مسائل اینترنت اشیاء بر پایه زنجیره بلوک توزیع شده در ایران

محمدحسین رونقی[1,*]

چکیده

اینترنت اشیاء اشاره به اشیاء هوشمند توزیع شده، شبکه‌های حسگر و ابزارهای پوشیدنی با هدف تبادل اطلاعات دارد و ارائه خدمات از طریق شبکه‌های حسگر عامل کلیدی برای ایجاد محیط‌های هوشمند است. در حال حاضر داده اینترنت اشیا در محیط خارجی قابل‌اطمینان نیست، از همین‌رو در زمان تسهیم با بخش‌های دیگر، کنترل داده دچار نقصان می‌شود. برای غلبه بر چنین محدودیتی فناوری ذخیره‌سازی غیرمتمرکز مطرح می‌شود. فناوری زنجیره بلوک اشاره به پایگاه داده یا دفتر کل توزیع شده ای دارد که از مجموعه ابزارهای متصل شده به شبکه همانند یک شی محافظت می‌کند. از همین‌رو در این پژوهش در مرحله اول به دنبال شناسایی نیازمندی‌های اساسی زنجیره بلوک با توجه به اینترنت اشیا با استفاده از روش تحلیل محتوا هستیم. در مرحله بعد تفسیر خبرگان با استفاده از روش دلفی مورد ارزیابی قرار می‌گیرد. پنل خبرگان شامل دوازده نفر از افراد دارای سابقه فعالیت در حوزه فناوری اطلاعات می‌شود. در انتها از روش تحلیل سلسله مراتبی بر پایه فازی نوع دو برای رتبه بندی مولفه‌ها استفاده گردید. یافته‌های اصلی پژوهش نشان داد که چالش‌های قوانین و حاکمیت (۰/۳۱)، استانداردها (۰/۲۱)، حریم خصوصی (۰/۱۶)، نقص امنیتی (۰/۱۰)، مدیریت داده مقیاس‌پذیر (۰/۰۸)، سرعت شبکه (۰/۰۵)، پیچیدگی (۰/۰۳)، قابلیت تعامل (۰/۰۳) و فورک (۰/۰۲) به ترتیب چالش‌های دارای اهمیت هستند. با توجه به نتایج به‌دست آمده می‌توان اذعان داشت افزایش درخواست کاربران برای ارتباط امن در شبکه اینترنت اشیا موجب شده است انطباق با شبکه زنجیره بلوک به‌عنوان راهکار امنیتی ارائه گردد. همچنین انطباق زنجیره بلوک در محیط اینترنت اشیا الزامات امنیتی و اعتمادی خاص خود را ایجاد می‌کند.

واژگان کلیدی: اینترنت اشیاء، زنجیره بلوک، حاکمیت، روش دلفی، مجموعه فازی نوع دو

* عهده‌دار مکاتبات: دانشیار،تلفن/نمابر: ۳۶۲۷۶۳۷۲(۰۷۱)، نشانی الکترونیکی: mh_ronaghi@shirazu.ac.ir

