APJ. 5(2):51-59, Summer 2024

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

# Apply Internet of Things and Block Chain for Smart Contracts

**A. Ghasemzadeh Dehabadi**[*,1]

[1] Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran

**RESEARCH PAPER**

Received: 2 April 2024
Accepted: 24 June 2024

**KEYWORDS:**
Smart Contracts,
Internet of Things
Artificial Intelligence,
Blockchain,
Smartening of Contracts,

**[1] Corresponding author:**
*arefeghasemzade@yahoo.com*

**ABSTRACT**

With the expansion of the cyber world, issues are directly and indirectly entered into this area and are studied; The Internet of Things and Blockchain are two developing technologies that create opportunities for new topics including smart contracts. A smart contract is a computer protocol based on blockchain technology to create or improve a contract. In these contracts, valid transactions are defined as programmed code and applied automatically without the need for intermediaries. In this research, we will first introduce the Internet of Things, blockchain, and then smart contracts created from the combination of these two technologies and the advantage of making smart contracts. The method of this research is descriptive and data analysis. The Internet of Things, which is undergoing growth in the IT industry; It provides limitless opportunities for smart contracts; So, in the absence of IoT sensors, these contracts have limited potential. Of course, the technical challenges of smart contracts are a set of programs that are self-verifying, self-executing, and tamper-resistant. By integrating blockchain technology, the smart contract is able to perform a task in real time at a low cost and provide a higher degree of security. Examining a few scenarios in real life shows; The technical challenges of smart contracts are very few along with the advantages of using these contracts. By identifying and analyzing the performance measurement of smart contracts, significant results are obtained for the development of these contracts.

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۲، تابستان ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

# بکارگیری اینترنت اشیاء و بلاکچین در قراردادهای هوشمند

**عارفه قاسم زاده ده آبادی** [۱،*]

[۱] گروه مهندسی کامپیوتر، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

## چکیده

**مقاله پژوهشی**

با گسترش دنیای سایبری مسائل به صورت مستقیم و غیر مستقیم وارد این حیطه شده و مورد مطالعه قرار میگیرند؛ اینترنت اشیاء و بلاکچین دو فناوری در حال توسعه هستند که فرصت هایی را برای موضوعات جدیدی از جمله قراردادهای هوشمند ایجاد می کنند. قرارداد هوشمند یک پروتکل کامپیوتری برپایه فناوری بلاکچین است که برای ایجاد یا بهبود قرارداد می باشد. در این قراردادها تراکنش های معتبر به صورت کد برنامه نویسی شده تعریف و به صورت خودکار بدون نیاز به واسطه اعمال می شوند. در این تحقیق ابتدا به معرفی اینترنت اشیاء، بلاکچین و سپس قراردادهای هوشمند ایجاد شده از ترکیب این دو فناوری و مزیت هوشمندسازی قراردادها می پردازیم، روش این تحقیق توصیفی و تجزیه و تحلیل داده ها است. اینترنت اشیاء که در حال گذراندن رشد در صنعت فناوری اطلاعات است؛ فرصت های بی حد و حصری را برای قراردادهای هوشمند فراهم می کند؛ به طوریکه در صورت فقدان سنسور اینترنت اشیاء، این قراردادها دارای پتانسیل محدودی هستند. البته چالش های فنی قراردادهای هوشمند، مجموعه ای از برنامه ها است که خود تأیید شونده، خود اجرا و مقاوم در برابر دستکاری هستند. قرارداد هوشمند با ادغام فناوری بلاک چین قادر به انجام یک کار در زمان واقعی با هزینه کم و ارائه درجه امنیت بیشتر است. بررسی چند سناریو در زندگی واقعی نشان می دهد؛ چالش های فنی قراردادهای هوشمند در کنار مزیت های استفاده از این قراردادها بسیار اندک است. با شناسایی و تجزیه و تحلیل سنجش عملکرد قراردادهای هوشمند نتایج قابل توجهی برای توسعه این قراردادها به دست می آید.

**واژگان کلیدی:**
قراردادهای هوشمند،
اینترنت اشیاء،
هوش مصنوعی،
بلاکچین،
هوشمندسازی قراردادها،

## مقدمه

اینترنت اشیاء که هم اکنون در سراسر دنیا در حال رشد تصاعدی است، برای نخستین بار در سال ۱۹۹۹ بیان شده و اخیراً به طور جدی در دنیای فناوری اطلاعات و ارتباطات در جریان است؛ این مهم می تواند از لحاظ اقتصادی و حتی به منظور صرفه جویی در وقت مفید باشد. اینترنت اشیا معمولاً با هدف از بین بردن شکاف بین دنیای فیزیکی و دیجیتال استفاده می شود، یک شبکه به هم پیوسته از دستگاه ها، از جمله حسگرها و دیگر سخت افزارهای تعبیه شده، که وظیفه جمع آوری و توزیع داده ها، بین یکدیگر یا با سایر نهادها، از طریق یک شبکه محلی و اینترنت را دارند، می باشد. پیشرفت اینترنت اشیاء، مرحله جدیدی را در کشورهای در حال توسعه ایجاد کرده و در پدیده های جدیدی از جمله قراردادهای هوشمند نیز کاربرد دارد. فناوری اینترنت اشیاء یا به اختصار IOT به ارتباط اینترنتی بین اشیاء و تجهیزات گفته می شود که متصل به شبکه اینترنت هستند؛ این مهم در قرارداد هوشمند به طرفین تجاری قرارداد کمک می کند تا میزان استفاده خود از منابع را کاهش دهند و با سپردن اجزای مختلف و جزئیات قرارداد به بستر بلاکچین، قرارداد منعقد شود [۱] .

