بلاک‌چین و اینترنت اشیا

رسول بوسعیدی

دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان

rasoolbousaidi@gmail.com

هانیه صولتی‌نیا

دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان

hanie.solaty@ec.iut.ac.ir

سبحان کریمی

دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان

Sobhantech۲۵۵۹@gmail.com

علی آهنگرپور

دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان

Ahangarpourali@gmail.com

مهدی علی‌پور

دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان

m.alipour@ec.iut.ac.ir

فهرست مطالب

چکیده

بلاک‌چین و اینترنت اشیا هر دو از موضوعات مهم در زمینه تکنولوژی هستند که کاربردهای زیادی دارند. هر کدام از این تکنولوژی‌ها مشکلات زیادی را برطرف کردند اما همچنان چالش‌های خودشان را دارند، ترکیب بلاک‌چین و اینترنت اشیا می‌تواند به برطرف کردن مشکلات هر دو کمک کند، اما این ادغام، خود چالش‌هایی دارد. در این تحقیق قصد داریم که ترکیب بلاک‌چین و اینترنت اشیا را بررسی کنیم. ابتدا به معرفی هر دو می‌پردازیم. سپس ترکیب این دو تکنولوژی را بررسی می‌کنیم و نگاهی به چالش‌های ایجادشده انداخته و راه‌حل های ارائه شده برای این چالش‌ها را بررسی می‌کنیم.

در ادامه به صورت متمرکز، به معرفی پلتفورم IOTA ، به عنوان راه‌حلی کاربردی، برای پاسخ به نیازهای بوجود آمده می‌پردازیم و با معماری و ساختار شبکه‌ی منحصر به فرد آن آشنا می‌شویم .

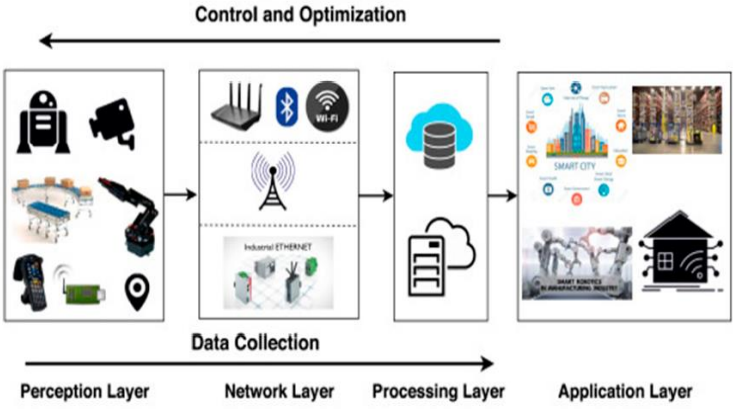
یکی از نتایج و بازخوردهای ترکیب اینترنت اشیا و بلاک‌چین، بدست آمدن داده‌های فراوان از این اشیا کوچک هوشمند است که می‌تواند موضوع جذابی برای انجام تحلیل‌هایی روی این داده‌ها باشد که شبکه بلاک‌چین می‌تواند به عمل رسیدن این فرایند را برای ما فراهم کند و با مفهومی به عنوان federated learning به عنوان بستری مناسب برای انجام این تحلیل‌ها به صورت توزیع‌شده آشنا می‌شویم.

در انتها شبکه IOTA بر روی شبکه خصوصی اجرا شده و transaction های اولیه به صورت عملی روی این شبکه تست و اجرا شد که در قسمت‌های انتهایی مقاله به گزارشی جامع بر روی پیاده‌سازی‌های انجام شده می‌پردازیم.

کلمات کلیدی: IOTA، Federated learning، بلاک‌چین، اینترنت اشیا، Data Marketplace

۱. مقدمه

اینترنت اشیا: اینترنت اشیا که اینترنت همه‌چیز یا اینترنت صنعتی نیز نامیده می‌شود، یک الگوی فناوری جدید است که به عنوان یک شبکه جهانی از ماشین‌ها و دستگاه‌هایی که قادر به تعامل با یکدیگر هستند تصور می‌شود. اینترنت اشیا به عنوان یکی از مهم‌ترین حوزه‌های فناوری آینده شناخته می‌شود و توجه گسترده‌ای را از سوی طیف وسیعی از صنایع به خود جلب کرده است. ارزش واقعی اینترنت اشیا برای شرکت‌ها زمانی قابل درک است که دستگاه‌های متصل، قادر به برقراری ارتباط با یکدیگر و ادغام با سیستم‌های موجودی مدیریت شده توسط فروشنده، سیستم‌های پشتیبانی مشتری، برنامه‌های کاربردی هوش تجاری و تجزیه و تحلیل تجاری باشند. پذیرش این فناوری به سرعت در حال افزایش است زیرا فشارهای فنی، اجتماعی و رقابتی، شرکت‌ها را به سمت نوآوری و تغییر سوق می‌دهد. با پیشرفت فناوری اینترنت اشیا و افزایش تعداد شرکت‌هایی که از این فناوری استفاده می‌کنند، تجزیه و تحلیل cost-benefit اینترنت اشیا به موضوعی بسیار مهم تبدیل شده است. شرکت‌ها باید هر فرصت و چالش مرتبط به اینترنت اشیا را به دقت ارزیابی کنند تا اطمینان حاصل کنند که منابع آن‌ها به طور عاقلانه مصرف می‌شود. [۱] [۱۳]

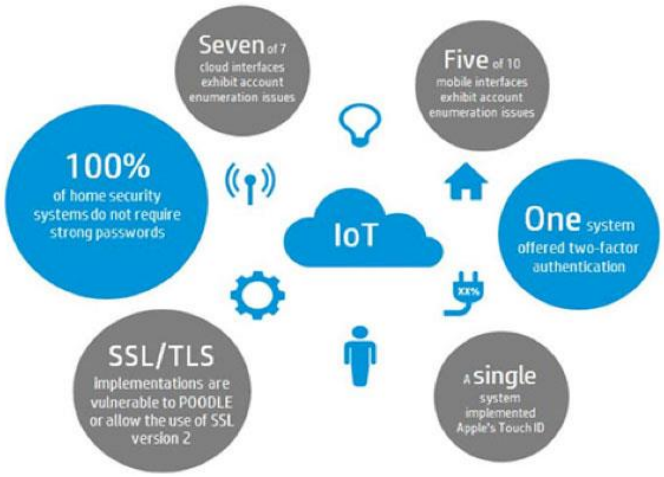


شکل ۱. معماری سیستم اینترنت اشیا تعمیم یافته

چالش‌های این حوزه: حسگرها و دستگاه‌های اینترنت حجم عظیمی از داده‌ها را تولید می‌کنند که باید پردازش و ذخیره شوند. معماری فعلی مرکزی برای مقابله با ماهیت ناهمگون و حجم انبوه داده‌های شخصی و سازمانی آماده نیست. تعداد کمی از شرکت‌ها می‌توانند روی ذخیره‌سازی داده سرمایه‌گذاری کنند تا تمام داده‌های اینترنت اشیا جمع‌آوری‌شده از شبکه‌هایشان را در خود جای دهند. در نتیجه، آنها داده‌ها را برای عملیات یا پشتیبان‌گیری بر اساس نیازها و ارزش اولویت‌بندی می‌کنند. با استفاده گسترده‌تر از دستگاه‌های اینترنت اشیا و مصرف پهنای باند بیشتر، مراکز داده برای بهبود کارایی پردازش و زمان پاسخگویی بیشتر توزیع می‌شوند.

از چالش‌های اصلی اینترنت اشیا می‌توان به پنج مورد اشاره کرد. (۱) چالش مدیریت داده: با توجه به حجم عظیم داده‌های تولیدشده، سیستم مرکزی فعلی برای مدیریت این داده‌ها مناسب نیست. (۲) چالش داده‌کاوی: همانطور که داده‌های بیشتری برای پردازش و تجزیه و تحلیل در دسترس است، استفاده از ابزارهای داده‌کاوی یک ضرورت حساب می‌شود. داده‌ها نه تنها از داده‌های گسسته سنتی، بلکه از جریان‌های داده تولیدشده از حسگرهای دیجیتال در تجهیزات صنعتی، خودروها، کنتورهای الکتریکی و جعبه‌های حمل و نقل تشکیل شده‌اند. این داده‌های جریانی در مورد مکان، حرکت، ارتعاش، دما، رطوبت و حتی تغییرات شیمیایی در هوا هستند و باید با استفاده از مدل‌های کامپیوتری و ریاضی درک شوند. (۳) چالش حریم خصوصی: دستگاه‌های اینترنت اشیا می‌توانند حجم وسیعی از داده‌ها را در مورد مکان و جابجایی کاربران اینترنت اشیا، شرایط سلامتی و مراجع خرید ارائه دهند، که همه اینها می‌تواند باعث ایجاد نگرانی‌های مهم در مورد حریم خصوصی شود. در حالی که اینترنت اشیا از طریق سیستم‌های خانه هوشمند و دستگاه‌های مختلف به شتاب خود ادامه می‌دهد، اعتماد به اینترنت اشیا و پذیرش آن به حفاظت از حریم خصوصی کاربران بستگی دارد. (۴) چالش امنیت: از آنجایی که تعداد و

تنوع دستگاه‌های متصل به شبکه‌های اینترنت اشیا رو به افزایش است، تهدید امنیتی بالقوه تشدید می‌شود. اگرچه اینترنت اشیا بهره‌وری شرکت‌ها را بهبود می‌بخشد و کیفیت زندگی مردم را افزایش می‌دهد، اما اینترنت اشیا سطوح احتمالی حمله را برای هکرها و سایر مجرمان سایبری افزایش می‌دهد. مطالعات اخیر نشان می‌دهد که بسیاری از رایج ترین دستگاه‌های اینترنت اشیا دارای آسیب‌پذیری‌های جدی هستند. دستگاه‌های اینترنت اشیا به دلیل عدم رمزگذاری حمل و نقل، رابط‌های وب ناامن، حفاظت نرم‌افزاری ناکافی و مجوز ناکافی دارای آسیب‌پذیری هستند. (۵) چالش هرج و مرج: تکامل فناوری‌های اینترنت اشیا در یک چرخه نوآوری بیش‌ازحد سریع است که بسیار سریع‌تر از چرخه نوآوری محصولات مصرف‌کننده معمولی است. هنوز مشکلاتی مانند استانداردهای رقابتی، امنیت ناکافی، مسائل مربوط به حریم خصوصی، ارتباطات پیچیده، و تعداد دستگاه‌های تست‌شده ضعیفِ درحال‌افزایش، وجود دارند. اگر این مسائل به دقت بررسی نشوند، دستگاه‌های چندمنظوره و برنامه‌های کاربردی مشترک می‌توانند زندگی ما را به هرج و مرج تبدیل کنند. در دنیای غیرمرتبط، یک خطا یا اشتباه کوچک، یک سیستم را از بین نمی‌برد. با این حال، در یک دنیای بیش‌ازحد متصل، یک خطا در یک بخش از یک سیستم می‌تواند باعث اختلال در سراسر آن شود. [۱].

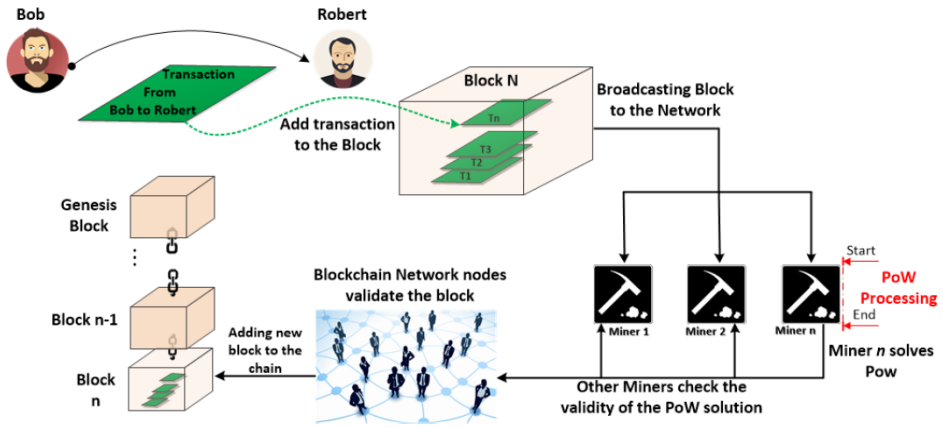


شکل ۲. چالش‌های امنیتی اینترنت اشیا

بلاک‌چین: بلاک‌چین به صورت یک مفهوم از سال ۱۹۹۱ مطرح بود اما زمانی که ساتوشی ناکاموتو بیت‌کوین را در سال ۲۰۰۹ تعریف و ابداع کرد، معروف شد و بر سر زبان‌ها افتاد. یک بلاک در یک شبکه بلاک‌چین از قسمت‌های مختلفی تشکیل شده است و همانطور که از نامش مشخص است، ما زنجیره‌ای از بلاک‌ها را در بلاک‌چین می بینیم. این قسمت ها عبارت اند از: (data(payload، current block hash و previous block hash که به مانند یک لینک لیست به هم متصل شده‌اند. نکته مهمی که درباره بلاک‌ها وجود دارد، بحث امنیت آنها است. ممکن است افرادی با قصد قبلی بخواهند data یا همان payload یک بلاک را تغییر دهند که در پی این اتفاق hash آن بلاک هم تغییر خواهد کرد. خوبی بلاک‌چین این است که ما hash این بلاک خراب را در بلاک‌های بعدی این بلاک داریم و بر همین اساس، این تغییر ناگهانی تشخیص داده می‌شود و بلاک بعدی، این بلاک نامعتبر را دیگر verify نمی‌کند؛ و عملاً این هک و نفوذپذیری با شکست مواجه می‌شود. اما نکته دیگری که در این جا وجود دارد، این است که سرعت محاسبات کامپیوترها بسیار زیاد شده‌است و ممکن است که فردی با نیت شوم اقدام به تغییر data برای چندین و چند بلاک پشت سر هم بکند که این، یکی از چالش‌های جدی بلاک‌چین است و کامپیوترها ممکن است که hash تعداد زیادی بلاک را در یک زمان محاسبه کنند. برای مقابله با این چالش الگوریتم‌های اجماعی معرفی شده‌اند. اجماع یک مشکل اساسی در سیستم‌های توزیع‌شده است که به دو یا چند عامل نیاز دارد تا بر روی یک مقدار معین مورد نیاز برای اهداف محاسباتی به توافق برسند. برخی از این عوامل ممکن است غیرقابل اعتماد باشند و بنابراین فرآیند اجماع باید وابسته

باشد. بلاک‌چین‌ها می‌توانند از الگوریتم‌های اجماع مختلفی استفاده کنند. برخی از آنها عبارت‌اند از: Proof-of-Work (PoW)، Proof-of-Stake (PoS)، Proof-of-Storage، Proof-of-Burn، Proof-of-Capacity.

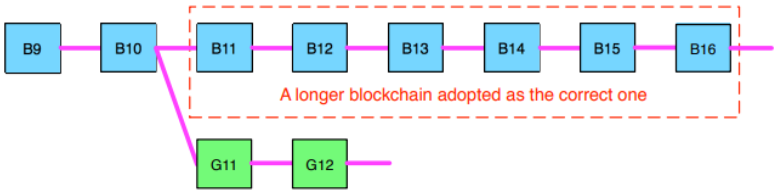
PoW توسط سایر ماینرها هر بار که بلاکی دریافت می‌کنند، تایید می‌شود. هدف اصلی mining این است که به نودهای یک سیستم اجازه دهد به یک اجماع امن و مقاوم در برابر دستکاری برسند. mining همچنین مکانیزمی است که برای معرفی ارزهای دیجیتال جدید (به عنوان مثال بیت‌کوین) به سیستم استفاده می‌شود. هنگام تایید یک بلوک، به ماینرها کارمزد تراکنش و همچنین مقدار مشخصی از کوین‌های تازه ایجادشده پرداخت می‌شود. این روش با هدف انتشار سکه‌های جدید به صورت غیرمتمرکز و همچنین تامین امنیت سیستم انجام می‌شود. سیستم به طور خودکار با کل قدرت mining شبکه، سازگار می‌شود و آن را برای مدت زمان مشخصی ثابت نگه می‌دارد (مثلاً ۱۰ دقیقه در بیت‌کوین). میزان دشواری PoW نیز پس از هر مقدار مشخصی از بلاک‌ها (به عنوان مثال بلاک‌های ۲۰۱۶ در بیت‌کوین) بر اساس عملکرد شبکه تنظیم می‌شود. یک تراکنش برای رسیدن به تمام نودهای شبکه زمان می‌برد و تاخیر تضمین می‌کند که تمام تراکنش‌ها توسط همه نودهای شبکه تایید می‌شوند تا از مشکل Double spending جلوگیری شود. Double spending نتیجه استفاده همزمان از چند ارز دیجیتال است.[۲]



شکل ۳. اعتبارسنجی بلاک‌های تراکنش و روند اضافه‌شدن بلاک

چالش‌های این حوزه: (۱) چالش مقیاس‌پذیری: با افزایش روزانه حجم تراکنش‌ها، بلاک‌چین سنگین می‌شود. در حال حاضر، بلاک‌چین بیت‌کوین از ۴۱۳ گیگابایت فضای ذخیره‌سازی فراتر رفته است. همه تراکنش‌ها باید برای تایید تراکنش ذخیره شوند. علاوه بر این، به دلیل محدودیت اصلی اندازه بلاک و فاصله زمانی مورد استفاده برای تولید یک بلاک جدید، بلاک‌چین بیت‌کوین تنها می‌تواند نزدیک به هفت تراکنش در ثانیه را پردازش کند، که نمی‌تواند نیاز پردازش میلیون‌ها تراکنش را به صورت بلادرنگ برآورده کند. در همین حال، از آنجایی که ظرفیت بلاک‌ها بسیار کم است، بسیاری از تراکنش‌های کوچک ممکن است به تعویق بیفتند، زیرا ماینرها تراکنش‌هایی را با کارمزد بالا ترجیح می‌دهند. با این حال، اندازه بزرگ بلاک، سرعت انتشار را کاهش می‌دهد و منجر به شاخه‌های بلاک‌چین (fork) می‌شود. بنابراین مشکل مقیاس‌پذیری بسیار دشوار است. (۲) چالش نشت حریم خصوصی: اعتقاد بر این است که بلاک‌چین بسیار ایمن است زیرا کاربران فقط با آدرس‌های تولیدشده تراکنش می‌کنند نه هویت واقعی. کاربران همچنین می‌توانند آدرس‌های زیادی را در صورت نشت اطلاعات ایجاد کنند. با این حال، در بررسی‌های گذشته نشان داده شده است، که بلاک‌چین نمی تواند حریم خصوصی تراکنش‌ها را تضمین کند زیرا مقادیر تمام تراکنش‌ها و موجودی‌های هر public key به صورت عمومی قابل مشاهده است. علاوه بر این، مطالعات اخیر نشان داده است که تراکنش‌های بیت‌کوین کاربر می‌تواند برای افشای اطلاعات کاربر مرتبط شود. علاوه بر این، روشی را برای پیوند نام مستعار

کاربران به آدرس‌های IP حتی زمانی که کاربران در حالت NAT یا در حال استفاده از فایروال قرار دارند، ارائه کردند. در مطالعات اخیر نشان داده شده است که هر مشتری را می‌توان به طور منحصربه‌فرد توسط مجموعه‌ای از نودهایی که به آنها متصل می‌شود، شناسایی کرد. با این حال، این مجموعه را می‌توان آموخت و برای یافتن مبدا یک تراکنش استفاده کرد. (۳) چاش استخراج خودخواهانه: بلاک‌چین در معرض حملات ماینرهای خودخواه تبانی‌گر است. باور کلی بر این است که نودهایی با بیش از ۵۱٪ قدرت محاسباتی می‌توانند بلاک‌چین و تراکنش اتفاق‌افتاده را معکوس کنند. با این حال، تحقیقات اخیر نشان می‌دهد که حتی نودهایی با قدرت کمتر ۵۱٪ هنوز خطرناک هستند. به طور خاص نشان داده شده است که شبکه آسیب‌پذیر است حتی اگر تنها بخش کوچکی از قدرت hash برای تقلب استفاده شود. در استراتژی استخراج خودخواهانه، ماینرهای خودخواه بلاک‌های استخراج‌شده خود را بدون پخش نگه می‌دارند و private branch تنها در صورت برآورده‌شدن برخی الزامات برای عموم آشکار می‌شود. از آنجایی که private branch طولانی‌تر از public branch فعلی است، همه ماینرها آن را پذیرفته‌اند. قبل از انتشار بلاک‌چین خصوصی، ماینرهای صادق منابع خود را در یک شعبه بی‌فایده تلف می‌کنند در حالی که ماینرهای خودخواه زنجیره خصوصی خود را بدون رقبا استخراج می‌کنند. بنابراین ماینرهای خودخواه تمایل به کسب درآمد بیشتری دارند و ماینرهای منطقی جذب می‌شوند تا به جمع خودخواهان بپیوندند و خودخواهان می‌توانند به سرعت از ۵۱٪ قدرت فراتر بروند. [۳] [۶]



شکل ۴. شاخه طولانی‌تر، معتبر است.

