاعـات بـرای تمـام ذینفعـان، از جملـه گمـرک، شـرکت‌های حمل‌ونقـل و واردکننـدگان/صـادرکنندگان، قابـل دسترسـی اسـت. امنیـت بلاکچـین تضـمین می‌کنـد کـه هـیچ طرفـی نمی‌تواند به‌طور مخفیانـه اطلاعـات را تغییـر دهـد، و هرگونـه تـلاش بـرای تقلـب بـه سـرعت قابـل تشـخیص اسـت(Daiane, 2024, p: 52). ایـن امـر، احتمـال ارائـه اظهارنامـه‌های نادرسـت یـا قاچـاق کـالا را کـاهش می‌دهـد. همچنـین، اسـتفاده از امضـای دیجیتـال در بلاکچـین هویـت طـرفین را تاییـد کـرده و از جعـل هویـت و تقلب در اسـناد جلـوگیری می‌کنـد. بـه عنـوان مثـال، گمـرک می‌توانـد بـا اسـتفاده از امضـای دیجیتـال اسـناد تـرخیص کـالا را تاییـد کنـد و از اصـالت آن‌هـا اطمینـان یابـد، در نتیجـه، اسـتفاده از اسـناد جعلـی بـه شـدت کاهش یافته و به پیشگیری از جرایم گمرکـی کمـک می‌کنـد. کـه بـه کشـور سـنگاپور بـه عنـوان نمونـه عملـی می‌تـوان اشـاره کـرد کـه سـنگاپور یکـی از پیشـروها در اسـتفاده از بلاکچـین در تجـارت بین‌المللـی اسـت. پلتفـرم TradeTrust کـه توسـط Infocomm Media Development Authority(IMDA) توسـعه یافتـه، امکـان تبـادل دیجیتـال اسـناد تجـاری را فـراهم می‌کنـد و از بلاکچـین بـرای تأییـد اصـالت و جلـوگیری از جعل استفاده می‌کند (Yotaro, 2018, p: 15).

چالش‌های کاربرد بلاکچین در پیشگیری از جرایم اقتصادی

با وجود مزایای متعدد فناوری بلاکچین در پیشگیری غیرکیفری از جرایم اقتصادی، به‌کارگیری عملی این فناوری با چالش‌های مهمی مواجه است که توجه به آن‌ها برای تحقق اثربخشی کامل این سیستم‌ها ضروری می‌باشد. در این بخش، دو چالش اساسی مورد بررسی قرار می‌گیرد: نخست مسأله مقیاس‌پذیری که محدودیت‌های فنی در پردازش حجم بالای تراکنش‌ها را شامل می‌شود، و دوم چالش حریم خصوصی که ناشی از تعارض ذاتی بین شفافیت بلاکچین و الزامات محرمانگی داده‌هاست. تحلیل این چالش‌ها می‌تواند راهگشای توسعه راهکارهای عملی برای بهینه‌سازی استفاده از بلاکچین در حوزه مبارزه با جرایم اقتصادی باشد.

مقیاس پذیری

یکی از چالش‌های اساسی در بکارگیری فناوری بلاکچین برای پیشگیری از جرایم اقتصادی، مسئله مقیاس‌پذیری است. در این بخش به بررسی محدودیت‌های فنی شبکه‌های بلاکچین در پردازش حجم بالای تراکنش‌های مالی می‌پردازیم. مقیاس‌پذیری پایین می‌تواند موجب کاهش سرعت تراکنش‌ها و افزایش هزینه‌های عملیاتی شود که این امر کارایی سیستم را در مقابله با جرایم اقتصادی تحت تأثیر قرار می‌دهد. در این تحلیل، راهکارهای موجود برای بهبود مقیاس‌پذیری از جمله استفاده از راه‌حل‌های لایه دوم، الگوریتم‌های اجماع جدید و شاردینگ مورد بررسی قرار خواهند گرفت.

