ارتقاء امنیت اینترنت اشیاء با ارائه یک طرح احراز هویت متقابل غیرمتمرکز بر بستر اتریوم

فاطمه حاجی زاده[۱]، رحیم اصغری[۲]

[۱] کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، تهران
F73.hajizadeh@gmail.com

[۲] استادیار، دانشگاه صنعتی مالک اشتر، تهران
meisam.mathhome@gmail.com

چکیده

اینترنت اشیاء قدرت اینترنت و پردازش داده‌ها را به دنیای واقعی اشیاء فیزیکی می‌آورد. یکی از مهم‌ترین چالش‌های امنیتی در اینترنت اشیاء مسئله احراز هویت است. احراز هویت سبک یکی از روش‌های تأیید هویت مدرن است که برای شبکه‌ها با دستگاه‌های توان محدود مانند اینترنت اشیاء در نظر گرفته می‌شود. با توجه به ناهمگونی و سایر ویژگی‌های اینترنت اشیاء، ایجاد یک سیستم احراز هویت متمرکز کارآمد تقریباً غیرممکن است. برای اصلاح این محدودیت در این مقاله، یک طرح غیرمتمرکز مبتنی بر زنجیره بلوکی پیشنهاد می‌شود، که در آن احراز هویت متقابل تضمین می‌شود. علاوه بر این، از یکپارچگی داده‌ها و در دسترس بودن آن‌ها محافظت می‌کند. طرح ارائه‌شده به مزایای امنیتی زنجیره بلوکی متکی است و با جایگزینی زنجیره احراز هویت بجای دروازه‌های موجود در طرح‌های احراز هویت متداول مشکلات ناشی از تمرکز مانند شکست تک نقطه‌ای و تنگنای مرکزی در دروازه را حل می‌کند. در این مقاله زنجیره احراز هویت با در نظرگرفتن دستگاه‌های توان محدود اینترنت اشیاء بر روی زنجیره بلوکی خصوصی اتریوم که از گره‌های سبک پشتیبانی می‌کند، پیشنهاد می‌شود. طرح احرازهویت با استفاده از برنامه‌های غیر متمرکز اتریوم در دو ماژول جداگانه پشتیبان و توسعه رابط کاربری اجرا می‌شود. بخش پشتیبان شامل قرارداد هوشمند است و بر روی بستر اتریوم، ایجاد می‌شود. بخش توسعه رابط کاربری یک برنامه وب است که بر روی مرورگر کاربر اجرا می‌شود و با استفاده از پروتکل-های سبک وزن با بخش پشتیبان در زنجیره بلوکی تعامل دارد.

کلمات کلیدی: اینترنت اشیاء، احراز هویت، زنجیره بلوکی، غیر متمرکز، اتریوم، قراردادهای هوشمند.

۱. مقدمه

اینترنت اشیاء[۱] به دستگاه‌ها در شبکه خصوصی اینترنت، اجازه می‌دهد تا با یکدیگر ارتباط برقرار کنند. مسائل امنیتی اینترنت اشیاء می‌تواند تاثیر مهمی بر زندگی روزمره، دولت، صنایع و زیرساخت‌های امنیتی یک کشور داشته باشد. احراز هویت و کنترل دسترسی، در مدیریت ایمن منابع و شبکه‌های رایانه‌ای نقش مهمی دارند. احراز هویت، با بررسی اینکه آیا اعتبار کاربر در اعتبارنامه در پایگاه داده‌ی کاربران مجاز یا در یک خدمت‌رسان تأیید داده، مطابقت دارد، کنترل دسترسی را برای سامانه‌ها فراهم می‌کند. شبکه اینترنت اشیاء از هزاران یا ده‌ها هزار دستگاه ناهمگن متصل بهم تشکیل می‌شود، استفاده از مدل احراز هویت متداول، که به یک مرجع مرکزی نیاز دارد مناسب این شبکه ناهمگون نیست. هم‌چنین مانند هر مدل خدمت‌رسان - کاربر، اگر خدمت‌رسان آسیب‌پذیر باشد، تمام دستگاه‌های وابسته دچار مشکل خواهند شد. طرح احراز اصالت دیابو [1] در اینترنت اشیاء نمونه‌ای از مدل احراز اصالت متداول و متمرکز در اینترنت اشیاء است. این طرح

شامل سه بخش، حسگرها، کاربر و دروازه به‌منظور تسهیل ارتباط بین طرفین می‌شود. دروازه نقش مهمی در احراز اصالت این طرح دارد زیرا یکی از وظایف آن ترجمه پیام‌های مبادله شده در پروتکل است. حسگرها با توان پردازشی محدود از دروازه برای پردازش‌های اضافی و ذخیره‌سازی نیز استفاده می‌کنند. هم‌چنین دروازه اصالت یک کاربر یا حسگری را که می‌خواهد به داده‌ها، منابع یا برنامه‌های کاربردی دسترسی داشته باشد را تائید می‌کند. وجود دروازه موجب تنگنای مرکزی[۲] و شکست تکنقطه‌ای[۳] که دو مشکل بزرگ در طرح‌های متمرکز هستند، می‌شود.

از زمان شروع کار بیت کوین[۴] در سال ۲۰۰۸ [2]، فن‌آوری زنجیره بلوکی[۵] به‌عنوان فن‌آوری انقلابی جدید مطرح شد. اگرچه زنجیره بلوکی به‌عنوان فن‌آوری اصلی بیت کوین شروع به کار کرد، اما استفاده از آن در بسیاری از موارد دیگر ازجمله امور مالی، اینترنت اشیاء، امنیت و موارد دیگر در حال گسترش است. با استفاده از زنجیره بلوکی در اینترنت اشیاء، دستگاه‌های اینترنت اشیاء می‌توانند به دلیل داشتن دفترچه توزیع‌شده، به‌راحتی با سایر دستگاه‌ها همگام شوند. همچنین با استفاده از الگوریتم اجماع[۶]، جعل داده‌ها در زنجیره بلوکی یا انجام حمله انکار سرویس[۷] دشوار خواهد بود. فن‌آوری زنجیره بلوکی برای ایجاد زنجیره‌ای تغییرناپذیر از معاملات از رمزنگاری کلید عمومی استفاده می‌کند. طبیعت ذاتی آن برای تقویت امنیت و حفظ حریم خصوصی شبکه‌های اینترنت اشیاء قابل‌استفاده است. با توجه به ویژگی‌های بیان‌شده برای زنجیره بلوکی، می‌توان از آن برای احراز هویت در شبکه‌های اینترنت اشیاء استفاده نمود و احراز هویت غیرمتمرکز و غیر وابسته به نهاد مرکزی را اجرا نمود.

دو طرح ماهواره لئو[۸] [3] و سامانه‌های نظارت تصویری [4] کاربرد زنجیره بلوکی در احراز اصالت را برای نوع خاصی از اشیاء مطرح می‌کنند. در طرح [3]، یک پروتکل احراز اصالت سبک‌وزن مبتنی‌بر زنجیره بلوکی جهت احراز اصالت ماهواره‌های لئو ارائه می‌شود. در این پروتکل، مرکز تولید کلید[۹] برای ایجاد امنیت لازم در نگهداری و توزیع کلیدها، تمامی اطلاعات ثبت‌نام کاربر را در بلوک‌ها بسته‌بندی می‌کند و این بلوک‌ها روی زنجیره بلوکی محلی ذخیره می‌شوند. از طرفی، زنجیره بلوکی با استفاده از الگوریتم‌های اجماع تمرکززدایی می‌شود. طرح پیشنهادی شامل ماهواره‌ها، کاربران و مرکز تولید کلید است. ماهواره‌هایی که در یک موقعیت مکانی قرار دارند بر روی یک زنجیره بلوکی محلی مستقر هستند.