۱-۲. روند پروژه

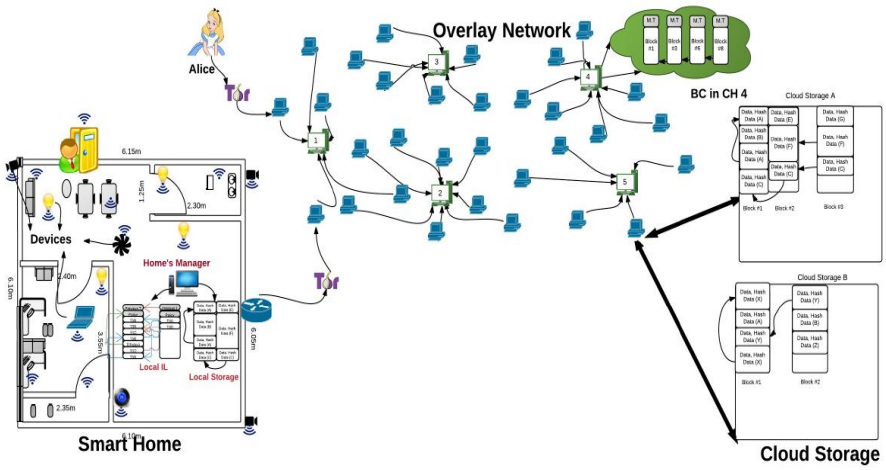
در فاز اول پروژه نه مقاله توصیه‌شده همراه با یک مقاله‌ی با موضوع IOTA مطالعه کردیم. تقسیم بندی فاز اول بر مبنای موضوعات مختلف صورت گرفت. در رابطه با دو موضوع معماری مقیاس‌پذیر بلاک‌چین برای اینترنت اشیا و بهره‌گیری از بلاک‌چین برای تضمین امنیت در محیط اینترنت اشیا و cloud آقای علی آهنگرپور دو مقاله را مطالعه کرد. برای دو موضوع استفاده از بلاک‌چین برای تامین امنیت و حریم خصوصی در محیط اینترنت اشیا (The case study of a smart home) و سیستم کنترل دسترسی بر مبنای Permissioned Blockchain برای اینترنت اشیا، آقای مهدی علی‌پور دو مقاله مطالعه کرد. برای دو موضوع انطباق بلاک‌چین‌های بر مبنای PoS برای Data Stream های اینترنت اشیا و پلتفرم Edgence : یک پلتفرم Edge-Computing با قابلیت بلاک‌چین برای اپلیکشین‌های هوشمند و توزیع شده‌ی مبتنی بر اینترنت اشیا خانم هانیه صولتی‌نیا دو مقاله مطالعه کرد. برای دو موضوع به سمت یک بلاک‌چین بهینه شده برای اینترنت اشیا و به سمت یک data marketplace تقویت‌شده با بلاک‌چین برای اینترنت اشیا آقای سبحان کریمی دو مقاله مطالعه کرد. برای دو موضوع مجتمع‌سازی بلاک‌چین و اینترنت اشیا (Systematic Survey) و IOTA آقای رسول بوسعیدی دو مقاله مطالعه کرد.

در فاز دوم تقسیم کار و تعیین موضوعات و بخش‌های اصلی برای فاز سوم صورت گرفت. برای اینکه درک عمیق‌تر نسبت به موضوعات پیدا کنیم و با چالش‌های دنیای واقعی هم آشنا شویم تصمیم گرفته شد که در کنار حفظ جنبه‌ی آکادمیک، پیاده سازی در زمینه‌ی IOTA که به صورت اولیه در صورت تعریف‌شده‌ی پروژه نبود، به لیست کارهای مورد نیاز اضافه شود. همچنین بر مبنای پیشنهاد استاد و خروجی جلسات برگزار شده در گروه و با دستیار آموزشی، موضوعات مطرح روز که در روند پیشرفت

این تکنولوژی‌ها موثر هستند، به لیست موضوعات فاز اول اضافه شدند، از جمله Federated learning. همچنین یک تسک به صورت R&D با هدف بررسی شرکت‌هایی که در حال بهره‌گیری از بلاک‌چین در فناوری اینترنت اشیا خود هستند اختصاص دادیم تا بهتر بتوانیم کاربردهای عملی در حال حاضر در این حوزه را با توجه به سطح علمی جدید بدست آمده بر روی مسئله بررسی کنیم. با توجه به تسک‌های تعریف شده اعضای گروه به زیرگروه‌های دو نفره تقسیم شدند.

۲-۲. چکیده‌ای از فاز اول

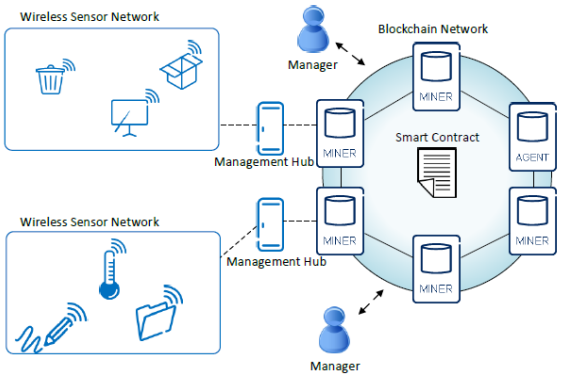
در فاز اول برای آشنایی بیشتر با دو موضوع بلاک‌چین و اینترنت اشیا و ترکیب آنها ده مقاله را مطالعه کردیم که در اینجا خلاصه‌ای از آنها را بیان می‌کنیم. در مقاله‌ی اول حرکت به سمت یک بلاک‌چین بهینه سازی شده برای اینترنت اشیا بررسی شد. علاقه فزاینده ای به پذیرش بلاک‌چین، در اینترنت اشیا برای امنیت و حفظ حریم خصوصی وجود دارد. با این حال، بلاک‌چین ها از نظر محاسباتی گران هستند و شامل overhead های پهنای باند بالا و تاخیرهای بالا هستند که برای اکثر دستگاه‌های اینترنت اشیا مناسب نیستند. برای حرکت به سمت یک بلاک‌چین بهینه سازی شده برای اینترنت اشیا ما به بررسی معماری سبک وزن مبتنی بر بلاک‌چین برای اینترنت اشیا پرداختیم که عملاً هزینه‌های overhead کلاسیک بلاک‌چین را حذف می‌کند، در حالی که بیشتر مزایای امنیت و حریم خصوصی آن را حفظ می‌کند. دستگاه‌های اینترنت اشیا از یک ledger خصوصی غیرقابل تغییر بهره می‌برند که شبیه به بلاک‌چین عمل می‌کند اما به صورت مرکزی مدیریت می‌شود تا مصرف انرژی را بهینه کند. دستگاه‌های با منابع بالا یک شبکه، overlay ایجاد می‌کنند تا یک بلاک‌چین توزیع‌شده در دسترس عموم را پیاده‌سازی کنند که امنیت و حریم خصوصی end-to-end را تضمین می‌کند. معماری پیشنهادی از اعتماد توزیع‌شده برای کاهش زمان پردازش اعتبار بلوک استفاده می‌کند. ارزیابی کیفی معماری تحت مدل‌های تهدید رایج، اثربخشی آن را در تأمین امنیت و حریم خصوصی برای برنامه‌های اینترنت اشیا برجسته می‌کند. شبیه‌سازی‌ها نشان می‌دهند که این روش در مقایسه با اجرای بلاک‌چین در بیت‌کوین، overhead پکت و پردازشی را به‌طور قابل‌توجهی کاهش می‌دهد. [۵]



شکل ۵. یک خانه‌ی هوشمند مبتنی بر بلاک‌چین

در مقاله‌ی دوم ترکیبی از بلاک‌چین با اینترنت اشیا از طریق معرفی یک معماری برای مدیریت مقیاس‌پذیر دسترسی در اینترنت اشیا بررسی می‌شود. اینترنت اشیا از مراحل اولیه خود خارج شده و به بلوغ کامل رسیده و خود را به عنوان بخشی از

اینترنت آینده تثبیت می‌کند. یکی از چالش‌های فنی استقرار میلیاردها دستگاه در سراسر جهان، توانایی مدیریت آنها است. اگرچه فناوری‌های مدیریت دسترسی در اینترنت اشیا وجود دارند، اما بر اساس مدل‌های متمرکزی هستند که انواع جدیدی از محدودیت‌های فنی را برای مدیریت آن‌ها در سطح جهانی معرفی می‌کنند. ما یک معماری جدید برای داوری نقش‌ها و مجوزها در اینترنت اشیا را بررسی کردیم. این معماری جدید، یک سیستم کنترل دسترسی کاملاً توزیع‌شده برای اینترنت اشیا مبتنی بر فناوری بلاک‌چین است. این معماری توسط پیاده‌سازی proof of concept پشتیبانی می‌شود و در سناریوهای واقعی اینترنت اشیا ارزیابی می‌شود. نتایج نشان می‌دهد که فناوری بلاک‌چین می‌تواند به عنوان فناوری مدیریت دسترسی در سناریوهای مقیاس‌پذیر اینترنت اشیا خاص مورد استفاده قرار گیرد. [۲]

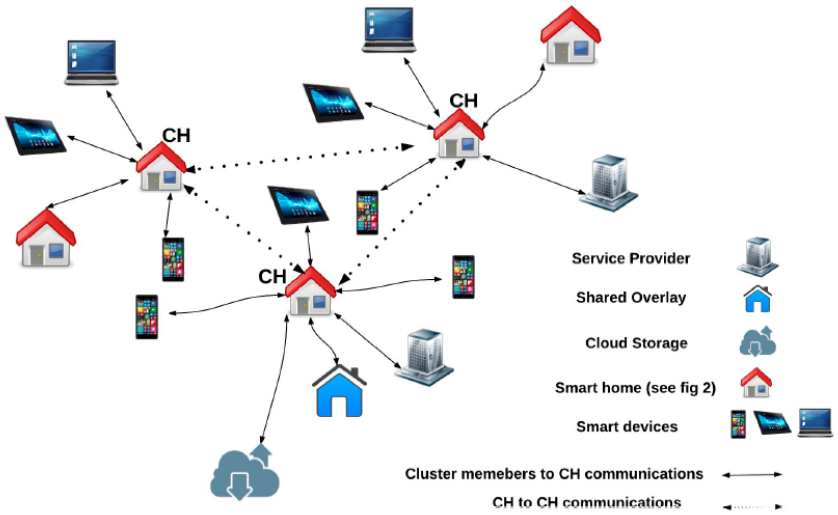


شکل ۶. سیستم کنترل دسترسی غیر متمرکز

در مقاله‌ی سوم، که یک systematic survey بود، به مجتمع‌سازی بلاک‌چین و اینترنت اشیا پرداخته شده بود. اینترنت اشیا به اتصال دستگاه‌های هوشمند برای جمع‌آوری داده‌ها و تصمیم‌گیری هوشمندانه اشاره دارد. با این حال، فقدان اقدامات امنیتی ذاتی، اینترنت اشیا را در برابر تهدیدات امنیتی آسیب‌پذیر می‌کند. بلاک‌چین با "security by design" خود می‌تواند به رفع نیازهای امنیتی اصلی در اینترنت اشیا کمک کند. قابلیت‌های بلاک‌چین مانند تغییرناپذیری، شفافیت، قابلیت حسابرسی، رمزگذاری داده‌ها و انعطاف‌پذیری عملیاتی می‌تواند به حل اکثر کاستی‌های معماری اینترنت اشیا کمک کند. در این بخش ما یک بررسی جامع در مورد بلاک‌چین و ادغام آن با اینترنت اشیا انجام دادیم و این نوآوری‌ها در این بخش وجود داشت: (۱) حوزه‌های کاربردی مختلف پوشش داده می‌شد (۲) دو الگوی استفاده، یعنی دستکاری دستگاه و مدیریت داده معرفی می‌شد، و (۳) در مورد سطح توسعه برخی از راه‌حل‌های ارائه‌شده گزارش داده می‌شد. ما همچنین چالش‌های اصلی جامعه تحقیقاتی را در ادغام بلاک‌چین و اینترنت اشیا تجزیه و تحلیل کردیم و به مسائل باز اشاره کردیم. [۶]

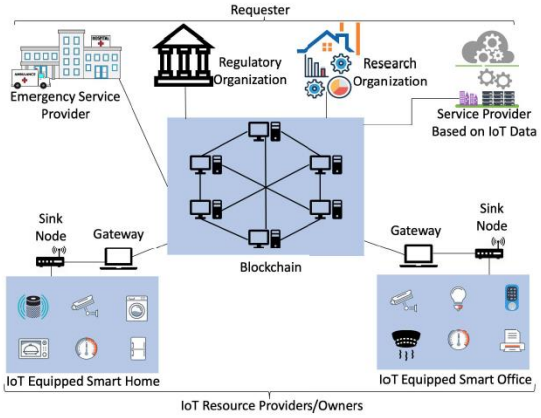
در مقاله‌ی چهارم به بهره‌گیری از بلاک‌چین جهت تامین امنیت و حفظ حریم خصوصی در اینترنت اشیا پرداخته شد، این بخش به طور بخصوص به بررسی یک خانه هوشمند می‌پرداخت. امنیت و حفاظت از حریم خصوصی یکی از چالش‌های اصلی اینترنت اشیا است، که عمدتاً به دلیل مقیاس گسترده و ماهیت توزیع‌شده شبکه‌های اینترنت اشیا است. رویکردهای مبتنی بر بلاک‌چین، امنیت و حریم خصوصی غیرمتمرکز را فراهم می‌کنند، با این حال آنها شامل انرژی، تاخیر و overhead محاسباتی قابل توجهی هستند که برای اکثر دستگاه‌های اینترنت اشیا با محدودیت منابع مناسب نیستند. رویکرد مقاله‌ی چهارم در یک محیط خانه هوشمند نمونه است و از سه لایه اصلی تشکیل شده است: ذخیره سازی ابری، پوشش و خانه هوشمند. در مقاله چهارم اجزای اصلی و عملکردهای لایه خانه هوشمند تشریح می‌شود. هر خانه هوشمند مجهز به یک دستگاه همیشه آنلاین و با منابع بالا، معروف به "ماینر" است که وظیفه مدیریت تمام ارتباطات درون و بیرون خانه را بر عهده دارد. ماینر همچنین یک

بلاک‌چین خصوصی و امن را حفظ می کند که برای کنترل و ممیزی ارتباطات استفاده می شود. نشان داده می‌شود که چارچوب خانه هوشمند مبتنی بر بلاک‌چین با تجزیه و تحلیل کامل امنیت آن با توجه به اهداف امنیتی اساسی محرمانگی، یکپارچگی و در دسترس بودن، ایمن است. در نهایت، نتایج شبیه‌سازی ارائه می‌شود تا تأکید شود که هزینه‌های overhead (از نظر ترافیک، زمان پردازش و مصرف انرژی) ایجاد شده توسط رویکرد ما نسبت به دستاوردهای امنیت و حریم خصوصی آن ناچیز است. [۷]



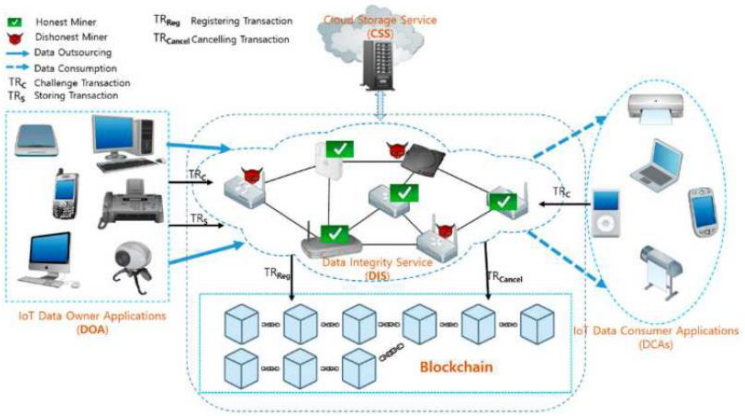
شکل ۷. نمایی از معماری مبتنی بر بلاک‌چین پیشنهادی

در مقاله‌ی پنجم به بررسی سیستم کنترل دسترسی در اینترنت اشیا با رویکرد مبتنی بر Permissioned Blockchain پرداخته می‌شود. دستگاه‌های اینترنت اشیا داده‌های ارزشمند و حساس زیادی تولید می‌کنند که اغلب با طرف‌های خارجی به اشتراک گذاشته می‌شوند تا انواع مختلف خدمات مفید را ارائه دهند. سیستم‌های کنترل دسترسی سنتی اینترنت اشیا، متمرکز هستند و همه ذی‌نفعان را در فرآیند تصمیم‌گیری کنترل دسترسی شامل نمی‌شوند. برای پر کردن این شکاف، ما یک سیستم کنترل دسترسی مبتنی بر Permissioned Blockchain برای اینترنت اشیا را پیشنهاد می‌کنیم که در آن، فاز متفاوتی از کنترل دسترسی مانند ایجاد سیاست دسترسی و تصمیم‌گیری کنترل دسترسی بر اساس اجماع همه سهامداران اتفاق می‌افتد. برای دقیق‌تر بودن، ما کنترل دسترسی مبتنی بر ویژگی (ABAC) را در یک Permissioned Blockchain به نام Hyperledger Fabric طراحی و اجرا می‌کنیم و از قرارداد هوشمند و اجماع توزیع‌شده آن برای فعال‌کردن کنترل دسترسی توزیع‌شده برای اینترنت اشیا استفاده می‌کنیم. [۸]



شکل ۸. معماری سیستم

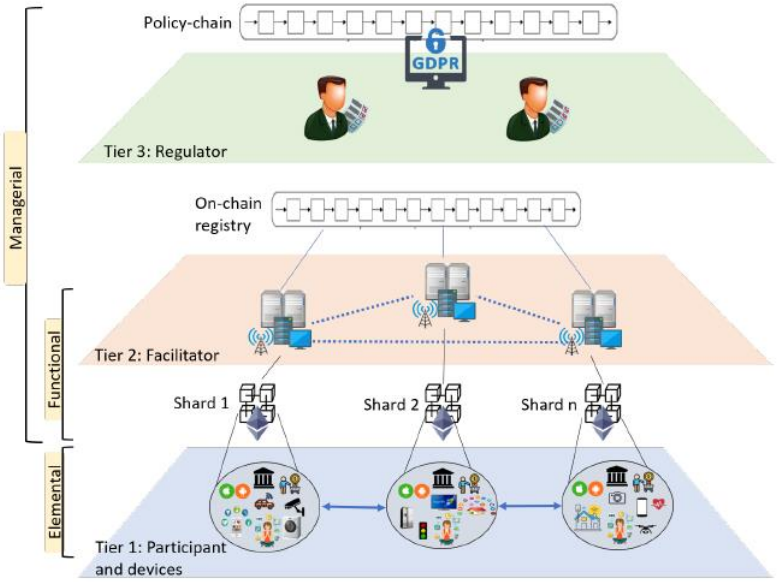
در مقاله‌ی ششم به بهره‌گیری از بلاک‌چین برای تضمین امنیت در محیط اینترنت اشیا و cloud پرداخته شده است. اینترنت اشیا و فناوری ابری بیش از یک دهه است که در حال توسعه هستند. توسعه سریع فناوری جدید در عصر مدرن، امکان معرفی فناوری‌های اینترنت اشیا و ابری در زمینه‌های کاری متنوع را افزایش داده است، اما در عین حال، افزایش چشمگیر تعداد دستگاه‌های متصل اینترنت اشیا، توجه به نگرانی‌ها و خطرات مرتبط با امنیت آنها را ضروری می‌سازد. در مقاله‌ی ششم مشکلاتی را که می‌تواند در فناوری‌های ابری و اینترنت اشیا در زیرساخت‌های موجود ایجاد شود و همچنین توسعه فناوری‌های ابری و اینترنت اشیا در آینده با استفاده از فناوری بلاک‌چین برای حل این مشکلات بررسی می‌شود. [۹]