تاریخچه فناوری بلاکچین که از سال ۱۹۷۹ آغاز شده فناوری معرفی می کند که گونه ای از یک پایگاه داده و مشتمل بر یک دفترکل همگانی است که می توان در آن تراکنش ها را بدون نیاز به یک نهاد واسطه یا شخص ثالث ثبت و تأیید کرد. فناوری بلاک چین برای ارائه مدیریت کارآمد اشتراک گذاری و دسترسی به داده ها در نظر گرفته شده است ابتدائاً در خصوص کنترل در شبکه های اینترنت اشیاء چندین طرح در زنجیره بلوکی یکپارچه ارائه شده است اما به دلیل هزینه بالا و برخی مشکلات دیگر رد شده است. با ترکیب دو فناوری مذکور در هوشمند سازی قراردادها یک قرارداد با برقراری ارتباط و اعتبار سنجی ارتباط بین دستگاه های مختلف اینترنت اشیاء منعقد می شود و نیازی به شخص ثالثی برای نظارت بر تراکنش ها نیست، این قرارداد های هوشمند می توانند به طور موثر بر پرداخت های خرد بین گره های مختلف اینترنت اشیاء نظارت کنند. در بخش انرژی، ادغام اینترنت اشیا با بلاک چین امکان یک بازار همتا به همتا را فراهم می‌کند که در آن ماشین‌ها می‌توانند به صورت خودکار انرژی بخرند و بفروشند. قراردادهای هوشمند روی پلتفرمی مشترک، متن باز و قابل اعتماد اجرا می شوند. می توان گفت قرارداد هوشمند موجودی است که در بستر بلاک چین زندگی می کند و از امنیت بالایی برخوردار است؛ به طوریکه ذخیره و بازیابی قرارداد ذاتاً محافظت شده است [۳-۲] .

هدف از این تحقیق معرفی اینترنت اشیاء، بلاکچین و سپس قراردادهای هوشمند ایجاد شده از ترکیب این دو فناوری و مزیت هوشمندسازی قراردادها می باشد.

## اینترنت اشیاء و کارکردها

اینترنت اشیا یک تغییر پارادایم جدید در عرصه فناوری اطلاعات است. عبارت «اینترنت اشیا» از دو کلمه اینترنت و اشیاء ساخته شده است. اینترنت یک سیستم جهانی از شبکه های کامپیوتری متصل به هم است که از اینترنت استاندارد استفاده می کند. مجموعه پروتکل (TCP/IP) برای خدمت به میلیاردها کاربر در سراسر جهان می باشد. این شبکه ای از شبکه است که از میلیون ها شبکه تشکیل شده است. شبکه های خصوصی، عمومی، دانشگاهی، تجاری، و دولتی، با گستره محلی تا جهانی است. کلمه چیز ها به هر شی یا شخصی که با دنیای واقعی قابل تشخیص باشد، گفته می شود. اشیاء روزمره نه تنها شامل وسایل الکترونیکی است که ما با آنها روبرو می شویم و از محصولات روزانه و فناوری پیشرفته مانند تجهیزات و ابزارها استفاده می کنیم، اما «چیزهایی» که معمولاً آنها را الکترونیکی نمی‌دانیم مانند غذا، لباس. و مبلمان؛ مواد، قطعات و تجهیزات، کالاها و اقلام تخصصی؛ نشانه ها، بناهای تاریخی و آثار هنری و همه متفرقه تجارت، فرهنگ و پیچیدگی ها را نیز شامل می شود. این بدان معناست که در اینجا چیزها می توانند هر دو موجود غیر زنده و زنده باشد مانند شخص، حیوانات [۵-۴] .

هیچ تعریف منحصر به فردی برای اینترنت اشیا وجود ندارد که توسط جامعه جهانی کاربران قابل قبول باشد. در واقع، گروه های مختلفی از جمله دانشگاهیان، محققان، شاغلین، نوآوران، توسعه دهندگان و افراد شرکتی وجود دارند که این اصطلاح را تعریف کرده اند، اگرچه استفاده اولیه از آن به کوین اشتون نسبت داده شده است. کارشناس نوآوری دیجیتال آنچه در همه تعاریف مشترک است این ایده است که نسخه اول از اینترنت در مورد داده های ایجاد شده توسط افراد بود، در حالی که نسخه بعدی در مورد داده های ایجاد شده توسط چیزها است. بهترین تعریف اینترنت اشیا این خواهد بود: شبکه ای باز و جامع از اشیاء هوشمند که ظرفیت سازماندهی خودکار، اشتراک گذاری را دارند اطلاعات، داده ها و منابع، واکنش و عمل در مواجهه با موقعیت ها و تغییرات محیطی [۷-۶] .