در مرجع [4]، یک طرح احراز اصالت اجراشده بر روی زنجیره بلوکی برای پرسمان تصویری رویداد گرا بی‌درنگ ارائه می شود. این طرح امنیت سامانه نظارتی هوشمند را بهبود می‌بخشد. از طریق اجرای تشخیص و ردیابی در دستگاه‌های لبه تعبیه‌شده، خلاصه اطلاعات خدمات نظارت رویداد گرا به‌وسیله پردازش فریم‌های ورودی استخراج می‌شود. سپس خدمت‌رسان نمایه‌ساز بی‌درنگ، یک شاخص منحصربه‌فرد را برای جلوگیری از تغییرات مخرب در تصویر ایجاد می‌کند. درنهایت شاخص‌های قاب بر روی زنجیره بلوکی ثبت‌شده و به‌وسیله پروتکل احراز اصالت مبتنی‌بر قرار داد هوشمند[۱۰] غیرمتمرکز، تأیید می‌شوند.

سه طرح [5 -7] برای مدیریت و ارتقاء امنیت کاربر در اینترنت اشیاء مطرح شده‌اند. در مقاله [5] هدف ایجاد محیط ایمن اینترنت اشیاء خانه با کنترل خطرپذیری شخصی در زمان واقعی است. این پروژه از اصول طراحی وابسته به رفتار برای تهیه یک معماری مرجع جدید برای امنیت سایبری کاربر محور در محیط خانه‌های هوشمند استفاده می‌کند. سامانه پیشنهادی جریان داده‌های سطح بسته را برای ایجاد الگوهای ارتباطاتی بین دستگاه‌های اینترنت اشیاء و کاربران خارجی تجزیه‌وتحلیل می‌کند. برای اطمینان از عدم تکذیب، یکپارچگی و تأیید صحت داده‌های دریافت شده، آن‌ها در قالب معاملات، زنجیره بلوکی ذخیره می‌کند. در [5] طراحی و پیاده‌سازی یک نمونه از برنامه‌های غیرمتمرکز[۱۱] در تعامل با مجموعه قراردادهای هوشمند مستقر در یک شبکه خصوصی اتریوم[۱۲] ارائه‌شده است.

در مقاله [6] آقای ایتری و همکاران، به‌منظور کنترل و پیکربندی دستگاه‌های اینترنت اشیاء استفاده از زنجیره بلوکی را پیشنهاد می‌کنند. در این طرح کلیدها با استفاده از رمزنگاری کلید عمومی RSA ایجاد می‌شود، کلیدهای عمومی در اتریوم و کلیدهای خصوصی در دستگاه‌های انفرادی ذخیره و کنترل می‌شوند. برای امکان‌سنجی این طرح، به‌جای یک سامانه کامل که متشکل از هزاران دستگاه اینترنت اشیاء است، از چند دستگاه اینترنت اشیاء استفاده می‌شود. سه رزبری

پای[۱۳]، به‌عنوان کنتور هوشمند برای ردیابی مصرف برق، تهویه هوا و یک لامپ کم‌مصرف به کار می‌رود. با استفاده از تلفن هوشمند، کاربر می‌تواند خط‌مشی را تنظیم کند. وقتی کاربر پیکربندی را از طریق تلفن هوشمند تنظیم می‌کند، داده‌ها به شبکه اتریوم ارسال می‌شوند. در این میان، دستگاه‌هایی مانند لامپ یا کولرگازی مقادیر خط‌مشی را به‌طور دوره‌ای از اتریوم بازیابی می‌کنند. همچنین کنتور هوشمند میزان مصرف برق را ردیابی کرده و آن را در اتریوم به‌روز می‌کند.

در مقاله [7]، آقای آلفند و همکاران، طرحی ترکیبی از معماری امنیتی شیء برای اینترنت اشیاء [8] و چارچوب صدور مجوز [9] را به‌منظور رسیدن یک‌راه حل انتها به انتها[۱۴] در دسترسی مجاز ایمن به منابع اینترنت اشیاء، ارائه می‌دهد. در چارچوب [9]، مشتریان باید یک کانال رمزگذاری شده و تأییدشده را با یک مرکز صدور مجوز معتبر راه‌اندازی کنند تا بتوانند، مجوزهای مالک و نشانه‌های دسترسی ایمن را تبادل کنند. برای این کار نیاز به استفاده از گواهینامه‌ها دارند. علاوه بر این، مراکز صدور مجوز نادرست می‌توانند، آزادانه مجوزهای دسترسی را برای هر منبع محافظت‌شده صادر کنند. در [7] آقای آلفند و همکاران مرکز صدور مجوز معتبر منفرد در چارچوب [9] را با یک زنجیره بلوکی صدور مجوز بی‌اعتماد جایگزین می‌کنند. زنجیره بلوکی مدل صدور مجوز در [9] را با کنترل دسترسی کارآمدتر منابع، مقیاس‌پذیری و احتمالاً حفظ حریم خصوصی بهبود می‌بخشد.

دو طرح [5] و [7] با استفاده از شبکه خصوصی اتریوم پیاده‌سازی شده‌اند. پروتکل مبتنی‌بر زنجیره بلوکی ارائه‌شده در این مقاله با روشی مشابه با کارهای مروری، با استفاده از شبکه خصوصی اتریوم پیشنهاد می‌شود. مطالعات فوق بیشتر بر مدیریت اعتماد، امنیت داده‌ها، حفاظت از امنیت تمرکز دارد. مزیت مدل ارائه‌شده در این مقاله در مقایسه با سایر آثار به ماهیت عمومی و سادگی آن مربوط می‌شود. تحقیقات ارائه‌شده در مقاله ما به امنیت اینترنت اشیاء و به ویژه تأیید هویت و محافظت از امنیت دستگاه‌های اینترنت اشیاء می‌پردازد. در این مقاله با ارائه طرح احراز اصالت غیرمتمرکز برای اینترنت اشیاء، اصالت مبتنی‌بر شناسه دستگاه و کاربران در این شبکه با استفاده از قراردادهای هوشمند اتریوم وارسی می‌شود. در این طرح بعد از احراز اصالت کاربران، نواحی ایمن برای اینترنت اشیاء بر روی زنجیره بلوکی ایجاد می‌شود. به دلیل اجرای این طرح بر روی زنجیره بلوکی و حذف دروازه در پروتکل‌های متداول احراز اصالت اینترنت اشیاء از خطر تنگنای مرکزی و شکست تک‌نقطه‌ای به دلیل وجود دروازه، اجتناب می‌شود. علاوه براین به خطر افتادن دروازه در این پروتکل‌ها تأثیرات گسترده‌ای بر شبکه اینترنت اشیاء، مانند امکان تغییر داده‌های مربوط به احراز اصالت و در دسترس نبودن تمام یا برخی از دستگاه‌ها می‌شود. داده‌های ذخیره‌شده بر روی زنجیره بلوکی تغییرناپذیر و غیرقابل‌برگشت هستند، درنتیجه با استفاده از زنجیره بلوکی در طرح ارائه‌شده می‌توان به عدم دست‌کاری داده و جعل اصالت در شبکه دست‌یافت و طرح احراز اصالت غیرمتمرکز ایمن در برابر خطرات ذکرشده را ارائه نمود.