[1] دانشکده اقتصاد، مدیریت و علوم اجتماعی، دانشگاه شیراز، شیراز، ایران

DOR: 20.1001.1.2008935.1401.13.1.8.1

مقدمه

هدف اینترنت اشیا توانمندسازی اشیا برای اتصال در هر زمان و مکان، با هر چیزی و هر شخصی است که از هر مسیر یا شبکه و خدمت به‌صورت ایده‌آل استفاده می‌کند. اینترنت اشیا تکامل جدیدی از اینترنت است. اینترنت اشیا فناوری جدیدی است که به حضور نافذ محیطی توجه می‌کند و از تنوع چیزهایی با اتصالات بی سیم و سیم‌دار به محاوره با یکدیگر می‌پردازد [۱]. توسعه فناوری اینترنت اشیاء موجب شده است تا بسیاری از اشیاء قادر به اتصال به اینترنت برای برقراری ارتباط با یکدیگر بدون دخالت انسان باشند. در اصل اینترنت اشیاء ورود داده‌های انسانی را کاهش داده و از انواع مختلف حسگرها برای جمع‌آوری داده‌ها از محیط استفاده می‌کند و اجازه ذخیره‌سازی و پردازش خودکار تمام داده‌ها را ایجاد می‌کند [۲]. با افزایش استفاده از اینترنت اشیا بر تعداد ابزارهای مرتبط افزوده می‌شود و سرعت انتقال اطلاعات، امنیت شبکه و کنترل اطلاعات از دغدغه‌های این فناوری محسوب می‌شوند [۳]. زنجیره بلوک فناوری بر پایه دفتر کل توزیع شده است. دفتر کل توزیع‌شده، پایگاه داده‌ای است که توسط هر شرکت‌کننده (یا گره) در یک شبکه بزرگ به‌طور مستقل به‌روز می‌شود. توزیع اشاره به همگانی بودن دارد. پرونده‌ها توسط یک مقام مرکزی به گره‌های مختلف انتقال نمی‌یابند، بلکه به‌طور مستقل توسط هر گره (کامپیوتر) ساخته و نگهداری می‌شوند. به این معنی که هر گره در شبکه، هر تراکنش را پردازش می‌کند، به نتیجه‌گیری‌های خود می‌پردازد و سپس آن نتیجه‌گیری را به رأی می‌گذارد تا اکثریت آن را تأیید کنند [٤]. استفاده از اینترنت اشیا بر پایه زنجیره بلوک توزیع شده موجب می‌شود تا کنترل اطلاعات در این بستر به نحو بهتری صورت پذیرد اما به‌کارگیری چنین فناوری با چالش‌هایی همراه است. در زمان انجام پژوهش مطالعه‌ای در خصوص چالش‌های حوزه اینترنت اشیا بر پایه زنجیره بلوک در ایران انجام نشده بود لذا مسأله اصلی این پژوهش شناسایی و رتبه‌بندی چالش‌ها و مسائل به‌کارگیری اینترنت اشیا در بستر زنجیره بلوک غیرمتمرکز در ایران است.

ادبیات پژوهش

چالش‌های اینترنت اشیا بر پایه زنجیره بلوک

• **مدیریت داده مقیاس‌پذیر:** یکی از مسائل اصلی فناوری زنجیره بلوک مدیریت دفاتر کل یا پایگاه‌های داده توزیع شده است که شامل حجم زیاد رکوردهای اطلاعاتی ابزارهای مرتبط با هم می‌باشد. همچنین شبکه‌های جهانی بر سرعت افزایش این رکوردهای اطلاعاتی افزوده‌اند. هم‌راستا با این ازدیاد اطلاعات مسائل امنیتی استفاده از ابزارهای ناهمگون در مقیاس زنجیره بلوک به خوبی توسعه نیافته است. همچنین این ناهمگونی ابزارها می‌تواند موجب توسعه نرم‌افزارهای امنیتی سطح پایین جهت مدیریت داده‌های مختلف باشد که موجب نفوذ انواع بدافزارها و ایجاد حفره‌های امنیتی می‌شود [۵]. ناهمگونی ابزارهای مختلف مساله سازگاری داده‌ها و ایجاد یکپارچگی بین آنها را نیز با چالش مواجه کرده است. حتی شورای نظارت بر ثبات مالی امریکا (FSOC) نیز راهکاری برای مواجهه با حملات به مقیاس کلان داده بر پایه فناوری زنجیره بلوک ارائه نداده است. یکسان‌سازی و تطبیق داده‌ها در شبکه‌های زنجیره بلوک جهت شناسایی، ذخیره و محاسبه داده از منابع مختلف کاری وقت‌گیر و پرهزینه محسوب می‌شود [٦]. در اینجا به‌کارگیری قراردادهای هوشمند مصداق پیدا می‌کند. قراردادهای هوشمند بر پایه زنجیره بلوک در شرایطی که طرفین شناخت زیادی از یکدیگر ندارند می‌تواند توسعه پیدا کند [۷].