شکل ۹. ارتباط cloud ، بلاک‌چین و اینترنت اشیا

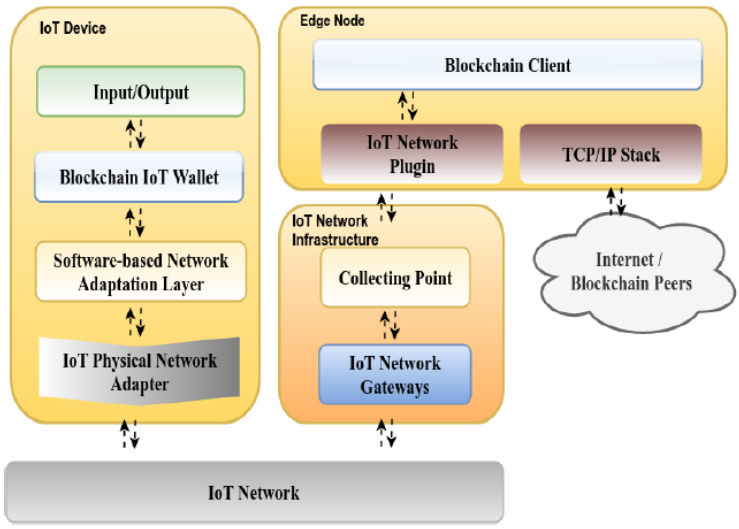
در مقاله‌ی هفتم هدف، حرکت به سمت یک data marketplace تقویت‌شده با بلاک‌چین برای اینترنت اشیا است. نرخ بی سابقه پذیرش اینترنت اشیا فرصتی را برای صاحبان دستگاه‌ها فراهم می‌کند تا داده‌های اینترنت اشیا خود را با خریداران علاقه‌مند معامله کنند. یک بازار داده با قابلیت بلاک‌چین می‌تواند تجارت داده‌های اینترنت اشیا خصوصی را با توانمندسازی صاحبان داده برای انتخاب اینکه چه چیزی را با چه کسی می‌خواهند به اشتراک بگذارند، دموکراتیزه کند. با این حال، برخی از ویژگی‌های اینترنت اشیا، تجارت داده‌های تولیدشده را در بازارهای متمرکز مرسوم دشوار می‌کند. این تحقیق بر توسعه یک چارچوب marketplace برای پرداختن به چالش‌های طراحی تحمیل‌شده توسط ویژگی‌های اینترنت اشیا، مانند منابع محدود

و قابلیت‌های محاسباتی، تحرک، حریم خصوصی داده‌ها و مسائل مربوط به فروش مجدد تمرکز دارد. مقاله‌ی هفتم یک چارچوب سه لایه را برای مقابله موثر با این چالش‌ها در زمینه‌های پایه‌ای، عملکردی و مدیریتی پیشنهاد می‌کند. [۱۰]



شکل ۱۰. معماری سیستم سه لایه

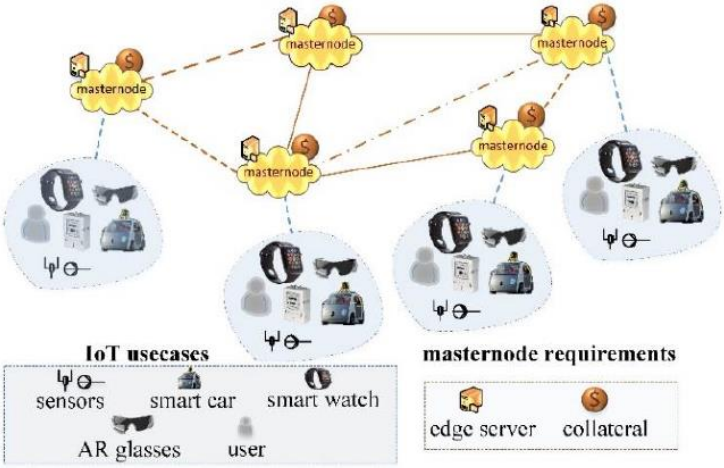
در مقاله‌ی هشتم به بررسی به‌کارگیری بلاک‌چین های مبتنی بر PoS برای جریان داده‌های اینترنت اشیا پرداخته شده است. Proof-of-Work در بلاک‌چین، یک الگوریتم اجماع پرکاربرد است، که از مصرف انرژی بالای ماینرها و نرخ تراکنش پایین رنج می‌برد. مقاله‌ی هشتم یک بلاک‌چین مبتنی بر Proof-of-Stake به نام Bazo را معرفی می‌کند که به‌طور ویژه برای جریان‌های داده اینترنت اشیا طراحی و سازگار شده است. Bazo عملکرد بهبود یافته‌ای را از نظر مصرف انرژی و پردازش تراکنش‌ها در مقایسه با بلاک‌چین مبتنی بر PoW نشان می دهد. برای بهبود بیشتر عملکرد Bazo، روش‌های اشتراک‌گذاری و تجمیع تراکنش‌ها به کار گرفته می‌شود. علاوه بر این، IoT-BC adaptation helper ها با یک معماری ماژولار و لایه‌ای ارائه شده‌اند تا به دستگاه‌های بی‌سیم اجازه دهند داده‌ها را به راحتی به بلاک‌چین ارسال کنند. معماری پیشنهادی می‌تواند از چندین پلتفرم سخت‌افزاری و نرم‌افزاری و همچنین فناوری‌های شبکه پشتیبانی کند. [۱۱]



شکل ۱۱. مولفه های سازگاری اینترنت اشیا در یک معماری لایه ای

در مقاله‌ی نهم به بررسی پلتفرم Edgence، که یک پلتفرم Edge-Computing با قابلیت بلاک‌چین برای اپلیکشین‌های هوشمند و توزیع شده‌ی مبتنی بر اینترنت اشیا است، پرداخته می‌شود. امروزه مدیریت مقیاس‌پذیر اینترنت اشیا به دلیل توزیع پراکنده جغرافیایی، مالکیت‌های پراکنده و جمعیت روزافزون دستگاه‌های اینترنت اشیا، یک گلوگاه توسعه اینترنت اشیا است. برای مدیریت هوشمندانه برنامه‌های غیرمتمرکز (dApps) در موارد استفاده اینترنت اشیا،

Edgence (EDGe + IntelligENCE) پیشنهاد شده است تا از ابرهای لبه برای دسترسی به دستگاه‌ها و کاربران اینترنت اشیا استفاده کند و سپس از بلاک‌چین داخلی خود برای تحقق خودگردانی و نظارت بر خود استفاده کند. Edgence پیشنهاد می‌کند از فناوری master node برای معرفی دستگاه‌ها و کاربران اینترنت اشیا به یک سیستم بلاک‌چین بسته استفاده شود که می‌تواند دامنه بلاک‌چین را به dApp های مبتنی بر اینترنت اشیا گسترش دهد. علاوه بر این، مسترنودها با افزایش TPS (تراکنش در ثانیه) شبکه بلاک‌چین، به بهبود مقیاس‌پذیری آن کمک می‌کنند. برای پشتیبانی از dApp های مختلف، یک اعتبار سنجی سه لایه پیشنهاد شده است، یعنی اعتبار سنجی اسکریپت، اعتبار سنجی قرارداد هوشمند، و اعتبارسنجی Master node. برای جلوگیری از مصرف انرژی ناشی از اجماع بلاک‌چین، Edgence یک روش تصادفی اما قابل تایید را برای انتخاب یک مسترنود برای تولید هر بلاک جدید پیشنهاد می‌کند. پتانسیل Edgence در نمونه‌هایی از crowdsourcing غیرمتمرکز و آموزش هوش مصنوعی نشان داده شده می‌شود. [۱۲]



شکل ۱۲. اجرای پلتفرم غیرمتمرکز Edgence روی ابرهای لبه Edge-Computing mobile

۳-۲. مثال‌هایی از مجتمع‌سازی بلاک‌چین و اینترنت اشیا

مجتمع‌سازی بلاک‌چین و اینترنت اشیا با معماری‌ها و فریم‌ورک‌های مختلفی امکان‌پذیر است، که این معماری‌ها در فاز اول بررسی شدند و در قسمت چکیده‌ی فاز اول هم به آنها اشاره شد. در اینجا قصد داریم به بررسی مثال‌های واقعی ترکیب بلاک‌چین و اینترنت اشیا بپردازیم. شرکت‌های متنوعی هستند که بر ترکیب بلاک‌چین و اینترنت اشیا تمرکز دارند در این بخش هشت مورد از این شرکت‌ها و اهداف آنها را بررسی می کنیم. (۱) شرکت Helium در سن‌فرانسیسکو، اولین شبکه ماشینی غیرمتمرکز جهان است. این شرکت از بلاک‌چین برای اتصال ماشین‌های اینترنت اشیا کم‌مصرف (مانند روترها و ریزتراشه‌ها) به اینترنت استفاده می‌کند. زیرساخت اینترنت بی‌سیم مبتنی بر بلاک چین Helium از فناوری رادیویی برای تقویت اتصال به اینترنت و کاهش شدید قدرت مورد نیاز برای راه‌اندازی ماشین‌های هوشمند استفاده می‌کند. از اهداف این شرکت پس از انجام اولین تراکنش موفقیت‌آمیز بلاک‌چینشان، پیاده سازی نودهای خود جهت آزمایش شبکه‌های غیرمتمرکز peer-to-peer شان است.

(۲) شرکت Chronicled در سن‌فرانسیسکو، محصولات بلاک‌چین و اینترنت اشیا را برای ارائه یک راه‌حل زنجیره‌ی تامین end-to-end ترکیب می کند. Chronicled با تمرکز بر صنایع دارویی و تامین مواد غذایی، از کانتینرهای حمل و نقل و حسگرهای مجهز به اینترنت اشیا برای ارائه به‌روزرسانی‌های بی‌درنگ در مورد فرآیندهای حمل و نقل استفاده می‌کند. پیاده‌سازی بلاک‌چین در دستگاه‌های اینترنت اشیا به همه‌ی طرف‌های درگیر در فرآیند ارسال دارو یا عرضه مواد غذایی این امکان را می‌دهد تا از زنجیره نگهداری آگاه باشند و در صورت بروز هرگونه مشکل در طول فرآیند از آن اطلاع یابند. Chronicled موفق به انجام آزمایشی فنی جهت ثبت رویدادهای زنجیره‌ی تامین در یک بلاک‌چین شده است. این بلاک‌چین برای ثبت موفقیت‌آمیز زنجیره‌ی تامین رویدادها، سیاست‌های سختگیرانه حفظ حریم خصوصی داده‌ها و قوانین مدیریت پیچیده صنعت داروسازی را در نظر گرفته است.

(۳) شرکت ArcTouch در سن‌فرانسیسکو، نرم‌افزار مبتنی بر بلاک‌چین را برای طیف وسیعی از موارد هوشمند توسعه داده است که در دستیارهای صوتی، پوشیدنی‌ها و تلویزیون‌های هوشمند کاربرد دارد. این شرکت برنامه‌های شخصی‌سازی شده و غیرمتمرکز را برای ده‌ها شرکتی که به دستگاه‌های اینترنت اشیا پیوند دارند، ساخته است. اپلیکشین‌های غیرمتمرکز

ArcTouch سطح بیشتری از امنیت اینترنت اشیا را ارائه می‌دهند و می‌توانند توافق‌نامه‌ها را سریع‌تر از قراردادهای هوشمند پردازش کنند. این شرکت چندین اپلیکشین غیرمتمرکز بلاک‌چین ساخته است که به دستگاه‌های اینترنت اشیا مانند Amazon Alexa و Facebook Messenger متصل می‌شوند.

(۴) شرکت Filament در رنو، نوادا، سخت‌افزار و نرم‌افزاری با پشتوانه بلاک‌چین طراحی می‌کند که به راحتی با محصولات اینترنت اشیا ادغام می‌شود. مجموعه بلاک‌چین این شرکت که Blocklet نام دارد، بر تقویت امنیت داده‌ها در دستگاه‌های اینترنت اشیا برای صنایع ساخت‌وساز، تولید، انرژی و حمل و نقل تمرکز دارد. (۵) شرکت netObjex در ایروین، یک مکانیسم استاندارد و غیرمتمرکز برای ارتباط دستگاه‌های اینترنت اشیا با یکدیگر ایجاد کرده است. IoToken این شرکت که از بلاک‌چین پشتیبانی می کند، یک پلتفرم دیجیتال امن برای دستگاه‌های هوشمند در همان اکوسیستم برای تعامل و ارتباط فراهم می‌کند. NetObjex ادعا می‌کند که IoToken آن می‌تواند برای برقراری ارتباط یکپارچه با دستگاه‌های دیگر در صنایع بی‌شماری استفاده شود. در یک رستوران درایو، مشتریان می‌توانند از IoToken در کیف پول رمزنگاری خود برای پرداخت هزینه وعده غذایی خود استفاده کنند. در تحویل هواپیمای بدون سرنشین، IoToken را می‌توان برای علامت‌گذاری نقطه تحویل و تأیید پرداخت استفاده کرد. این شرکت با کتابخانه عمومی بروکلین برای نصب فناوری ایستگاه شارژ تلفن همراه هوشمند خود شریک شد. با استفاده از فناوری NetObjex Blockchain-IoT، ایستگاه‌های شارژ از کاربران می‌خواهند که یک ویدیوی اطلاعاتی مختصر را تماشا کنند و یک نظرسنجی کوتاه انجام دهند. نتایج این نظرسنجی به‌طور ایمن در یک بلاک‌چین برای کتابخانه عمومی بروکلین ذخیره می‌شود تا به عنوان بخشی از ابتکار روبه‌رشد خود برای بهبود تجربه مشتریان، تجزیه و تحلیل شود.

(۶) شرکت HYPR در نیویورک، از شبکه‌های غیرمتمرکز برای ایمن‌کردن دستگاه‌های خودپرداز، خودروها، قفل‌ها و خانه‌های متصل استفاده می‌کند. یکی از دلایل اصلی ویرانگر و گسترده‌بودن حملات سایبری این است که پایگاه‌های داده متمرکز میلیون‌ها رمز عبور را ذخیره می‌کنند. HYPR لاگین‌های بیومتریک را در بلاک‌چین ذخیره می‌کند و اطلاعات مهم را ایمن و غیرمتمرکز می‌کند. پروتکل‌های امنیتی بیومتریک این شرکت شامل ابزارهای منحصربه‌فرد تشخیص چهره، چشم، صدا و کف دست برای دستگاه‌های اینترنت اشیا است. HYPR با موفقیت، چندین کاربرد غیرمتمرکز مختلف را برای پلتفرم امنیتی اینترنت اشیا خود آزمایش کرده است. آن‌ها اسکن‌های بیومتریک را روی تلفن‌های هوشمند برای دسترسی به بانک‌های شخصی ATM آزمایش کرده‌اند و این شرکت یک کلید دیجیتال DLT برای صاحبان خانه ایجاد کرد تا یک نقطه دسترسی واحد به همه چیز از درهای مجهز به اینترنت اشیا گرفته تا مراکز سرگرمی هوشمند داشته باشند.

(۷) شرکت Xage Security در پالوآلتو، کالیفرنیا، اولین پلتفرم امنیتی محافظت‌شده توسط بلاک‌چین برای اینترنت اشیا است. بلاک‌چین Xage با تمرکز بر صنایع صنعتی مانند کشاورزی، انرژی، حمل و نقل و خدمات آب و برق، دستگاه‌های اینترنت اشیا را قادر می‌سازد تا از دستکاری جلوگیری کنند و به خطوط ارتباطی امن بین اشیا هوشمند دسترسی داشته باشند. Xage مجموعه‌ای از برنامه‌های غیرمتمرکز اینترنت اشیا دارد که همه کارها را از مدیریت ایمن خط مشی گرفته تا ارائه ابزارهایی که هشدارهای فوری درباره فعالیت‌های هک مشکوک صادر می‌کنند، انجام می‌دهند. Xage اخیراً به اتحاد برق هوشمند (SEPA) ملحق شده است تا بر این موضوع تمرکز کند که چگونه می‌تواند دستگاه‌های اینترنت اشیا خود را به بخش انرژی پاک بیاورد. این شرکت می‌خواهد فناوری ledger خود را به منظور خنثی‌کردن حملات سایبری گسترده‌تر کند.

(۸) شرکت +Grid در آستین، از بلاک چین Ethereum برای دسترسی مصرف‌کنندگان به دستگاه‌های صرفه‌جویی انرژی اینترنت اشیا استفاده می‌کند. یک نماینده شرکت از طرف یک کاربر +Grid برق می‌خرد و می‌فروشد، برنامه +Grid به ارائه اطلاعات به‌روز در مورد مصرف انرژی کمک می‌کند و کنتور هوشمند شرکت به صورت بی‌سیم به دستگاه‌های هوشمند کم‌مصرف متصل می‌شود. بلاک‌چین Ethereum این شرکت به نمایندگی‌ها این امکان را می‌دهد که هر ۱۵ دقیقه یک مقدار کارآمد برق پرداخت کنند. پرداخت‌ها و امنیت سایبری در برنامه با استفاده از رمزنگاری بلاک‌چین پیشرفته انجام می‌شود. به عنوان اولین خرده‌فروش انرژی مبتنی بر بلاک‌چین، +Grid اخیرا اولین نمونه اولیه از نماینده خود، Lattice۱ را معرفی کرد. با استفاده از Ethereum، Lattice۱ قادر به شناسایی نوسانات در بازار انرژی و تعیین کارآمدترین نقطه قیمت در زمان واقعی است. این سخت‌افزار ارزهای دیجیتال را ذخیره می‌کند و از آنها برای پرداخت انرژی استفاده می‌کند. [۴]

IOTA .۲-۴

۲-۴-۱. مقدمه‌ای بر IOTA

IOTA [۲۰] یک بلاک‌چین نیست. IOTA یک Distributed Ledger منبع باز[۱] و ارز دیجیتال[۲] است که برای IoE[۳] طراحی شده است. از DAG[۴] برای ذخیره تراکنش‌ها در ledger استفاده می‌کند، که انگیزه آن مقیاس‌پذیری بالقوه بالاتر نسبت به Distributed Ledger مبتنی بر بلاک‌چین است. IOTA توسط بنیاد غیرانتفاعی IOTA با دفتر مرکزی در برلین توسعه و ارائه شده است. هدف بنیاد IOTA ایجاد یک لایه اعتماد برای IoE است که دستگاه‌ها را قادر می‌سازد تا داده‌ها و مقادیر را غیرقابل تغییر و رایگان مبادله کنند. آیوتا در حال همکاری با صنعت و Object Management Group[۵] است تا پروتکل ارتباطی خود را استاندارد کند.

شبکه IOTA در ابتدا به صورت متمرکز[۶] معرفی شد. تراکنش در شبکه تنها در صورتی معتبر تلقی می‌شود که توسط یک milestone صادر شده توسط نودی که توسط بنیاد IOTA به نام Coordinator اداره می‌شود ارجاع داده شود. در سال ۲۰۱۹، بنیاد IOTA اعلام کرد که می‌خواهد در آینده با استفاده از یک به‌روزرسانی شبکه دو مرحله‌ای، به نام Chrysalis برای IOTA ۱.۵ و Coordicide برای IOTA ۲.۰، شبکه را بدون Coordinator راه‌اندازی کند. به‌روزرسانی Chrysalis در ۲۸ آوریل ۲۰۲۱ منتشر شد و برخی طراحی‌های بحث‌برانگیز آن مانند رمزگذاری سه‌گانه و امضاهای یک‌بار مصرف Winternitz را حذف کرد تا یک راه‌حل آماده برای سازمان ایجاد کند. به طور موازی، Coordicide برای ایجاد یک شبکه غیرمتمرکز که دیگر به Coordinator برای Consensus متکی نیست، توسعه یافته است. شبکه آزمایشی Coordicide در اواخر سال ۲۰۲۰، با هدف انتشار نسخه نهایی در سال ۲۰۲۱ راه اندازی شد.