اینترنت اشیا در حال بلوغ است و همچنان جدیدترین و پرطرفدارترین مفهوم در دنیای فناوری اطلاعات است. در دهه گذشته، اصطلاح اینترنت اشیاء (IoT) با ارائه چشم انداز زیرساختار جهانی از اشیاء فیزیکی شبکه ای توجه را به خود جلب کرده است، که امکان اتصال در هر زمان و مکان را برای هر چیزی فراهم می کند. اینترنت اشیا را می توان به عنوان یک شبکه جهانی نیز در نظر گرفت که امکان ارتباط را فراهم می کند؛ بین انسان به انسان، انسان به چیز و چیز به چیز، هر چیزی که در جهان با ارائه هویت منحصر به فرد برای هر شیء است. اینترنت اشیا دنیایی را توصیف می کند که تقریباً هر چیزی را می توان به هم متصل کرد و به شیوه ای هوشمندانه که تا کنون ارتباط برقرار می کند [۸] . بسیاری از ما در مورد "متصل بودن" به اصطلاح فکر می کنیم تجهیزات الکترونیکی مانند سرور، رایانه، تبلت، تلفن و تلفن های هوشمند. آنچه اینترنت اشیاء نامیده می شود، حسگرها و

محرک های تعبیه شده در اشیاء فیزیکی - از جاده ها گرفته تا ضربان سازها - هستند. از طریق شبکه‌های سیمی و بی‌سیم، اغلب از همان IP اینترنتی که اینترنت را متصل می‌کند، پیوند داده می‌شود. اینها شبکه ها حجم عظیمی از داده ها را تولید می کنند که برای تجزیه و تحلیل به رایانه ها سرازیر می شوند. وقتی اشیاء هر دو می توانند حس کنند محیط و ارتباط، آنها به ابزاری برای درک پیچیدگی و پاسخ سریع به آن تبدیل می شوند. آنچه در همه اینها انقلابی است این است که این سیستم های اطلاعات فیزیکی اکنون شروع به استقرار کرده اند. و برخی از آنها حتی تا حد زیادی بدون دخالت انسان کار می کنند. "اینترنت اشیا" به کدگذاری اشاره دارد و شبکه ای از اشیاء و چیزهای روزمره برای تبدیل آنها به صورت جداگانه توسط ماشین و اینترنت قابل ردیابی است [۱و۳و۹و۱۰] .

با تصور هوشمند سازی قراردادها برنامه ها به راحتی با یکدیگر در تعامل هستند و اینترنت اشیاء به روشی شبیه به سخت افزار می باشد که در آن درایوها برنامه ها را قادر می سازند تا با دستگاه های سخت افزاری تعامل داشته باشند. قراردادهای هوشمند با بکارگیری اینترنت اشیاء می توانند قابلیت های یک شیء را توصیف کنند، همچون خدماتی که ارائه می دهد و نحوه دسترسی به آن. با تمدید قراردادهای هوشمند موجود، توسعه دهندگان باید قادر به ادغام اشیاء در سیستم ها و فرآیندهای آن باشند، و همچنین سعی در ارائه خدمات نوآورانه تر و پایدار داشته باشند [۱۱] .

## اینترنت اشیاء و بلاکچین

فناوری بلاک چین در اصل نامی است که به طراحی زیربنای عملیات دیجیتال تبادلات ارزی داده شده است. خالق ارز بیت کوین هرگز از واژه بلاک چین در مقاله خود استفاده نکرد. این موضوع متصور است که نویسنده فناوری جدیدی را در مقاله معرفی نکرده است معنای سنتی این واژه این است که بیت کوین برای ایجاد یک «نسخه کاملاً همتا به همتا از پول نقد الکترونیکی» است که ماهیت عملکرد آن این است که هر زمان که دو عضو شبکه تراکنش انجام می دهند، آن ها تراکنش خود را به تمام اعضای شبکه (گره ها) اعلام می کنند که تراکنش را در یک بلوک با a ثبت می کنند هنگامی که ظرفیت محدود بلوک پر شد، گره ها به طور همزمان اثبات ریاضی را انجام می دهند. عملیاتی که حل آنها سخت است اما تأیید راه حل صحیح آنها آسان است. این عملیات های ریاضی به تراکنش های بیت کوین مرتبط نیستند، اما برای عملکرد سیستم ضروری هستند [۱۲] . زیرا آنها گره‌های تأیید کننده را مجبور می‌کنند تا قدرت پردازشی را صرف کنند تا در صورت گنجاندن هر یک از آنها تلف شود.

معاملات متقلبانه یا نامعتبر اولین گره ای که موفق به حل مسئله اثبات کار می شود؛ راه حل را همراه با بلوک تراکنش ها به تمام گره های دیگر پخش می کند. گره ها می توانند به سرعت و به طور ارزان صحت تراکنش ها و راه حل ها را بررسی کنند و زمانی که ۵۱ درصد از قدرت پردازش شبکه به تأیید یک بلوک رأی می‌دهد، گره‌ها شروع به ضبط تراکنش‌های جدید در یک بلوک جدید می‌کنند، بلوک اصلاح شده به تمام بلوک های قبلی اولین گره ای که مشکل اثبات کار را حل می کند با مقدار مشخصی ارز پاداش می گیرد. از شبکه این پاداش تأیید معاملات را به طور بالقوه سودآور می کند و منجر به آن می شود معمولاً به عنوان "کاوش" نامیده می شود، اگرچه "تأیید" احتمالاً توصیف دقیق تری است. بلاکچین ضد دستکاری و غیر متمرکز است [۱۳-۱۴] .