۲. زنجیره بلوکی، اتریوم و قراردادهای هوشمند

پس از اینترنت، زنجیره بلوکی به‌عنوان انقلاب بزرگ بعدی در حوزه فن آوری مطرح می شود. پس از بیت کوین رمز ارزهای متعددی با ویژگی‌های بسیار پیشرفته مانند اتریوم که قراردادهای هوشمند را معرفی می‌کند، شروع به فعالیت کردند. در چندین دهه گذشته تبادل اطلاعات و انتقال پول یا سایر دارایی‌ها به‌واسطه معاملات آنلاین در بستر اینترنت انجام می‌شود. درحالی‌که همه این معاملات درگیر یک میانجی قابل‌اعتماد هستند و این میانجی قابل‌اعتماد مسئولیت هر مورد از خرابی‌ها یا رخنه‌های امنیتی را بر عهده دارد. در یک تغییر الگو، زنجیره بلوکی با استفاده از دفترکل عمومی توزیع‌شده، نیاز به هر مرجع مجازشناس مرکزی، بین طرفین متعدد اجرای معاملات مالی و انتقال داده¬ها را حذف می کند. این دفترکل عمومی یک پایگاه داده توزیع‌شده است که درمیان تمام اعضای شبکه به اشتراک گذاشته می‌شود. این پایگاه داده ضد دست‌کاری، ایمن شده به‌وسیله رمزنگاری و بایگانی دائمی از تمام معاملات انجام‌شده بین طرفین است. اعضای شبکه می‌توانند معاملات مربوط به خود را در هر زمانی که می‌خواهند ببینند، اما معاملات پس از تائید و اضافه

شدن به زنجیره بلوکی نمی‌توانند حذف یا ارسال شوند، که این امر باعث می‌شود زنجیره بلوکی تغییرناپذیر و غیرقابل‌برگشت باشد.

هرمعامله بدون تائید یا احراز اصالت توسط هر مرجع مجازشناسی مرکزی، توسط اعضای شبکه با استفاده از اعتبارسنجی از پیش تعریف‌شده و الگوریتم‌های اجماع، وارسی می‌شود. این روند نه‌تنها در هزینه صرفه‌جویی می‌کند، بلکه باعث کاهش احتمال از دست رفتن اطلاعات ناشی از شکست تک نقطه‌ای، می‌شود. زیرا رونوشت‌های دفترکل میان تمام شرکت‌کنندگان در شبکه هماهنگ می‌شود. این دفترکل دنباله‌ای از بلوک‌ها است، همان‌گونه که در شکل ۱ به تصویر کشیده شده است. این بلوک‌ها از طریق مقدار چکیده‌هایشان به ترتیب وقوع زمانی برای یکپارچگی داده‌ها و حفظ ترتیب زمانی به‌هم متصل می‌شوند. هر بلوک شامل مجموعه‌ای از تراکنش‌های رقمی امضاء شده توسط مالکانشان است.

شکل ۱- نمونه‌ای از زنجیره بلوکی شامل دنباله‌ای از بلوک‌ها

اتریوم یک زنجیره بلوکی محبوب بعد از بیت کوین است. این زنجیره بلوکی یک نوع رمز ارز به نام اتر را برای انجام معاملات مالی و هم‌چنین پردازش برنامه‌های غیرمتمرکز ارائه می‌دهد. یک زنجیره بلوکی اتریوم شبیه به زنجیره بلوکی بیت کوین است. تفاوت اصلی در این است که بلوک‌های اتریوم نه‌تنها تعداد بلوک، سختی کار و تک شمار را شامل می شود بلکه لیست معاملات و جدیدترین حالت را نیز شامل می‌شود. برای هر تراکنش در لیست تراکنش‌ها، حالت جدید با اعمال حالت قبلی ایجاد می‌شود. سرآیند بلوک در اتریوم متشکل از چکیده ۲۵۶ بیتی سرآیند بلوک والدین، آدرس گیرنده هزینه معدن، چکیده ریشه‌های درختان حالت، معامله و رسیدها، سختی بلاک، میزان گاز فعلی بلوک، عددی برای نمایش کل گاز مورد استفاده در معاملات بلوک، مهر زمانی و چندین هشدار اضافی برای اهداف تأیید است. ویژگی اصلی این پلت فرم تورینگ کامل است، به این معنی که اتریوم از انواع محاسبات پیچیده ازجمله حلقه‌ها پشتیبانی می‌کند. همچنین اتریوم از حالت معامله و چندین پیشرفت دیگر در ساختار زنجیره بلوکی پشتیبانی می‌کند.

همانطورکه بیان شد اتریوم نمایانگر یک زنجیره بلوکی با زبان برنامه‌نویسی تورینگ کامل است. این امر لایه انتزاعی را فراهم می‌کند و به هر کسی امکان ایجاد قوانین خاص خود برای مالکیت، قالب معاملات و توابع انتقال حالت را می‌دهد. این کار با قراردادهای هوشمند انجام می‌شود، مجموعه‌ای از قوانین رمزنگاری که فقط در صورت تحقق شرایط خاص اجرا می‌شوند. قراردادهای هوشمند اتریوم را به سکویی برای اجرای برنامه‌های غیرمتمرکز تبدیل می‌کند. قراردادهای هوشمند با استفاده از یک سیستم‌عامل معروف به نام ماشین مجازی اتریوم توسط گره‌های شرکت‌کننده اجرا می‌شوند. هر گره در شبکه اتریوم تحت ماشین مجازی اتریوم اجرا می‌شود و دستورالعمل‌های آن را اجرا می‌کند. قراردادهای هوشمند به کد ماشین مجازی اتریوم ترجمه‌شده و توسط گره‌ها اجرا می‌شوند. ماینرها در شبکه اتریوم داده‌ها را تکثیر کرده، به آن‌ها اعتبار داده و ذخیره می‌کنند؛ مانند بیت کوین، عملیات استخراج معادن از تشکیل و اعتبار دهی بلوک‌ها تشکیل می‌شود. اندازه بلوک اتریوم کمتر از بلوک بیت کوین است و زمان اعتبار سنجی در شبکه اتریوم، تنها چهارده ثانیه است. درحالی‌که در بیت کوین، ده دقیقه طول می‌کشد. همچنین سامانه پاداش اتریوم با بیت کوین متفاوت است.

۳. احراز اصالت در اینترنت اشیاء

در اینترنت اشیاء، اطمینان از صحت هویت دستگاهی که به شبکه دسترسی پیدا می‌کند، از ارکان اصلی امنیتی است. احراز هویت مکانیسمی است که توسط آن شبکه مشخص می‌کند آیا کاربر به منابع خاصی دسترسی دارد یا خیر. معماری احراز اصالت مناسب اینترنت اشیاء برای اطمینان از پایداری و مقاومت در برابر اکوسیستم باید الزامات امنیتی بی‌شماری را برآورده کند. در ادامه اهداف اصلی امنیتی و معیارهای موردنیاز برای ارزیابی مناسب بودن برنامه‌های تأیید اعتبار به‌منظور ایمن‌سازی دستگاه‌های اینترنت اشیاء معرفی می‌شود [10].

- یکپارچگی : یکپارچگی نیاز اساسی است که هر طرح باید از آن اطمینان داشته باشد. یکپارچگی به دو بخش تقسیم می شود.

۱. یکپارچگی پیام‌ها (معاملات / ارتباطات): یک پیام مبادله شده نباید در هنگام انتقال شبکه تغییر یا اصلاح شود.

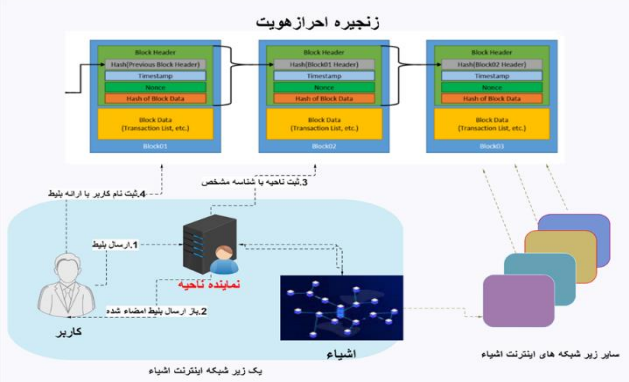
۲. یکپارچگی داده‌ها: شامل حفظ ثبات و امانت داده‌ها در کل چرخه زندگی آن‌ها است؛ بنابراین، فقط کاربران مجاز می‌توانند داده‌های ذخیره‌شده را تغییر دهند.

