

## امنیت تکنولوژی های متاورس و اینترنت اشیا براساس امنیت بلاکچین

زهرا لرزمانی

دانشجو رشته ارشد فناوری اطلاعات موسسه آموزش عالی مارلیک

[zahra.zamani1234@gmail.com](mailto:zahra.zamani1234@gmail.com)

مهدی علیرضانژاد

هیئت علمی دانشگاه

[me.alirezanejad@gmail.com](mailto:me.alirezanejad@gmail.com)

### چکیده

فناوری بلاک چین به طور فزاینده ای برای نسل بعدی جذاب می شود، زیرا به طور منحصر به فردی برای عصر اطلاعات مناسب است. فناوری بلاک چین همچنین می تواند در اینترنت اشیا (IoT) اعمال شود. بلاکچین روشی انعطاف پذیر و بدون نیاز به اعتماد برای مدیریت مجوز ارائه می دهد. پیشرفت فناوری اینترنت اشیا در حوزه های مختلف منجر به پیشرفت قابل توجهی در سیستم های توزیع شده شده است. مفهوم بلاک چین به یک سیستم مدیریت داده غیرمتمرکز برای ذخیره و به اشتراک گذاری داده ها و تراکنش ها در شبکه نیاز دارد. برای درک بهتر نقش بلاکچین در متاورس، هدف ما ارائه یک بررسی گسترده در مورد کاربردهای بلاکچین برای متاورس است. ابتدا مقدماتی در مورد بلاکچین و متاورس ارائه می دهیم و انگیزه های استفاده از بلاکچین برای متاورس را برجسته می کنیم. در ادامه، روش های مبتنی بر بلاکچین برای متاورس را از دیدگاه های فنی، مانند اکتساب داده ها، ذخیره سازی داده ها، اشتراک گذاری داده ها، قابلیت همکاری داده ها و حفظ حریم خصوصی داده ها، به طور گسترده مورد بحث قرار می دهیم. این مقاله به بررسی مفهوم بلاک چین و عوامل مرتبط می پردازد که تجزیه و تحلیل دقیقی از حملات امنیتی بالقوه ارائه می دهد و راه حل های موجود را که می توانند به عنوان اقدامات متقابل در برابر چنین حملاتی به کار گرفته شوند، ارائه می دهد.

**واژگان کلیدی:** کوانتوم، بلاک چین، متاورس، اینترنت اشیا، امنیت

### مقدمه

فناوری بلاکچین، یک فناوری دفتر کل دیجیتال توزیع شده که می تواند برای حفظ ایمن فهرست های رو به رشد و مداوم سوابق داده ها و تراکنش ها مورد استفاده قرار گیرد، اخیراً جهان را به شدت تحت تأثیر قرار داده است. سه معیار اصلی مربوط به هویت و دسترسی بلاکچین عبارتند از عمومی یا کمتر مجاز، خصوصی یا مجاز و کنسرسیوم. مهمترین و منحصر به فردترین عامل مفهوم بلاکچین این است که اطلاعات ذخیره شده کاملاً در بلوک های تراکنش های بلاکچین ایمن هستند. مدل اجماع غیرمتمرکز آن دارای سه ویژگی اصلی سازگاری، زنده بودن و تحمل خطا است. فناوری بلاکچین در حال بازتعریف مدل سازی داده ها است و دولت ها بلاکچین را در بسیاری از کاربردهای اینترنت اشیا پیاده سازی کرده اند. این فناوری عمدتاً به دلیل توانایی بی سابقه اش در تطبیق و همچنین بخش بندی، محافظت و اشتراک گذاری داده ها و خدمات اینترنت اشیا، برای چنین کاربردهایی جذاب است. فناوری بلاکچین در مرکز بسیاری از تحولات فعلی در صنعت اینترنت اشیا قرار

دارد. یکی از دلایل این امر این است که بسیاری از خدمات اینترنت اشیا در برابر حملات و چالش‌ها آسیب‌پذیر هستند. استفاده از فناوری بلاکچین می‌تواند بسیاری از مشکلات سیستم‌های سایبری-فیزیکی در بخش اینترنت اشیا را حل کند. (s.singh, 2021)

متاورس به یک فضای مشترک مجازی جمعی اشاره دارد که شامل واقعیت افزوده (AR)، واقعیت مجازی (VR) و سایر محیط‌های دیجیتال است که در آن کاربران می‌توانند با یکدیگر و دارایی‌های دیجیتال تعامل داشته باشند. متاورس ترکیبی از فناوری، خلاقیت، تجربیات و تعامل انسانی است که به طور یکپارچه افراد، اشیاء و فضاها را ادغام می‌کند. (Yousafzai, A., 2025)

متاورس مرحله بعدی تکامل دیجیتال است که می‌تواند پذیرش دیجیتال را به سطح شگفت‌انگیزی متحول کند و دامنه خدمات را فراتر از سیستم‌های استاندارد با دسترسی آنلاین گسترش دهد. دیجیتالی شدن خدمات به روندی برای بهبود کارایی در حوزه‌های کسب و کار تبدیل شده است. (Gadekallu, T. R., 2022)

این مقاله برخی از راه‌حل‌های موجود و کاربردهای بلاکچین برای عوامل مختلفی که می‌توانند بر سیستم بلاکچین تأثیر بگذارند، ارائه می‌دهد. فناوری بلاکچین به دلیل ویژگی‌های تمرکززدایی، پایداری، ناشناس بودن و حساسیتی، توجه صنعتی و دانشگاهی قابل توجهی را به خود جلب کرده است. در این بررسی، پیاده‌سازی فناوری بلاکچین را در طیف وسیعی از کاربردها بررسی می‌کنیم و تعدادی از چالش‌های مربوطه را مورد بحث قرار می‌دهیم. (s.singh, 2021)

## مفاهیم بلاکچین

مفهوم بلاکچین از یک مقاله سفید نوشته شده توسط ناکاموتو ساتوشی در سال ۲۰۰۸ سرچشمه می‌گیرد. بلاکچین، که دفتر کل توزیع شده نیز نامیده می‌شود، دارای بلوک‌های متوالی است که از طریق مقدار هش هدر بلوک قبلی به یکدیگر مرتبط هستند. به غیر از هش رمزنگاری اجتناب‌ناپذیر، مهر زمانی، نانس و داده‌های تراکنش نیز در یک بلوک گنجانده شده‌اند. مهر زمانی بلوک تنها در صورتی معتبر تلقی می‌شود که مقدار آن بیشتر از زمان تنظیم‌شده توسط شبکه به علاوه دو ساعت و بیشتر از میانگین مهر زمانی یازده بلوک قبلی باشد، که از دستکاری احتمالی بلاکچین توسط دشمن جلوگیری می‌کند. توجه داشته باشید که زمان تنظیم‌شده توسط شبکه به میانگین مهرهای زمانی از کل گره‌های متصل اشاره دارد. اجرای روان بلاکچین فقط توسط یک یا چند گره حفظ نمی‌شود، بلکه هر گره در شبکه بلاکچین باید از یک پروتکل اجماع مشترک برای تولید و اعتبارسنجی بلوک‌های جدید پیروی کند.