دفتر کل در بلاک چین تمام تراکنش هایی که در شبکه های توزیعی مرتبط و در سطح زیرساخت انجام می شود را ثبت می کند. بلاک چین به عنوان یک فناوری دفتر کل توزیع شده شناخته می شود و غیر قابل حذف و دستکاری است [۱۵] . فناوری بلاک چین دخالت شخص ثالث را از طریق قراردادهای هوشمند حذف می کند. قراردادهای هوشمند، برنامه های کامپیوتری مکتوب هستند که تمام قوانین برای معامله بین دو طرف در آن تعریف شده است، تا زمانی که تمام توافقات قرارداد هوشمند محقق نشود، معامله انجام نمی شود. هر زمان که قرار است هر معامله ای در شبکه های مبتنی بر بلاک چین انجام شود، قرارداد هوشمند به طور خودکار راه اندازی می شود [۱۶] . دفتر کل در تمام گره های شبکه توزیع می شود. حفظ سوابق هماهنگ شده برای حفظ ثبات داده ها در بلاک چین، ضروری است. مفهوم مرجع واحد نیز با سازوکارهای اجماع حذف می شود. تصمیمات در شبکه پس از توافق بین اکثریت گره ها ساخته می شوند. علاوه بر این، مکانیسم های اجماع مورد استفاده در فناوری بلاک چین عبارتند از: اثبات کار (PoW)، اثبات مفهوم (PoC)، اثبات اقتدار (PoA)، اثبات سهام (PoS)، تحمل خطای عملی (PBFT)، و غیره [۱۷] .

رمزنگاری، امنیت را برای کل شبکه به ارمغان می آورد. از تکنیک های رمزنگاری در بلاک چین برای امن تر کردن داده ها و تراکنش ها و جلوگیری از دستکاری دادهه ها استفاده می شود. با توجه به پیشرفت سریع فناوری بلاک چین، استفاده از رمزنگاری در حال افزایش است. بنابراین تقریبا در هر زمینه، سیستم اشتراک گذاری داده و کنترل دسترسی مبتنی بر بلاک چین برای ارائه استفاده می شود [۱۸-۱۹] .

قراردادهای هوشمند را می توان به عنوان یک پیشرفت بزرگ در نظر گرفت. فناوری بلاک چین در دهه ۱۹۹۰، یک قرارداد هوشمند را به عنوان یک پروتکل تراکنش کامپیوتری پیشنهاد داد [۲۰] .ایجاد یک قرارداد هوشمند توسط یک کلید عمومی در بلاکچین صورت میگیرد بنابراین باید حداقل یک جفت کلید عمومی-خصوصی وجود داشته باشد. نوع این کلیدها و همچنین الگوریتم های رمزگذاری شده می تواند نشانه ای برای اجرای مخصوص بلاک چین باشد [۲۱] . معمولاً در قراردادهای هوشمند شرایطی تعیین می شود، زمانی که یک شرط خاص برآورده شود (به عنوان مثال، یک طرف به شرط مقرر عمل کند) قرارداد به صورت خودکار اجرا می شود، همچنین هرکس شرطی از قرارداد را نقض کند خود به خود مجازات می شود. بلاک چین ها قراردادهای هوشمند را فعال می کنند. قراردادهای هوشمند اساساً توسط بلاک چین

پیاده سازی می شوند. بندهای قراردادی تایید شده به برنامه های کامپیوتری قابل اجرا تبدیل می شوند و ارتباطات منطقی بین قراردادی بندها نیز در قالب منطقی حفظ می شوند و در برنامه ها جریان می یابند، اجرای هر بیانیه قرارداد به عنوان یک تراکنش تغییرناپذیر ذخیره شده در بلاک چین ثبت می شود. قراردادهای هوشمند دارای تضمین کنترل دسترسی مناسب و اجرای صحیح قرارداد هستند. به طور مثال شرطی که در مورد نقض قرارداد ضمانت اجرایی پیش بینی کرده است اگر دو طرف الف و ب در مورد مجازات نقض قرارداد توافق کنند و ب قرارداد را نقض کند به طور خودکار جریمه از سپرده ب کسر می شود [۲۳-۲۲] . یک بلاک چین را می توان به عنوان یک دفتر کل عمومی در نظر گرفت که در آن همه معاملات ثبت شده اند و هیچ معامله ای را نمی توان جعل کرد، بلاک چین یک زنجیره در حال رشد از بلوک هاست، هنگامی که یک بلوک جدید ایجاد می شود، به تمام گره ها وارد می شود و شبکه اعتبارسنجی بلوک ها شرکت خواهد کرد. از وقتی که یک بلوک اعتبار سنجی شده است، به بلاک چین اضافه می شود. فناوری بلاک چین دارای ویژگی های کلیدی تمرکززدایی، تغییر ناپذیری، تداوم و ناشناس بودن است [۲۴و۲۰] . قرارداد هوشمند به قراردادهایی که گفته می شود که ابتدائاً بدون دخالت اشخاص ثالث در بستر بلاکچین منعقد می شوند و یا بعد از انعقاد قرارداد فیزیکی، قرارداد به صورت هوشمند ادامه پیدا میکند. مدیریت دارایی و تراکنش انجام وظایفی مانند نظارت بر فرآیند تراکنش و اعطای مجوزهای دارایی های موجود به کاربران هر تراکنش که می تواند به صورت خودکار تکمیل و ثبت شود سناریوهایی هستند که در قسمت دوم تعریف قرارداد های هوشمند می گنجد. به بیان دیگر قرارداد هوشمند قطعه کدی است که متن قرارداد نوشته شده در یک کامپیوتر خاص را اجرا می کند. الگوریتم طرفین قرارداد بر اساس کد قرارداد امضاء و اجرا می شود [۶] . داده های موجود در قراردادهای هوشمند را نمی توان حذف کرد یا تغییر داد. هر رفتاری به طور دائم ثبت می شود. بنابراین، شفافیت و قابلیت ردیابی کل عملیات را می توان تضمین کرد و از تداخل مخرب مطمئن شد. برای مثال زمانی که شرایط تعیین شود، کد قرارداد به صورت خودکار اجرا می شود، که از فرآیند دستی جلوگیری می کند. تا زمانی که توسعه دهندگان این کار را انجام دهند، به طور دائم روی بلوک چین هستند. قراردادهای هوشمند برای تکمیل نقش اینترنت اشیاء نیز به کار گرفته می شوند [۲۵و۱۳] .