- در دسترس بودن : در دسترس بودن به معنای دسترسی به منابع قانونی در صورت تقاضا است؛ بنابراین، یک سیستم باید در برابر حملات انکار خدمات بخصوص حملاتی که سرویس تأیید اعتبار را هدف قرار می‌دهند، مقاوم باشد.
- مقیاس‌پذیری : مقیاس پذیری نشان می‌دهد که اندازه سیستم هیچ تاثیری در عملکرد آن ندارد. به‌عنوان‌مثال، با افزایش تعداد موارد استفاده‌شده، زمان لازم برای عملکرد سامانه اینترنت اشیاء مانند سرویس تأیید اعتبار نباید افزایش یابد.
- عدم تکذیب :عدم تکذیب به توانایی اطمینان از اینکه یک نهاد نمی‌تواند منکر انجام یک عمل خاص باشد، اشاره دارد. به‌طور مثال یک دستگاه نمی‌تواند پیام ارسال‌شده را انکار کند.
- تعیین اصالت : تعیین اصالت در اکثر موارد استفاده اینترنت اشیاء یک نیاز اصلی است. تعیین اصالت برخلاف گمنامی است. گمنامی تضمین می‌کند که هر نهاد از شبکه برای همه افراد سامانه ناشناس است. به‌عنوان‌مثال، در سناریوی پارکینگ هوشمند، هنگامی‌که یک حس‌گر در محل پارکینگ یک اعلان ارسال می‌کند، سیستم مدیریت باید دقیقاً بداند که کدام حس‌گر در حال برقراری ارتباط است تا بتواند پارکینگ را به‌روز کند.
- احراز اصالت متقابل : احراز اصالت مکانیسم اثبات اصالت است. احراز اصالت متقابل بیانگر شرایطی است که هر دو طرف ارتباط گیرنده یکدیگر را تصدیق می‌کنند. این شرط لازم برای مصون ساختن سیستم در برابر شنودگرها است.

۴. ارائه طرح احراز اصالت متقابل سبک‌وزن مبتنی‌بر زنجیره بلوکی

طرح‌های متداول احراز اصالت ارائه شده در شبکه‌های اینترنت اشیاء شامل سه بخش، اشیاء، کاربر و دروازه به منظور تسهیل ارتباط بین طرفین است. همانطور که در بخش مقدمه بیان شد دروازه نقش میانجی در طرح‌های احراز اصالت را دارد زیرا یکی از وظایف آن ترجمه پیام‌های مبادله شده در پروتکل است. هدف اصلی در این مقاله حذف دروازه به عنوان خدمت‌رسان متمرکز و تاثیر گذار در احراز اصالت و اجرای مراحل احراز اصالت با استفاده از قراردادهای هوشمند بر روی زنجیره بلوکی است. در طرح پیشنهادی، شبکه اینترنت اشیاء به چندین زیر شبکه از دستگاه‌ها تقسیم شده است، که هریک از این زیر شبکه‌ها که در یک موقعیت مکانی قرار گرفته و باید یک نماینده ناحیه برای آن‌ها تعریف شود. هر زیرشبکه اینترنت اشیاء شامل دستگاه‌ها، کاربران و یک نماینده ناحیه برای تائید اعضای ناحیه است. هر کاربر فقط با دستگاه‌های ناحیه‌ای که در آن ثبت‌نام می‌کند، ارتباط برقرار می‌کند و دستگاه‌های غیر عضو محافظت شده و غیرقابل

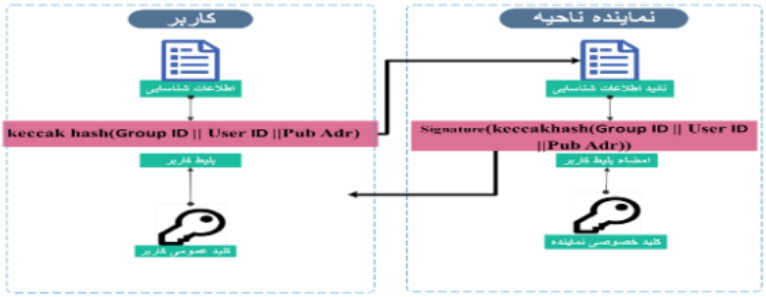
دسترسی است. ارتباطات موجود در سامانه به عنوان معاملات در نظر گرفته می‌شود و باید مورد تأیید زنجیره بلوکی قرار گیرد تا در سامانه اعمال شود.



شکل ۲- طرح احرازاصالت پیشنهادی مبتنی بر زنجیره بلوکی

شکل ۳- نحوه ایجاد آدرس کاربر [11].

شکل ۲ مراحل کلی در طرح احراز اصالت پیشنهادی و مدل شبکه را نشان می‌دهد. همانطورکه ذکر شد یک دستگاه به عنوان نماینده هر ناحیه، صاحب یک جفت کلید خصوصی / عمومی تعیین می‌شود که می‌تواند شبیه به یک مرکز صدور گواهینامه برای امضاء بلیط باشد. درفاز اول این طرح که شامل موارد ۱ و۲ در شکل ۲ است، هر کاربر یا شیء، که بخشی از سامانه را تشکیل می‌دهد یک جفت کلید خصوصی / عمومی منحنی بیضوی[۱۵] ایجاد می کند. سپس، باید ساختاری به نام بلیط را تهیه کند، که نشان دهنده یک گواهی سبک وزن ۶۴ بایتی شامل شناسه گروه، شناسه کاربر و آدرس عمومی کاربر است. آدرس عمومی کاربر، بیست بایت کم-ارزش چکیده کلید عمومی کاربر با الگوریتم چکیده ساز keccak-256 است. شکل ۳ نحوه ایجاد آدرس کاربر را نشان می‌دهد. همانطور که در شکل ۴ مراحل فاز اول نمایش داده می‌شود، کاربر بلیط ارائه‌شده را به نماینده ناحیه ارسال می‌کند، اگر نماینده بلیط را تائید کرد آن را امضاء کرده و برای کاربر ارسال می-کند.



شکل ۴- مراحل تخصیص بلیط معتبر به کاربر

در فاز دوم طرح که مرحله سوم در شکل ۲ است، نواحی بر سطح زنجیره بلوکی ایجاد می‌شوند. نماینده ناحیه یک تراکنش شامل شناسه خود و شناسه گروهی که می‌خواهد ایجاد کند به زنجیره بلوکی ارسال می‌کند. زنجیره بلوکی هر دو شناسه را بررسی می‌کند اگر معتبر باشند، ناحیه مورد نظر ایجاد می‌شود. مرحله چهارم در شکل ۲ فاز سوم طرح احراز اصالت پیشنهادی است، در این مرحله کاربرهای گروه تراکنش را به‌منظور پیوستن به ناحیه مورد نظر به زنجیره بلوکی ارسال می‌کنند. بر روی زنجیره بلوکی، قرارداد هوشمند، شناسه کاربران را بررسی نموده، سپس اعتبار بلیط کاربر را با استفاده از کلید عمومی گره نماینده ناحیه ارزیابی می‌کند، اگر شناسه کاربر یا امضای گره نماینده ناحیه معتبر نباشد، کاربر درخواست دهنده نمی‌تواند به ناحیه بپیوندد.