---

[۱] Open Source

[۲] Cryptocurrency

[۳] Internet of Everything

[۴] Directed Acyclic Graph - گراف بدون دور جهت دار

[۵] The Object Management Group is a computer industry standards consortium. OMG Task Forces develop enterprise integration standards for a range of technologies

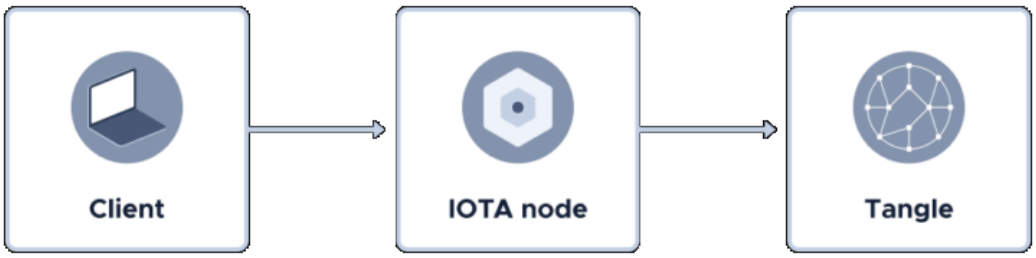
[۶] Centralized

۲-۴-۲. Tangle

IOTA بر اساس فناوری بلاک‌چین سنتی کار نمی‌کند، اما با مفهوم نوآورانه "Tangle" کار می‌کند. Tangle در واقع Distributed Ledger در IOTA است که شامل تاریخچه معاملات فعلی است. Tangle تنها منبع حقیقت است. هر مشتری در سراسر جهان می‌تواند تراکنش‌های معتبر را به یک نود ارسال کند. این تراکنش در سراسر شبکه تکرار می‌شود تا این نسخه واحد از حقیقت شکل بگیرد.

معماری IOTA شامل اجزای اساسی زیر است:

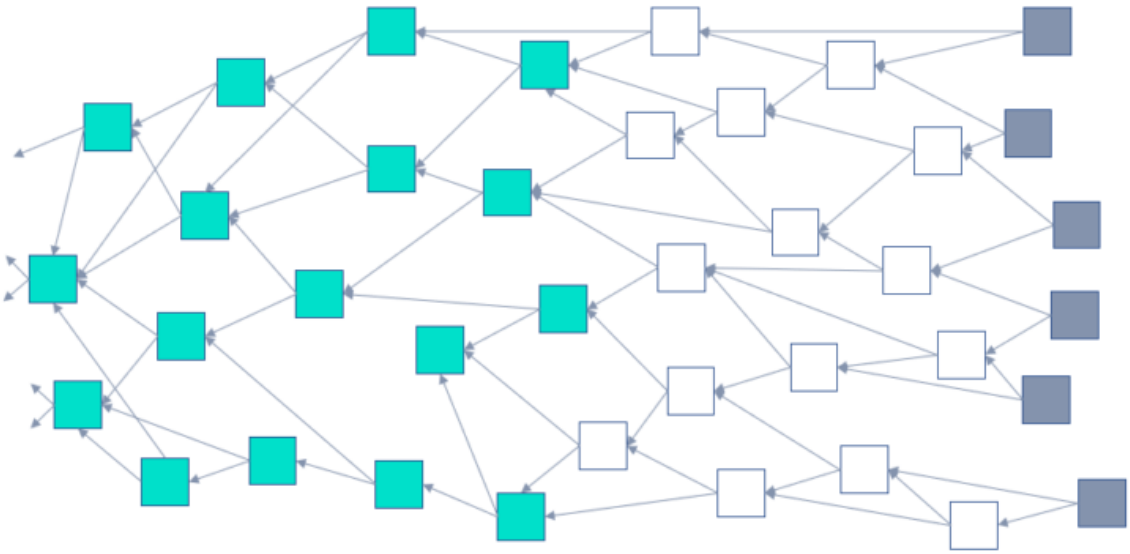
- Clients : کاربران یک شبکه IOTA (کیف پول، برنامه‌ها و غیره) که تراکنش‌ها را به نودها ارسال می‌کنند تا به Tangle متصل شوند.
- Nodes : دستگاه‌های متصلی که مسئول اطمینان از یکپارچگی Tangle هستند. این دستگاه‌ها یک شبکه IOTA را تشکیل می‌دهند.
- Tangle: یک ساختار داده پیوست شده (Public Ledger، Main ledger) ، که در تمام نودهای یک شبکه IOTA تکرار می‌شود. تمام داده‌ها در Tangle در اشیایی به نام تراکنش‌ها ذخیره می‌شوند. هنگامی که یک تراکنش به Tangle متصل می‌شود، نمی‌توان آن را تغییر داد و تغییر ناپذیر[۷] است.



شکل ۱۳. معماری کلی شبکه

از نظر ریاضی، Tangle یک گراف بدون دور جهت‌دار - DAG است.

[۷] Immutable

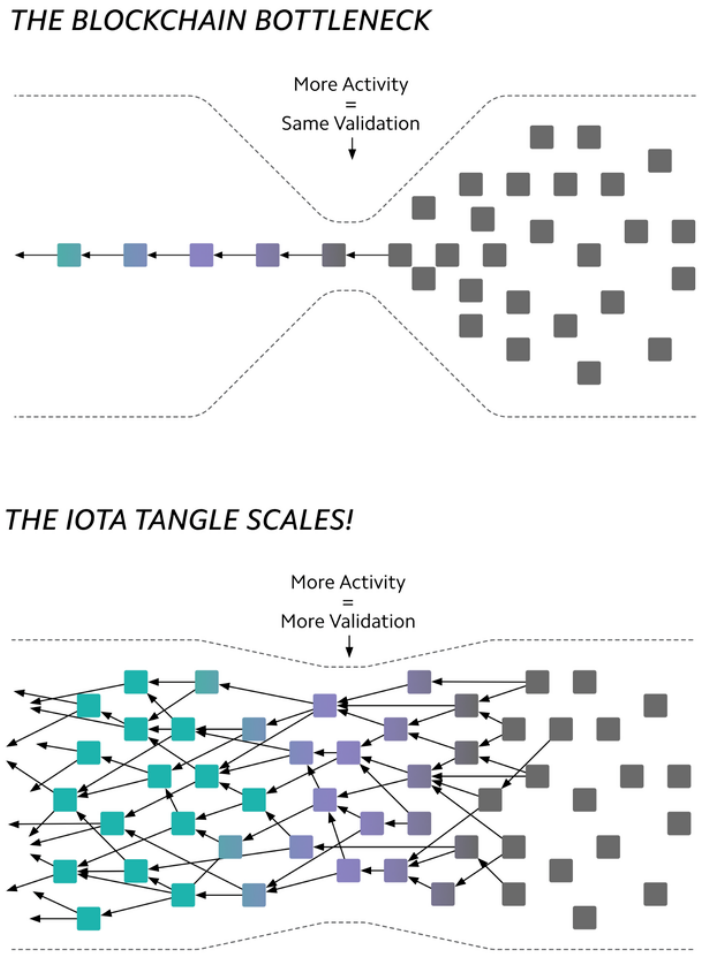


شکل ۱۴. گراف‌جهت‌دار مطرح در Tangle

۱-۲-۴-۲. فرق بلاک چین با Tangle چیست؟

ساختار داده بلاک‌چین شامل زنجیره‌ای از بلوک‌های متوالی است که هر بلاک حاوی تعداد محدودی پیام است. در نتیجه، بلاک‌های جدید فقط می‌توانند به یک مکان متصل شوند؛ یک بلاک در انتهای زنجیره. با توجه به این محدودیت، شبکه‌های بلاک‌چین اغلب زمان تأیید کندی را تجربه می‌کنند. این محدودیت به عنوان گلوگاه بلاک‌چین شناخته می‌شود. همچنین تمام تراکنش‌های یک بلاک‌چین باید منتظر بمانند تا در یک بلوک گنجانده شوند. به دلیل اندازه بلوک و محدودیت‌های زمان تولید بلوک، این امر باعث ازدحام و زمان انتظار برای تراکنش‌ها می‌شود.

در مقابل ساختار داده Tangle یک گراف بدون دور جهت‌دار (DAG) است که در آن هر پیام به دو تا هشت پیام قبلی متصل می‌شود. به جای محدود شدن به یک مکان برای پیوست کردن پیام‌های جدید، می‌توانید پیام‌ها را در مکان‌های مختلف در جلوی Tangle ضمیمه کنید. پروتکل می‌تواند این پیوست‌های مختلف را به صورت موازی پردازش کند و پردازش موازی ازدحام را از بین می‌برد.



شکل ۱۵. مشکل گلوگاه در شبکه‌های سنتی بلاک‌چین

در بلاک‌چین، شرکت کنندگان شبکه به Validators (ماینرها، Stakers) و کاربران تقسیم می‌شوند. ماینرها مقادیر زیادی از توان محاسباتی را برای تکمیل PoW[۸] مورد نیاز برای زنجیر کردن بلوک‌ها به یکدیگر مصرف می‌کنند. ماینرها و سهامداران به دلیل موارد زیر تشویق می‌شوند تا پیام‌ها را تایید کنند:

- هزینه‌هایی که کاربران مایلند برای گنجاندن پیام‌های خود در یک بلوک بپردازند،
- پاداشی که شبکه در قالب توکن‌های تازه ایجاد شده به Validators برای تولید بلوک جدید پرداخت می‌کند.

تنها راه معکوس کردن پیام‌ها در یک بلاک‌چین PoW، استخراج یک بلاک جدید در همان مدت زمانی است که سایر ماینرها برای استخراج یک بلاک واحد نیاز دارند. برای انجام این کار، یک ماینر به ۵۱ درصد از توانایی شبکه برای انجام PoW

[۸] Proof-of-Work

نیاز دارد که به عنوان Hash Power شناخته می‌شود. در نتیجه، الزام Validators به انجام PoW، شبکه‌های بلاک‌چین را با دشوار کردن حمله، تغییر یا توقف آن، ایمن می‌کند. هرچه ماینرها بیشتر مشارکت کنند، امنیت شبکه بیشتر می‌شود.

در Tangle برای ارسال یک تراکنش، باید دو تراکنش قبلی که دریافت کرده‌اید را تایید کنید. هر چه تراکنش‌های بیشتری به Tangle اضافه شود Consensus برا اساس two-for-one و pay-it-forward اعتبار تراکنش‌ها را تقویت می‌کند. از آنجا که Consensus توسط تراکنش ها ایجاد می‌شود، از نظر تئوری، اگر کسی بتواند یک سوم تراکنش‌ها را ایجاد کند، می‌تواند بقیه شبکه را متقاعد کند که تراکنش‌های نامعتبر آنها معتبر هستند. تا زمانی که حجم تراکنش کافی وجود نداشته باشد که ایجاد یک سوم تراکنش‌ها غیرممکن شود، IOTA به نوعی همه تراکنش‌های شبکه را روی یک گره متمرکز به نام Coordinator بررسی مضاعف می‌کند. آیوتا می‌گوید Coordinator مانند چرخ‌های آموزشی برای سیستم عمل می‌کند و زمانی که Tangle به اندازه کافی بزرگ شد حذف می‌شود.

۲-۴-۲-۲. چرا تراکنش‌ها در IOTA بدون هزینه است؟

اکثر ارزهای دیجیتال غیرمتمرکز، از جمله شناخته‌شده‌ترین آن‌ها مانند Bitcoin، Ethereum و بسیاری دیگر از هر کسی که در شبکه تراکنش انجام می‌دهد، باید هزینه‌ای را برای خدمات ارائه شده بپردازد. این صرفاً یک ویژگی الحاقی برای آن ارزهای دیجیتال نیست که به راحتی قابل حذف باشد بلکه یک جنبه اساسی از نحوه کار آنها است.

از آنجایی که Consensus در IOTA Tangle به گونه‌ای طراحی شده است که اضافه کردن هر تراکنش ملزم به تأیید دو تراکنش قبلی است، هزینه‌ای برای اضافه کردن تراکنش نیازی نیست.

۲-۴-۳. چه چیزهایی باعث شده IOTA برای IOT بهینه باشه؟

اینترنت اشیا روز به روز در حال گسترش است که این امر منجر شده مدیریت آن سخت و دشوار باشد و همچنین به دلیل رشد سریع این حوزه، مسائلی مانند پرایوسی، امنیت و کنترل شبکه‌ی آن‌ها مسائلی بسیار حساس بوده که با توجه به این رشد سریع، کمتر به آن‌ها پرداخته شده و همزمان با خود تکنولوژی پیشرفت مناسبی نکرده‌اند. اما در مقابل شبکه‌های بلاک‌چینی سابقه مشابهی دارند اما هدف از بوجود آمدن آن‌ها دقیقا نواقص اینترنت اشیا بوده و هدف اصلی آن، ایجاد شبکه‌ای ایمن و گسترده با شفاف بودن تمام تراکنش‌ها بوده است که گزینه مناسبی برای کمک به اینترنت اشیا می‌باشد.

برای این منظور کمپانی IOTA برای اولین بار دست به کار شد و با بهره‌گیری از شبکه‌های بلاک‌چینی و با هدف قرار دادن اینترنت اشیا، بستری مناسب برای ایجاد شبکه‌ای امن در این حوزه فراهم نموده است.

یکی از ویژگی‌هایی که در قسمت ۲-۴-۲ به آن اشاره شد، تراکنش‌های بدون هزینه در این شبکه بود که به علت فراوانی نودهای اینترنت اشیا و همچنین هدفی که این شبکه‌ها دنبال می‌کنند، IOTA گزینه مناسبی برای شبکه‌های اینترنت اشیا می‌باشد.

نودهای اینترنت اشیا به طور معمول از قدرت پردازشی مناسبی برخوردار نیستند و استفاده‌ی آن‌ها ایجاب می‌کند تا بر روی مسائل دیگر مانند کوچک بودن، بهینه بودن مصرف انرژی و ارتباطات شبکه محدودتر در این حوزه پرداخته شود که این امر باعث می‌شد شبکه‌های بلاک‌چینی مرسوم مانند اتریوم و بیت‌کوین، به علت عملیات PoW که در آن‌ها تعریف می‌شود

گزینه‌مناسبی برای این حوزه نباشند زیرا نودها متحمل هزینه‌های محاسباتی سنگینی می‌شدند که این مشکل در IOTA به دو دلیل کم‌رنگ‌تر شده است:

- حذف هزینه تراکنش و حذف عملیات پیچیده PoW که در ۲-۴-۲ مفصل توضیح داده شد،
- استفاده از Tangle که باعث حذف گلوگاه‌های مرسوم در شبکه‌های بلاک‌چینی می‌شود.

حذف این تراکنش‌ها و همچنین استفاده از قاعده two-for-one، باعث تراکنش‌های سریع‌تر در شبکه می‌شود و به علت تعداد زیاد نودهایی که در شبکه‌های اینترنت اشیا داریم، این یک مزیت بسیار مناسب برای استفاده از IOTA در این شبکه‌ها شده است.

همچنین در شبکه‌ی IOTA شرایطی فراهم آورده شده است که می‌توان از اکثر VMهای مطرح برای ایجاد قراردادهای هوشمند بر روی chain مربوط به هر نود wasp استفاده کرد که باعث می‌شود بتوان عمکردهای مختلف بر روی شبکه و نودها ایجاد کرد. استفاده از قراردادهای هوشمند در شبکه باعث ایجاد قابلیت‌های متنوعی در شبکه‌های اینترنت اشیا می‌شود که کمپانی IOTA علاقه‌مند است به این اهداف برسد. با بوجود آمدن این شبکه و استفاده‌ی نودها از آن، هر نود می‌تواند به صورت انفرادی، هزینه‌ها و قبض‌های مربوط به سرویس‌های شبکه، سرویس‌های برق‌رسانی و تمامی هزینه‌های خود را به صورت مستقل و با توکن مطرح در شبکه، به ISP[1] یا دیگر ارائه‌دهنده‌های مطرح پرداخت کند و یا از آن‌ها سرویس‌های جدید اتخاذ کند. همچنین با پیشرفت شبکه، هر نود می‌تواند براساس مصرف و نیاز خود، مازاد منابع خود را به دیگر نودها در شبکه بفروشد و یا در شرایط ضروری، منابع را از دیگران خریداری کند که این امر باعث تسریع تراکنش‌ها و پویایی شبکه و همچنین ارتباط بیشتر نودها با یکدیگر می‌شود.در واقع ارزش هر چیز در شبکه با ارزش توکن داخل شبکه سنجیده شده و تمامی داد و ستدها بهینه می‌شود.

همیشه در کنار اسم اینترنت اشیا، مفاهیم دیگری مانند بیگ‌دیتا مطرح می‌شود و علت آن، توسعه‌پذیر بودن و گستردگی استفاده از نودهای اینترنت اشیا است. به این منظور داده‌ای که توسط این نودها تولید می‌شود می‌تواند ارزش‌مند باشد و با استفاده از قراردادهای هوشمند، می‌توان عملیات‌های مختلفی بر روی این داده‌ی تولیدی انجام داد. همچنین شرکت‌های زیادی هستند که امروزه، داده خام تولیدی توسط سنسورها را از یک شرکت مربوطه و برای اهداف آکادمیکی/ تجاری خریداری می‌کنند و با بوجود آمدن شبکه بلاک‌چینی مذکور در این حوزه، هر نود سنسور می‌تواند داده‌ای که حس می‌کند را مستقیما و به صورت خام به مرکز درخواست کننده بفروشد و بر روی شبکه توکن معادل دریافت کند و هزینه‌های خود را با آن پرداخت کند.

۳-۴-۲. توضیحات فنی

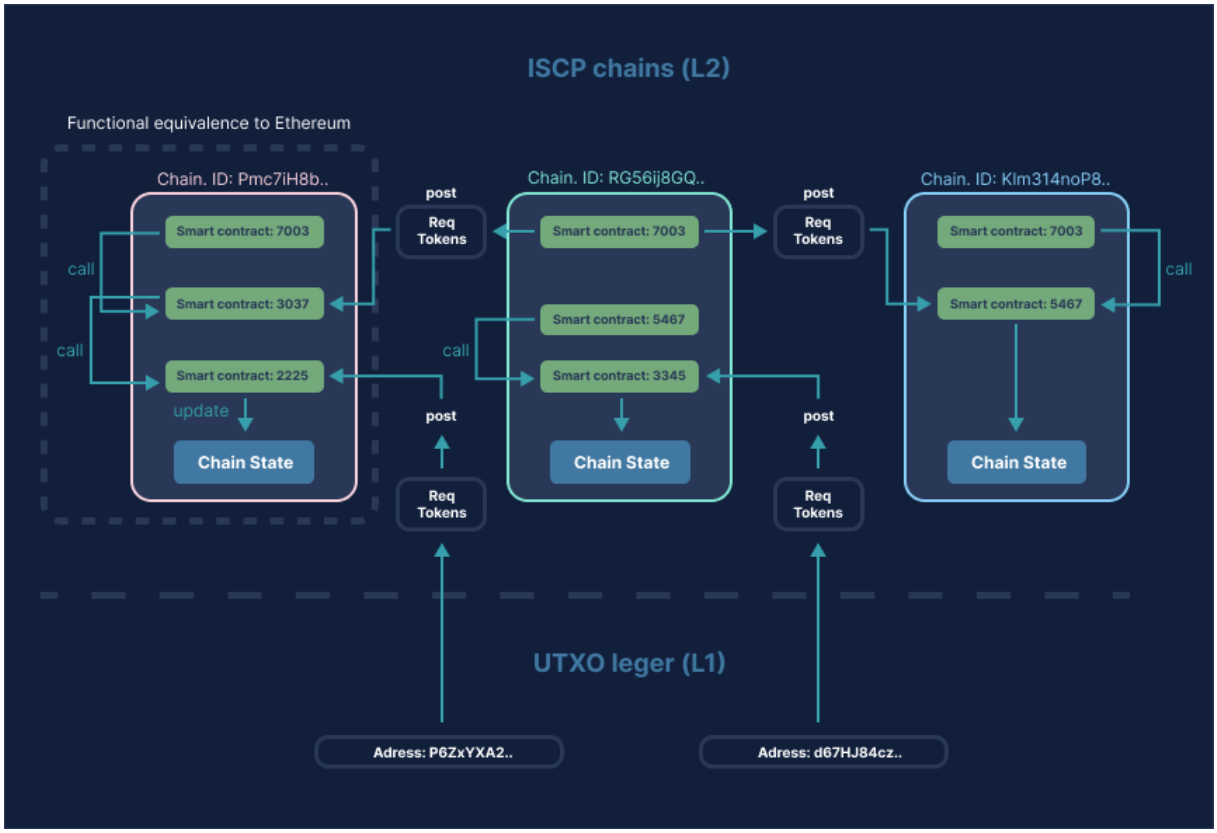
۲-۴-۳-۱ .توضیح اولیه معماری کلی

با توجه به فاز اولیه IOTA ۲.۰ و وجود Coordinatorها در شبکه، شبکه‌ای برای اهداف توسعه‌ای توسط کمپانی مربوطه به اسم شبکه devnet ایجاد شده است که برای توسعه دهندگان قابل استفاده است و هیچ توکنی درون آن ارزش مادی ندارد.