پروتکل اجماع ستون فقرات بلاکچین است که در آن اصول عملیاتی و اقدامات مشروع همگی تنظیم شده‌اند. بیت‌کوین معروف از مکانیزم اثبات کار (PoW) استفاده می‌کند که از ماینرها برای یافتن پاسخ مسئله ریاضی تصادفی، قدرت محاسباتی زیادی را به کار گیرند. به منظور جلوگیری از تمرکز قدرت محاسباتی، سختی که به آن نانس (nonce) تولید بلوک بعدی نیز می‌گویند، به صورت پویا بر اساس ۱۰ دقیقه برای هر بلوک تغییر می‌کند. اگرچه قدرت محاسباتی غیرقابل تصور، مانع از کار اکثر مهاجمان می‌شود، اما اثبات کار همچنان منجر به نرخ تراکنش ناکارآمد و مصرف انرژی بیش از حد می‌شود. اثبات سهام (PoS)



<https://icaics.ir>  
[info@icaics.ir](mailto:info@icaics.ir)

# اولین کنفرانس بین‌المللی هوش مصنوعی و علوم کامپیوتری نو ظهور: از الگوریتم تا آینده‌نگری

## First International Conference on Artificial Intelligence and Emerging Computer Science: From Algorithm to Foresight

March 17, 2026-GEORGIA

۲۶ اسفند ماه ۱۴۰۴ - گرجستان

مشکلات ناشی از اثبات کار را کاهش می‌دهد، بنابراین ماینری که برنده نهایی می‌شود، به مقدار دارایی‌های خود در ارز دیجیتال مربوطه بستگی دارد تا قدرت محاسباتی. سیستم فایل بین سیاره‌ای (IPFS) که اخیراً در حال ظهور است، اجماع اثبات فضا (PoSpace) را منتشر می‌کند که مستلزم آن است که شرکت‌کنندگان مقداری فضای ذخیره‌سازی برای اثبات چالشی که توسط ارائه‌دهنده خدمات ارسال شده است، ارائه دهند. داده‌های تراکنش به شکل درخت مرکب برای هر بلوک سازماندهی می‌شوند که کارایی تأیید را بهبود می‌بخشد (Gadekallu, T. R., 2022)

### مفاهیم متاورس

#### متاورس چیست؟

کلمه "متا" از زبان یونانی گرفته شده است که پیشوندی به معنای "جامع‌تر" یا "فرا تر" است. کلمه "Verse" نسخه مختصر شده universe است که نشان دهنده یک ظرف فضا/زمان است.

وقتی این دو کلمه با هم ترکیب می‌شوند، کلمه کاملاً جدیدی به نام «Metaverse» وارد تصویر می‌شود، جایی که سیستم‌های اجتماعی سنتی به یک فضای زندگی دیجیتال جدید تبدیل می‌شوند. فناوری‌های پیشرفته‌ای مانند واقعیت مجازی (VR)، دوقلوی دیجیتال، بلاکچین و غیره برای ساخت متاورس استفاده می‌شوند که همه چیز را در دنیای واقعی ما به یک جهان موازی نگاشت می‌کند. به عنوان مثال، کاربران می‌توانند از هر مکانی در متاورس با دوستان خود کار کنند، زندگی کنند و بازی کنند. در سال ۱۹۹۲، نیل استفنسون، در رمان علمی تخیلی معروف خود به نام «Snow Crash»، ابتدا مفهوم اولیه متاورس را پیشنهاد کرد، جایی که افراد از آواتارهای دیجیتال برای کنترل و رقابت با یکدیگر برای ارتقاء وضعیت خود استفاده می‌کنند. با این حال، تاکنون، متاورس در مرحله مفهومی خود است. استانداردهای مشترکی وجود دارد و پیاده‌سازی‌های واقعی بسیار کمی در دسترس است. (Gadekallu, T. R., 2022)

### نقش بلاکچین در متاورس

وقتی صحبت از متاورس می‌شود، ممکن است تصور انواع تجربیات خیره‌کننده یا بازی‌های سرگرم‌کننده در ذهن ما شکل بگیرد. با این حال، سناریویی که به ما نزدیک است، فقط یک دنیای موازی است که در آن بوم‌شناسی اقتصادی اجتناب‌ناپذیر است. علاوه بر این، دارایی‌های دیجیتال، عملکردهای اصلی ارائه شده توسط بلاکچین هستند، مانند توکن‌های همگن مبتنی بر ERC-20 و توکن‌های غیر همگن مبتنی بر ERC-721 یا ERC-1155. از آنجایی که فناوری بلاکچین می‌تواند عملکرد اقتصادی روان متاورس را حفظ کند، فناوری بلاکچین روح متاورس است. (Gadekallu, T. R., 2022)