۵. شبکه اتریوم خصوصی پیشنهادی برای طرح ارائه‌شده

طرح احراز اصالت ارائه‌شده در این مقاله بر بستر زنجیره بلوکی خصوصی اتریوم توسعه می‌یابد، با توجه به ویژگی‌های زنجیره بلوکی خصوصی شامل پردازش کم، سرعت بالا در معاملات و شناسایی گره‌ها، این نوع زنجیره، مناسب برای شبکه‌های اینترنت اشیاء است. طرح احراز اصالت ارائه‌شده در شبکه خصوصی اتریوم بر اساس منطق نوشته شده در قرارداد هوشمند اجرا می‌شود. در عمل اجرای قراردادهای هوشمند نمونه‌ای از انجام معامله است. هر زمان که از یک قرارداد هوشمند در یک معامله استفاده شود، تمام گره‌های کامل باید تمام دستورالعمل‌ها را اجرا کنند تا اطمینان حاصل شود که آن‌ها در حالت صحیح و توافق شده بعدی زنجیره بلوکی قرار می‌گیرند. هر گره معدنچی[۱۶] لیستی از معاملات معلق را از صندوق معامله انتخاب کرده و این معاملات را از جمله درج و اجرای کد قرارداد هوشمند، انجام می‌دهد. نتایج حاصل از اعمال فوق باعث تعادل حساب‌ها و داده‌های ذخیره شده با کد قرارداد هوشمند می شود. معاملات و داده‌های به‌روز شده توسط گره معدنچی از طریق یک پروتکل اجماع در یک بلوک بسته بندی می‌شوند و در شبکه ارسال می‌شوند. هر گره کامل[۱۷] دریافت‌کننده این بلوک توزیع‌شده معاملات و کد قرارداد هوشمند را به ترتیبی که توسط گره برنده مشخص شده‌است، انجام می‌دهد و تغییرات ناشی از موجودی حساب و داده های ذخیره‌شده با کد قرارداد هوشمند را ثبت می‌کند. سپس درستی الگوریتم اثبات کار[۱۸] را بررسی می‌کند. اگر درست باشد بلوک را به زنجیره خود اضافه می‌کند. در نتیجه همه گره‌های کامل باید کد و معاملات را انجام دهند و اثبات کار معتبر در روند اجماع را قبل از پذیرش بلوک به‌عنوان بلوک زنجیره، تائید کنند.

از آنجا که زنجیره بلوکی توسعه یافته از نوع خصوصی است، پیوستن به این شبکه نیاز به مجوز دارد، خواندن هر داده‌ای که در زنجیره بلوکی ذخیره می‌شود، عمومی است. در این طرح، کاربران، اشیاء، نماینده ناحیه و صاحبان منابع به‌عنوان گره عمل می‌کنند، اگرچه همه آن‌ها لزوماً کل زنجیره بلوکی را ذخیره نمی‌کنند و در پروتکل اجماع شرکت نمی‌کنند. صاحبان

منابع، نماینده ناحیه و برخی از کاربران و اشیاء با قدرت پردازش و فضای ذخیره‌سازی بالا، گره‌های کامل هستند و با شرکت در ذخیره‌سازی بلوک‌ها امنیت زنجیره بلوکی را کامل تضمین می‌کنند. کاربران و اشیاء با توان محدود به عنوان گره سبک[۱۹] در شبکه قرار می‌گیرند و سطح امنیت کمتری را برای زنجیره بلوکی بررسی می‌کنند. آن‌ها به عنوان یک گره سبک به یک گره کامل زنجیره بلوکی وصل می‌شوند که معاملاتشان را در شبکه زنجیره بلوکی پخش کند. البته در شبکه-های اینترنت اشیاء زمانی که اشیاء از قدرت پردازش بالایی برخوردار باشند می‌توان آن‌ها را به عنوان گره کامل نیز در نظر گرفت زیرا بار محاسباتی در زنجیره بلوکی خصوصی به علت کمتر بودن گره‌ها و راندمان بالای الگوریتم اجماع به مراتب کمتر از زنجیره بلوکی عمومی است.

با تعاریف ارائه‌شده از انواع گره‌های در شبکه اتریوم و نحوه عملکرد آن‌ها در زنجیره، مشخص است که همه آن‌ها در ثبت و امنیت داده‌های زنجیره شرکت می‌کنند. اما با توجه به‌اینکه گره‌های کامل قراردادهای هوشمند را اجرا می‌کنند، در این طرح هر گره کامل زنجیره احراز اصالت معرفی شده در شکل ۲ است. هر گره کامل به‌عنوان زنجیره اصالت می‌تواند در نقش معدنچی فعالیت می‌کند، اما با توجه به نیاز بی‌درنگ بودن رویدادها در اینترنت اشیاء باید تعداد معدنچیان طوری انتخاب شود که سختی و زمان اجماع کم باشد. با توجه به سرعت مورد نیاز برای شبکه می‌توان تعداد معدنچیان را تنظیم کرد. نماینده ناحیه به عنوان یک گره کامل قرارداد هوشمند را مستقر می‌کند. پس از اضافه شدن قرارداد به زنجیره احراز اصالت، کاربران و اشیاء می‌توانند با فراخوانی توابع عمومی منحصربه‌فرد خود، با آن تعامل برقرار کنند. تعامل با قراردادهای هوشمند، مشتری‌ها و اشیاء از طریق معاملات انجام می‌شود.

۶. توسعه طرح احراز اصالت پیشنهادی با استفاده از برنامه غیرمتمرکز اتریوم

برنامه غیرمتمرکز ارائه‌شده برای پروتکل احرازاصالت اینترنت اشیاء در این مقاله براساس قراردادهای هوشمند و ویژگی‌های امنیتی فن‌آوری زنجیره بلوکی است. این پروتکل از زنجیره بلوکی استفاده می‌کند، تا کاربران بتوانند به‌جای اینکه با یک واسط متمرکز ارتباط برقرار کنند، در سطح همتا به همتا با یکدیگر ارتباط برقرار کنند. در این طرح از شبکه خصوصی اتریوم استفاده می‌شود، پلتفرم اتریوم به دلیل امنیت و انعطاف پذیری موجود، کامل بودن و بلوغ ابزارهای توسعه موجود، برای ایجاد این برنامه غیرمتمرکز ارجحیت داشته است. برای توسعه برنامه غیرمتمرکز از محیط توسعه ترافِل[۲۰] استفاده می‌شود، برنامه در دو ماژول جداگانه پشتیبان و توسعه رابط کاربری اجرا می‌شود. بخش پشتیبان از قراردادهای هوشمند و بستر اتریوم، ایجاد می‌شود. بخش توسعه رابط کاربری شامل برنامه متاماسک[۲۱] و برنامه وب است که بر روی مرورگر کاربر اجرا می‌شود و به‌طور مستقیم با بخش پشتیبان در زنجیره بلوکی تعامل دارد. در بخش پشتیبان، از GanacheCLI استفاده می‌شود، که یک ابزار اتریوم برای اهداف آزمایش و توسعه است و تعامل با زنجیره بلوکی را، بدون پردازش لازم برای اجرای یک گره واقعی اتریوم شبیه‌سازی می کند. بخش GanacheCLI دقیقاً به روش شبکه اتریوم عمل می‌کند. قراردادهای هوشمند به زبان برنامه‌نویسی سالیدی، یک زبان سطح بالا و با هدف اجرا توسط ماشین مجازی اتریوم نوشته می‌شود. برای تعامل بین گره‌های انتهایی و زنجیره بلوکی، از متاماسک استفاده می‌شود، که داده‌ها در ارسال به /دریافت از زنجیره بلوکی رمزگذاری/رمزگشایی می‌کند. این فعل و انفعالات با استفاده از پروتکل تماس از راه دور[۲۲] فراخوانی محقق می‌شوند.

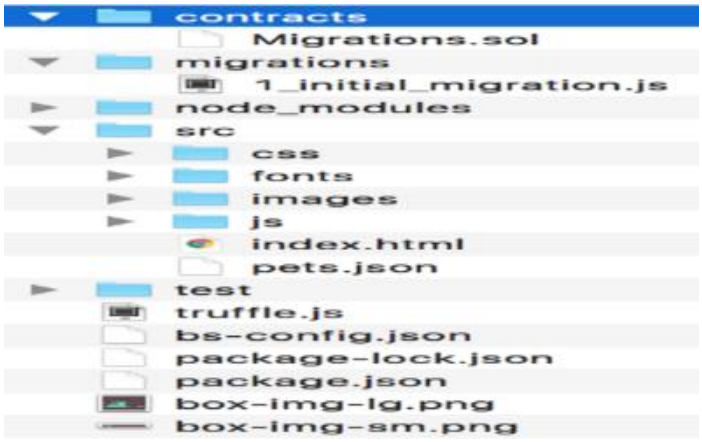
۶,۱ محیط توسعه ترافل

ترافِل یک محیط توسعه مبتنی بر زنجیره بلوکی اتریوم است، که برای توسعه برنامه‌های توزیع شده استفاده می‌شود. ترافِل یک راه حل برای ایجاد برنامه‌های غیرمتمرکز است که کارهای زیر را انجام می‌دهد.