## سیستم سازی قراردادهای هوشمند

نیک سابو این مفهوم را در سال ۱۹۹۴ معرفی کرد؛ قرارداد هوشمند به عنوان یک پروتکل تراکنش کامپیوتری است و مفاد قرارداد را هم از این طریق اجرا می کند. و آن ها را به صورت دارایی در سخت افزار و نرم افزار جای گذاری می کند که می تواند آن ها را به صورت خودکار اعمال کند؛ به طوریکه نیازبه واسطه های مورد اعتماد بین طرف های معامله را به حداقل می رساند. این اطلاعات همانند رویه ذخیره شده روی سیستم های مدیریت پایگاه داده روی بلاک چین ذخیره می شوند و در یک زنجیره قرار می گیرند و هر یک آدرس منحصر به فرد خود را دارند برای مثال یک قرارداد هوشمند با آدرس دادن یک تراکنش راه اندازی می شود سپس به طور خودکار به روش تعیین شده در هر گره در شبکه، با توجه به داده هایی که در راه اندازی شده گنجانده می شود. قراردادهای هوشمند به ما این امکان را می دهند که محاسبات با هدف کلی در زنجیره انجام شود. با این حال، جایی که آنها برتری دارند. در ادامه، فرآیند قراردادهای هوشمند را به دو مرحله تقسیم میکنیم و آنها را مورد بررسی قرار می دهیم:

### ساخت و ساز

طرح های مربوط به ساخت و ساز بر طراحی تمرکز دارند. پارادایم ها و چارچوب های کمکی در معماری فعلی، برای تسهیل توسعه ایمن و انعطاف پذیر هستند. بلوک‌های سازنده مهم و امیدوارکننده ای برای ارتباط داده‌های قابل اعتماد وجود دارند، زیرا تبادل اطلاعات و ارزش را در یک راه قابل تایید با توجه به الزامات خواسته شده درقراردادهای هوشمند، به طور کارآمد و ایمن و برای حفظ حریم خصوصی برای رسیدن به عملکرد مطلوب طراحی می کند. شکل‌های قراردادهای هوشمند بسته به فرم‌هایی که روی آن اجرا می‌شوند، متفاوت است. بنابراین، طراحی قراردادهای هوشمند نیز به پلتفرم ها، به ویژه زبانی که پشتیبانی می کنند، متکی می باشد. قراردادهای هوشمند نوشته شده در اسکریپت بیشتر برای توصیف تراکنش های مالی استفاده می شود، در حالی که قراردادهای هوشمند نوشته شده در زبان های تورینگ کامل می تواند به لحاظ نظری

هر پروتکل قطعی را به عنوان یک برنامه کامپیوتری توصیف کند. پلتفرم های بلاک چین موجود را به دو دسته تقسیم می شود؛ بلاک چین مبتنی بر اسکریپت که توسط بیت کوین ارائه می شود و بلاک چین های کامل تورینگ که توسط اتریوم ارائه می شوند.

اولی فقط از عبارات محدودی از عملیات پشتیبانی می کند (به خصوص بدون حلقه)، و دومی از توابع دلخواه پشتیبانی می کند

با زبان های برنامه نویسی کامل تورینگ؛ از آنجایی که قراردادهای هوشمند در این دو نوع پلتفرم وجود دارد تفاوت های قابل توجه در شکل و مکانیسم اجرا وجود دارد و طرح های ساخت و ساز نیز کاملا متفاوت است. بنابراین، ما طرح های ساخت قرارداد هوشمند را به طور جداگانه مورد بحث قرار دهید. در فرآیند توسعه قراردادهای هوشمند برخی از ابزارها به توسعه دهندگان کمک می کنند تا امنیت قراردادها را تأیید کنند تا از ضررهای اقتصادی جلوگیری شود که ناشی از آسیب پذیری ها یا اشکالات احتمالی است.