• **پیچیدگی:** از الگوریتم‌های پیچیده رمزنگاری در زنجیره بلوک استفاده می‌شود که ماینرها به‌دنبال حل این معادلات و الگوریتم‌های پیچیده هستند. ماینرها می‌توانند گره‌هایی را که دارای منابع محاسباتی قوی‌تری هستند تشخیص دهند و برای حل آنها اقدام کنند. گاهی ممکن است گره‌هایی که هویت آنها مشخص نیست خود را به‌عنوان ماینر معرفی کنند که در اینجا زنجیره بلوک از رمزنگاری با استاندارد بالا استفاده می‌کند [۸]. در شبکه‌های زنجیره بلوک چالش‌های متعددی مانند مصرف انرژی رمز ارز و یا پیامدهای محیطی زیستی نیز مطرح می‌شود که نیاز به وضع قوانین خاص دارد. نمونه چالش‌های موجود در زمان تغییر الگو رفتار مصرف‌کنندگان از روش‌های سنتی به سمت شیوه‌های الکترونیکی و مجازی وجود داشت. شبکه‌های بیت کوین به‌دلیل گستردگی و سیستم توزیع دارای کندی و سنگینی هستند و ممکن است ساعت‌ها فرایندهای این شبکه طول بکشد. مورد دیگر توجه به پیچیدگی ذهنی افراد در خصوص مواجه به جامعه بدون پول سنتی و ارائه خدمات غیرمتمرکز است [۹].

• **سرعت شبکه:** با گسترش رمز ارزهایی همچون بیت کوین و اتریوم بر پایه شبکه‌های توزیع شده غیرمتمرکز سرعت پردازش در این شبکه‌ها از اهمیت زیادی برخوردار است. بررسی سرعت چنین شبکه‌هایی نیاز به ارزیابی فنی تراکنش‌ها و محاسبه تأخیرهای مربوطه دارد. بر همین اساس توسعه‌دهندگان سیستم تلاش در جهت ارائه راهبردها و تاکتیک‌های جدید برای حل مشکل سرعت شبکه اینترنت اشیا بر پایه دفتر توزیع شده زنجیره بلوک می‌کنند [۱۰].

• **قابلیت تعامل:** زنجیره بلوک، دفتر دیجیتالی غیرمتمرکز از رکوردهای تراکنشی یک شبکه توزیع شده نقطه به نقطه است که به‌منظور ایجاد رابطه بین دو بخش یا گروه ناشناس طراحی شده است. چنین شبکه انتقال اطلاعات در خصوص اینترنت اشیا بر پایه زنجیره بلوک باید قابل‌اطمینان و امن باشد [۱۱]. زمانی که ابزارهای گوناگون به شبکه زنجیره بلوک اضافه می‌شوند قابلیت همکاری بین آنها حائز اهمیت می‌شود. همکاری بین ابزارهای مختلف باید به‌خوبی مدیریت شود تا قابلیت انتقال داده‌های مالی، انسانی و سخت‌افزاری و تحلیل خروجی‌ها در بستر زنجیره بلوک وجود داشته باشد. به‌منظور مدیریت و اجرای شبکه‌های کارا، توسعه‌دهندگان نیاز به ارائه راهکارهای نوآورانه اینترنت اشیا بر پایه سیستم پرداخت الکترونیکی دارند [۳].

• **حریم خصوصی:** میلیون‌ها حسگر اینترنت اشیا با یکدیگر در ارتباط هستند و اطلاعات خصوصی افراد را منتقل می‌کنند. زمانی‌که بر پایه شبکه غیرمتمرکز زنجیره بلوک اجرا می‌شود امنیت و محرمانگی اطلاعات اهمیت زیادی پیدا می‌کند. این اطلاعات ممکن است در مورد بیماری‌ها یا اطلاعات خصوصی یک شخص حقیقی تا اطلاعات مالی یک شخص حقوقی را شامل شود. هر چه تعداد ابزارهای شبکه اینترنت اشیا بر پایه زنجیره بلوک افزایش می‌یابد، حجم اطلاعات در شبکه نیز زیاد می‌شود و نیاز به سازوکارهای تشخیص هویت افراد و تعیین دسترسی دقیق در شبکه وجود دارد [۱۲]. در شبکه زنجیره بلوک همانند سیستم متمرکز نیاز به کنترل فهرست اعضای ثبت‌شده در شبکه است اما برای تشخیص و امنیت شبکه از ابزارهای رمزنگاری مانند توابع هش و امضای دیجیتال استفاده می‌شود. همانند شبکه‌های متمرکز در زنجیره بلوک نیز نیاز به حفظ امنیت شبکه در مقابل هک شدن و کنترل افراد ناشناس در شبکه جهت ایجاد تراکنش‌های امن وجود دارد [۱۳].