- ✓ کامپایل قراردادهای هوشمند
- ✓ استقرار قراردادهای هوشمند بر روی زنجیره بلوکی

- ✓ ایجاد امکان برقراری ارتباط با قراردادهای هوشمند هم از طریق کنسول هم از طریق برنامه های تحت وب
- ✓ ایجاد رابط گرافیکی کاربری
- ✓ تست برنامه

پس از نصب ترافِل و وارد کردن دستورات برای اجرای آن در فایل مورد نظر، ترافِل یک معماری از پیش تعریف شده برنامه غیرمتمرکز مانند شکل ۵ ایجاد می‌کند. که با اعمال تغییرات و استقرار برنامه‌های مربوط در هر یک از فایل ها، برنامه غیر متمرکز موردنظر ایجاد می‌شود.



شکل (۵) : محیط توسعه ترافِل.

۶,۲ایجاد قرارداد هوشمند

به‌منظور اجرای طرح احراز اصالت پیشنهادی با توسعه برنامه غیرمتمرکز پس از استقرار محیط توسعه تِرافل و شبکه محلی اتریوم با استفاده کلاینت GanacheCLI، باید قرارداد هوشمند نوشته شده را روی زنجیره بلوکی مستقر نمود. همانطور که قبلا اشاره شد برنامه‌های غیرمتمرکز بر اساس قوانین و شرایط نوشته شده در قراردادهای هوشمند عمل می‌کنند، در نتیجه توابع و شرایط لازم برای اجرای پروتکل احرازاصالت مبتنی بر زنجیره بلوکی و شناسه باید در قرارداد هوشمند نوشته شوند.

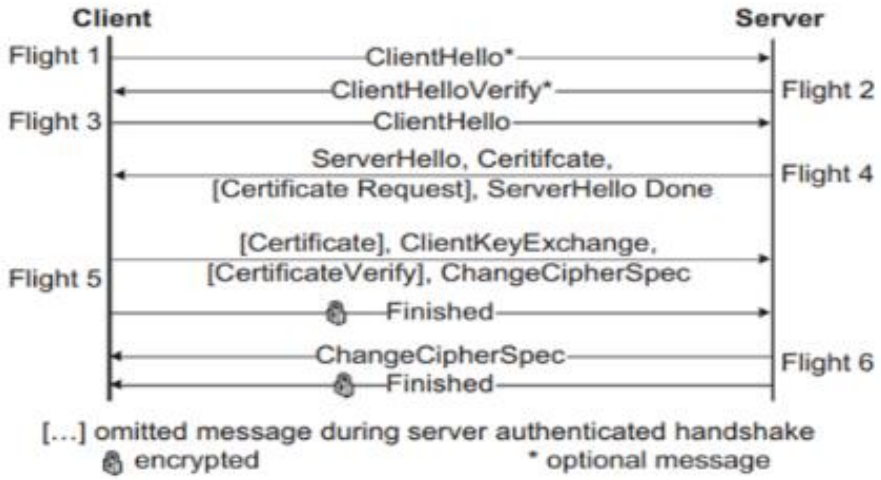
پس از ایجاد قرارداد هوشمند و ارسال از طریق معامله به زنجیره بلوکی ، قرارداد باید توسط معدنچیان تائید شود. اگر معامله تائید شود. پس از آن، صاحب قرارداد یک آدرس دریافت می‌کند، که به قرارداد در زنجیره بلوکی اشاره می‌کند. این آدرس عمومی است و بدون هیچ محدودیتی توسط هر کاربر قابل استفاده است. بخش اصلی پروتکل پیشنهادی تائید بلیط کاربر است. این تابع بر اساس ویژگی تائید اعتبار امضاء در برنامه‌های توزیع شده در شکل ۶ آمده است، کار می‌کند. سالیدیتی یک روش تائید امضای دیجیتال مبتنی بر خم بیضوی[۲۳] با تابع(recover) ، ارائه می‌دهد که آدرس کاربر را برمی‌گرداند. اگر آدرس برگشتی برابر با آدرس امضاء کننده باشد، امضاء معتبر است. پس از ارسال قرارداد هوشمند به زنجیره بلوکی، کد قراردادهای هوشمند نهایی است و قابل تغییر نیست. بنابراین، در زمان توسعه قراردادهای هوشمند، در فرآیند آزمایش احتیاط بیشتری به عمل آمد تا هر چه بیشتر اشکالات شناسایی و برطرف شود. برای توسعه قراردادها با زبان سالیدیتی در مرورگر وب مبتنی بر IDE از "Remix" استفاده می‌شود.

```
pragma solidity ^0.5.2;

contract test {

  function test() {
  }

  function verify(bytes32 _message, uint8 _v, bytes32 _r, bytes32 _s) constant returns (address) {
    address signer = ecrecover(_message, _v, _r, _s);
    return signer;
  }
 {
 var r = `0x${sig.slice(0, 64)}
 var s = `0x${sig.slice(64, 128)}
 var v = web3.toDecimal(sig.slice(128, 130)) + 27
}
```

شکل (٦) : تابع تائید امضاء

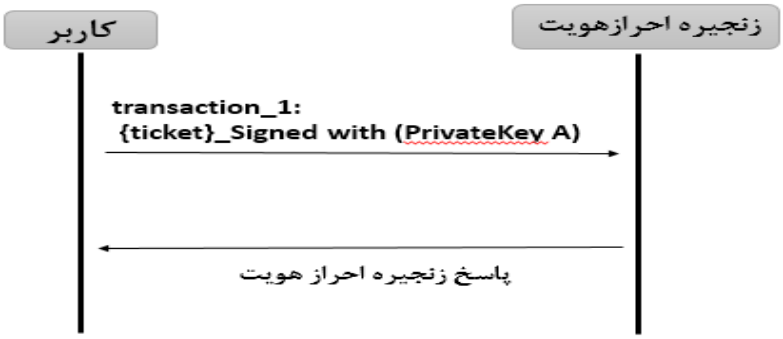
٦,٣ تحلیل و ارزیابی طرح پیشنهادی

معیارهای عملکرد سیستم مانند توان و تأخیر عمدتاً به پلت‌فرم استفاده شده برای زنجیره بلوکی بستگی دارند، درنتیجه این جزئیات در اینجا مورد بحث قرار نمی‌گیرد. بنابراین طرح احرازاصالت پیشنهادی با روش‌های احرازاصالت که به یک مرحله پیوستن متکی هستند، مقایسه می‌شود. طرح‌های احرازاصالت ارائه‌شده در [13,14]، که متکی به یک مرحله پیوستن هستند، براساس الگوریتم پروتکل امنیت لایه ترابُرد دیتاگرام[۲۴] پیشنهاد می‌شوند. پروتکل امنیت لایه ترابُرد دیتاگرام یک پروتکل ارتباطی است که امنیت برنامه‌های مبتنی بر دیتاگرام را برای جلوگیری از استراق سمع، دستکاری یا جعل پیام فراهم می‌کند. در پروتکل امنیت لایه ترابُرد دیتاگرام مرحله پیوستن یا دستداد حداقل به پنج پیام نیاز دارد (شکل ۷). علاوه‌بر این، پیام‌های دیگری نیز مانند پیام تغییر متن رمز نگاری اضافه می‌شوند. سرانجام، مرحله پیوستن می‌تواند شامل هشت پیام باشد.



شکل (۷) : مرحله دستداد پروتکل امنیت لایه ترابُرد دیتاگرام[14].