### اجرای قراردادهای هوشمند

طرح‌های مرتبط با اجرا شامل استراتژی‌های پیاده‌سازی قراردادهای هوشمند یا اصلاحات زیربنایی هستند. زبان های برنامه نویسی، دو نوع پلتفرم قرارداد هوشمند که در بالا ذکر شد نیز در این مرحله متفاوت

است [۲۶] . پروتکل های رمزنگاری یا سخت افزار مفید برای محافظت از حریم خصوصی کاربر در هنگام اجرای قراردادهای هوشمند به کار گرفته می شود. نیازی به ابزار اضافی یا اصلاحات سازو کارزیرین نیست. ایده اصلی آنها این است که اجرا را به خارج از زنجیره منتقل کنند و فقط از بلاک چین برای تسویه وضعیت نهایی استفاده کنند. چارچوب اساسی یک قرارداد هوشمند عمدتاً شامل پنج لایه است: ۱) لایه داده. ۲) لایه حمل و نقل؛ ۳) لایه قرارداد؛ ۴) لایه اجرا. و ۵) لایه کاربردی.

لایه داده شامل روی زنجیره و خارج از زنجیره است، داده ها، که منابع داده لازم برای اجرای قرارداد هوشمند هستند. کد قرارداد اصلی یا روی زنجیره یا خارج از آن ذخیره می شود. کد و داده های برنامه را به زنجیره بلوکی وارد می شود و سپس آنها را روی زنجیره اجرا می کند. با این حال، از آنجایی که همه چیز در زنجیره است برای همه شفاف است، مسائل امنیتی و حریم خصوصی نیاز دارند روی بلاک چین و بر روی قرارداد اصلی از طریق یک سیستم فایل یا پلت فرم داده قابل اعتماد با استفاده از شاخص هش ذخیره شوند.این امر، فشار قابل مشاهده و مقیاس پذیری را کاهش می دهد. لایه انتقال پروتکل‌های ارتباطی و مکانیسم‌های ارتباطی برای پشتیبانی از انتقال داده‌های زنجیره به زنجیره و زنجیره به خارج از زنجیره را در بر می‌گیرد. لایه قرارداد حاوی پارامترهایی برای عملکردهای خاص (مانند مدیریت قرارداد، مدیریت کاربر و مدیریت داده) و منطق تجاری به عنوان قوانین اجرا، و کد منطق برنامه و محتوای قانونی نوشته شده در زبان های برنامه نویسی استاندارد در این لایه است. لایه اجرا به زمان اجرا اشاره دارد، محیط قراردادهای هوشمند، از جمله ماشین های مجازی و داکر که جعبه‌های ماسه‌ای را برای اجرای کد قرارداد و جداسازی و محدود کردن منابع فراهم می‌کنند. اجرای واقعی یک قرارداد هوشمند متفاوت است در پلتفرم های مختلف بلاک چین در میان این همه پلتفرم، اتریوم پیشگام در پیاده سازی ایده قرارداد هوشمند به صورت عملی است و سپس به پرکاربردترین تبدیل می شود [۱۳] .

## مدیریت اطلاعات و امنیت در قراردادهای هوشمند

قراردادهای هوشمند و فناوری بلاک چین می توانند و مدیریت اطلاعات را از بسیاری جهات بهبود بخشند وتسهیل کنند. کنترل دسترسی، اصلاح متغیرهای قرارداد هوشمند و اجرای روش های آن محدود به برخی از کاربران مجاز (بلاک چین) است که می توان به راحتی آن را انجام داد. علاوه بر این، قراردادهای هوشمند می توانند برای احراز هویت یک کاربر استفاده شوند [۱۹] . هیچ آسیب پذیری شناخته شده ای در قراردادهای هوشمند وجود ندارد زیرا همانطور که گفته شد بر مبنای بلاک چین است و از هرگونه انکار و جعل و مخاطرات امثال آن پیشگیری می کند. بنابراین مشکلات رایج سیستم های اطلاعاتی امروزی در آن راه ندارد. از طریق تحلیل استاتیک و پویا و اجرای نمادین در قراردادهای هوشمند مدیریت اطلاعات و امنیت تأیید شده است [۹] . قراردادهای هوشمند از پروتکل ها و رابط های کاربری برای تسهیل تمام مراحل فرآیند قرارداد استفاده می کنند. برای اینکه آن را به طور گسترده با سلامت و کامل استفاده کنیم، هشت ویژگی اساسی زیر را تعریف می کنیم که قراردادهای هوشمند باید رعایت کنند: قانونی بودن، اثبات پذیری، سازگاری، سفارشی‌سازی، قابل مشاهده بودن، قابلیت تأیید، خوداجراپذیری و کنترل دسترسی. ویژگی های اصلی به شرح زیر است:

**قانونمندی:** کد مطابق با مقررات قانونی است. دارایی های کنترل شده مالکیت دارند، و آنها معتبر هستند.

**اثبات پذیری:** داده ها و سناریوهای فرآیند باید به طور ایمن ذخیره شوند و می توان از آنها استفاده کرد.

**سازگاری:** قراردادهای هوشمند باید با متن قانون موجود سازگار باشد. قبل از انتشار قرارداد هوشمند، باید توسط اشخاص حقوقی حرفه ای بررسی شود تا اطمینان حاصل شود که این قرارداد انجام می شود؛ با قوانین موجود مغایرت نداشته باشد.