## انگیزه ادغام بلاکچین در متاورس

- **تضمین حریم خصوصی و امنیت داده‌ها:** متاورس حجم وسیعی از اطلاعات حساس را جمع‌آوری می‌کند تا بهترین تجربیات ممکن را در اختیار کاربر قرار دهد. سازمان‌ها یا برنامه‌ها برای توسعه موفقیت‌آمیز سیستم‌های هدف‌گیری به این داده‌ها نیاز دارند. اگر اطلاعات به دست افراد نادرست بیفتد، ممکن است کاربران را در دنیای واقعی نیز هدف قرار دهند. بلاکچین، با مکانیزم‌های احراز هویت، کنترل دسترسی و اجماع خود، کنترل کامل داده‌های کاربران را در اختیار آنها قرار می‌دهد و از این طریق حریم خصوصی داده‌های کاربران را تضمین می‌کند. بلاکچین از رمزگذاری کلید نامتقارن و توابع هش استفاده می‌کند که امنیت داده‌ها را در متاورس تضمین می‌کند.
- **تضمین کیفیت داده‌ها:** متاورس داده‌ها را از برنامه‌های مختلف از مراقبت‌های بهداشتی گرفته تا سرگرمی دریافت می‌کند. مدل‌های هوش مصنوعی در متاورس برای تصمیم‌گیری‌های کلیدی برای ذینفعان خود به این داده‌ها متکی هستند. ایجاد اشیاء در متاورس به شدت به کیفیت داده‌های به اشتراک گذاشته شده توسط کاربران از دنیای واقعی وابسته است. بلاکچین، مسیرهای حسابرسی کاملی از تراکنش‌ها را ارائه می‌دهد و به افراد و سازمان‌ها اجازه می‌دهد تا تمام تراکنش‌ها را اعتبارسنجی کنند. این امر کیفیت داده‌ها را در متاورس افزایش می‌دهد.
- **فعال کردن اشتراک‌گذاری یکپارچه و امن داده‌ها:** متاورس به دستگاه‌های AR و VR وابسته است و در نتیجه دنیایی متصل‌تر و فراگیرتر ایجاد می‌کند. مزیت واقعی متاورس در ادغام آن با AR در اشیاء دیجیتال و فیزیکی نهفته است. موفقیت متاورس به اشتراک‌گذاری یکپارچه داده‌های AR و VR بستگی دارد که امکان توسعه برنامه‌های جدید و پیشرفته‌ای را فراهم می‌کند که به حل مشکلات دنیای واقعی کمک می‌کنند. سیستم اطلاعات رمزگذاری پیشرفته بلاکچین، امکان اشتراک‌گذاری یکپارچه و ایمن داده‌های متاورس را فراهم می‌کند.
- **فعال‌سازی قابلیت همکاری داده‌ها:** در متاورس، ذینفعان باید به دارایی‌ها در جهان‌های مجازی مختلف دسترسی داشته باشند و آنها را نگهداری کنند و از برنامه‌های متنوعی استفاده کنند. قابلیت همکاری داده‌ها در این جهان‌های مجازی به دلیل محیط‌های مختلفی که در آنها ساخته شده‌اند، محدود است. با استفاده از یک پروتکل بین زنجیره‌ای، می‌توان داده‌ها را در دو یا چند بلاکچین واقع در جهان‌های مجازی مجزا تبادل کرد. کاربران به دلیل قابلیت همکاری بلاکچین می‌توانند راحت‌تر بین این جهان‌های مجازی مهاجرت کنند.
- **تضمین یکپارچگی داده‌ها:** داده‌های متاورس باید به طور مداوم و دقیق نگهداری شوند. در صورت به خطر افتادن یکپارچگی داده‌ها، ذینفعان ممکن است اعتماد خود را به متاورس از دست بدهند. داده‌های متاورس به عنوان یک کپی در هر بلوک در سراسر زنجیره ذخیره می‌شوند که به دلیل تغییرناپذیری ارائه شده توسط بلاکچین، بدون رضایت اکثر شرکت‌کنندگان قابل اصلاح یا حذف نیست. این مکانیسم بلاکچین، یکپارچگی داده‌های متاورس را تضمین می‌کند.

برخی از موارد استفاده از بلاکچین در متاورس در زیر مورد بحث قرار گرفته است:



- **سیستم مالی:** ضد دستکاری، باز بودن، شفافیت و غیرمتمرکز بودن چهار ویژگی مهم در بلاکچین هستند. در متاورس، میلیون‌ها تراکنش برای تبادل کالا در مدت زمان کوتاهی انجام می‌شود، بنابراین امنیت و کارایی این تراکنش‌ها باید تضمین شود. بر اساس ویژگی‌های ذکر شده، بلاکچین کاندیدای خوبی برای ساخت سیستم اقتصادی در مقیاس بزرگ و مقیاس‌پذیر در دنیای مجازی است.
- **استقرار قرارداد هوشمند:** ماهیت ذاتی شبکه بلاکچین به قراردادهای هوشمند اجازه می‌دهد تا خودکار، قابل برنامه‌ریزی، باز، شفاف و قابل تأیید باشند، در کنار سایر ویژگی‌های قابل توجه، تعاملات قابل اعتماد درون زنجیره‌ای را بدون نیاز به پلتفرم تأیید شخص ثالث امکان‌پذیر می‌سازد. اگر سیستم مالی در متاورس بر روی بلاکچین ساخته شود، می‌توان از ویژگی‌های قراردادهای هوشمند برای غیرمتمرکز کردن عملکرد قراردادها به روشی برنامه‌ریزی‌شده، غیرمتمولی، قابل تأیید، قابل ردیابی و قابل اعتماد استفاده کرد و در نتیجه رفتارهای مضر مانند رانت‌جویی، فساد و عملیات مخفیانه که ممکن است در سیستم مالی وجود داشته باشد را به میزان قابل توجهی کاهش داد و می‌توان از آن به طور گسترده در بخش‌های مالی، اجتماعی و بازی استفاده کرد.
- **NFT:** مهم‌ترین ویژگی NFT، تفکیک‌پذیری و منحصربه‌فرد بودن آن است که آن را برای نمایش هویت مناسب می‌کند، برای مثال، دارایی‌هایی که انحصاری و تفکیک‌ناپذیر هستند و می‌توانند آزادانه معامله و منتقل شوند. در متاورس، این دارایی‌های مجازی با گواهی‌هایی به نام NFT ارائه می‌شوند که نشان‌دهنده مالکیت هستند. (Gadekallu, T. R., 2022)

### مفاهیم کلیدی IoT برای امنیت داده‌ها

محققان از دیدگاه‌های مختلف، تفاسیر متعددی از اینترنت اشیا ارائه می‌دهند. برخی بر اشیاء فیزیکی متصل به شبکه‌ها تمرکز دارند، برخی دیگر بر فناوری شبکه و پروتکل‌ها، در حالی که برخی بر عناصر معنایی، از جمله ذخیره‌سازی داده‌ها، اطلاعات و جستجو، تأکید دارند. کمیسیون اروپا اینترنت اشیا را به عنوان ادغام دامنه‌های فیزیکی و مجازی برای ایجاد محیط‌های هوشمند تعریف می‌کند. به طور کلی، اینترنت اشیا به شبکه‌ای از دستگاه‌های هوشمند متصل به اینترنت اشاره دارد که قادر به شناسایی و تعامل با یکدیگر با انتقال و جمع‌آوری داده‌ها در سراسر شبکه هستند. این تعامل، ارتباطات و تعاملات بین افراد، فرآیندها و اشیاء را در هر زمان، هر مکان، در هر شبکه و با هر سرویسی تسهیل می‌کند. (s.singh, 2021)

از نظر فنی، دستگاه‌هایی که دارای حسگرها و تراشه‌ها هستند، از جمله برچسب‌های NFC و RFID، از طریق آدرس‌های پروتکل اینترنت (IP) و پروتکل‌های ارتباطی مانند MQTT با یکدیگر ارتباط برقرار می‌کنند و لزوم مداخله انسان را از بین می‌برند. هنگامی که این دستگاه‌ها به اینترنت متصل می‌شوند، داده‌ها را به راه‌حل‌های محاسباتی مانند سیستم‌های ابری منتقل می‌کنند که داده‌ها را با هم ادغام می‌کنند. ذخیره‌سازی، ابزارهای تحلیلی و مدل‌های تحویل برای ارائه خدمات به افراد و سازمان‌ها. پس از رسیدن به ابر، داده‌ها با استفاده از نرم‌افزار مناسب پردازش می‌شوند و در نتیجه به ایجاد یک محیط هوشمند کمک می‌کنند. این