تعریف مقیاس پذیری در بلاکچین

مقیاس‌پذیری در بلاکچین به قابلیت شبکه در حفظ یا بهبود عملکرد خود با افزایش تعداد کاربران و تراکنش‌ها اشاره دارد. این مفهوم در دو حوزه اصلی مطرح می‌شود: پردازش تراکنش‌ها و ذخیره‌سازی داده‌ها. در حالی که سیستم‌های مالی سنتی مانند شبکه‌های پرداخت بین‌المللی توانایی مدیریت هزاران تراکنش در ثانیه را دارند، بسیاری از بلاکچین‌های عمومی به‌دلیل ماهیت غیرمتمرکز و الگوریتم‌های اجماع پیچیده، با محدودیت‌های جدی در این زمینه مواجه هستند.

مقیاس پذیری تراکنش در ثانیه

یکی از بزرگترین چالش‌های بلاکچین، پایین بودن نرخ تراکنش در ثانیه (TPS) است. برای مثال، بیتکوین تنها قادر به پردازش ۷ تراکنش در ثانیه است، در حالی که اتریوم در حالت پایه حدود ۱۵ تا ۳۰ تراکنش را مدیریت میکند. این محدودیت ناشی از عوامل متعددی از جمله اندازه ثابت بلوک‌ها و زمان تأیید بلوک‌های جدید است. در مقابل، سیستم‌های متمرکز مانند شبکه‌های کارت اعتباری به‌راحتی به چند هزار تراکنش در ثانیه می‌رسند.

(Sanka, 2021, p: 7) این اختلاف فاحش، استفاده از بلاکچین را در کاربردهای گسترده اقتصادی، مانند پرداخت‌های خرد یا سیستم‌های نظارتی بلادرنگ، با مشکل مواجه میکند. به این صورت که پذیرش بالای ارزهای دیجیتال، مسئله مقیاس پذیری در بلاکچین‌های عمومی را تشدید می‌کند. تعداد تراکنش‌های بیت‌کوین و اتریوم هر روز در حال افزایش است و روزانه بیش از ۱۳۰۰۰ تراکنش با بیت‌کوین انجام می‌شود این تعداد بالای تراکنش‌ها، تراکنش‌های بیت‌کوین را حجیم می‌کند. یکی از فرآیندهای بلاکچین‌های عمومی، تأیید منبع تراکنش است و هر گره باید هر تراکنش را ذخیره و تأیید کند. بنابراین، تأیید هر تراکنش در بیت‌کوین با افزایش حجم آن، برای ماینرها یک چالش است. این امر به دلیل ناکارآمدی مکانیسم اجماع اثبات کار (PoW) که در بیت‌کوین برای تأیید و تأیید هر تراکنش به کار گرفته شده است، اتفاق می‌افتد. PoW متأسفانه پرکاربردترین پروتکل اجماع است شایان ذکر است که تعداد کل تراکنش‌ها در اتریوم در طول سال‌ها به طور مداوم افزایش یافته است. در سال‌های اخیر هزاران تراکنش هر روز رخ داده است. در اتریوم، اندازه محدود بلوک نمی‌تواند تمام تراکنش‌های ارسالی توسط ماینرها را در خود جای دهد. بنابراین، تأیید هر تراکنش برای ماینرها چالش برانگیز است. نتیجه این است که ماینرها تمایل دارند.

مقیاس پذیری ذخیره‌سازی داده

علاوه بر ناکارآمدی در فرآیند تأیید تراکنش، یکی دیگر از عوامل مهم، ذخیره‌سازی است که باید به طور جدی مورد توجه قرار گیرد. با افزایش تراکنش‌ها، ظرفیت ذخیره‌سازی مورد نیاز برای بلاک‌ها باید به طور همزمان افزایش یابد در غیر این صورت مشارکت را دشوار یا غیر ممکن می‌کند، به خصوص توسط گره هایی که حافظه کمی دارند (Si, Honghao, 2023, p:1). و همچنین با رشد بلاکچین، نیازهای ذخیره‌سازی برای گره‌ها به صورت تصاعدی افزایش می‌یابد و این رشد، مشارکت گره‌های منفرد را چالش برانگیز می‌کند و به طور بالقوه کنترل را متمرکز می‌کند. یکی از ویژگی‌های کلیدی بلاکچین‌های عمومی، ذخیره‌سازی تمام تاریخچه تراکنش‌ها در تمام نودهای شبکه است. در بیت‌کوین، حجم دفترکل از حدود ۲۰ گیگابایت در سال ۲۰۱۵ به بیش از ٤۰۰ گیگابایت در سال ۲۰۲۳ رسیده است. با افزایش تراکنش‌ها، حجم دفترکل بلاکچین به سرعت رشد می‌کند این مسئله دو مشکل اساسی ایجاد میکند:

۱. کاهش تعداد نودهای کامل: با بزرگتر شدن دفترکل، اجرای یک نود کامل به منابع محاسباتی و فضای ذخیره‌سازی بیشتری نیاز دارد که باعث کاهش غیرمتمرکزسازی شبکه میشود.

۲. افزایش هزینه‌های عملیاتی: برای کسب‌وکارها و نهادهای نظارتی که نیاز به پیاده‌سازی بلاکچین در مقیاس بزرگ دارند، هزینه‌های نگهداری داده‌ها میتواند مانع جدی باشد.

حفظ حریم خصوصی در استفاده از فناوری بلاکچین

فناوری بلاکچین به دلیل ویژگی‌های منحصربه‌فرد خود، از جمله شفافیت، غیرمتمرکز بودن و امنیت بالا، به‌عنوان ابزاری نوین در پیشگیری غیرکیفری از جرایم اقتصادی مانند پولشویی، تقلب مالی و فساد اقتصادی مورد توجه قرار گرفته است. این فناوری با ایجاد بستری شفاف و غیرقابل‌تغییر برای ثبت تراکنش‌ها، امکان نظارت و ردیابی فعالیت‌های مالی را فراهم می‌کند. با این حال، یکی از چالش‌های اساسی در بهره‌گیری از بلاکچین، حفظ حریم خصوصی کاربران است. حریم خصوصی به‌عنوان یکی از حقوق بنیادین بشری، در اسناد بین‌المللی مانند ماده ۱۲ اعلامیه جهانی حقوق بشر (۱۹۴۸)[1] و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶)[2] به رسمیت شناخته شده و در نظام حقوقی ایران نیز تحت اصول قانون اساسی (مانند اصل ۲۲) مورد حمایت قرار گرفته است. در حوزه پیشگیری غیرکیفری، حریم خصوصی نه‌تنها به‌عنوان یک حق فردی، بلکه به‌عنوان عاملی برای جلب اعتماد کاربران به سیستم‌های مبتنی بر بلاکچین اهمیت دارد. این مبحث، ابتدا به اهمیت حفظ حریم خصوصی در بلاکچین پرداخته و سپس چالش‌های مرتبط با آن را از منظر حقوقی و جرم‌شناختی تحلیل می‌کند.

اهمیت حفظ حریم خصوصی در فناوری بلاکچین

حفظ حریم خصوصی در فناوری بلاکچین از دو منظر حقوقی و عملیاتی حائز اهمیت است. از منظر حقوقی، حریم خصوصی به‌عنوان یکی از مؤلفه‌های کرامت انسانی و حق بر خودمختاری، در پیشگیری از نقض حقوق بنیادین و سوءاستفاده از داده‌های شخصی نقش کلیدی دارد. از منظر عملیاتی، اعتماد کاربران به سیستم‌های بلاکچین به توانایی این فناوری در حفاظت از اطلاعات حساس آن‌ها وابسته است. فقدان مکانیزم‌های مؤثر برای حفظ حریم خصوصی می‌تواند پذیرش این فناوری را در پیشگیری از جرایم اقتصادی با مانع مواجه کند. در ادامه، دو جنبه اصلی این اهمیت بررسی می‌شود.