• **استانداردها:** توسعه استانداردها یکی از مباحث مهم در استقرار فناوری زنجیره بلوک در اینترنت اشیا است [۱۳]. استانداردها نقش مهمی در قابلیت همکاری در شبکه از طریق کانال‌های امن و کارایی بالا ایفا می‌کنند. استانداردهای شبکه در خصوص اشیاء موجود می‌تواند شامل محرمانگی شی، تشخیص هویت شی، جامعیت شی و قابلیت دسترسی شی شود. محرمانگی شی باید جلو هرگونه نشت اطلاعاتی در شبکه موجود و اینترنت گرفته شود. همچنین ایجاد امنیت در هر لایه بر پیچیدگی سیستم می‌افزاید. فناوری‌های ارتقای امنیت جدید همانند شبکه‌های خصوصی مجازی (VPN) و امنیت لایه انتقال (TLS) برای دسترسی به امنیت شبکه طراحی شده‌اند [۳].

• **فورک:** فورک مشکلی است که به وسیله بروزرسانی نرم‌افزار به وجود می‌آید [۱٤]. هر گاه در بروزرسانی‌های انجام شده در شبکه اختلاف نظر بین توسعه‌دهندگان به‌وجود آید ممکن است منجر به پیدایش فورک جدید شود [۱۵]. به‌عنوان مثال بر سر حجم بلوک در بیت کوین اختلاف نظر بین توسعه‌دهندگان و یا ماینرها به‌وجود آمد و فورک بیت کوین کش به‌وجود آمد. یکی از راهکارها این است که همه بلوک‌های مرتبط با یک گره از نسخه یکسانی استفاده می‌کنند و گره‌های دارای تعارض جدا شده و به‌طور مستقل عمل می‌کنند [۱٦].

• **قوانین و حاکمیت:** تحول بزرگ در خصوص شبکه توزیع شده منجر به معرفی رمز ارزها شد و در ادامه انتقال الکترونیک و نامشهود در فضای اقتصادی رخ داد. سازوکارهای پرداخت الکترونیکی منجر به رشد اقتصادی و گردش مالی تحت قوانین خاص می‌شود [۱۷]. در طرف مقابل پول الکترونیکی موجب عدم‌کنترل بر پول‌های کثیف، شرطبندی‌ها، بازارهای زیرزمینی و فعالیت‌های غیرقانونی می‌شود [۱٦]. بر اساس این چالش فناوری دفترکل غیرمتمرکز نیاز مشارکت حاکمیت و قوانین مورد توافق جهت حفظ امنیت و اعتماد رمزارز و ارز مجازی دارد. از طرف دیگر به‌دلیل عدم‌کنترل متمرکز مسأله پرداخت مالیات یکی از دغدغه‌های نهاد حاکمیت محسوب می‌شود. همچنین قوانین منطقه‌ای کسب و کار و تراکنش‌های مالی در این شبکه‌ها نیاز به بررسی بیشتر و کنترل دارد [۱۸]. اعمال چنین شرایطی ممکن است منجر به ایجاد فورک‌های جدید شود.

• **سیاست:** زنجیره بلوک سیستم تراکنش‌های غیرمتمرکز را دیجیتالی می‌کند؛ یکی از نرم‌افزارهای کاربردی زنجیره بلوک رأی دادن و انتخابات است. ابزارهای رای‌گیری دیجیتالی بسیار امکان هک شدن دارند از همین‌رو شفافیت و اعتبار فرایند رای‌گیری بسیار مهم است. ایجاد اعتماد و اعمال محدودیت در خصوص کیف‌های پول (اعتبار رای‌دهندگان) و میزان پول (شانس رای‌دهندگان) اهمیت زیادی دارد [۱۹]. در نتیجه داده مورد اطمینان باید در گره‌های فردی ذخیره شود. هیچ‌کس نباید به کل اطلاعات اعتبارها دسترسی داشته باشد. اگر چه امنیت زنجیره بلوک در گره‌های توزیع شده مسأله اساسی است اما سازوکارهای خلاقانه نظارت بهنگام بر اساس سیاست‌های نهادهای محلی و حکومتی می‌تواند جهت جلوگیری از حملات افراد ناشناس و افزایش ضریب امنیت شبکه مؤثر باشد [۳].