شامل تصمیم‌گیری آگاهانه، پیش‌بینی مشکلات بالقوه، صرفه‌جویی در زمان و هزینه و ایجاد ادراک، شبکه و پردازش هوشمند به عنوان اجزای حیاتی اینترنت اشیا است. (s.singh, 2021)

### بلاکچین برای حریم خصوصی و امنیت

تراکنش‌های بلاکچین در بخش مالی معمولاً بسیار ایمن هستند و توسط کمیسیون مرکزی (در بلاکچین‌های خصوصی) یا کنسرسیوم ذینفعان نظارتی (در بلاکچین‌های اجماعی) تأیید می‌شوند. در حوزه مراقبت‌های بهداشتی، داده‌های پزشکی بیماران که در پایگاه‌های داده مرکزی ذخیره می‌شوند، می‌توانند در معرض نشت اطلاعات باشند، در حالی که معماری بلاکچین به بیماران اختیار کامل در مورد داده‌هایشان می‌دهد. در ذخیره‌سازی ابری، کاملاً واضح است که داده‌ها مجاز نیستند و این باعث آسیب‌پذیری می‌شود. داده‌ها همچنین توسط مقامات مرکزی مدیریت و دسترسی می‌شوند و یک مرجع نظارتی سرکش می‌تواند خسارات زیادی از جمله نشت داده‌ها به اشخاص غیرمجاز ایجاد کند. در مقابل، در بلاکچین‌ها، داده‌ها در شبکه‌های نظیر به نظیر ذخیره می‌شوند و کاربران اختیار کامل در مورد داده‌های خود دارند، بنابراین امنیت و حریم خصوصی کامل داده‌ها را تضمین می‌کنند.

سیستم پیشنهادی همچنین اهداف امنیتی محافظت از ارتباطات، مقیاس‌پذیری، تضمین کارایی سیستم‌ها و محافظت در برابر انواع حملات را برآورده می‌کند. معماری پیشنهادی، فناوری بلاکچین و محاسبات ابری را در یک راه‌حل جامع گنجانده است. مدل پیشنهادی ما از تکنیک تحلیل همبستگی چند متغیره (MCA) برای تجزیه و تحلیل ترافیک شبکه و شناسایی همبستگی بین ویژگی‌های ترافیک برای تضمین امنیت شبکه‌های محلی خانه هوشمند استفاده می‌کند. الگوریتم تشخیص ناهنجاری برای تشخیص و کاهش حملات DoS/DDoS ارائه شده است. (s.singh, 2021)

### عناصر بلاکچین و نگرانی‌های مرتبط

#### ۱) تمرکززدایی

در فناوری بلاکچین، تمرکززدایی مستلزم پراکندگی توابع در سراسر یک سیستم است، نه اینکه همه واحدها به یک مرجع مرکزی متصل و توسط آن کنترل شوند. به عبارت دیگر، هیچ نقطه کنترل مرکزی وجود ندارد و این عدم وجود مرجع متمرکز در بلاکچین، آن را نسبت به سایر فناوری‌ها ایمن‌تر می‌کند. به هر کاربر بلاکچین، که ماینر نامیده می‌شود، یک حساب تراکنش منحصر به فرد اختصاص داده می‌شود و پس از تأیید ماینر، بلوک‌ها اضافه می‌شوند. ماهیت غیرمتمرکز سوابق داده مورد استفاده در فناوری بلاکچین، کیفیت انقلابی آن را نشان می‌دهد؛ شبکه‌های بلاکچین از پروتکل‌های اجماع برای ایمن‌سازی گره‌ها استفاده می‌کنند. به این ترتیب، تراکنش‌ها تأیید می‌شوند و داده‌ها نمی‌توانند از بین بروند. در حالی که ماهیت غیرمتمرکز شبکه‌ها امکان عملیات نظیر به نظیر را فراهم می‌کند، چالش‌های عمده‌ای را نیز برای حریم خصوصی داده‌های شخصی ایجاد می‌کند. گای و همکاران برخی از این مسائل امنیتی و حریم خصوصی را بررسی کردند که شامل تهدیدها، دشمنان مخرب و حملات در صنایع

مالی می‌شود. زیسکیند و همکاران مدیریت داده‌های شخصی غیرمتمرکز را در زمینه نگرانی‌های مربوط به حریم خصوصی داده‌های شخصی بررسی کردند. (s.singh, 2021)

## ۲) مدل اجماع

اجماع به توافق بین نهادها اشاره دارد و مدل‌های اجماع به شبکه‌های غیرمتمرکز کمک می‌کنند تا تصمیمات متفق‌القول بگیرند. این امر امکان ردیابی همه سوابق از یک مرجع واحد را فراهم می‌کند. فناوری بلاکچین به الگوریتم‌های اجماع نیاز دارد تا اطمینان حاصل شود که هر بلوک بعدی تنها نسخه واقعی است. یعنی الگوریتم‌ها تضمین می‌کنند که همه گره‌ها موافق باشند که هر بلوک جدید اضافه شده به بلاکچین، پیام یکسانی را حمل می‌کند. مدل‌های اجماع، در برابر حملات فوروک تضمین می‌کنند و حتی می‌توانند در برابر حملات مخرب محافظت کنند. سه ویژگی اصلی مدل‌های اجماع به شرح زیر است:

- سازگاری - این پروتکل زمانی ایمن و سازگار است که همه گره‌ها خروجی یکسانی تولید کنند.
- زنده بودن - پروتکل اجماع، زنده بودن را در صورتی که همه گره‌های شرکت‌کننده نتیجه‌ای تولید کرده باشند، تضمین می‌کند.
- تحمل خطا - این مکانیسم، تحمل خطا را برای بازیابی از گره‌های خراب ارائه می‌دهد. (s.singh, 2021)

## ۳) شفافیت و حریم خصوصی

جذاب‌ترین جنبه فناوری بلاکچین، میزان حریم خصوصی ارائه شده توسط آن است، اما این می‌تواند در مورد شفافیت، سردرگمی ایجاد کند. شبکه‌های بلاکچین به صورت دوره‌ای (یعنی هر ۱۰ دقیقه) اکوسیستم‌های ارزش دیجیتال را که تراکنش‌ها را هماهنگ می‌کنند، خودارزیابی می‌کنند. یک مجموعه از این تراکنش‌ها، بلوک نامیده می‌شود و این فرآیند منجر به دو ویژگی می‌شود: شفافیت و عدم امکان فساد. در یک بلاکچین، هویت کاربر پشت یک رمز قوی پنهان است و این امر پیوند دادن آدرس‌های عمومی به کاربران شخصی را به ویژه دشوار می‌کند. بنابراین این سوال مطرح می‌شود که چگونه می‌توان بلاکچین را واقعاً شفاف دانست. (s.singh, 2021)