**قابلیت سفارشی سازی:** قراردادهای هوشمند قابل تنظیم هستند. چندین قرارداد اساسی را می توان با یکدیگر ترکیب کرد

**قابلیت مشاهده:** قراردادهای هوشمند به رابط هایی برای مشاهده وضعیت قراردادها از جمله خود قرارداد، عملکرد آن و همه چیز درباره قرارداد مجهز هستند.

**قابلیت تأیید:** سوابق مربوط به قراردادهای هوشمند را می توان براساس این ویژگی تأیید کرد. منطق کار و صحت اجرای قراردادهای هوشمند قابل تایید است.

**خوداجراپذیری:** برای محافظت در برابر نقض و اشخاص ثالثی که این کار را نمی کنند به اجرا توسط افراد نیاز ندارد

متکی به اجرای قانون قراردادهای رمزنگاری کنترل توسط کلیدهای رمزنگاری که به آنها اموال را برای افرادی که بر اساس قرارداد حق مالکیت دارند اداره کنند، می باشد.

**کنترل دسترسی:** اطلاعات قراردادها مانند دانش، کنترل و عملکرد، باید فقط برای افراد مرتبط با قرارداد قابل دسترسی باشد. مگر زمانی که درگیری رخ دهد، این ویژگی های قرارداد در معرض اشخاص ثالث قرار خواهد گرفت [۱۴] .

با ادغام قراردادهای هوشمند و بلاک چین، قراردادهای تجاری از توسعه و طراحی منعطف تری برخوردار شده اند و چالش ها و مشکلات دنیای واقعی کمتر در آن ها مشاهده خواهد شد. قرارداد هوشمند یک برنامه رایانه‌ای است که دارای ویژگی‌های برتر خود تأیید، خود اجرا و مقاوم در برابر دستکاری است و پس از ایجاد مستقل عمل می شوند و نیازی به نظارت ندارند [۱۸و۷] .

اگر یک جستجوی وب، مرتبط با اینترنت اشیا انجام دهید، به سرعت متوجه استفاده بیش از حد از عبارت «هوشمند» خواهید شد. بنابراین، وقتی چیزی هوشمند است واقعاً به چه معناست و چه چیزی یک شی را هوشمند می کند؟به عنوان مثال، چگونه یک یخچال یا اجاق توستر که هوشمند در نظر گرفته نشده است؛ تبدیل به یک دستگاه

هوشمندشود! برای مثال توستر قدیمی شما بتواند به صورت مکانیکی رنگ نان تست شما را با استفاده از صفحه لمسی یا سوئیچ هایی که با آن به صورت الکترونیکی با شما ارتباط برقرار کند، کنترل کند. از آنجا که در حال حاضر یک توستر هوشمند است، این توانایی را دارد بعد از اینکه این دستگاه از طریق ادغام پردازش تعبیه شده هوشمند شد، در مرحله بعدی با ارتباط از راه دور با یک دستگاه هوشمند برای کمک به آسان‌تر کردن زندگی عمل کند. مزایای بهره گیری از چنین قراردادهای هوشمندی عبارتند از:

- سرعت به روز رسانی قرارداد ها
- ریسک کمتر به هنگام اجرا
- هزینه کمتر
- دقت و تمرکز بیشتر
- مدل های جدید تجاری یا عملیاتی
- واسطه های کمتر

اشکالات برنامه نویسی، پلت فرم، زبان برنامه نویسی و محیط اجرا، و تمرین کدنویسی از جمله چالش های اصلی توسعه قراردادهای هوشمند هستند و موضوعات فرعی همچون چالش های محرمانگی و چالش های قابلیت عملیات متقابل چالش های خاص توسعه قراردادهای هوشمند هستند [۱۶]. برای مثال در یک سناریو زمانی که یک خودرو وارد یک پارکینگ هوشمند می شود این امکان وجود دارد که توسط سنسور های بی سیم شغل فرد را شناسایی کند و جای پارک متناسب با فرد را به وی پیشنهاد یا اجبار کند و هنگام خروج از پارکینگ با توجه به اینکه خودرو در چند ساعت و در چه محلی پارک شده از حساب بانکی فرد هزینه پارکینگ کسر شود؛ در این مثال کاربردی یک قرارداد هوشمند از طریق اینترنت اشیاء در بستر بلاک چین بین صاحب پارکینگ و صاحب خوردو منعقد می شود که شامل اطلاعات پرداخت، نوع خودرو، شغل فرد، ساعات پارک ماشین و شرایط قرارداد از جمله به روز رسانی در مورد نرخ های پرداخت بر اساس زمان و روز می باشد[۴].

## نتیجه گیری

ترکیبی از بلاک چین و اینترنت اشیا می تواند بسیار قدرتمند باشد. بلاک چین ها به ما انعطاف پذیری می دهند، قراردادهای هوشمند به ما این امکان را می دهند که فرآیندهای پیچیده چند مرحله ای را خودکار کنیم. دستگاه های موجود در اکوسیستم اینترنت اشیا نقاط تماس با دنیای فیزیکی هستند؛ وقتی که همه آنها با هم ترکیب شوند می‌توانیم گردش‌های کاری وقت‌گیر جدید را خودکار کنیم. راه های منحصر به فردی برای دستیابی به قابلیت تایید رمزنگاری، و همچنین صرفه جویی قابل توجهی در هزینه و زمان در این فرآیند وجود دارد. ادغام مداوم بلاک چین ها در دامنه IoT باعث تحولات قابل توجهی در سراسر جهان شده است. چندین صنعتی، مدل های جدید کسب و کار را به ارمغان می آورد . قراردادهای هوشمند ابزار جدید و هیجان انگیزی هستند که چیزهای جدیدی خلق می کنند. پتانسیل های اینترنت اشیاء برای قراردادهای هوشمند دارای ویژگی های منحصر به فردی می باشد. ویژگی هایی که فرصت هایی را برای برنامه های کاربردی جدید و امن ایجاد می کند.

## تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

## منابع


[1] Hu B, Zhang Z, Liu J, Liu Y, Yin J, Lu R, Lin X. A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. Patterns. 2021 Feb 12;2(2).

[2] Mohanta BK, Panda SS, Jena D. An overview of smart contract and use cases in blockchain technology. In2018 9th international conference on computing, communication and networking technologies (ICCCNT) 2018 Jul 10 (pp. 1-4). IEEE.

[3] Profentzas C, Almgren M, Landsiedel O. Tinyevm: Off-chain smart contracts on low-power iot devices. In2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS) 2020 Nov 29 (pp. 507-518). IEEE.

[4] Chenhao Xu, Jiaqi Ge, Yong Li, Yao Deng, Longxiang Gao, A Smart-Contract Driven Edge Intelligence Framework for IoT Systems, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. XX, NO. X, JUNE 2023.

[5] Kouzinopoulos CS, Giannoutakis KM, Votis K, Tzovaras D, Collen A, Nijdam NA, Konstantas D, Spathoulas G, Pandey P, Katsikas S. Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust. In2018 Innovations in Intelligent Systems and Applications (INISTA) 2018 Jul 3 (pp. 1-6). IEEE.

[6] Negara ES, Hidayanto AN, Andryani R, Syaputra R. Survey of smart contract framework and its application. Information. 2021 Jun 22;12(7):257.

[7] Ramezan G. *Blockchain for decentralized trusted communication networks* (Doctoral dissertation, University of British Columbia).

[8Wickström J, Westerlund M, Pulkkis G. Smart contract based distributed IoT security: A protocol for autonomous device management. In2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid) 2021 May 10 (pp. 776-781). IEEE.

[9] Ali J, Ali T, Musa S, Zahrani A. Towards secure IoT communication with smart contracts in a blockchain infrastructure. arXiv preprint arXiv:2001.01837. 2020 Jan 6.

[10] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE access. 2016 May 10;4:2292-303.

[11] Karimi K, Atkinson G. What the Internet of Things (IoT) needs to become a reality. White Paper, FreeScale and ARM. 2013 Jun:1-6.

[12] Peng K, Li M, Huang H, Wang C, Wan S, Choo KK. Security challenges and opportunities for smart contracts in Internet of Things: A survey. IEEE Internet of Things Journal. 2021 Apr 20;8(15):12004-20.

[13] Giancaspro M. Is a 'smart contract'really a smart idea? Insights from a legal perspective. Computer law & security review. 2017 Dec 1;33(6):825-35.

[14] Kannengiesser N, Lins S, Sander C, Winter K, Frey H, Sunyaev A. Challenges and common solutions in smart contract development. IEEE Transactions on Software Engineering. 2021 Oct 1;48(11):4291-318.

[15] Fotiou N, Pittaras I, Siris VA, Voulgaris S, Polyzos GC. Secure IoT access at scale using blockchains and smart contracts. In2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) 2019 Jun 10 (pp. 1-6). IEEE.

[16] Fotiou N, Polyzos GC. Smart contracts for the internet of things: Opportunities and challenges. In2018 European conference on networks and communications (EuCNC) 2018 Jun 18 (pp. 256-260). IEEE.

[17] Fareghzadeh N, Seyyedi MA, Vatanian G. A Security Modeling Approach Using Web Service-Based Infrastructure In E-Government.

[18] Kumar SG, Murugan A, Muruganantham B, Sriman B. IoT–smart contracts in data trusted exchange supplied chain based on block chain. International Journal of Electrical and Computer Engineering. 2020 Feb 1;10(1):438.

[19] Sarmah SS. Understanding blockchain technology. Computer Science and Engineering. 2018 Aug;8(2):23-9.

[20] Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Applied Sciences. 2020 Jan 9;10(2):488.

[21] Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Applied Sciences. 2020 Jan 9;10(2):488.

[22] Huang Y, Bian Y, Li R, Zhao JL, Shi P. Smart contract security: A software lifecycle perspective. IEEE Access. 2019 Oct 14;7:150184-202.

[23] Zhang Y, Yutaka M, Sasabe M, Kasahara S. Attribute-based access control for smart cities: A smart-contract-driven framework. IEEE Internet of Things Journal. 2020 Oct 23;8(8):6372-84.

[24] Chen YH, Chen SH, Lin IC. Blockchain based smart contract for bidding system. In2018 IEEE International Conference on Applied System Invention (ICASI) 2018 Apr 13 (pp. 208-211). IEEE.

[25] Zheng Z, Xie S, Dai HN, Chen W, Chen X, Weng J, Imran M. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems. 2020 Apr 1;105:475-91.

[26] Zhongming Z, Linong L, Xiaona Y, Wangqiang Z, Wei L. State Key Laboratory of Software Development Environment, 2011.