• **نقص امنیتی:** یکی از نقص‌های امنیتی شبکه زنجیره بلوک و بیت کوین زمانی است که بیش از نیمی از کامپیوترها موجود در شبکه

به‌عنوان اشیاء موجود به‌طور هم‌زمان کار کنند آنگاه اختلالاتی در شبکه ایجاد می‌شود. امنیت زنجیره بلوک در اینترنت اشیاء تحت تأثیر فناوری‌های دفتر کل غیرمتمرکز قرار می‌گیرد و باید توسط کنترل‌های امنیتی ویژه‌ای محافظت شود [۲۰]. یکی دیگر از نواقص امنیتی در زمان انجام تراکنش رمز ارز توسط یکی از پایانه‌های شبکه است که ممکن است اطلاعات اعتبار آنها افشا شود. حدس خودکار رمزهای موجود در شبکه یکی از راه‌های نفوذ هکرها محسوب می‌شود. از همین‌رو فناوری‌های دفترکل غیرمتمرکز به‌طور مداوم در حال به‌روزرسانی خود جهت مقاومت از نفوذ افراد ناشناس هستند [۲۱].

روش پژوهش

این پژوهش از لحاظ هدف کاربردی و از منظر روش ترکیبی است. در فاز اول با استفاده از روش تحلیل محتوای کیفی چالش‌های امنیتی حوزه اینترنت اشیا و زنجیره بلوک بر اساس مطالعات پیشین استخراج و شناسایی شدند. روش دلفی مطالعه و بررسی است که به وسیلهٔ یک گروه نظارت‌کننده، رهبری و هدایت می‌شود و شامل چندین دور است. با استفاده از یک گروه متخصص انجام می‌شود که برای همدیگر ناشناس هستند و هدف این روش رسیدن به یک اجماع‌نظر در بین گروهی از متخصصان، بر اساس شناخت شهودی و ذهنی آنان است، که پس از هر دور یک بازخورد استاندارد آماری از قضاوت گروه به اعضا ارائه می‌شود [۲۲]. در مرحله دوم پژوهش با استفاده از روش دلفی شاخص‌های استخراج شده از منابع پیشین جهت بومی‌سازی چالش‌ها مورد نظرسنجی گروه خبرگان پژوهش قرار گرفت. در فاز نهایی با استفاده از تحلیل سلسله مراتبی بر اساس منطق فازی نوع دو توسط خبرگان اولویت‌بندی گردید تا اهمیت هر عامل بر اساس خبرگان داخلی مشخص گردد. گروه خبرگان پژوهش متشکل از دوازده نفر از متخصصان حوزه فناوری اطلاعات دارای تألیفات در حوزه فناوری اطلاعات یا بیش از بیست سال سابقه کار در این حوزه بودند. گروه خبرگان با استفاده از روش نمونه‌گیری در دسترس صورت گرفت. دلیل انتخاب این افراد آشنایی با فناوری اینترنت اشیا و زنجیره بلوک بود. کلمات برای افراد مختلف دارای معانی متفاوتی هستند و با این استدلال که کلمات دارای عدم‌قطعیت و مجموعه‌های فازی نوع یک دارای یک بعد قطعی هستند، مجموعه‌های فازی نوع دو، عدم‌قطعیت کلمه را بهتر می‌توانند مدل کنند [۲۳]. از همین‌رو از اعداد فازی نوع دو در تحلیل سلسله مراتبی در این پژوهش استفاده شده است.