در IOTA برای ایجاد یک شبکه حداقلی نیاز به یک یا تعدادی نود validator داریم که بتوانند هر کدام یک chain را مدیریت کرده و همچنین تراکنش‌ها و قراردادهای هوشمندی که درون آن chain ایجاد می‌شوند را کنترل کند. به این نود validator در شبکه IOTA، نود WASP می‌گوییم که برای ایجاد یک شبکه حداقلی نیاز به حداقل یک نود Wasp داریم. حال می‌توانیم تعداد بیشتری نود wasp بر روی شبکه قرار دهیم و در واقع هر نود یک committee member شده و همگی تراکنش‌های موجود در هر chain را بررسی و تایید می‌کنند.

۲-۴-۳-۲. قراردادهای هوشمند

در IOTA معماری قراردادهای هوشمند معماری ISC[۲] نام دارد و در آن هر شخص می‌تواند یک chain شخصی بسازد و بقیه را دعوت به validate کردن آن زنجیر بکند که به مجموعه این‌ها، لایه ۲ گفته می‌شود. هر زنجیر state و قراردادهای هوشمند مربوط به خود دارد که آن قرارداد را هر نود wasp بر روی زنجیر خود اجرا می‌کند و بعد از تغییر در state آن زنجیر، کمیته آن را تایید کرده و به لایه ۱ که Tangle است فرستاده می‌شود. برای هر زنجیر، VM های معروف متعددی می‌تواند اجرا شود که از معروف‌ترین آن‌ها می‌توان به WASM[۳] و EVM[۴] اشاره کرد. عملکرد هر زنجیر لایه ۲ کاملا مشابه قراردادهای هوشمند در اتریوم است اما در اینجا همه‌ی زنجیرها با یکدیگر و همچنین لایه ۱ می‌توانند ارتباط برقرار کنند که همین امر باعث می‌شود قراردادهای هوشمند در این معماری کمی پیچیده‌تر از قراردادهای هوشمند در معماری اتریوم باشد.



شکل ۱۶. معماری چند زنجیری قراردهای هوشمند در IOTA

۲-۴-۳-۳. نود GoShimmer

همانطور که در قسمت‌های قبلی گفته شد، IOTA ۲.۰ در نسخه آلفا قرار دارد و برای اتصال بدون coordinator به شبکه devnet اصلی، پروتوتایپی نوشته شده با زبان Go تحت عنوان GoShimmer ارائه شده است که توسعه‌دهندگان می‌توانند با استفاده از این نودها، شبکه شخصی خودشان را به شبکه devnet متصل کنند. داخل توضیحات سایت عنوان شده است که بهتر است هر نود wasp و زنجیر شخصی ساخته شده به یک نود GoShimmer جدا متصل شود اما امکان اتصال چند validator به یک نود واحد نیز وجود دارد.

۲-۴-۳-۴. نود Hornet و نود Bee

راحت‌ترین راه برای اتصال به شبکه اصلی استفاده از یکی از دو نود Hornet و یا Bee است که توسط کمپانی IOTA ارائه شده‌اند. تفاوت Hornet و Bee در تکنولوژی برنامه‌نویسی پشت آن‌هاست و Hornet به زبان Go نوشته شده و اما Bee به زبان Rust توسعه داده شده است. در حال حاضر این دو بر روی شبکه IOTA ۱.۵ (شبکه‌ی Chrysalis) قابل استفاده هستند. شخص با استفاده از هر یک از این دو نود، قابلیت‌های زیر را در اختیار می‌گیرد:

- اتصال مستقیم به شبکه IOTA بدون نیاز به اتصال و تایید نود شخص دیگر
- کمک به شبکه‌ی IOTA که باعث scalable تر شدن شبکه و همچنین امن‌تر شدن شبکه با تایید پیام‌ها و تراکنش‌های درون شبکه

۲-۴-۴. کاربرهای IOTA

با پیشرفت شبکه IOTA استفاده‌های زیادی می‌توان برای آن متصور شد.

استفاده‌هایی مانند:

- تاثیرات اجتماعی (Social Impact)
- استفاده در دستگاه‌های در حال حرکت مانند خودرو خودران
- شهرهای هوشمند
- تجارت جهانی
- هویت دیجیتال

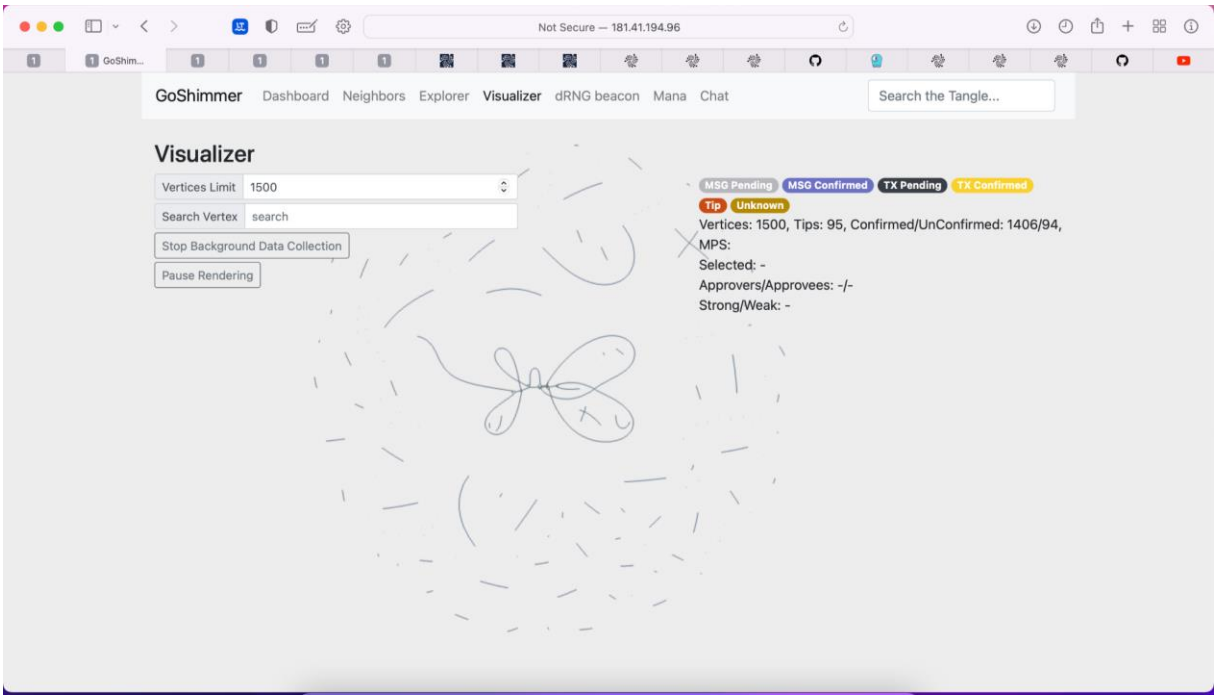
۲-۴-۵. پیاده‌سازی‌های انجام شده

با توجه به توضیحات داده‌شده در قسمت‌های بالاتر، تصمیم بر آن شد پروتوتایپی از شبکه IOTA بر روی شبکه‌ی خصوصی (private network) پیاده‌سازی شود و سپس به صورت عملی با مفاهیم تراکنش‌های اولیه و یکسری از مفهوم‌های

اولیه بلاک‌چین بر روی شبکه ساخته شده آشنایی صورت گیرد. برای این منظور، ابتدا یک سرور مجازی (VPS) تهیه شد تا بتوانیم دسترسی گروهی به زیرساخت‌های مورد انتظار داشته باشیم.

۱-۵-۴-۲. پیاده‌سازی نود GoShimmer

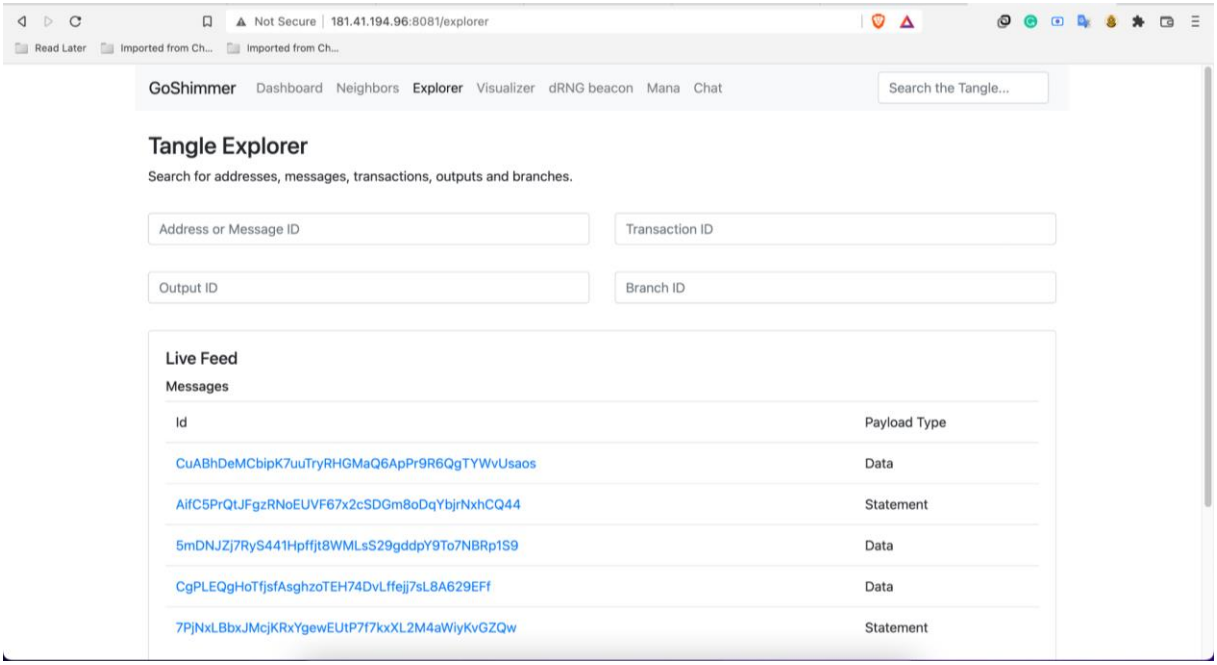
بعد از تنظیمات اولیه سرور مذکور، در ابتدا یک نود GoShimmer بر روی سرور به صورت کانتینر داکر اجرا شد و تنظیمات مربوط به شبکه آن صورت گرفت که این نود بعنوان پروتوتایپی از شبکه IOTA ۲.۰ و به صورت gateway ای برای شبکه داخلی ما با شبکه devnet اصلی قرار گرفت که بتوانیم بدون استفاده از Coordinator[پانویس] و با بهره‌گیر از پروتوتایپ ارائه شده در فاز آلفا توسط بنیاد IOTA، شبکه داخلی خود را به زیرساخت این شبکه تست متصل کنیم. نود GoShimmer داشبوردی در اختیار ما قرار می‌دهد که ویژگی‌های متنوعی دارد که در ادامه به بررسی این ویژگی‌ها می‌پردازیم:



شکل ۱۷. نمای نود GoShimmer اجرا شده

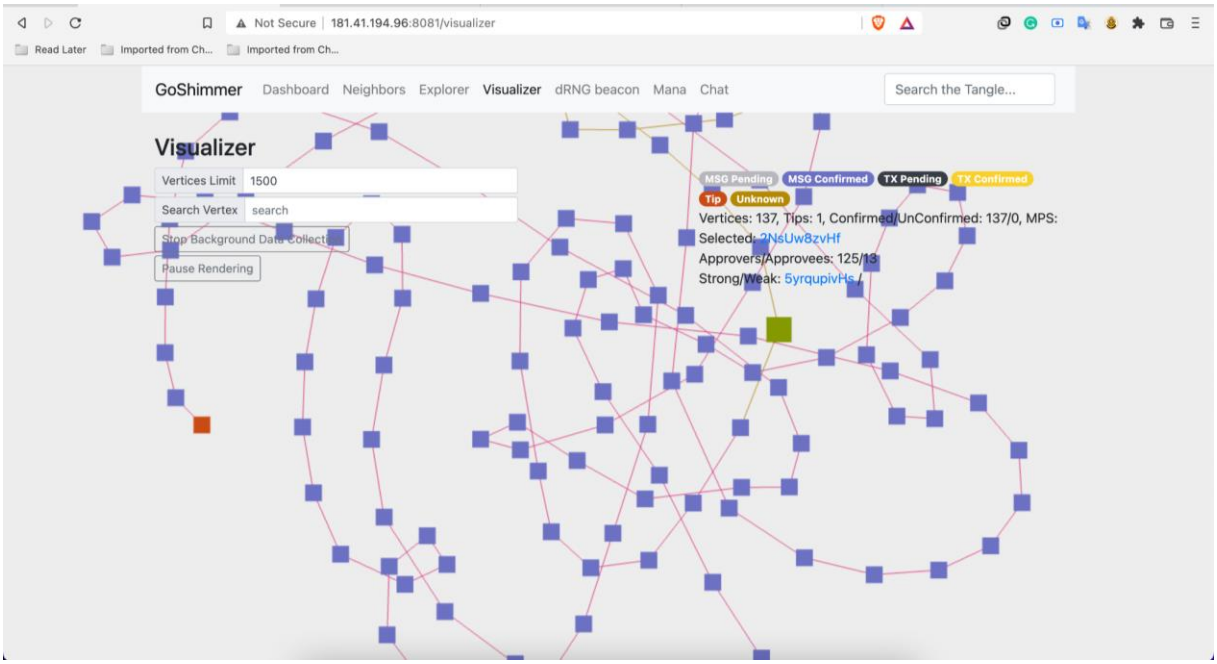
بر روی داشبورد ارائه شده توسط GoShimmer امکانات زیر فراهم شده است:

- امکان پیدا کردن همسایه‌ها در قسمت Neighbors
- مشاهده لاگ‌های شبکه به صورت زنده و همچنین پیدا کردن تراکنش‌ها و یا پیام‌های رد و بدل شده در قسمت اکسپلورر که در قسمت زیر می‌توانید مشاهده کنید:



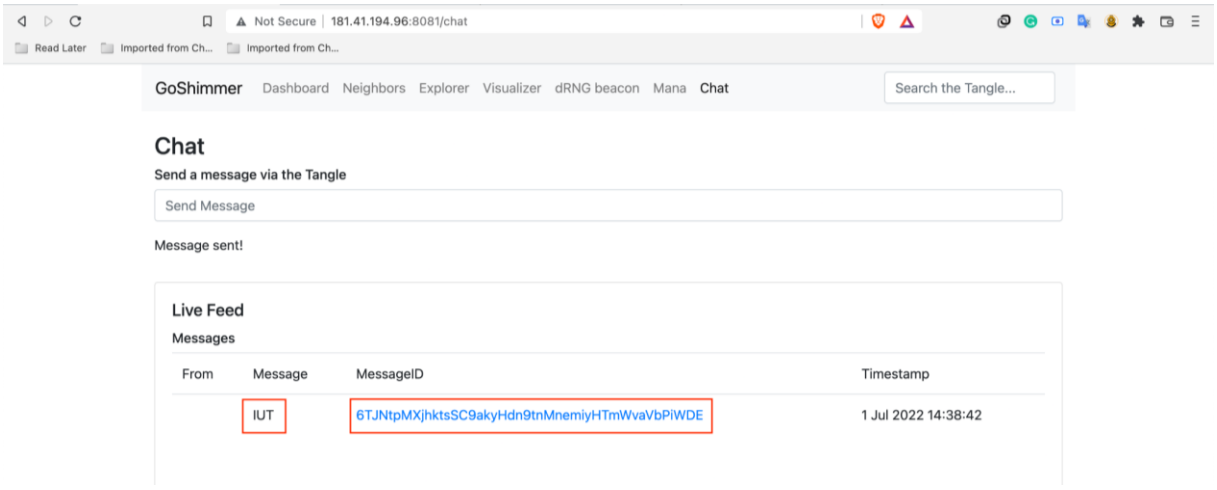
شکل ۱۸. داشبورد نود GoShimmer

- در قسمت visualizer می‌توانید معماری شبکه تا جایی که شبکه اجرا شده و با محدودیت‌های اعمال شده را مشاهده کنید که در عکس زیر یک نمونه دیگر از معماری شبکه ساخته شده قابل مشاهده است:

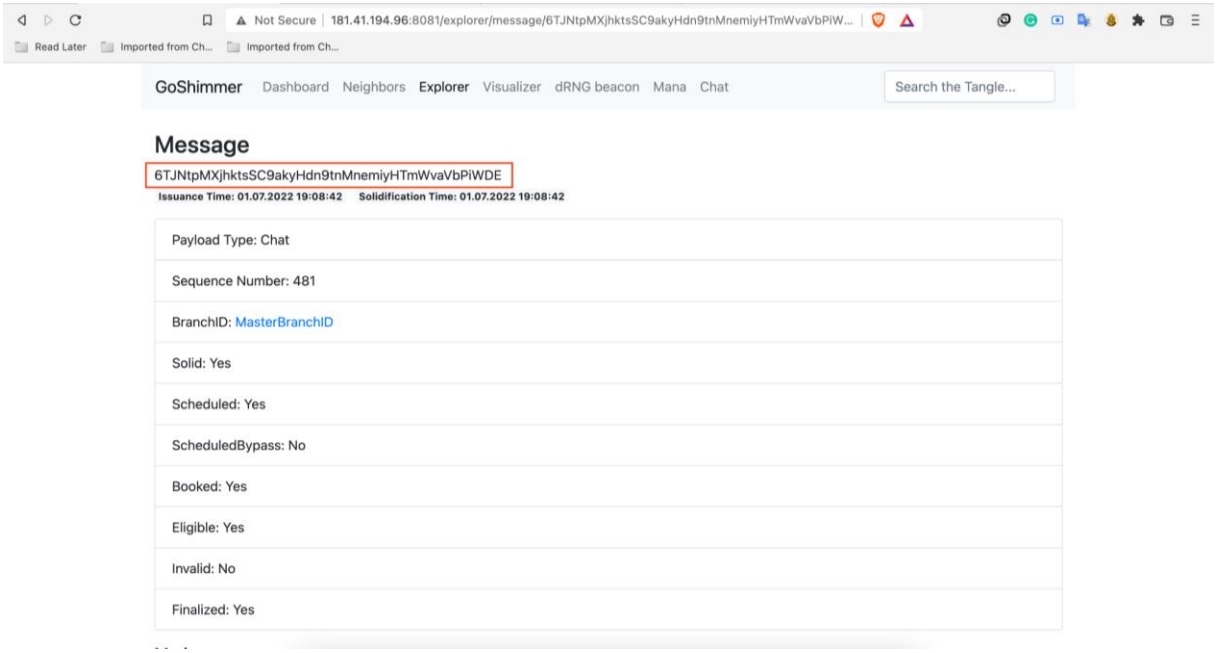


شکل ۱۹. شمای شبکه‌ی شکل گرفته بوسیله‌ی نودهای شبکه devnet بر روی نود GoShimmer اجرا شده

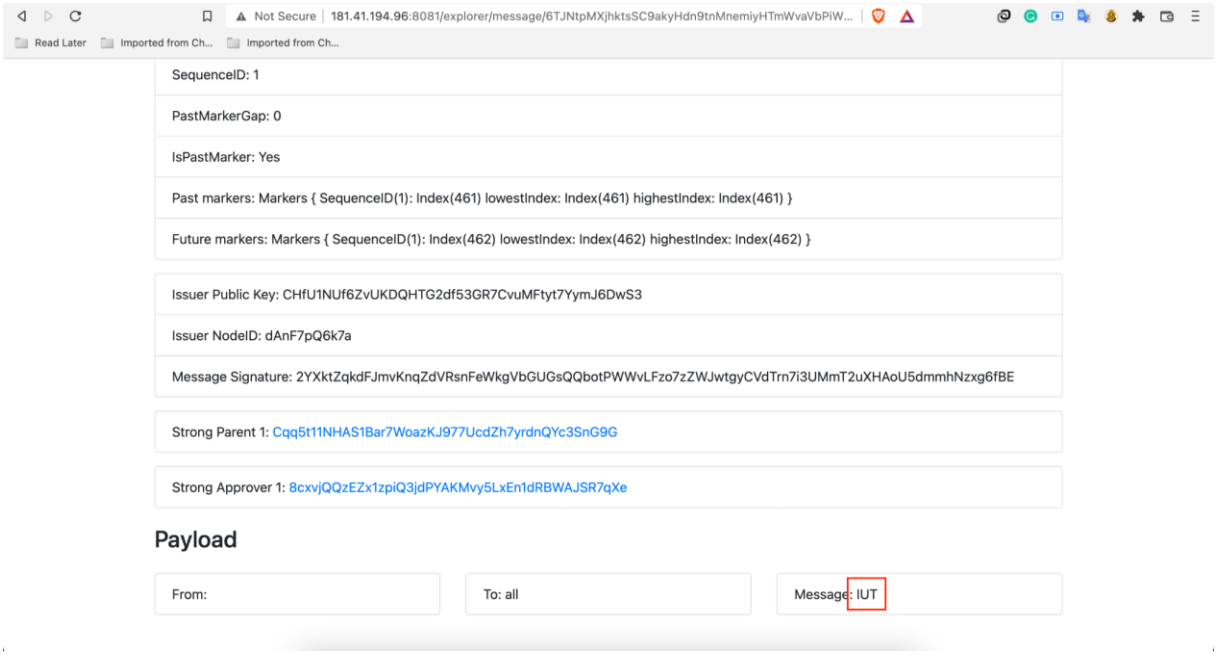
- در قسمت Chat می‌توان پیام‌هایی به صورت دستی و بدون نیاز به کد نویسی، به صورت همه‌پخشی در شبکه ارسال کرد:



شکل ۲۰. قسمت مربوط به Chat در نود GoShimmer



شکل ۲۱. در بالا پیام message ای که در قسمت Chat ایجاد شده بود قابل مشاهده است



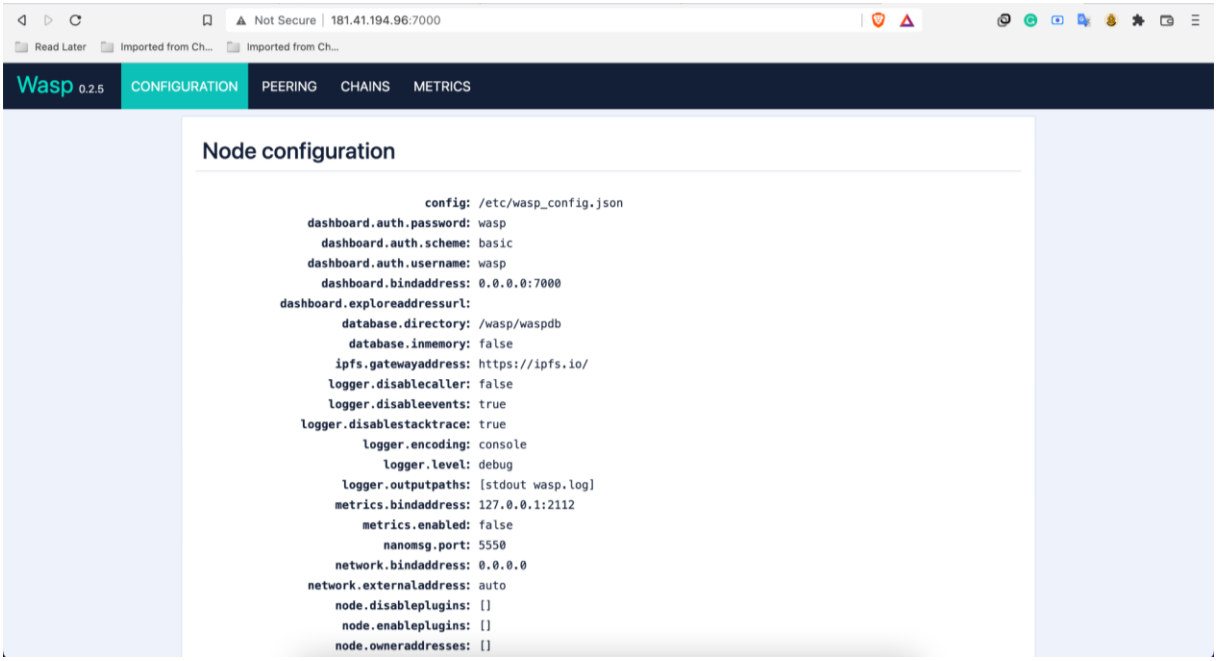
شکل ۲۲. در بالا در باکس قرمز محتوای پیام ایجاد شده در شبکه بلاک‌چین قابل مشاهده است

در عکس‌های بالا قابل مشاهده است که پیامی تحت عنوان IUT در قسمت Chat به شبکه ارسال شده است و با توجه به Transaction ID آن تراکنش، در قسمت اکسپلورر آن را پیدا کرده و محتوای آن را در شبکه مشاهده می‌کنیم که هرکسی با داشتن Transaction ID می‌تواند آن را در شبکه مشاهده کند.

۲-۴-۵-۲. پیاده‌سازی نود Wasp

با پیاده‌سازی نود wasp نیز داشبوردی در اختیار ما قرار می‌گیرد که در آن می‌توانیم نودها را به یکدیگر متصل کرده و chain

مربوط به نود را بررسی و همچنین تعداد توکن‌های موجود در والت نود wasp را نیز مشاهده کرد.

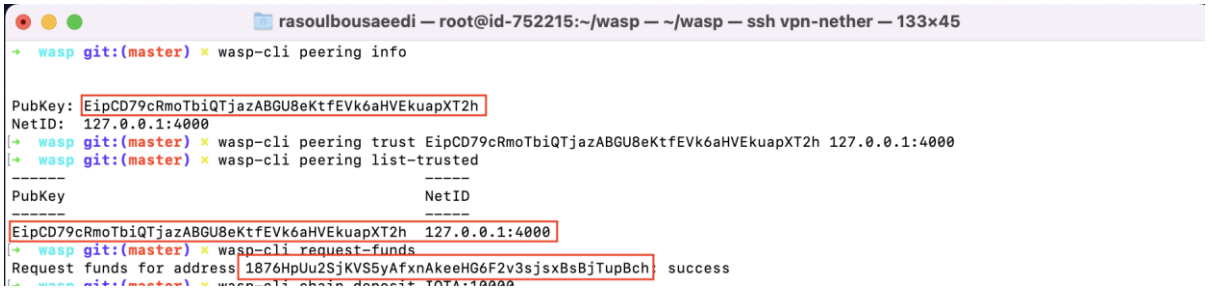


شکل ۲۳. نود Wasp اجرا شده در بالا قابل مشاهده است

۲-۴-۵-۳. ساخت تراکنش

حال در ابتدا نود wasp را به شبکه نود GoShimmer متصل می‌کنیم.

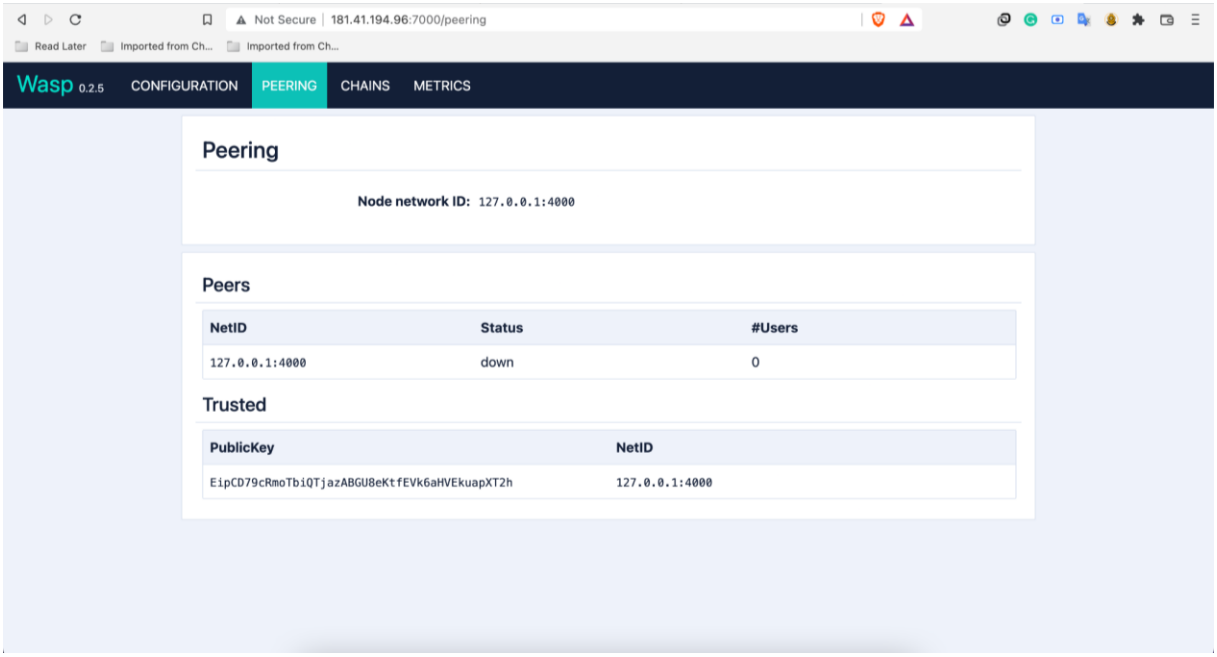
برای اینکار ابتدا باید hash address نود شبکه را پیدا کرده و سپس به trusted list نود wasp اضافه کنیم که برای این کار از ابزار wasp-cli که توسط بنیاد IOTA عرضه شده و در ریپوزیتوری گیت‌هاب موجود است استفاده می‌کنیم (لازم به ذکر است که باید کامل ریپوزیتوری را بیلد کرده و سپس تنظیمات اولیه wasp-cli را نیز انجام دهیم که از این مرحله در گزارش صرفه نظر شده است):



شکل ۲۴. نود Wasp اجرا شده، به شبکه بالا آمده متصل شده و با یکدیگر peer شدند

مربع سوم wallet address مربوط به نود wasp است که با دستور اجرا شده مبلغ ۱میلیون توکن به ولت این نود واریز شده است.

همچنین trusted list را می‌توان در نود wasp نیز مشاهده کرد که اضافه شده است:



شکل ۲۵. قسمت peering نود wasp

حال باید یک chain برای این نود بسازیم. سپس می‌خواهیم مقدار ۱۰ هزار توکن از این ولت برداشت کرده و به درون شبکه chain ساخته شده واریز کنیم که در شکل زیر قابل مشاهده است:

```
[→  wasp git:(master) ✗ wasp-cli chain deploy --committee=0 --quorum=1 --chain=mychain --description="My chain"

creating new chain. Owner address: 1876HpUu2SjKVS5yAfxnAkeeHG6F2v3sjsxBsBjTupBch. State controller: Ry3ya7mmpc4stnLrcNfr3Rh7469ai67dT
5YBxEq1CV2Y, N = 1, T = 1
creating chain origin and init transaction GD3yTTwNnxcWxpXfyrYH7dBrbNsxzptiFQt8t8MH7BMP.. OK
sending committee record to nodes.. OK
activating chain sBpYw2X4Rtmyuxogns7f1Fm5XiqYRrJPaUHwVtD9G9LS.. OK.
chain has been created successfully on the Tangle. ChainID: $/sBpYw2X4Rtmyuxogns7f1Fm5XiqYRrJPaUHwVtD9G9LS, State address: Ry3ya7mmpc
4stnLrcNfr3Rh7469ai67dT5YBxEq1CV2Y, N = 1, T = 1
[→  wasp git:(master) ✗ wasp-cli chain deposit IOTA:10000
Posted on-ledger transaction 3FGzuzzqLgaX3yRsGMcgBaMqEcQPwhBapQxnGgRHJDEe containing 1 request:
  - #0 (check result with: /root/wasp/wasp-cli chain request kkyiDbHko8jJArBaahadvLCZJqpNNz6R8Qa79MuLqCBrvT)
Waiting for tx requests to be processed...
→  wasp git:(master) ✗
```

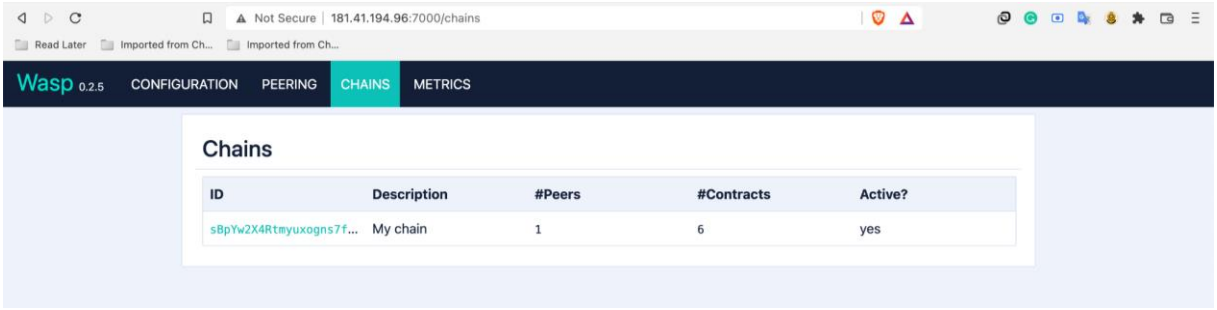
شکل ۲۶. هش آی‌دی تراکنش ایجاد شده

در دستور اول تعداد نودهای committee و id نودها مشخص شده است که در اینجا ۰ به معنای wasp.۰ است که در تنظیمات wasp-cli کانفیگ‌های مربوطه را انجام داده‌ایم و در زیر این تنظیمات قابل مشاهده است:

```
  GNU nano 4.8                                                wasp-cli.json
{
  "chain": "mychain",
  "chains": {
    "mychain": "sBpYw2X4Rtmyuxogns7f1Fm5XiqYRrJPaUHwVtD9G9LS"
  },
  "goshimmer": {
    "api": "127.0.0.1:8080",
    "faucetpowtarget": -1
  },
  "wallet": {
    "seed": "4iNFetKxDuNegRLviCfqRKtqkXRrqV1UtqmpfVBCTzqj"
  },
  "wasp": {
    "0": {
      "api": "0.0.0.0:9090",
      "nanomsg": "0.0.0.0:5550",
      "peering": "0.0.0.0:4000"
    }
  }
}
```

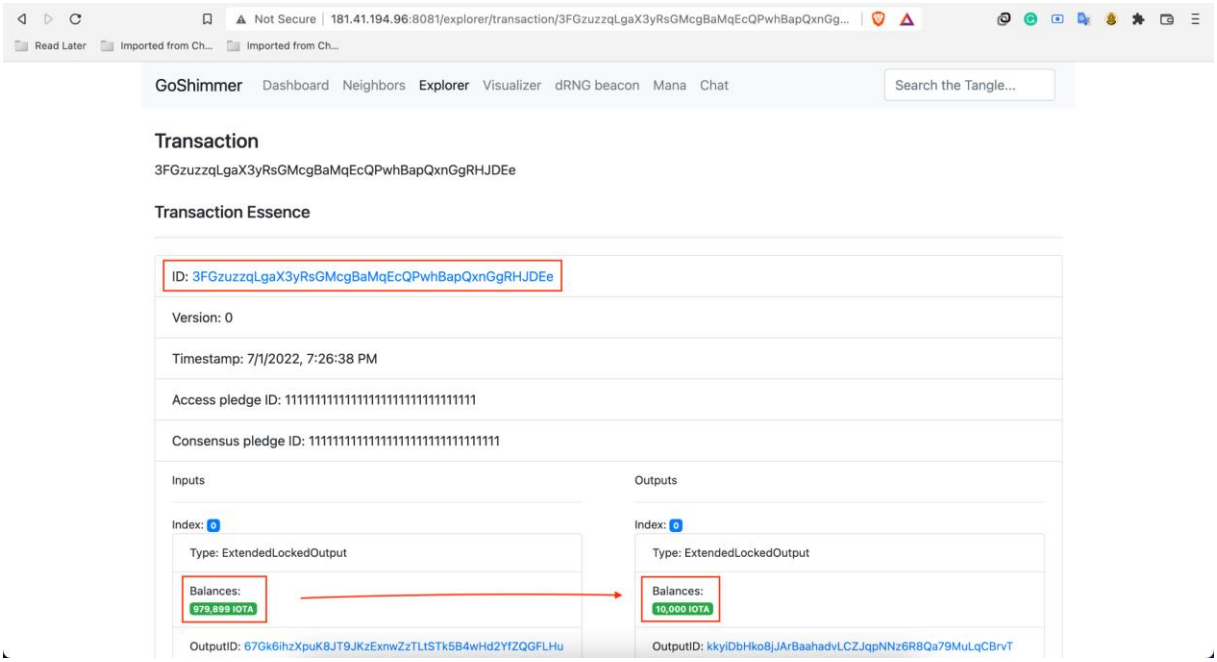
شکل ۲۷. تنظیمات مربوط به wasp-cli

همچنین chain ساخته شده در نود Wasp نیز قابل مشاهده است:



شکل ۲۸. زنجیر ایجاد شده در داشبورد Wasp

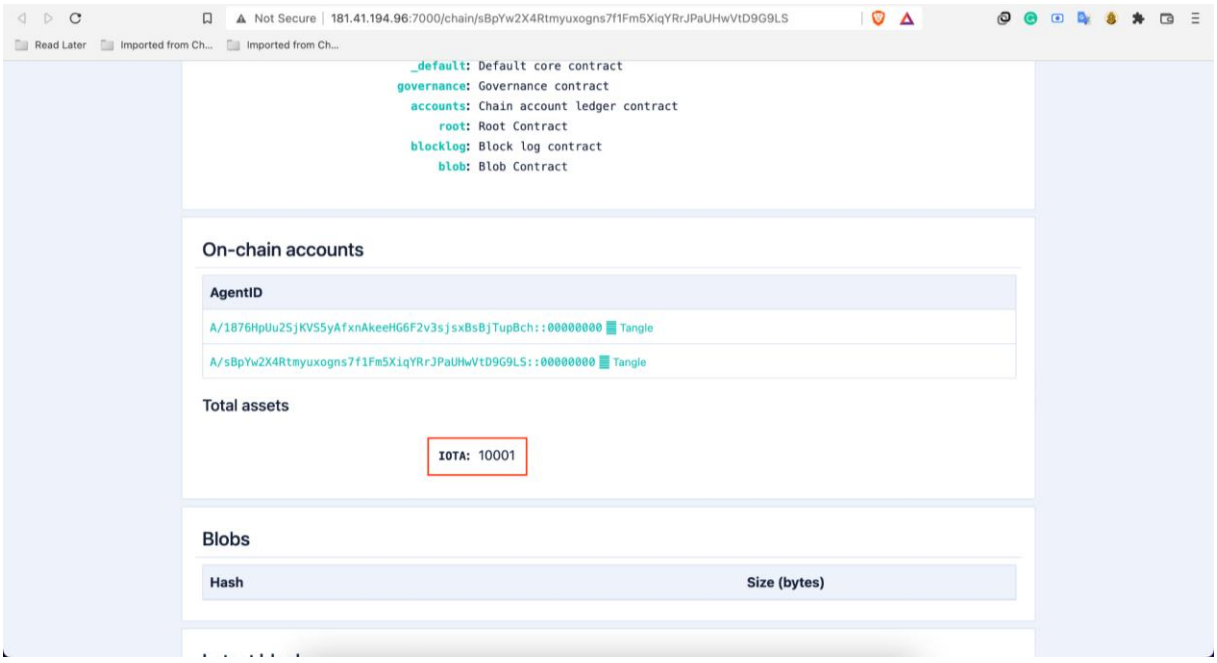
حال transaction ID را در explorer سرچ می‌کنیم:



شکل ۲۹. هش آی‌دی تراکنش ایجاد شده در قسمت Explorer داشبورد نود GoShimmer

قابل مشاهده است که مبلغ ۱۰ هزار توکن از حساب اصلی کم شده و موجودی حساب قبل ۱ میلیون توکن بوده است.