بلاکچین در حال حاضر به عنوان یک فناوری قدرتمند در نظر گرفته می‌شود. این فناوری تعاملات را به گونه‌ای سازماندهی می‌کند که قابلیت اطمینان را تا حد زیادی بهبود می‌بخشد و در عین حال خطرات تجاری و سیاسی مرتبط با مدیریت فرآیندها از طریق نهادهای مرکزی را نیز از بین می‌برد و در نتیجه نیاز به اعتماد را کاهش می‌دهد. شبکه‌های بلاکچین پلتفرم‌هایی ایجاد می‌کنند که می‌توانند همزمان برنامه‌های مختلف را از شرکت‌های مختلف اجرا کنند و گفتگوی یکپارچه و کارآمد و ایجاد مسیرهای حسابرسی را امکان‌پذیر سازند که از طریق آن همه می‌توانند تأیید کنند که همه چیز به درستی پردازش می‌شود. (s.singh, 2021)

## ۴) هویت و دسترسی

بلاکچین یک فناوری دفتر کل توزیع شده امن (DLT) است که در سال‌های اخیر نقش جدیدی را ایفا کرده است. در مورد وضعیت فناوری بلاکچین، برنامه‌ها و راه‌حل‌های مربوط به مدیریت هویت ارائه شده است. ارتقای هویت و کنترل دسترسی به سطح بعدی و بررسی اینکه آیا استفاده از فناوری بلاکچین، مدیریت شناسه دستگاه را بهبود می‌بخشد یا خیر، یکی از پروژه‌های امنیتی اولویت‌دار Sentara Healthcare است و ویرجینیا و کارولینای شمالی از طریق یک سیستم توزیع یکپارچه به هم متصل هستند. به گفته جرمی کرک، متخصص صنعت، در حال حاضر شش پروژه در حال انجام وجود دارد که به چگونگی آسان‌تر شدن مدیریت هویت توسط بلاکچین می‌پردازند. (s.singh, 2021)

سه معیار اصلی مربوط به هویت و دسترسی بلاکچین عبارتند از عمومی یا کمتر مجاز، خصوصی یا مجاز و کنسرسیوم. پیلکینگتون تمایز اصلی بین فناوری‌های بلاکچین عمومی و خصوصی را ارائه داد و مبنای و ماهیت تحول‌آفرین فناوری بلاکچین را مورد بحث قرار داد. بلاکچین‌های عمومی کاملاً باز هستند و به هر کسی اجازه می‌دهند به شبکه بپیوندند. آنها به گونه‌ای طراحی شده‌اند که واسطه‌ها را کاهش دهند تا شرکت‌کنندگان بیشتری بتوانند به آن بپیوندند. در مقابل، بلاکچین‌های خصوصی امتیازات شبکه را محدود می‌کنند. شرکت‌کنندگان برای پیوستن به مجوز نیاز دارند و مکانیسم کنترل دسترسی می‌تواند تغییر کند. (s.singh, 2021)

#### ۵) منبع باز

با برنامه‌های توزیع‌شده و منبع بسته، کاربران باید به برنامه‌ها اعتماد کنند و نمی‌توانند به هیچ داده‌ای از منابع مرکزی دسترسی داشته باشند. می‌توان برنامه‌های منبع بسته غیرمتمرکز را راه‌اندازی کرد و به نتایج دلخواه دست یافت، اما انجام این کار عواقب فاجعه‌باری خواهد داشت. این دلیل اصلی است که شرکت‌کنندگان برنامه‌های منبع باز غیرمتمرکز را با پلتفرم‌های مربوطه از جمله اتریوم، بیت‌کوین کش، لایت‌کوین و دش ترجیح می‌دهند. پلتفرم‌های بلاکچین با قابلیت سایدچین، مزایای قدرتمندی را که توسط اعضای جامعه توسعه داده شده‌اند، ارائه می‌دهند، مانند

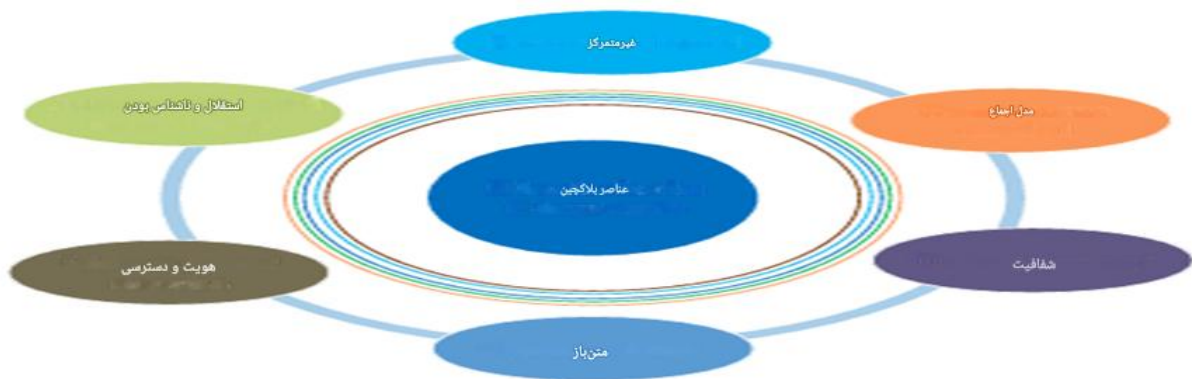
- پیکربندی‌های انعطاف‌پذیر: بدون ریسک در سازماندهی مجدد چند بلوکی و امکان تراکنش‌های سریع،
- تراکنش‌های محرمانه: با بهره‌گیری از ثبات،
- پیوند دو طرفه فدرال: صدور دارایی‌های چند قابل انتقال در بلاکچین‌های واحد، و
- صدور دارایی‌های چندگانه: توسط فدراسیونی از طرفین با انگیزه‌های همسو تضمین می‌شود.

برنامه‌های متن‌باز به کاربران کمک می‌کنند تا فناوری‌های جدید را بپذیرند. یکی از ویژگی‌های اصلی چنین برنامه‌هایی، همانطور که بوت‌ترین تأکید کرده است، یک مدل مجوز متن‌باز و مکانیسم دولتی است که امکان تغییر در پلتفرم‌های ارزی دفتر کل عمومی یا برنامه‌های بلاکچین را فراهم می‌کند. گول فناوری IBM با ترویج پروژه‌هایی مانند Linux Foundations Hyperledger Composer به تکامل فناوری‌های متن‌باز کمک کرده است. در مورد اکوسیستم‌های سازمانی، MentaGo یک راه‌حل بلاکچین برای سیستم‌های مالی ارائه می‌دهد و SXSW از Hyperledger fabric و IBM استفاده می‌کند. (s.singh, 2021)



## ۶) ناشناس سازی

ناشناس بودن یکی از مهمترین عناصر (نشان داده شده در شکل ۱ در فناوری بلاکچین برای حفظ حریم خصوصی تراکنش ها در شبکه ها است، اما تضمین ناشناس بودن دشوار است زیرا دفتر کل بلاکچین عمومی است.



شکل ۱ عناصر بلاکچین.