یافته‌های پژوهش

خروجی فاز اول پژوهش نشان‌دهنده چالش‌های امنیتی اینترنت اشیا بر بستر زنجیره بلوک است که عبارتند از: مدیریت داده مقیاس‌پذیر [۵،۶]، پیچیدگی [۹،۲۴]، سرعت شبکه [۱۰]، قابلیت تعامل [۳،۱۱]، حریم خصوصی [۱۲،۲۵]، استانداردها [۱۳]، فورک [۱۴،۱۵]، قوانین و حاکمیت [۱۷،۱۸]، نقص امنیتی [۲۰،۲۱]، و سیاست [۳].

جهت بومی‌سازی چالش‌های استخراجی و همچنین استفاده از متخصصان ایرانی حوزه فناوری اطلاعات در قالب پرسشنامه‌ای جهت ارزیابی میزان اهمیت هر چالش توزیع گردید. چالش‌های شناسایی‌شده، با استفاده از روش دلفی و اوزان آنها مطابق نظر خبرگان فناوری اطلاعات در جدول ۱ نشان داده شده است. با توجه به ضرایب به‌دست آمده بعد قوانین و حاکمیت و استانداردها از منظر خبرگان دارای بیشترین اهمیت می‌باشد. این یافته نشان‌دهنده اهمیت کنترل‌های مالی و نظارت بر روابط اشیا در شبکه است. حریم خصوصی، نقص امنیتی و داده مقیاس‌پذیر در اولویت‌های بعدی قرار می‌گیرند.

جدول ۱: اوزان فازی و دقیق مؤلفه‌های پژوهش

مؤلفه	اوزان فازی	مقادیر دقیق نرمال
قوانین و حاکمیت	(۱، ۱، ۰/۶۷۰، ۰/۴۵۸، ۰/۲۲۲، ۰/۱۴۲) (۰/۸، ۰/۸، ۰/۶۲۱، ۰/۴۲۷، ۰/۲۴۰، ۰/۱۵۷)	۰/۳۱
قابلیت تعامل	(۱، ۱، ۰/۰۷۶، ۰/۰۴۸، ۰/۰۲۳، ۰/۰۱۷۲) (۰/۸، ۰/۸، ۰/۰۶۹، ۰/۰۴۴، ۰/۰۲۵، ۰/۰۱۸)	۰/۰۳
حریم خصوصی	(۱، ۱، ۰/۳۲۵، ۰/۲۲۵، ۰/۱۰۹، ۰/۰۷۲) (۰/۸، ۰/۸، ۰/۳۰۸، ۰/۲۰۷، ۰/۱۱۸، ۰/۰۷۹)	۰/۱۶
فورک	(۱، ۱، ۰/۰۶۲، ۰/۰۳۲، ۰/۰۱۴، ۰/۰۱۰) (۰/۸، ۰/۸، ۰/۰۵۳، ۰/۰۲۹، ۰/۰۱۵، ۰/۰۱۰)	۰/۰۲
داده مقیاس‌پذیر	(۱، ۱، ۰/۱۷۷، ۰/۱۱۰، ۰/۰۵۲، ۰/۰۳۵) (۰/۸، ۰/۸، ۰/۱۶۰، ۰/۱۰۱، ۰/۰۵۶، ۰/۰۳۸)	۰/۰۸
سرعت شبکه	(۱، ۱، ۰/۱۲۶، ۰/۰۷۴، ۰/۰۳۴، ۰/۰۲۳) (۰/۸، ۰/۸، ۰/۱۱۱، ۰/۰۶۸، ۰/۰۳۶، ۰/۰۲۵)	۰/۰۵
پیچیدگی	(۱، ۱، ۰/۰۷۷، ۰/۰۴۲، ۰/۰۱۹، ۰/۰۱۳) (۰/۸، ۰/۸، ۰/۰۶۷، ۰/۰۳۸، ۰/۰۲۰، ۰/۰۱۴)	۰/۰۳
نقص امنیتی	(۱، ۱، ۰/۲۱۰، ۰/۱۴۱، ۰/۰۷۰، ۰/۰۴۷) (۰/۸، ۰/۸، ۰/۱۹۳، ۰/۱۳۱، ۰/۰۷۵، ۰/۰۵۱)	۰/۱۰
استانداردها	(۱، ۱، ۰/۴۶۲، ۰/۳۱۴، ۰/۱۵۰، ۰/۰۹۶) (۰/۸، ۰/۸، ۰/۴۲۷، ۰/۲۹۰، ۰/۱۶۴، ۰/۱۰۶)	۰/۲۱