همانطور که در شکل ۸ مشاهده می‌شود، در روش پیشنهادی مرحله پیوستن فقط به دو پیام نیاز دارد. (۱) ارسال معامله از طرف کاربر یا شیء به زنجیره احرازاصالت. (۲) پاسخ زنجیره احراز اصالت. هرچه تعداد پیام‌ها کمتر باشد، مصرف سیستم به‌ویژه برای دستگاه‌هایی با توان محدود محاسباتی، کمتر است.



شکل (۸) : تعداد پیام‌ها در مرحله پیوستن پروتکل پیشنهادی.

به‌عنوان یک تحلیل نظری از هزینه‌های محاسباتی مورد نیاز در پروتکل پیشنهادی، اگر امضای دیجیتال مبتنی‌بر خم بیضوی به‌عنوان S و تأیید امضاء به عنوان V، مرحله اولیه پیوستن نیاز به ۲ S و۲ V دارد و در مراحل بعدی که کاربر نیاز به ارائه بلیط ندارد، تنها به یک S و یک V نیاز است.

٦,٤ مقایسه با کارهای مرتبط

در زنجیره بلوکی‌های عمومی ناشناس بودن کامل کاربران تضمین می‌شود، که در این حالت هر مهاجم مخربی می‌تواند از سامانه استفاده کند. این روش نیاز اصلی شبکه‌های اینترنت اشیاء به شناسایی کاربرها را دچار مشکل می‌کند. راه حل این مشکل استفاده از زنجیره بلوکی خصوصی است، همانطور که اشاره شد پیوستن به این زنجیره نیاز به مجوز دارد. طرح پیشنهادی همانند طرح‌های ارائه‌شده در [5،4و7] نوع زنجیره بلوکی خصوصی است، اما در [6] زنجیره بلوکی عمومی استفاده شده است.

معماری اینترنت اشیاء با دستگاه‌هایی با محدودیت منابع، همواره مانع اصلی در ادغام اینترنت اشیاء با زنجیره بلوکی است. زیرا الگوریتم‌های اجماع باید برای کار در این محدودیت ها طراحی شوند. در پروتکل ارائه‌شده برای ماهواره‌های لئو[3] برای حل این مشکل الگوریتم اجماع از طرح حذف شده و فرض شده زنجیره بلوکی محلی از اطمینان کامل برخوردار است. در [4] شبکه خصوصی اتریوم با چهار معدنچی پیاده‌سازی شده است که این شبکه شامل دستگاه‌های اینترنت اشیاء نمی‌شود، در نتیجه به‌طور قطع پردازش الگوریتم اجماع در آن کم است، اما علاوه بر نبودن دستگاه‌ها در زنجیره، نحوه قرارگیری معدنچیان در مقیاس بزرگ در نظر گرفته نشده است. در [5] نیز معدنچیان در خارج از خانه‌های هوشمند قرارگرفته‌اند و فقط دروازه ورودی هر خانه به‌عنوان گره سبک در شبکه خصوصی اتریوم هستند. در نتیجه دستگاه‌ها را کاملا از فرآیند اجماع خارج کرده‌است. در [7] صاحبان منبع می‌توانند به‌عنوان گره کامل در اجماع شرکت کنند، ولی دستگاه‌ها در زنجیره بلوکی شرکت نمی‌کنند. دراین مقاله دستگاه‌ها به‌عنوان گره در زنجیره بلوکی شرکت می‌کنند، دستگاه‌ها با توان محدود به‌عنوان گره سبک و دستگاه‌ها با توان بالا به‌عنوان گره کامل و معدنچی می‌توانند فعالیت کنند و طراحی شبکه خصوصی اتریوم با تعداد گره کمتر نسبت به زنجیره بلوکی‌های عمومی و انتخاب معدنچیان و گره-

های سبک در این شبکه با حفظ تعادل میان امنیت و میزان پردازش مورد نیاز پیشنهاد می‌شود. جدول ۱ مقایسه‌ای میان طرح‌های مروری فصل دو و طرح پیشنهادی را نشان می‌دهد.

جدول (۱) : مقایسه میان طرح پیشنهادی و کارهای مرتبط

	نوع زنجیره بلوکی	شناسایی	قرارداد هوشمند	مقیاس پذیری	سربارمحاسباتی در الگوریتم‌های اجماع	دستگاه به‌عنوان گره زنجیره بلوکی	گره سبک
[3]	مشخص نشده	✓	☒	✓	حذف الگوریتم اجماع	✓	☒
[4]	خصوصی	✓	✓	✓	به علت تعداد گره‌های کمتر در شبکه خصوصی میزان محاسبات کم است.	☒	☒
[5]	خصوصی	✓	✓	✓	به علت تعداد گره‌های کمتر در شبکه خصوصی و انتخاب مناسب معدنچیان میزان محاسبات کم است.	☒	✓
[6]	عمومی	☒	✓	☒	به علت استفاده از زنجیره بلوکی عمومی میزان محاسبات زیاد است.	☒	☒
[7]	خصوصی	✓	✓	✓	به علت تعداد گره‌های کمتر در شبکه خصوصی و انتخاب مناسب معدنچیان میزان محاسبات کم است.	☒	✓
طرح ارائه شده در مقاله	خصوصی	✓	✓	✓	به علت تعداد گره‌های کمتر در شبکه خصوصی و انتخاب مناسب معدنچیان میزان محاسبات کم است.	✓	✓

۶,۵ تحلیل امنیتی

امنیت طرح پیشنهادی ما به استحکام الگوریتم اجماع زنجیره بلوکی متکی است. با فرض اینکه الگوریتم اجماع اتریوم از امنیت بالایی برخوردار است، به تحلیل نحوه عملکرد طرح احراز اصالت ارائه شده، در الزامات امنیتی پرداخته می‌شود.

- ✓ احراز اصالت متقابل و یکپارچگی پیام‌ها : هر یک از کاربرها و اشیاء از بلیط که معادل یک گواهی است، برای اولین اتصال به شبکه استفاده می‌کنند. بلیط فقط در مرحله اول ثبت‌نام به کاربران و اشیاء قانونی تعلق می‌گیرد. تمام پیام‌های انتقالی با استفاده از الگوریتم امضای دیجیتال مبتنی‌بر منحنی بیضوی توسط کلیدهای خصوصی مرتبط با آن بلیط‌ها، امضاء می‌شوند. بنابراین، با بررسی امضاءها از اصالت کاربر(دستگاه) و همچنین صحت پیام‌ها اطمینان حاصل می‌شود. علاوه‌بر این، حفظ یکپارچگی پیام‌ها در دو سطح، از مهم‌ترین ویژگی‌های زنجیره بلوکی است.