هر کاربر یک آدرس ایجاد می کند و هیچ مکانیسمی برای حفظ اطلاعات خصوصی کاربر وجود ندارد. به همین دلیل است که بیت کوین شبه ناشناس در نظر گرفته می شود: کاربران می توانند با آدرس های عمومی خود مرتبط شوند، اما یادگیری نام یا آدرس واقعی آنها امکان پذیر نیست. موزر مقاله ای در مورد ناشناس بودن تراکنش های بیت کوین ارائه داد که در آن یک سرویس ویژه ترکیب بیت کوین پیشنهاد شد که می تواند آدرس های تراکنش بیت کوین مبدا را پیچیده یا گیج کننده کند و در نتیجه ناشناس بودن را افزایش دهد. نگرانی اصلی امنیتی در مورد بلاکچین این است که کلیدهای عمومی و تراکنش ها نباید هویت واقعی را فاش کنند. (s.singh, 2021)

## تأثیر بلاکچین بر فناوری های کلیدی فعال کننده در متاورس

بلاکچین می تواند فناوری های کلیدی فعال کننده در متاورس را تقویت کند که به کاربران امکان می دهد بدون ترس از عواقب، در فعالیت های اجتماعی و اقتصادی شرکت کنند. تصویر بلاکچین بر روی فناوری های کلیدی فعال کننده در متاورس در شکل ۲ نشان داده شده است. (Gadekallu, T. R., 2022)

### الف. بلاکچین برای اینترنت اشیا در متاورس

۱) مقدمه: پلتفرم متاورس داده ها را از انواع دستگاه های اینترنت اشیا (IoT) جمع آوری می کند تا از عملکرد کارآمد آن در چندین کاربرد متاورس مانند پزشکی، آموزش و شهرهای هوشمند اطمینان حاصل شود. دستگاه های اینترنت اشیا، متاورس را از طریق طیف متنوعی از سخت افزارها، کنترل کننده ها و اقلام فیزیکی متصل می کنند. اتصال به متاورس و پیمایش فیزیکی و مجازی

توسط دستگاه‌های اینترنت اشیا مجهز به حسگرهای تخصصی امکان‌پذیر است. ظرفیت دستگاه‌های اینترنت اشیا برای انجام عملیات در متاورس برای توانایی کاربر در عملکرد در متاورس بسیار مهم خواهد بود. (Gadekallu, T. R., 2022)

۲) چالش‌های مربوط به اینترنت اشیا در متاورس: تعداد زیادی حسگر اینترنت اشیا متصل در متاورس وجود خواهد داشت. با وجود این همه دستگاه متصل، ذخیره‌سازی و امنیت اینترنت اشیا بدون شک یک نگرانی است. تجزیه و تحلیل داده‌های اینترنت اشیا که بدون ساختار و بلادرنگ هستند، فوق‌العاده دشوار است. کیفیت داده‌ها را می‌توان با مقدار، دقت و سرعت داده‌ها قضاوت کرد. علاوه بر این، داده‌های متاورس برای تجزیه و تحلیل باید بدون خطا باشند. استفاده از یک استراتژی متمرکز در هنگام ذخیره داده‌ها در سراسر جهان‌های مجازی مفید نیست. اگر حتی یک قطعه داده دستکاری شده باشد، به کل مجموعه نتایج تولید شده توسط دستگاه‌های اینترنت اشیا آسیب می‌رساند. قابلیت‌های چند پلتفرمی دستگاه‌های اینترنت اشیا برای به اشتراک گذاری داده‌ها بین جهان‌های مجازی بسیار مهم است. داده‌های اینترنت اشیا باید به دلایل ایمنی و رعایت مقررات ردیابی شوند. (Gadekallu, T. R., 2022)

۳) چگونه بلاکچین می‌تواند کمک کند: بلاکچین دستگاه‌های اینترنت اشیا در متاورس را قادر می‌سازد تا داده‌ها را از طریق شبکه‌های بین زنجیره‌ای منتقل کنند، که به نوبه خود سوابق مقاوم در برابر دستکاری از تراکنش‌های مشترک در جهان‌های مجازی را تولید می‌کنند، همانطور که در شکل ۲ نشان داده شده است. در نتیجه فناوری بلاکچین، برنامه‌ها و کاربران قادر خواهند بود بدون نیاز به مدیریت یا کنترل متمرکز، داده‌های اینترنت اشیا را به اشتراک بگذارند و به آنها دسترسی داشته باشند. برای از بین بردن اختلافات و افزایش اعتماد بین کاربران متاورس، هر تراکنش ثبت و تأیید می‌شود. در متاورس، بلاکچین فعال شده با اینترنت اشیا امکان ذخیره داده‌ها را در زمان واقعی فراهم می‌کند. همه ذینفعان می‌توانند به داده‌ها اعتماد کنند و به دلیل تراکنش‌های بلاکچین تغییرناپذیر، به سرعت و به طور کارآمد اقدام کنند. فناوری بلاکچین به ذینفعان این امکان را می‌دهد تا سوابق داده‌های اینترنت اشیا خود را در دفاتر کل بلاکچین مشترک پیگیری کنند، این امر به حل مشکلات در متاورس کمک می‌کند. (Gadekallu, T. R., 2022)



شکل ۲. بلاکچین برای فناوری‌های کلیدی توانمندساز متاورس.

۴) خلاصه: بلاکچین دستگاه‌های اینترنت اشیا را قادر می‌سازد تا داده‌های واقعی را به طور ایمن در چندین جهان مجازی به اشتراک بگذارند و ذخیره کنند. فناوری‌های بلاکچین برای ادامه کار خود به مقدار قابل توجهی از قدرت پردازش نیاز دارند. اگر گروه کوچکی از ماینرها بیشتر نرخ هش کل استخراج شبکه را کنترل کنند، بلاکچین‌ها آسیب‌پذیر هستند. به دلیل فقدان حاکمیت، تأیید داده‌های اینترنت اشیا که عمومی نیستند، قبل از انتشار در بلاکچین در متاورس امکان‌پذیر نیست. قراردادهای هوشمند در متاورس که بر روی یک دفتر کل تراکنش توزیع شده اجرا می‌شوند، ممکن است قوانین را نقض کنند. ردیابی تمام تراکنش‌های اینترنت اشیا که شامل خدمات غیرقانونی در متاورس هستند، به دلیل ناشناس بودن ارائه شده توسط فناوری بلاکچین دشوار است. در حالی که عملکرد خودکار بلاکچین مزایای بی‌شماری را ارائه می‌دهد، مشخص کردن اینکه کدام طرف‌ها مسئول رفتارهای خاص هستند، همچنان یک چالش دشوار است. بلاکچین باید برای گسترش متاورس، منظم شود.