---

[1] . Universal Declaration of Human Rights

[2] . International Covenant on Civil and Political Rights

تعارض شفافیت غیرقابل تغییر با حقوق حریم خصوصی

یکی از اصلی‌ترین چالش‌های بلاکچین در زمینه حریم خصوصی، ویژگی تغییرناپذیری و شفافیت ذاتی آن است مانند بیت‌کوین و اتریوم در حالی که این ویژگی‌ها برای پیشگیری از جرایم اقتصادی مانند پولشویی یا فساد مالی مفید هستند، زیرا امکان ردیابی و نظارت بر تراکنش‌های مشکوک را فراهم می‌کند، اما با اصل حفظ حریم خصوصی در تعارض است. به‌عنوان مثال، در بلاکچین بیت‌کوین، هر تراکنش با یک آدرس عمومی[1] ثبت می‌شود که اگرچه مستقیماً به هویت واقعی فرد متصل نیست، اما در صورت اتصال این آدرس به اطلاعات هویتی (مانند اطلاعات ثبت‌شده در صرافی‌های ارز دیجیتال)، حریم خصوصی کاربر به خطر می‌افتد.این مسئله به‌ویژه در مواردی که اطلاعات حساس مالی افراد یا شرکت‌ها به‌صورت عمومی در بلاکچین ثبت شده باشد، می‌تواند مشکلات حقوقی و امنیتی جدی ایجاد کند(Joshi, 2018, p:133,134). به عبارت دیگرعصر کلان‌داده، حریم خصوصی کاربران را در سناریوهای دیجیتال متعددی تضعیف می‌کند. اشخاص ثالث بزرگ با جمع‌آوری، تجزیه و تحلیل، مرتبط‌سازی و کنترل حجم عظیمی از داده‌های شخصی، از مدیریت داده‌های کاربران خود سود می‌برند. این سازمان‌ها و خدمات آنها در معرض نقض امنیتی و سوءاستفاده از داده‌های کاربران هستند که ممکن است حریم خصوصی کاربران را حتی بدون آگاهی کاربر به خطر بیندازد. تراکنش‌ها در بلاکچین نیز از این مسائل مربوط به حریم خصوصی مصون نیستند. علاوه بر این، به افراد گزینه‌های کمی برای کنترل داده‌های شخصی و حریم خصوصی آنها در طول تراکنش‌های آنلاینشان داده می‌شود، از جمله اینکه چگونه، چه زمانی، کجا، توسط چه کسی و کدام اطلاعات شخصی خاص در هر تراکنش خاص افشا می‌شود. این مشکل در بلاکچین تشدید می‌شود، زیرا داده‌های خصوصی موجود در دفتر کل تغییرناپذیر هستند و حق کاربر برای کنترل و اصلاح اطلاعات شخصی کاهش می‌یابد. این وضعیت با ظهور سناریوهای اینترنت اشیا تشدید می‌شود، جایی که میلیاردها شیء هوشمند محدود، با قابلیت‌های اندک برای اجرای مکانیسم‌های امنیتی مناسب، تلاش می‌کنند با حملات سایبری که ممکن است داده‌های مدیریت شده آنها و در نهایت اطلاعات حساس و خصوصی صاحبان/کاربران آنها را فاش کند، مقابله کنند. علاوه بر این، در اینترنت اشیا، اعمال کنترل‌های حریم خصوصی کاربر دشوار است، زیرا اشیاء هوشمند معمولاً بدون کنترل و رضایت کاربر، از طرف او عمل می‌کنند و این امر، پذیرش اصل حداقل افشای اطلاعات شخصی را تضعیف می‌کند(Bernabe, 2019, p: 164915). بنابراین تعارض، چالشی اساسی در طراحی سیستم‌های بلاکچین ایجاد می‌کند، زیرا از یک سو،

[1] . . Public Key

شفافیت برای پیشگیری از جرایم اقتصادی ضروری است و از سوی دیگر، حفظ حریم خصوصی به‌عنوان یک حق بنیادین باید تضمین شود.