این تغییرات را در داشبورد نود wasp نیز می‌توانیم مشاهده کنیم:



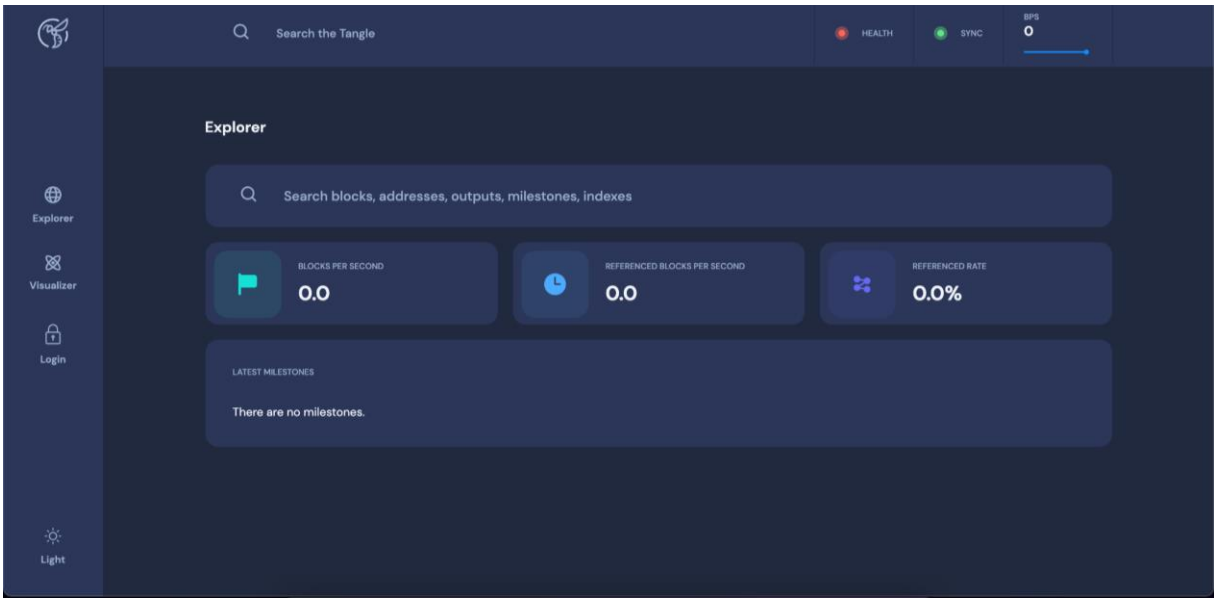
شکل ۳۰. تمام assetهای روی شبکه زنجیر ساخته شده

۲-۴-۵-۴. اجرای نود Hornet بر روی برد Raspberry Pi

از آنجایی که علاقه‌مند بودیم تا کمی به دنیای اینترنت اشیا نزدیک‌تر باشیم، یکی از بردهای معروف در این حوزه یعنی بورد رزبری‌پای را انتخاب کرده و یک نود بر روی آن اجرا کردیم.

برای تست این پلتفرم ترجیح دادیم نود Hornet را اجرا کرده و رزبری‌پای را به شبکه اصلی متصل کنیم تا با نود Hornet نیز آشنا شده باشیم.

در ادامه عکسی از داشبوردی که این نود در اختیار ما قرار می‌دهد قابل مشاهده است:

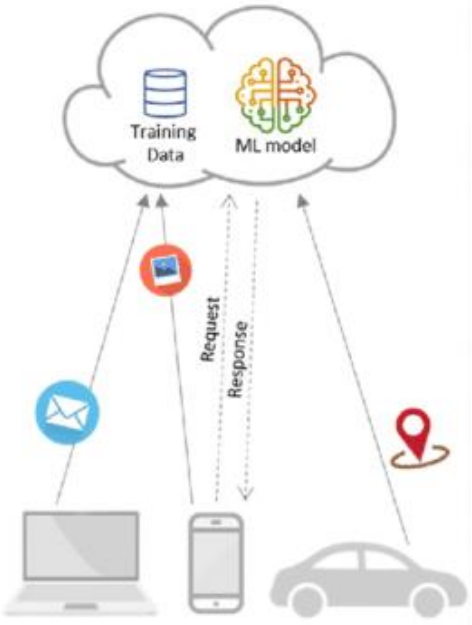


شکل ۳۱. داشبورد نود Hornet اجرا شده برروی رزبری‌پای

۲-۵. Federated learning

همانگونه که در قسمت‌های قبل نیز اشاره کردیم، اینترنت اشیا حجم عظیمی از داده‌ها را از میلیون‌ها دستگاه تولید می‌کند که استفاده صحیح و درست از این داده‌ها سبب می‌شود بتوانیم این داده‌ها را تجزیه و تحلیل کنیم تا در نهایت بتوانیم از نتایج آن بهره مند شویم. چه بخواهیم توانایی پیش‌بینی برای رویدادهای آینده را داشته باشیم، چه بخواهیم به عنوان یک شرکت تبلیغات مرتبط به هر مشتری را به او نمایش دهیم و یا هدفمان افزایش عملکرد شبکه اینترنت اشیا باشد استفاده از یادگیری ماشین در شبکه اینترنت اشیا برایمان اجتناب ناپذیر است. یادگیری ماشین با استفاده از داده‌ها به عنوان ورودی، یک بینش، روند، اطلاع و یا الگوریتم به عنوان خروجی می‌دهد. یادگیری ماشین از رفتار گذشته برای شناسایی الگوها و ایجاد مدل‌هایی استفاده می‌کند که به پیش‌بینی رفتار و رویدادهای آینده کمک می‌کند.

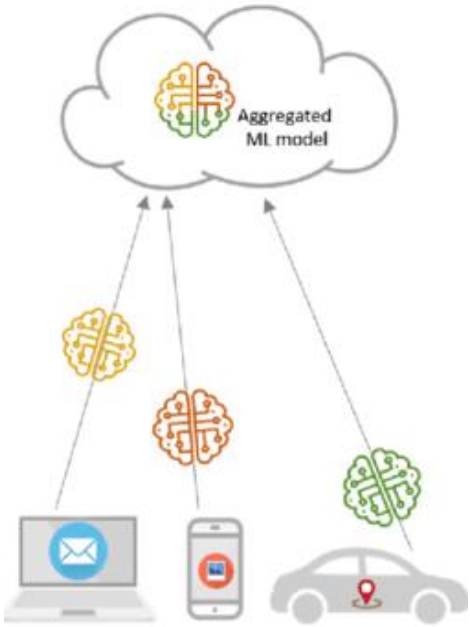
اگر بخواهیم از رویکرد یادگیری ماشین معمول و متمرکز در اینترنت اشیا استفاده کنیم باید داده‌ها را از دستگاه‌های مختلف جمع‌آوری کنیم و به یک سرور مرکزی بفرستیم، سپس با استفاده از روش‌های مناسب یک مدل به دست آوریم و به صورت مرتب این روند را تکرار کنیم، سپس داده‌های جدید جمع‌آوری کنیم و با استفاده از آنها مدل خود را تمرین دهیم و بهبود ببخشیم و سپس از آن استفاده کنیم. به طور خلاصه یعنی ما یک سرور مرکزی داریم که همه داده‌ها در آن جمع‌آوری می‌شوند و در همان سرور مدل یادگیری ماشین تمرین داده می‌شود.



شکل ۳۲. مدل‌سازی با رویکرد ML متمرکز

در این رویکرد چندین اشکال بنیادین وجود دارد. مهم‌ترین آنها حفظ نشدن حریم خصوصی افراد است. شاید فردی که صاحب اتوموبیلی است اجازه ندهد موقعیت مکانی او برای سرور مرکزی فرستاده شود. ممکن است بیمارها و مراکز پزشکی نخواهند اطلاعات حساس آنها که توسط دستگاه‌های اینترنت اشیا جمع‌آوری شده از دایره پزشک و بیمار خارج شود. اینجاست که باید به فکر یک رویکرد توزیع‌شده و غیرمتمرکز باشیم تا داده‌ها، نزد خود استفاده‌کنندگان و در خود دستگاه‌های اینترنت اشیا بمانند.

Federated learning یا به اختصار FL در سال ۲۰۱۶ میلادی توسط پژوهشگران شرکت گوگل توسعه داده شد تا به ایرادات وارده به رویکرد متمرکز یادگیری ماشین پاسخ داده شود. FL رویکردی توزیع‌شده از یادگیری ماشین است که در آن مدل‌ها، در دستگاه‌های انتهایی (end devices) ، تحت نظارت یک سرور مرکزی، تمرین داده می‌شوند. به این ترتیب داده‌ها از هیچ کدام از دستگاه‌ها خارج نمی‌شود و در نتیجه حریم خصوصی در فرایند تمرین مدل حفظ خواهد شد. در هر مرحله سرور مرکزی مدل را برای دستگاه‌ها می‌فرستد، هر دستگاه با استفاده از داده‌های خود مدل را تمرین می‌هد و سپس مدل تمرین داده‌شده را برای سرور مرکزی ارسال می‌کند. در مرحله بعد سرور مرکزی با توجه به تمامی مدل‌های دریافت شده از دستگاه‌ها یک مدل بهتر و دقیق‌تر می‌سازد و سپس دوباره آن را برای دستگاه‌ها می‌فرستد و این روند ادامه می‌یابد. [۱۵]



شکل ۳۳. مدل‌سازی با رویکرد FL

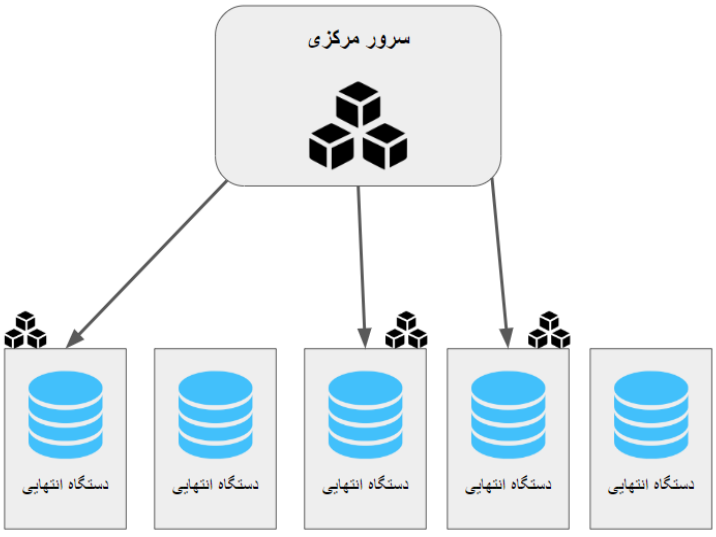
۲-۵-۱. Federated averaging

Federated learning یک روش خاص و منحصربه‌فرد نیست بلکه یک رویکرد است و می‌تواند به روش‌ها و با استفاده از الگوریتم‌های مختلف ارائه شود. برای مثال یکی از مهمترین این الگوریتم‌ها federated averaging نام دارد. مهم از این جهت که بسیاری از الگوریتم‌هایی که بعد از آن برای FL ارائه شده بر مبنای همین federated averaging هستند.

در این الگوریتم یک سرور و تعدادی دستگاه وجود دارند. هر کدام از دستگاه‌ها دیتابیس اختصاصی خود را دارند و در سرور مرکزی، مدل یادگیری ماشینی که کل شبکه در تلاش برای تمرین دادن آن هستند، وجود دارد. در ابتدای امر مدل موجود در سرور مرکزی کاملا تصادفی انتخاب شده.

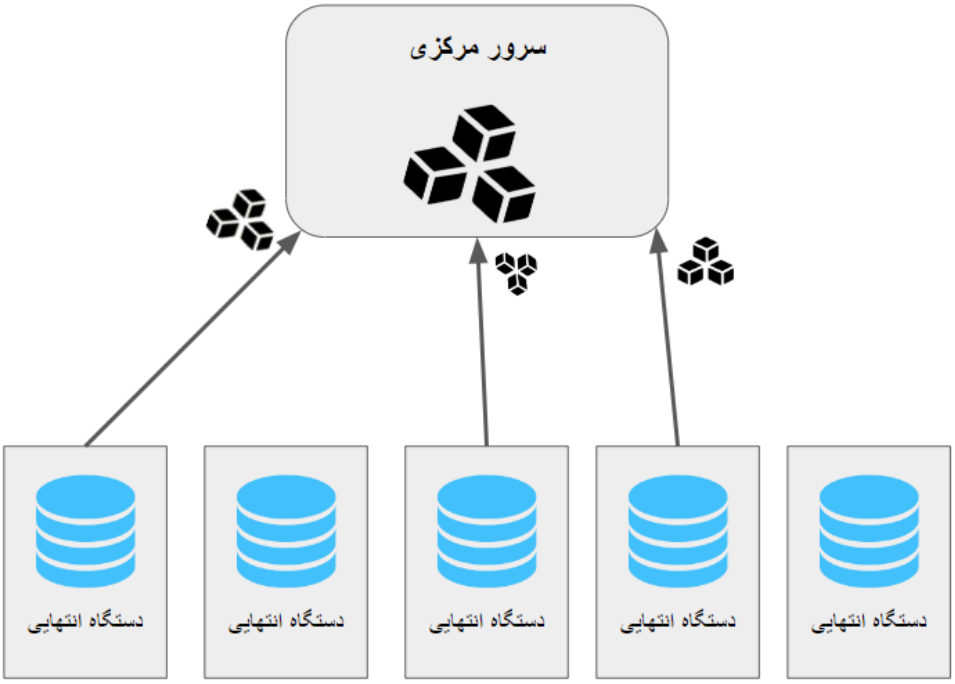
شکل ۳۴. حالت اولیه شبکه Federated

در قدم بعدی یک کپی از مدل به برخی از دستگاه‌ها که در دسترس‌اند ارسال می‌شود. هدف از عدم ارسال مدل برای تمام دستگاه‌ها این است که هم در انتقال داده صرفه جویی شود، و هم اگر دستگاهی به هر دلیلی توانایی انجام عملیات لازم را نداشت، فرایند تمرین‌دادن مدل مختل نشود. پس در نهایت از بین دستگاه‌های واجد شرایط تعدادی به صورت تصادفی انتخاب می‌شوند و مدل برای آن‌ها ارسال می‌شود.



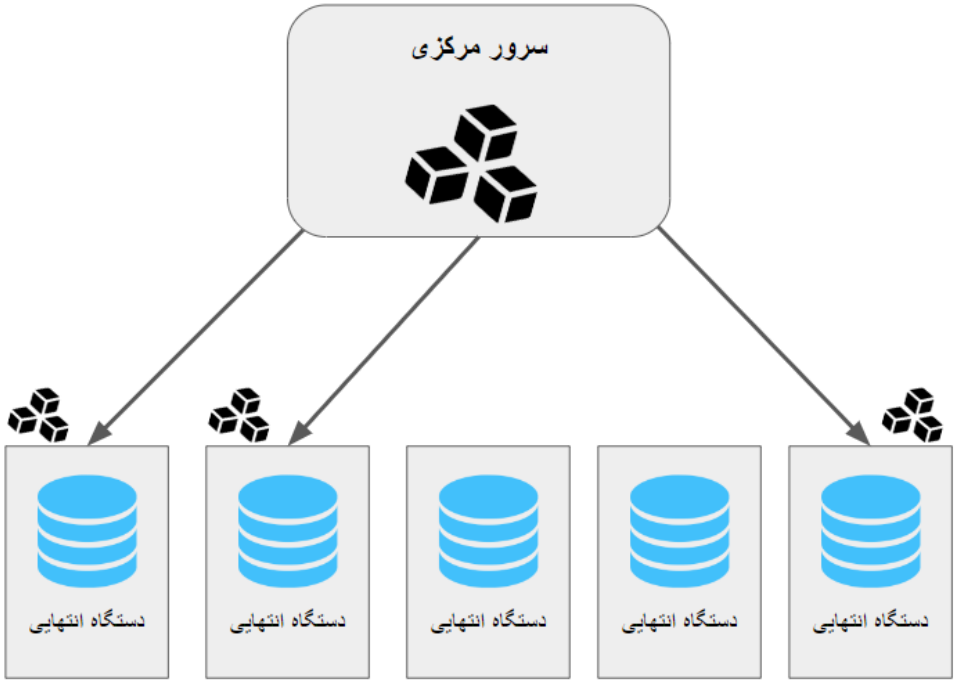
شکل ۳۵. ارسال مدل به دستگاه‌های انتهایی از سرور مرکزی

سپس هر دستگاه با توجه به دیتاستی که دارد مدل را تمرین می‌دهد. لازم به ذکر است که در این الگوریتم مدلی که هر دستگاه تمرین می‌دهد وزنی متناظر با اندازه دیتاست آن دستگاه دریافت می‌کند. این مدل‌های تمرین داده شده برای سرور فرستاده می‌شود و در آن یک میانگین بین تمامی مدل‌های دریافت‌شده گرفته می‌شود، و مدل جدید مشترک در سرور مرکزی ذخیره می‌شود.



شکل ۳۶. ارسال مدل‌های به‌روزرسانی شده به سرور مرکزی

حال مدل موجود در سرور به عنوان مدل مشترک دوباره به همان صورت قبل برای تعدادی از دستگاه‌ها فرستاده می‌شود تا چرخه تمرین مدل ادامه یابد. [۱۶]



شکل ۳۷. ادامه‌ی روند تمرین مدل

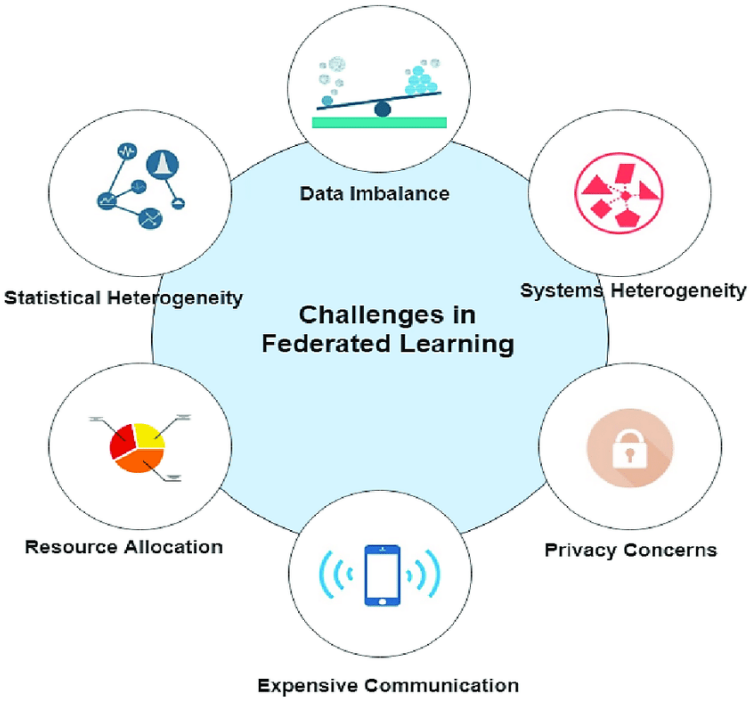
حال با توجه به این مثال کلی که از FL زده شد، چند نکته قابل توجه است. اول این که چالش حریم خصوصی که در ML متمرکز با آن رو به رو شدیم، با توجه به جابه‌جا نشدن داده‌ها بین دستگاه‌های انتهایی و سرور مرکزی، تا حدودی از بین رفت. علاوه بر آن با توجه به کاهش میزان انتقال داده هزینه انتقال داده نیز به تا حدودی کاهش یافت. در واقع در FL، بجای اینکه حجم میلیاردی داده بخواهد بین دستگاه‌ها و سرور جابه‌جا شود تنها مدل‌ها که حجمی به مراتب کمتر دارند انتقال می‌یابند. مورد بعدی توزیع‌شدن مصرف انرژی است. اینکه یک سرور بخواهد علاوه بر جمع‌آوری اطلاعات، تمرین مدل، که نیازمند محاسبات پیچیده است، را هم انجام دهد و در عین حال وظیفه ایجاد هماهنگی را نیز داشته باشد، به صرف انرژی بسیار زیاد می انجامد ولی در رویکرد FL با توجه به این که در هر دستگاه تمرین مدلی کوچک‌تر صورت می‌گیرد و سرور تنها یک میانگین از این مدل‌ها خواهد گرفت، که به انرژی زیادی نیاز ندارد، فشار بر روی یک نقطه از شبکه وارد نخواهد شد.

۲-۵-۲. مجتمع‌سازی Federated learning و بلاک‌چین

با وجود همه این مزایا که گفته شد، Federated learning همچنان با چالش‌های متنوعی روبرو است که ابتدا برخی از آنها را بررسی می‌کنیم. (۱) چالش ارتباطات هزینه‌بر: همانطور که اشاره شد Federated learning تلاش زیادی در جهت کاهش هزینه‌ی ارتباطات کرده است، اما چون همچنان یک سرور مرکزی و این نیاز که مدل‌ها برای این سرور ارسال شوند، وجود دارند، هزینه‌ی زمانی زیادی به ما تحمیل می‌شود. دلیل این چالش این است که شبکه‌های Federated به طور بالقوه از تعداد زیادی دستگاه تشکیل شده‌اند، و ارتباطات در این شبکه‌ها می‌تواند از محاسبات محلی به شدت کندتر باشد. این امر سبب می‌شود تا سرور مرکزی به یک bottleneck در شبکه‌های Federated تبدیل شود.