(Gadekallu, T. R.,2022 )

ب. بلاکچین برای هوش مصنوعی در متاورس

۱) مقدمه: هوش مصنوعی یکی از مهمترین فناوری‌های توانمندساز برای پایه‌گذاری و توسعه متاورس است که به آن در رسیدن به پتانسیل کامل خود کمک می‌کند. بر اساس تصویر اصلی یا اسکن سه‌بعدی، یک مدل هوش مصنوعی تصاویر کاربر را به طور



خودکار تجزیه و تحلیل می‌کند و یک نمایش شبیه‌سازی شده بسیار واقع‌گرایانه به نام آواتار ایجاد می‌کند. در متاورس، ویژگی‌ها و خصوصیات نمایشی آواتار بر کیفیت کلی تجربه کاربر تأثیر می‌گذارد. به طور مشخص، هوش مصنوعی می‌تواند انواع حالات چهره، احساسات، مدها، ویژگی‌های مرتبط با پیری و غیره را برای آواتار ترسیم کند تا آن را پویاتر کند. در نتیجه آموزش قابل توجه هوش مصنوعی، متاورس برای افراد در سراسر جهان، صرف نظر از شایستگی زبانی آنها، در دسترس خواهد بود. ایجاد تجربه متاورس که هم سرگرم‌کننده و هم معتبر باشد و در عین حال قابل فروش باشد، بدون استفاده از هوش مصنوعی چالش برانگیز خواهد بود. (Gadekallu, T. R., 2022)

۲) چالش‌های مربوط به هوش مصنوعی در متاورس: از نظر علم و فناوری، متاورس مرز جدیدی را نشان می‌دهد و ایجاد هوش مصنوعی در آنجا کار دشواری خواهد بود. ردیابی مالکیت مطالب مبتنی بر هوش مصنوعی در متاورس دشوار است. کاربران هیچ راهی برای دانستن اینکه آیا با یک شخص واقعی یا یک آواتار تولید شده توسط کامپیوتر در تعامل هستند، ندارند. کاربران ممکن است از فناوری‌های هوش مصنوعی برای مشارکت در تعاملات متاورس و بهره‌برداری غیرقانونی از منابع استفاده کنند، به عنوان مثال، با استفاده از کد هوش مصنوعی برای برنده شدن در بازی‌ها یا با سرقت منابع از سایر کاربران. همچنین ممکن است هوش مصنوعی اشتباهاتی مرتکب شود که در نتیجه باعث شود مردم اعتماد خود را به متاورس از دست بدهند. علاوه بر این، این یک مانع برای به کارگیری نوع مشابهی از بلاکچین در انواع برنامه‌های هوش مصنوعی در متاورس است. (Gadekallu, T. R., 2022)

۳) چگونه بلاکچین می‌تواند کمک کند: رمزگذاری ارائه شده توسط فناوری بلاکچین، کنترل کامل کاربران متاورس بر داده‌هایشان را تسهیل می‌کند و انتقال مالکیت رضایت هوش مصنوعی به طرف دیگر را ساده می‌کند. کاربران می‌توانند برنامه‌ها و دیگران را متقاعد کنند که اطلاعات خاص در مورد آنها دقیق است، بدون اینکه این اطلاعات را به خود برنامه‌ها از طریق استفاده از اثبات‌های دانش صفر افشا کنند، این امر حق استفاده از داده‌ها را برای آموزش مدل هوش مصنوعی فراهم می‌کند. به عنوان یک ویژگی مشترک، دفاتر کل بلاکچین یک مسیر حسابرسی ارائه می‌دهند که می‌تواند برای بررسی پاسخگویی تمام تراکنش‌های رخ داده در متاورس مورد استفاده قرار گیرد. یک سیستم شواهد دانش صفر به افراد این امکان را می‌دهد که حقایق حیاتی را در متاورس شناسایی کنند و در عین حال از حریم خصوصی خود محافظت کرده و مالکیت منابع خود را در برابر جعل عمیق حفظ کنند. این امر مانع از سوءاستفاده هوش مصنوعی از منابع در متاورس می‌شود. (Gadekallu, T. R., 2022)

۴) خلاصه: ترکیب هوش مصنوعی و بلاکچین از داده‌های بسیار حساسی که سیستم‌های مبتنی بر هوش مصنوعی باید به دست آورند، ذخیره کنند و استفاده کنند، محافظت می‌کند. داده‌ها و اطلاعات حساس، از درشت تا ریز، در متاورس به طور قابل توجهی در نتیجه این رویکرد محافظت می‌شوند. بلاکچین‌های عمومی ایمن هستند و پردازش داده‌های معتبری دارند، اما داده‌های جمع‌آوری شده برای همه ذینفعان در متاورس باز است. این می‌تواند منبع نگرانی باشد و به مدل‌های هوش مصنوعی در متاورس نیز آسیب برساند. اگر استانداردها یا مقررات بلاکچین وجود نداشته باشد، مهاجمان از ضعف هوش مصنوعی سوءاستفاده خواهند کرد. نکته قابل توجه این است که معرفی یک مبدل بین زنجیره‌ای که برنامه‌های هوش مصنوعی را قادر می‌سازد با متاورس‌های ساخته شده بر روی بلاکچین‌های مختلف آشنا شوند، ضروری است. (Gadekallu, T. R., 2022)



## راه‌حل‌های حمله

### (۱) حمله زنده بودن

برای مقابله با حمله‌ی فعال بودن، پروتکل اجماع Con uxs اساساً دو استراتژی تولید بلوک مختلف رمزگذاری می‌کند. یکی استراتژی بهینه است که امکان تأیید سریع را فراهم می‌کند و دیگری استراتژی محافظه‌کارانه است که پیشرفت اجماع را تضمین

ابزار امنیتی	رابط	ورود مجدد	وابستگی به مهر زمانی	استثنائات مدیریت نشده	افکالات تغییرناپذیر	هزینه گس الگوها،	بلاک‌هش کاربرد
اوینت	خط فرمان	✓	✓	✓	✓	*****	*****
ریمیکس	خط فرمان	✓	✓	✓	*****	✓	✓
گسپر		*****	*****	*****	*****	✓	*****
ایمن‌سازی	رابط کاربری	✓	*****	✓	*****	*****	*****
تحلیل S		*****	*****	✓	*****	*****	*****
بررسی هوشمند	رابط کاربری	✓	✓	✓	✓	✓	*****
مایتریل	خط فرمان	✓	*****	✓	✓	-----	*****

می‌کند. Con ux یک سیستم مقیاس‌پذیر و غیرمتمرکز با دقت بالا است.

جدول ۱ ابزارها و آسیب‌پذیری‌ها.