مخاطرات سوءاستفاده از داده‌های عمومی شده

شفافیت ذاتی بلاکچین می‌تواند زمینه سوءاستفاده از داده‌های کاربران را فراهم کند. با تحلیل تراکنش‌های ثبت‌شده در بلاکچین، امکان شناسایی الگوهای رفتاری و مالی کاربران وجود دارد که این اطلاعات می‌تواند توسط مجرمان برای اهدافی مانند کلاهبرداری هدفمند یا باج‌گیری مورد استفاده قرار گیرد. موارد متعددی از استفاده نادرست از داده‌های عمومی بلاکچین گزارش شده است، از جمله شناسایی آدرس‌های کیف پول افراد مشهور و ردیابی تراکنش‌های مالی آن‌ها. به عبارت دیگر داده‌های ذخیره‌شده در بلاکچین به دلیل ویژگی غیرقابل‌تغییر بودن و دسترسی عمومی در بلاکچین‌های عمومی، در معرض خطر سوءاستفاده قرار دارند. این داده‌ها ممکن است توسط نهادهای دولتی، هکرها یا شرکت‌های تحلیل داده برای مقاصدی مانند نظارت غیرقانونی، بازاریابی تهاجمی یا حتی فعالیت‌های مجرمانه مورد بهره‌برداری قرار گیرند. برای مثال، اطلاعات تراکنش‌های مالی که در بلاکچین ثبت می‌شوند، می‌توانند الگوهای رفتاری کاربران، مانند عادات خرید یا ارتباطات مالی آن‌ها، را آشکار کنند. این موضوع در پیشگیری غیرکیفری از جرایم اقتصادی، که نیازمند دسترسی به داده‌های مالی برای شناسایی فعالیت‌های مشکوک است، چالش‌ساز است. داده‌های بلاکچین به دلیل ماهیت دائمی و شفاف خود، در صورت نقض حریم خصوصی، قابل حذف یا اصلاح نیستند، که این امر خطر نقض حقوق کاربران را تشدید می‌کند و باعث عدم وجود اعتماد می‌گردد زیرا کاربران بدون اعتماد به سیستم، چه دیجیتال و چه آنالوگ، نمی‌توانند کاری انجام دهند. بلاکچین از سیستمی که در آن اعتماد ضروری است، به سیستم دیگری که بر اساس کد است و در آن اعتماد غیرضروری است، منتقل نمی‌شود. در ادبیات معمولاً به یک "رکورد قابل اعتماد" اشاره می‌شود، که نشان می‌دهد کاربران شروع به اعتماد به بازیگرانی می‌کنند که زیرساخت بلاکچین را ممکن می‌سازند. بدون اعتماد به توسعه‌دهندگان یا واسطه‌هایی که به عنوان ارائه‌دهنده خدمات عمل می‌کنند، کاربران از یک سیستم بلاکچین استفاده نمی‌کنند(Jiménez, 2019, p:295). در نظام حقوقی ایران، ماده ۱ قانون جرایم رایانه‌ای (۱۳۸۸) بر حفاظت از داده‌های شخصی تأکید دارد، اما فقدان مقررات خاص برای فناوری بلاکچین، این مخاطرات را افزایش می‌دهد. بنابراین، توسعه چارچوب‌های حقوقی و فنی برای محدود کردن دسترسی غیرمجاز به داده‌های بلاکچین و تضمین حقوق کاربران ضروری است.