- ✓ شناسایی : علاوه بر سطح اول شناسایی که در زنجیره بلوکی خصوصی یا مجوز دار محقق می‌شود، هر کاربر(شیء) دارای یک اصالت متشکل از شناسه خود، شناسه گروه و آدرس عمومی‌اش است. تائید اعتبار این اصالت با امضاء نماینده ناحیه در بلیط تضمین می‌شود. هر پیام ارسالی از یک کاربر یا شیء با کلید خصوصی مرتبط با اصالت آن امضاء می شود. در نتیجه، سامانه به راحتی می‌تواند کاربر را شناسایی کند.
- ✓ انکارناپذیری : از آنجا که پیام‌ها با استفاده از کلید خصوصی، که فقط توسط کاربر صاحب آن شناخته شده است، امضاء می‌شود، فقط این مالک است که می‌تواند از آن استفاده کند. بنابراین، نمی‌تواند واقعیت امضای پیام را انکار کند.
- ✓ مقیاس پذیری : سیستم ارائه‌شده به یک زنجیره بلوکی خصوصی متکی است. امکان اضافه کردن گره‌ها و خدمات در صورت تقاضا می‌تواند مزیت بزرگی را برای شبکه ایجاد کند و هم‌چنین شبکه‌های همتا به همتایکی از بهترین راه‌حل‌ها برای مقیاس-پذیری در مقیاس بزرگ است.
- ✓ محافظت در برابر حمله سیبل : در طرح ارائه‌شده، هر کاربر می‌تواند تنها یک اصالت داشته باشد و هر اصالت می‌تواند در یک زمان مشخص فقط یک جفت کلید داشته باشد. هر پیام ارتباطی باید توسط کلید خصوصی مرتبط با این اصالت امضاء شود. علاوه‌بر این، تمام اصالت‌ها باید توسط سامانه تأیید شوند. بنابراین، یک مهاجم نمی‌تواند از اصالت‌های جعلی استفاده کند.
- ✓ محافظت از حمله جعل اصالت : همانطور که برای حفاظت از حمله سیبل توضیح داده شده است ، یک مهاجم نمی‌تواند اصالت شیء دیگری را جعل کند، زیرا به کلید خصوصی آن احتیاج دارد.
- ✓ محافظت از جانشینی پیام : از آنجا که تمام پیام‌ها امضا شده اند، اگر یک مهاجم پیام را تغییر داده یا جایگزین کند، باید آن را با یک کلید خصوصی معتبر امضا کند. با این وجود ، در مرحله اولیه فقط به اشیاء معتبر بلیط و جفت کلید معتبر داده می‌شود.
- ✓ محافظت از حمله تکرار پیام : همه پیام ها به عنوان معاملات در نظر گرفته می شوند. هر معامله دارای یک نشانگر زمانی است و برای اعتباردهی به آن نیاز به یک مرحله اجماع است. بنابراین، یک مهاجم نمی تواند پیام ها را تکرار کند، زیرا ساز و کار اجماع آن‌ها را رد می‌کند.
- ✓ حریم شخصی : به‌دلیل استفاده از زنجیره بلوکی با مجوز، فقط کاربران مجاز راه‌یافته به شبکه می‌توانند معاملات را بخوانند و محرمانگی در مقابل اعضای خارج شبکه حفظ می‌شود، اما همه معاملات ذخیره‌شده در بلوک‌ها توسط اشخاص داخل شبکه قابل خواندن است. در نتیجه حریم شخصی کاربر در داخل شبکه محافظت نمی‌شود.
- ✓ نقش شخص سوم در مراحل احرازاصالت : در طرح ارائه شده کاربر و شیء فقط در مرحله تولید بلیط به نماینده وابسته هستند، اگر یک نماینده از دسترس خارج شود، عملکرد پروتکل به جزء افزودن دستگاه‌های جدید مختل نمی‌شود.

۷. نتیجه

در این مقاله، به ادغام زنجیره بلوکی با اینترنت اشیاء پرداخته شده است و با بررسی ساختار زنجیره بلوکی و نحوه به-کارگیری آن در اینترنت اشیاء طرح احراز اصالت مبتنی بر زنجیره بلوکی و مقاوم در برابر تغییر داده‌ها و جعل اصالت ارائه شد. در این طرح زنجیره احراز اصالت بجای دروازه در طرح‌های متداول قرار می‌گیرد و با پیشنهاد نحوه به‌کارگیری گره-های کامل، معدنچیان و گره‌های سبک زنجیره‌ای خصوصی با حفظ تعادل میان امنیت ، پردازش و زمان مورد نیاز پیشنهاد شد. با به‌کارگیری اشیاء دارای توان محدود در زنجیره بلوکی با استفاده از گره‌های سبک اتریوم می‌توان دستگاه‌های توان محدود اینترنت اشیاء را در زنجیره بلوکی قرارداد.

طرح پیشنهادی با برنامه غیرمتمرکز اتریوم با کمک ابزار ترافل و زبان برنامه نویسی سالیدیتی در ماژول پشتیبان و ابزار متاماسک و برنامه وب در بخش توسعه رابط کاربری اجرا می‌شود. در انتها طرح پیشنهادی با پژوهش‌های مرتبط از نظر نوع زنجیره بلوکی، مقیاس پذیری، گمنامی و سایر ویژگی‌ها مقایسه شده است و همچنین برای پژو هش‌های آتی موارد زیر پیشنهاد می‌شود.

- حفظ محرمانگی کاربران و اشیاء در داخل شبکه با استفاده از اعمال رمزنگاری سبک وزن بر روی تراکنش‌های شبکه.
- امکان برقراری ارتباط ایمن بین نواحی تعریف شده در طرح پیشنهادی، با طراحی مرحله انتقال در پروتکل.

- پیاده سازی مکانیسم ابطال بلیط برای دستگاه‌ها و کاربران به خطر افتاده.

۸. مراجع

[1] H. Debiao, C. Jianhua , *"An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security"*, Information Fusion, 13-3 (2012), 223–230.

[2] S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system.",* https://bitcoin.org/bitcoin.pdf, Last visited 11 Nov 2017.

[3] S. Li,M. Liu, and S.Wei, [1]*"A distributed authentication protocol using identity-based encryption and blockchain for LEO network*," in Proceedings of the International Conference on Security,Privacy and Anonymity in Computation, Communication and Storage, pp. 446–460, Springer, Cham, Switzerland, 2017.

[4] S.Nikouei, Xu. Ronghua, N.Deeraj, C.Yu, A.Alexander and B.Erik. *"Real-time index authentication for event-oriented surveillance video query using blockchain."* In 2018 IEEE International Smart Cities Conference (ISC2), pp. 8-1. IEEE, 2018.

[5] D.Konstantas, G.Spathoulas, P.Pandey, and S.Katsikas. *"Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust."* In *2018 Innovations in Intelligent Systems and Applications (INISTA)*, pp. 1-6. IEEE, 2018.

[6] H.Seyoung, S.Cho, and S.Kim. *"Managing IoT devices using blockchain platform."* In*2017 19th* international conference on advanced communication technology *(ICACT)*, pp. 464-467. IEEE, 2017.

[7] O.Alphand, M.Amoretti, T.Claeys, S.Dall'Asta and F.Zanichelli. "*IoTChain: A blockchain security architecture for the Internet of Things*." In 2018 *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6. IEEE, 2018.

[8] M. Vuˇcini´c, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti**,** *"OSCAR: Object Security Architecture for the Internet of Things,"* Ad Hoc Networks, vol. 32, pp. 3 – 16, 2015.

[9] d L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "*Authentication and Authorization for Constrained Environments (ACE***)**," Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07, Aug.2017.

[10] D. Dolev and A. Yao. "*On the security of public key protocols"*. IEEE Transactions on information theory, 29(2):198–208, 1983.

[11] Blocking**,** *How to steal the key of Ethereum wallet? (Part1***),** https://blocking.net/3520/how-to-steal-the-key-of-ethereum-wallet-part1/.

[12] T. Kothmayr, C. Schmitt, W.Hu, M.Brünig, and G.Carle**.** *"A dtls based end-to-end security architecture for the internet of things with two-way authentication"***.** In Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, pages 956–963. IEEE, 2012.

[13] K. Hartke and H. Tschofenig**.** *"A dtls 1.2 profile for the internet of things"***.** draft-ietf-dice-profile-01 (work in progress), 2014.

[14] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, *" A DTLS based end-to-end security architecture for the internet of things with twoway authentication"***.**in: Proceedings of the 37th IEEE Conference on Local Computer Networks, LCN, 2.

1

[1] Internet of Things
[2] Bottleneck
[3] Single point of failure
[4] Bitcoin
[5] Blockchain
[6] Consensus algorithm
[7] Denial of service attack
[8] LEO
[9] Key Generation Center (KGC)
[10] Smart contract
[11] Decentralized applications
[12] Ethereum
[13] Raspberry Pis
[14] End to End
[15] Elliptic Curve
[16] Miner
[17] Full nodes
[18] Proof-of-work
[19] Light nodes
[20] Truffle
[21] MetaMask
[22] RPC
[23] Elliptic Curve Digital Signature Algorithm
[24] Datagram Transport Layer