(۲) چالش ناهمگونی دستگاه‌ها: قابلیت‌هایی از جمله ذخیره‌سازی، توانایی محاسباتی و ارتباطی هر دستگاه در شبکه‌های Federated ممکن است متفاوت باشد. علاوه بر این، اندازه شبکه و محدودیت‌های مربوط به هر دستگاه، در شبکه معمولاً منجر به فعال شدن تنها بخش کوچکی از دستگاه‌ها در یک زمان می‌شود. هر دستگاه همچنین ممکن است غیرقابل اعتماد باشد، و همچنین ممکن است که یک دستگاه فعال در یک دور معین به دلیل مشکل در اتصال یا محدودیت‌های انرژی، از دور خارج شود. همچنین با توجه به اینکه سیستمی برای ترغیب دستگاه‌ها برای ادامه فعالیت و ارائه نمونه‌های بیشتر وجود ندارد احتمال فعال شدن مجدد دستگاه‌ها کم می‌شود. این عوامل چالش‌هایی مانند تحمل خطا را تشدید می‌کنند. به همین دلیل روش‌های Federated learning باید: (i) میزان مشارکت کم را پیش‌بینی کنند، (ii) سخت‌افزار ناهمگن را تحمل کنند، و (iii) توانایی مقابله با دستگاه‌های حذف‌شده در شبکه را داشته باشند.

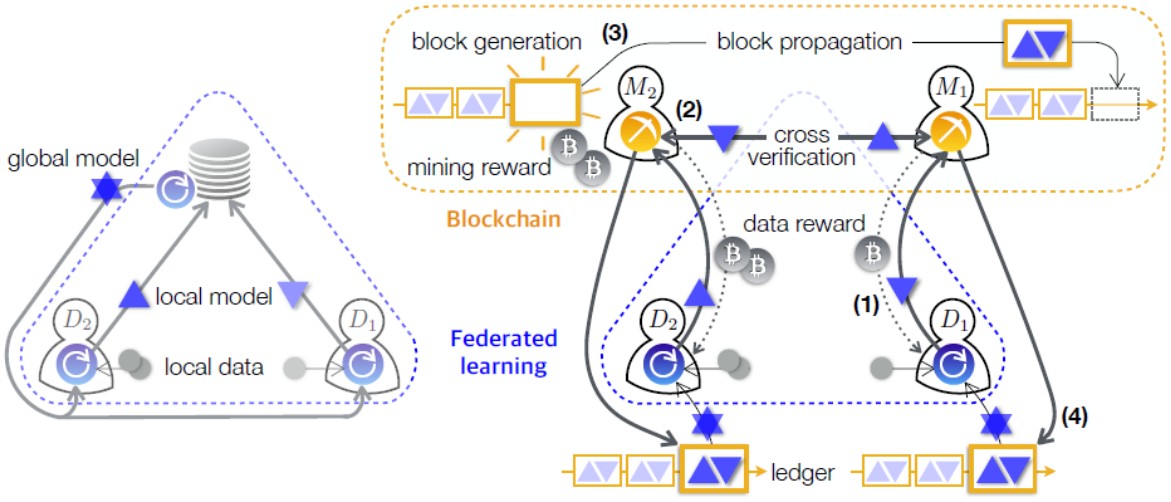
(۳) چالش حفظ امنیت: حفظ امنیت داده‌ها یک نگرانی عمده در روش‌های Federated learning است. همانطور که اشاره شد Federated learning در جهت حفاظت از داده‌های تولیدشده در هر دستگاه، به اشتراک گذاشتن به‌روزرسانی‌های مدل را بجای داده‌های خام پیشنهاد می‌کند. با این حال، تبادل مدل‌های به‌روزرسانی شده در طول فرآیند تمرین می‌تواند اطلاعات حساسی را برای شخص ثالث یا سرور مرکزی فاش کند. هر چند اخیرا روش‌هایی از جمله differential privacy یا multiparty computation پیشنهاد شده‌اند، اما به قیمت کاهش عملکرد مدل تمام می‌شوند. درک و متعادل کردن این مبادلات جهت حفظ امنیت داده‌ها، یک چالش مهم در شبکه‌های Federated است. علاوه بر این به کارگیری مکانیزم‌های مقابله با حمله‌های امنیتی و تشخیص تهدید، هم در سمت سرور و هم در سمت دستگاه‌ها ضروری است. مثلا به کارگیری سیستم تشخیص وزن مدل به‌روزرسانی شده در هر دستگاه به سرور کمک می‌کند تا دستگاه‌های تبلیغاتی و حمله‌هایی مانند model update poisoning یا data poisoning را تشخیص دهد و بتواند با آنها مقابله کند و همچنین در تبادل بی‌سیم داده‌ها توجه به اینکه رمزگذاری مناسب و تنظیمات امن و عملیات احراز هویت برای جلوگیری از نشت داده‌ها به درستی انجام شوند، از اهمیت بالایی برخودار است. در نهایت چون در شبکه یک سرور مرکزی وجود دارد، اگر حمله‌ای خارجی یا حمله‌ای توسط یک دستگاه داخلی خرابکار به این سرور صورت بگیرد، می‌تواند سبب اختلال در کل شبکه شود.



شکل ۳۸. چالش‌های Federated learning

بلاک‌چین با توجه به قابلیت‌های منحصربه‌فردش، می‌تواند به بهبود امنیت و سایر نقاط ضعف Federated learning کمک کند. اتکای مدل به یک سرور مرکزی واحد، منجر به آسیب‌پذیر شدن مدل در برابر خرابی سرور می‌شود و همین مسئله باعث می‌شود، به‌روزرسانی‌های مدل در سرور مرکزی تحریف شود و در نتیجه به‌روزرسانی‌های دقیقی برای دستگاه‌ها ارسال نشوند. استفاده از بلاک‌چین غیرمتمرکز امکان حذف سرور مرکزی در Federated learning را فراهم می‌کند. در واقع با ترکیب بلاک‌چین و Federated learning این امکان بوجود می‌آید که به جای سرور مرکزی از یک ledger تغییرناپذیر مشترک برای جمع‌آوری مدل‌ها و توزیع به‌روزرسانی‌ها، برای محاسبه مستقیم در دستگاه‌ها استفاده شود. تمرکززدایی نه تنها میزان آسیب ناشی از خرابی سرور مرکزی را، بلکه بار محاسباتی تحمیل‌شده بر روی سرور که ناشی از محاسبات لازم برای تجمیع مدل‌ها است، را (بخصوص زمانی که تعداد دستگاه‌های شبکه زیاد هستند) بیش از پیش کاهش می دهد. به‌روزرسانی‌ها در بلاک‌های تغییرناپذیر اضافه می‌شوند و در طول فرایند تمرین مدل برای تبادل اطلاعات استفاده می‌شوند که این روش امنیت بالایی را در برابر حملات خارجی ایجاد می‌کند. همچنین اضافه‌شدن بلاک‌ها در کل شبکه به همه کاربران این را اجازه می دهد تا پیشرفت مدل و به‌روزرسانی‌ها را تأیید و ردیابی کنند و این رویکرد با ایجاد شفافیت در سیستم، اعتماد به آن را آسان‌تر می‌کند. همچنین حذف یک سرور مرکزی در رفع چالش هزینه‌های ارتباطی نقش مهمی دارد که در نهایت منجر به جذب کاربران بیشتری برای شبکه غیرمتمرکز و کم‌هزینه می‌شود و مقیاس‌پذیری شبکه را افزایش می‌دهد.

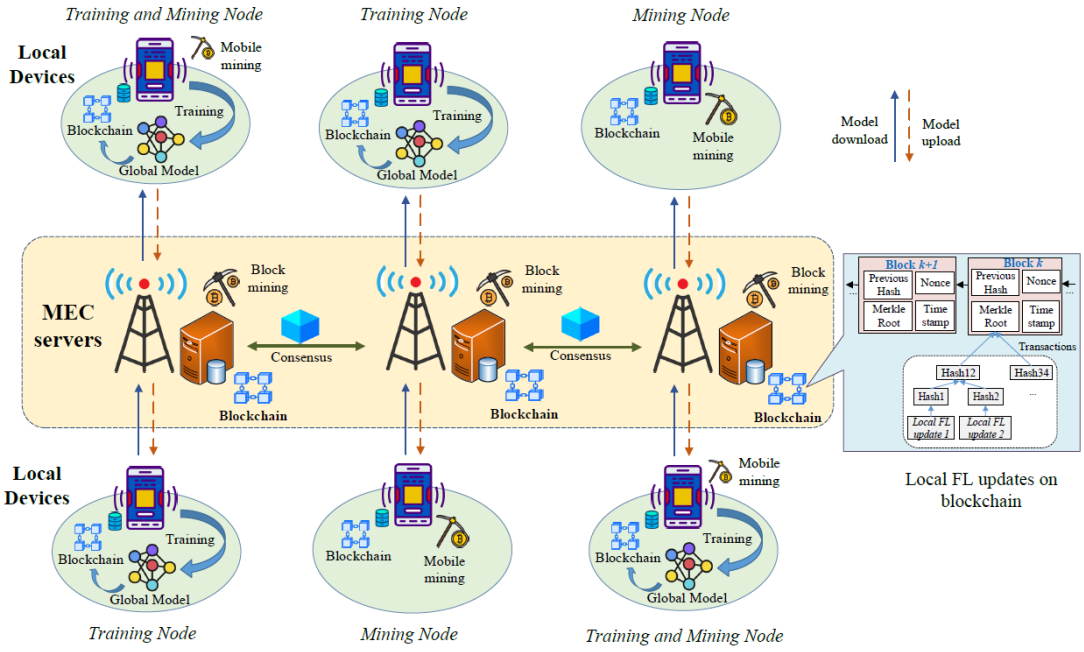
یک چالش دیگر که بلاک‌چین می‌تواند به حل آن کمک کند، این است که روش فعلی Federated learning سیستم پاداش‌دهی ندارد. دستگاهی که تعداد نمونه داده‌های بیشتری داشته باشد، به فرایند تمرین مدل‌ها کمک بیشتری می‌کنند. بدون ارائه پاداش، چنین دستگاه‌هایی تمایل کمتری به پیوستن به سایر دستگاه‌ها (با نمونه داده‌های کم‌تر) برای تمرین مدل دارند. ترکیب بلاک‌چین و Federated learning این امکان را بوجود می‌آورد که با ارائه پاداش‌های متناسب با اندازه دیتاست‌های هر دستگاه، دستگاه‌های دارای دیتاست بزرگ‌تر، بیشتر علاقه‌مند به تمرین‌دادن مدل شوند و همچنین انگیزه‌ی برگشت به شبکه را برای دستگاه‌هایی که از آن خارج شده‌اند، فراهم می‌کند. [۱۷] [۱۸] [۱۹]



شکل ۳۹. نمایی از یک معماری پیشنهادی برای ترکیب Federated learning با بلاک‌چین

FLchain .۲-۵-۳

با توجه به آن چه گفته شد معماری FLchain به عنوان یک جایگزین برای FL معمول مطرح می‌شود. در این معماری مدل مشترک به طور مستقیم در خود دستگاه‌ها محاسبه می‌شود و دیگر به سرور مرکزی نیاز نخواهد بود. در این معماری تعدادی سرور (MEC servers) وجود دارند که وظیفه ماینینگ و اجرای consensus را دارند و هرکدام برای یک نوع خاصی از فرایند یادگیری هستند. دستگاه‌ها که به این سرورها متصل می‌شوند همانند FL معمول وظیفه دارند که مدل مشترک را با توجه به دیتاست موجود در خود به‌روزرسانی کنند (برخی می‌توانند ماینینگ نیز انجام دهند). این مدل محلی به‌روزرسانی‌شده از طریق بلاک‌چین و با ایجاد یک تراکنش به سرور متناظر دستگاه منتقل می‌شود. سرور این تراکنش‌ها را با ساختمان‌داده مشخصی ذخیره می‌کند و هنگامی که تمامی مدل‌های محلی به‌روزرسانی‌شده برای سرور ارسال شدند، سرور سعی می‌کند یک بلاک که شامل تمامی این تراکنش‌ها است را بسازد. سپس سرور عملیات ماینینگ را انجام می‌دهد و اگر همه سرورها در مورد این بلاک به توافق برسند این بلاک به زنجیره اضافه خواهد شد. در نهایت هر دستگاه می‌تواند با دانلود این بلاک و میانگین گرفتن از همه مدل‌های محلی به دست‌آمده مدل اصلی و مشترک را به دست آورد. [۱۸]



شکل ۴۰. معماری FLchain

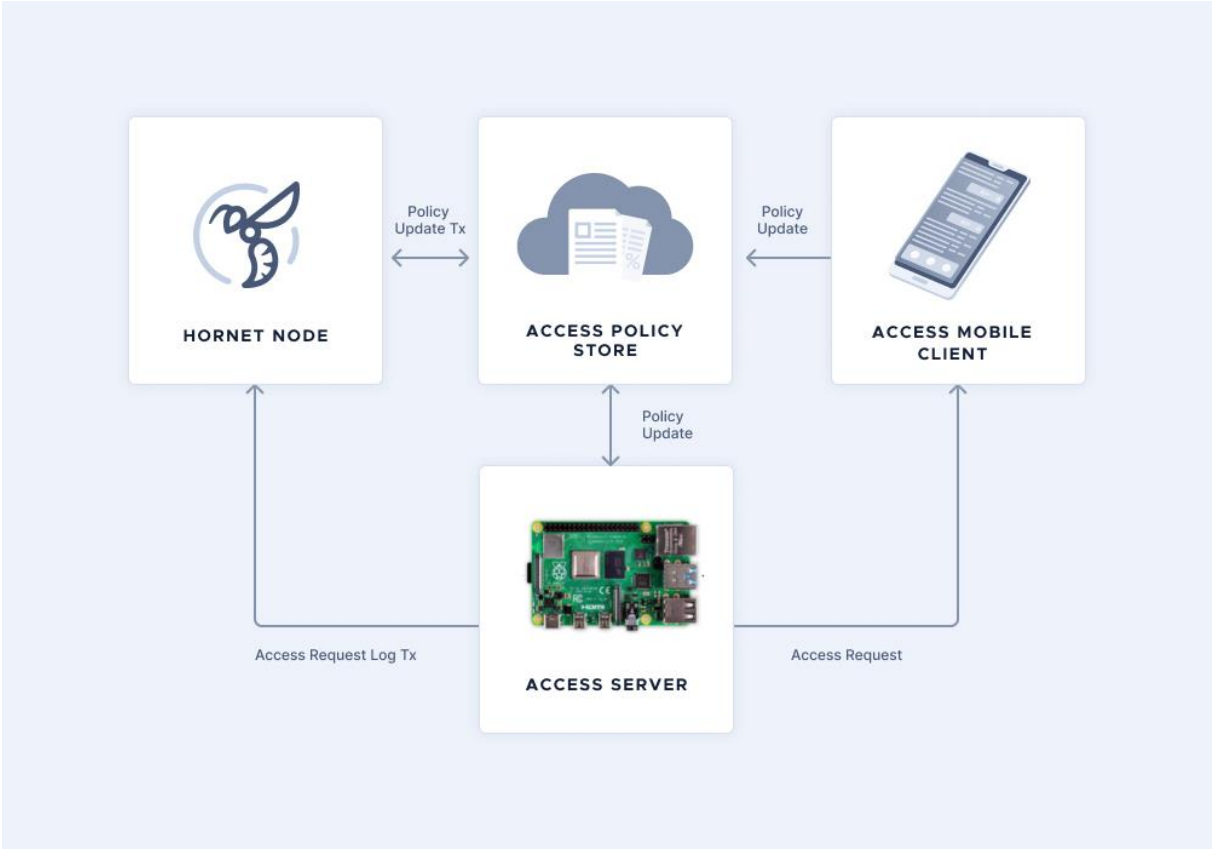
۳. نتیجه گیری

تا اینجا با مفاهیم اولیه IoT و بلاک‌چین آشنا شدیم و سپس با محوریت پروژه IOTA ، در مفاهیم بلاک‌چین عمیق شدیم و ساختارها و معماری‌های IOTA را بررسی کردیم. در ادامه با مفهومی با عنوان federated learning آشنا شده و کاربردهای آن را در IoT بررسی کردیم و در نهایت پیاده‌سازی‌های انجام شده بر روی پلتفورم IOTA گزارش شد.

حال در ادامه کار قصد داریم کارهای زیر را انجام دهیم:

۱) ادامه کار بر روی رزبری‌پای

قصد داریم در ادامه‌ی کار، با هدف کار بر روی یک نود واقعی اینترنت اشیا و اتصال آن به شبکه‌ی بلاک‌چین، معماری زیر را پیاده‌سازی کرده و سناریوهای مختلف را بر روی آن تست کنیم:



شکل ۴۱. معماری شبکه داخلی بلاک‌چینی با امکان ایجاد policy برای شبکه و نودهای اینترنت اشیای شبکه

۲) قراردادهای هوشمند

در ادامه قصد داریم بر روی قراردادهای هوشمند تحقیق عمیق‌تری داشته باشیم و به صورت تئوری مفاهیم آن را بررسی کنیم. برای این منظور ۴ مرحله متوالی برای ما مفروض است:

۱. اجرای مثال ارائه شده برای قراردادهای هوشمند توسط کمپانی IOTA برای آشنایی سریع‌تر و عملی با مفاهیم اولیه این حوزه

۲. آشنایی بیشتر باVM های مختلف مانند Wasm یا EVM و تفاوت‌های آن‌ها

۳. ایجاد یک قرارداد هوشمند با کاربرد خاص در اینترنت اشیا

۴. استفاده از مفاهیم Federated Learning فرا گرفته شده و آشنایی عملی با این حوزه بخصوص در ترکیب با حوزه اینترنت اشیا

مراجع

[1] Lee, In, Lee, Kyoochun. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." In Business Horizons, Volume 58, Issue 4, Pages 431-440, July–August 2015.

[2] Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." IEEE internet of things journal 5.2 (2018): 1184-1195.

[3] Zheng, Zibin, Wang, Huaimin, Xie, Shaoan, Dai, Hong-Ning. " Blockchain challenges and opportunities: a survey." In International Journal of Web and Grid Services 14(4): 352 – 375, DOI:10.1504/IJWGS.2018.10016848, October 2018.

[4] https://builtin.com/blockchain/blockchain-iot-examples

[5] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an optimized blockchain for IoT." In Proc. IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017.

[6] Panarello, Alfonso, et al. "Blockchain and iot integration: A systematic survey." Sensors 18.8, 2018.

[7] Dorri, Ali, et al. "Blockchain for IoT security and privacy: The case study of a smart home." In Proc. IEEE international conference on pervasive computing and communications workshops (PerCom workshops) , 2017.

[8] M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," In Proc. IEEE International Conference on Blockchain (Blockchain), 2019, pp. 469-476.

[9] V. A. Gasimov and S. K. Aliyeva, "Using blockchain technology to ensure security in the cloud and IoT environment," In Proc. 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021.

[10] P. Gupta, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Towards a blockchain powered IoT data marketplace," In Proc. International Conference on COMmunication Systems & NETworkS (COMSNETS), 2021, pp. 366-368.

[11] S. R. Niya et al., "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams," In Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019.

[12] J. Xu, S. Wang, A. Zhou and F. Yang, "Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps," in China Communications, vol. 17, no. 4, pp. 78-87, April 2020.

[13] Tsiknas, K, Taketzis, D, Demertzis, K, Skianis, C. "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures." in MDPI, 163–186, 2021.

[14] https://blog.equinix.com/wp-content/uploads/2015/10/attack2.jpg

[15] Abreha, H.G, Hayajneh, M, Serhani, M.A. "Federated Learning in Edge Computing: A Systematic Survey." in MDPI, 2022.

[16] McMahan, H.B, Moore, E, Ramage, D, Hampson, S, Ag¨uera y Arcas, B. "Communication-Efficient Learning of Deep Networks from Decentralized Data." in PMLR, vol. 54, 2017.

[17] Li, T, Sahu, A.K, Talwalkar, A, Smith, V. "Federated Learning: Challenges, Methods, and Future Directions." in IEEE Signal Processing Magazine, Vol 37, Issue 3, August 2019.

[18] Nguyen, C.D, Ding, M, Pham, Q, Pathirana, P, Le, L.B, Seneviratne, A, Li, J, Niyato, D, Vincent Poor, H. "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges." in IEEE Internet of Things Journal, Vol 8, Issue 16, 2021.

[19] Kim, H, Park, J, Bennis, M, Kim, S.L " Blockchained On-Device Federated Learning." in IEEE Communications Letters, Vol 24, Issue 6, July 2019.

[20] IOTA Foundation. (2021). IOTA Smart Contracts [White paper].