نتیجه‌گیری

این پژوهش با بررسی نظام‌مند کاربرد فناوری بلاکچین در پیشگیری غیرکیفری از جرایم اقتصادی با تمرکز بر ویژگی‌های امنیتی آن پرداخت و به یافته‌های ارزشمندی دست یافته است. مطالعه ابتدا با تبیین ماهیت پیچیده جرایم اقتصادی و ناکارآمدی نسبی روش‌های سنتی کیفری، ضرورت بهره‌گیری از راهکارهای نوین را نشان داد. سپس با تحلیل ویژگی‌های منحصر به فرد بلاکچین شامل ساختار غیرمتمرکز، تغییرناپذیری داده‌ها و مکانیسم‌های رمزنگاری پیشرفته، ظرفیت‌های این فناوری در ایجاد محیطی امن و شفاف برای مبادلات مالی مورد تأکید قرار گرفت. مطالعه حاضر در بخش سوم به بررسی عمیق نقش مکانیسم‌های امنیتی بلاکچین در پیشگیری غیرکیفری از جرایم اقتصادی پرداخته است. یافته‌ها به وضوح نشان می‌دهد که معماری امنیتی منحصر به فرد بلاکچین، شامل رمزنگاری پیشرفته، تغییرناپذیری داده‌ها و سیستم‌های اجماع توزیع‌شده، ابزاری کارآمد برای مقابله با جرایم مالی فراهم کرده است. سیستم‌های رمزنگاری مبتنی بر کلید عمومی و خصوصی امکان احراز هویت مطمئن را فراهم می‌آورند و از جعل هویت جلوگیری می‌کنند. ساختار تغییرناپذیر دفترکل توزیع‌شده، هرگونه دستکاری در سوابق مالی را غیرممکن می‌سازد و شفافیت ذاتی تراکنش‌ها امکان ردیابی جریان‌های مالی مشکوک را فراهم می‌آورد. مقاومت در برابر حملات سایبری از طریق پروتکل‌های اجماع توزیع‌شده، امنیت شبکه را در سطحی بی‌سابقه تضمین می‌کند. این ویژگی‌ها در عمل ثابت کرده‌اند که می‌توانند به طور مؤثری از کلاهبرداری‌های مالی پیشگیری کنند، امکان پولشویی را به حداقل برسانند و زمینه سوءاستفاده از اطلاعات مالی را مسدود نمایند. با این وجود، دو چالش اساسی مقیاس‌پذیری و حریم خصوصی وجود دارد که به تفصیل بررسی شدند. محدودیت سرعت تراکنش‌ها و مصرف انرژی بالا در برخی الگوریتم‌های اجماع، همراه با تعارض ذاتی بین شفافیت بلاکچین و قوانین محرمانگی داده‌ها، موانع مهمی در مسیر بهره‌برداری گسترده از این فناوری شناسایی شدند. با این حال، راهکارهای عملیاتی مانند توسعه لایه‌های دوم، استفاده از بلاکچین‌های مجاز و به کارگیری تکنیک‌های رمزنگاری پیشرفته، مسیرهای امیدبخشی برای غلبه بر این چالش‌ها پیشنهاد کردند.

منابع

۱. تفضلی، سیاوش،(۱۳۹۷) مبانی بلاکچین، تهران، شبکه راه پرداخت

۲. تینا لورنس، تهران برگردان: بهروز خدارحمی، مهری اسدی وصفی،(۱۴۰۰) چ۲ تهران، آوند دانش

۳. جنگروی، حسین، « و دیگران» (۱۴۰۱) بلاکچین: راهنمای عملی توسعه کسب و کار، قانونگذاری و راه‌حلهای تکنولوژی، چ۱، تهران خط آخر

٤. حاجی ملامیرزایی، حامد، «و دیگران»(۱۳۹۹) بلاکچین، تهران، مرکز انتشارات راهبردی،

۵. حیدری، حامد، غرایاق زندی، یاسر،(۱۳۹۷) بلاکچین و قانون حکمرانی کد، تهران ،شبکه راه پرداخت

٦. خدارحمی، بهروز، اسدی وصفی، مهری،(۱۴۰۰) زنجیره بلوکی (بلاکچین) ، چ۲، تهران ،آوند دانش

۷. رایت، آرون، مترجم؛ حیدری، حامد، (۱۳۹۷) بلاکچین و قانون؛ حکمرانی کد، چ۱، تهران، راه پرداخت.

۸. سراج. "جرایم اقتصادی سازمان‌یافته و تأثیر آن بر نظام اقتصادی کشور (مطالعه موردی: پرونده فساد بانکی سه هزار میلیارد تومانی)." فصلنامه تحقیق و توسعه در حقوق تطبیقی ٤,۱۱ (۲۰۲۱): ۵۵-۸۲.

۹. صمدی، فاطمه، کشاورزیان، ندا،(۱۳۹۹) ،بلاکچین از محتوی تا اجرا، چ۱، تهران دیبادخت،

۱۰. عبدالهی، علی،(۱۴۰۰) تجاری‌سازی بلاکچین، چ۱، تهران، بورس،

۱۱. مرجانی، مهدی، میر عباسی، سید باقر، (۱۳۹۹) پیشگیری غیر کیفری از جرایم اقتصادی در کنوانسیون مریدا، فصلنامه تحقیقات حقوق خصوصی و کیفری، شماره٤٤، تابستان

۱۲. معین، محمد، (۱۳۸٦)فرهنگ فارسی، چ٤، تهران، ادنا

۱۳. مهدوی پور، اعظم، (۱۳۹۵) سیاست کیفری افتراقی در قلمرو بزهکاری اقتصادی، ج۲ تهران، میزان،

۱٤. میر سعیدی, سید منصور and ,زمانی.(۱۳۹۲) "جرم اقتصادی؛ تعریف یا ضابطه؟." فصلنامه پژوهش حقوق کیفری ۲,٤ (۲۰۱۳): ۱٦۷-۱۹۹.