توان عملیاتی و تأیید سریع در سیستم بلاکچین. این سیستم از یک مکانیسم وزن تطبیقی جدید برای ترکیب این دو استراتژی در یک پروتکل اجماع یکپارچه استفاده می‌کند. (s.singh, 2021)

### (۲) حملات دو برابر کردن

برای مقابله با حمله دو برابر کردن، به استخر اجازه می‌دهد تراکنش‌ها را تأیید کند. چارچوب پیشنهادی شامل چهار مرحله برای غلبه بر این حمله است: الف) مرحله تشخیص، ب) مرحله تأیید، ج) مرحله ارسال و د) مرحله پخش. علاوه بر این، بگومتال پس از نشان دادن محدودیت‌های این حمله، مجموعه‌ای از راه‌حل‌ها را در برابر حملات دو برابر کردن ارائه می‌دهد. (s.singh, 2021)

### ۳) حمله آسیب‌پذیری ۵۱٪

برای مقابله با حمله ۵۱٪، بر روی ارزشهای دیجیتال با قدرت هش پایین تمرکز شده است تا حمله ۵۱٪ تجزیه و تحلیل شود و ضعف پروتکل اجماع را که باعث وقوع این حمله می‌شود، آشکار سازند. نویسندگان مشکل نرخ هش را تعریف کرده و پنج مکانیسم امنیتی در برابر حمله ۵۱٪ ارائه می‌دهند. کار اخیری که برای مقابله با حمله ۵۱٪ انجام شده است شامل استخراج دفاعی، پیاده‌سازی یک سیستم داوری نهایی «Permapoint» برای محدود کردن سازماندهی مجدد زنجیره است. (s.singh, 2021)

### ۴) حمله امنیتی کلیدهای خصوصی

محققان زیرساخت کلید عمومی مورد استفاده در فناوری بلاکچین را برای احراز هویت موجودیت‌ها برای مقابله با حمله امنیتی کلید پیشنهاد کرده‌اند. این تکنیک یکپارچگی شبکه بلاکچین را تضمین می‌کند. مدیریت کلید گروهی برای ایمن‌سازی ارتباطات گروهی برای دستیابی به محرمانگی در شبکه مورد بحث قرار گرفته است. (s.singh, 2021)

### ۵) نشت حریم خصوصی تراکنش

کار ارائه شده توسط محققان نمای کلی از حفره‌های امنیتی، انجام تراکنش‌ها و طرح روش‌شناسی تراکنش امن را ارائه داد. این طرح از یک سیستم رمزنگاری همومورفیک، امضای حلقه‌ای و بسیاری از اقدامات امنیتی دیگر برای کاهش تأثیر کلی تهدیدها برای بهبود قابلیت اطمینان در فرآیند تراکنش در شبکه استفاده می‌کند. (s.singh, 2021)

### ۶) حمله خودکاو

آسیب‌پذیری خودکاو توسط گروهی از دانشمندان مورد بحث قرار داده‌اند و راه حلی برای مقابله با این حمله ارائه داده‌اند. برای مقابله با این حمله، نویسندگان از یک روش صادقانه استخراج برای طراحی نمادگذاری حالت حقیقی برای بلوک‌ها در طول انشعاب خودکاو و همچنین اختصاص ارتفاع خودکاو به هر تراکنش استفاده می‌کنند. (s.singh, 2021)

### ۷) حمله DAO

گروهی از محققان به حمله داخلی DAO در شبکه RPLIoT پرداختند. برای کاهش این حمله، نویسندگان با انجام آزمایش‌هایی با استفاده از ابزار Contiki، ابزاری با طراحی کم‌مصرف برای دستگاه‌های با محدودیت منابع، طرحی را پیشنهاد کرده‌اند. (s.singh, 2021)

### ۸) حمله ربودن BGP

طرحی پیشنهاد شده است که یک راه‌حل منبع اینترنتی مبتنی بر بلاکچین قابل اعتماد است. این طرح، قرارداد هوشمند را برای انجام و نظارت بر تخصیص منابع در بلاکچین اتریوم مقاوم در برابر تغییرات دما توسعه می‌دهد. طرح BGPCoin یک راه‌حل امنیتی معتبر BGP را در بلاکچین اتریوم و برنامه‌نویسی قرارداد هوشمند ارائه می‌دهد. (s.singh, 2021)

## ۹) حمله SYBIL

برای جلوگیری از حملات Sybil در شبکه‌های بلاکچین، طرحی برای محدود کردن حمله Sybil با نظارت بر رفتار سایر گره‌ها و بررسی گره‌هایی که بلوک‌های فقط یک کاربر خاص را ارسال می‌کنند، پیشنهاد شده است. (s.singh, 2021)

## بحث و نتیجه‌گیری

در این مقاله، نقش بلاکچین در متاورس را بررسی کردیم. الگوی بلاکچین در حال تغییر صنعت فناوری اطلاعات است. بلاکچین می‌تواند شرکت‌ها، دولت‌ها و حتی کشورها را گرد هم آورد. فناوری بلاکچین به دلیل ماهیت غیرمتمرکز و ویژگی‌های نظیر به نظیر، به طور گسترده شناخته شده و بسیار ارزشمند است. نکته اصلی این مقاله این است که مدل‌های مختلف حمله به بلاکچین و مسائل امنیتی بلاکچین را بررسی کردیم. این مقاله با بررسی انواع حملات سعی در ایجاد نگرش جدید در غالب نگاه کلی در اشتراک تاثیر گذاری حملات در تکنولوژی‌های مرتبط نظیر بلاکچین، متاورس، اینترنت اشیا و حتی تاثیرات منتج در این مقاله بر دیگر تکنولوژی‌ها سعی در پاسخگویی به مدل‌های مقابله با حملات و ایجاد فضای امن برای فضای اشتراکی در فرآیند اجماع تکنولوژی‌ها با هم دارد.

## منابع

S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in *IEEE Access*, vol. 9, pp. 13938-13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

Yousafzai, A., Sheeraz, M. M., Pogrebna, G., Crowcroft, J., & Yaqoob, I. (2025). Blockchain for the metaverse: Recent advances, taxonomy, and future challenges. *Journal of Network and Computer Applications*, 244, 104355.

Yokubov, B. (2023). Post-quantum blockchain for Internet of Things domain (Doctoral dissertation, Brunel University London).

O. Alphand *et al.*, "IoTChain: A blockchain security architecture for the Internet of Things," 2018 *IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, Spain, 2018, pp. 1-6, doi: 10.1109/WCNC.2018.8377385.

Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranawera, P., Pham, Q.-V., da Costa, D. B., & Liyanage, M. (2022). Blockchain for the metaverse: A review. *IEEE Internet of Things Journal*.



**ICAICS**

<https://icaics.ir>

[info@icaics.ir](mailto:info@icaics.ir)

اولین کنفرانس بین المللی هوش مصنوعی  
و علوم کامپیوتری نوظهور: از الگوریتم تا آینده‌نگری

**First International Conference on Artificial Intelligence  
and Emerging Computer Science: From Algorithm to Foresight**

March 17, 2026-GEORGIA

۲۶ اسفند ماه ۱۴۰۴ - گرجستان

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 32979–33001. <https://doi.org/10.1109/ACCESS.2018.2842685>