۱۵. نیاز پور، امیر حسین، پیشگیری از جرم، (۱٤۰۰)چ۱، تهران، دادگستر،

۱٦. ولیدی، محمدصالح، (۱۳۹۳) حقوق کیفری اقتصادی، چ۱ تهران، جنگل،

۱۷. غضنفری, هنگامه and ,قاسمی‌کیا.(۱۳۹٤) "تأثیر پیشگیری غیرکیفری بر میزان احساس امنیت در میان جوانان شهر بروجرد." پژوهش های راهبردی مسائل اجتماعی ٤,۱ (۲۰۱۵): ۱٦۷-۱۸۲.

۱۸. هلاکوئی، محمد، محمدی، شبنم، (۱۳۹۹) امپراتوری بلاکچین، اصفهان، رهنج،

۱۹. همتی، مریم، زارع، ژاله، (۱٤۰۱) بلاکچین و بانکداری، چ،۱ ، تهران، نورعلم

References

1. (Balshetwar, sarita Vitthal, 2024) Blokchain Technology: Features, characteristics with a focus on its Types. International Journal of Engineering Technology and Management sciences. 2 Volume No 8 April
2. (Bernabe, Jorge Bernal, 2019) et al, Privacy-preserving solutions for blockchain: Review and challenges, Ieee Access 7: 164908-164940, p: 164915
3. (Hua Yi Lin. 2023) Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles, Sensors 2023, 23, p: 5
4. Jiménez-Gómez, Briseida Sofia,2019) (RISKS OF BL RISKS OF BLOCKCHAIN FOR D AIN FOR DATA PROTECTION: A EUROPEAN TION: A EUROPEAN APPROACH, Santa Clara High Technology Law Journal. p: 295

5. Joshi, Archana Prashanth, Meng Han, and Yan Wang, (2018) A survey on security and privacy issues of blockchain technology, Mathematical foundations of computing 1.2P: 133,134
6. (Kim, Member, 2004) Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY, p: 218
7. Philip Nwaga, Smart Idima, 2022) (Post-Quantum Cryptographic Algorithms for Secure Communication in Decentralized Blockchain and Cloud Infrastructure. Article in International Journal of Computer Applications Technology and Research • January. P: 156
8. Saad, Muhammad, et al. (2019). "Exploring the attack surface of blockchain: A systematic overview." arXiv preprint arXiv:1904.03487
9. Sanka, Abdurrashid Ibrahim, and Ray CC Cheung, (2021) A systematic review of blockchain scalability: Issues solutions, analysis and future research, Journal of Network and Computer Applications 195: 103232. P: 7
10. Si, Honghao, and Baoning Niu. (2023) "Research on blockchain data availability and storage scalability." Future Internet 15.6 :212
11. Songlin He ،and others.)2022 Blockchain-Based Automated and Robust Cyber Security Management© published by Elsevier. P: 8
12. Zawar Shah،and others. (2022) Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey, Sensors, 22. P: 10
13. ER-RAJY LATIFA and others, (2017) BLOCKCHAIN: BITCOIN WALLET CRYPTOGRAPHY SECURITY, CHALLENGES AND COUNTERMEASURES., Journal of Internet Banking and Commerce, December 2017, vol. 22, no. 3. P:8
14. Rodrigues dos Santos, (2024) Enhancing International Trade Security: Real-Time Risk Assessment in Brazilian Customs with Blockchain Technology, International Journal of Business and Management; Vol. 19, No. 6; p: 52
15. Yotaro Okaza (2018), Unveiling the Potential of Blockchain for Customs: WCO Research Paper No.45, P:15
16. Zawar Shah،and others. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT:) A Survey, Sensors 2022, 22. P: 10