بحث و نتیجه‌گیری

با توجه به نتایج به‌دست آمده مشخص گردید چالش قوانین و حاکمیت دارای بالاترین اهمیت از منظر خبرگان حوزه فناوری اطلاعات ایرانی است. می‌توان چنین نتیجه گرفت سیاست‌گذاران بخش پولی و مالی کشور باید آگاه باشند که دغدغه کنترل پول‌های کثیف و پول‌شویی و فرارهای مالیاتی اصلی‌ترین چالش در به‌کارگیری فناوری زنجیره بلوک است زیرا تراکنش‌های مالی در این شبکه در مقایسه با شبکه‌های متمرکز متفاوت است و نهادهای ذی‌ربط کنترل کمتری نسبت به آن دارد. استانداردهای هر شبکه از مهمترین ارکان آن محسوب می‌شود از همین‌رو جهت تامین امنیت و سایر ارتباطات شبکه، چالش استاندارد زنجیره بلوک و نحوه ارتباط اشیاء اهمیت زیادی از منظر خبرگان دارد. با در نظر گرفتن تعدد اشیاء در فناوری اینترنت اشیا و سیستم توزیع شده در زنجیره بلوک، چالش حریم خصوصی و حفظ محرمانگی اشیا اهمیت زیادی از منظر خبرگان دارد زیرا بلوک‌های اطلاعاتی توسط افراد مختلفی باید مورد تأیید قرار گیرند. از همین‌رو امکان دسترسی به بلوک‌های اطلاعاتی نیاز به پیچیدگی بیشتری دارد بدین جهت خبرگان چالش حریم خصوصی و محرمانگی اطلاعات افراد را یکی از موارد پراهمیت وزن‌دهی کردند. در صورتی‌که فناوری اینترنت اشیا بر پایه زنجیره بلوک استقرار یابد به فراخور نوع کارایی شبکه بر تعداد اشیا موجود در شبکه افزوده می‌شود از همین‌رو با افزایش تعداد گره‌ها و اشیا کیفیت و عملکرد شبکه حائز اهمیت است تا با آفت سرعت مواجه نشود و از ورود افراد ناشناس مقابله شود. همین امر بر اهمیت نقص امنیتی شبکه از منظر خبرگان دلالت دارد. با توجه به حجم زیاد داده‌های اینترنت اشیا و امکان ارتباط بین اشیا مختلف بر بستر سیستم توزیع شده مقیاس‌پذیری و توجیه کاربری آن حائز اهمیت است. همچنین سرعت شبکه زنجیره بلوک در مقایسه با کنترل اینترنت اشیا در سیستم متمرکز در اولویت بعدی قرار دارد؛ در کاربری‌های پزشکی اینترنت اشیا سرعت انتقال داده اهمیت بیشتری پیدا می‌کند زیرا با سلامت فرد مواجه می‌شود [۲۶]. در انتها نیز چالش‌های قابلیت تعامل، پیچیدگی و تشکیل فورک‌ها از منظر خبرگان در اولویت قرار می‌گیرند. با توجه به نتایج به دست آمده جهت استقرار و پیاده‌سازی فناوری اینترنت اشیا در بستر زنجیره بلوک پیشنهاد می‌گردد استفاده از فناوری رایانش مه موجب ارتقای سرعت و کنترل انتقال اطلاعات فناوری اینترنت اشیا می‌شود. استفاده از زنجیره بلوک انحصاری می‌تواند راهکار بعدی جهت اعمال قوانین حاکمیتی و منطقه‌ای باشد تا کنترل تبادل اطلاعات و تراکنش‌های صورت گرفته با اطمینان بیشتری صورت پذیرد. جهت کاهش مشکلات امنیتی پیشنهاد می‌شود مسیریاب‌ها طوری پیکربندی شوند که بتوانند از حملات ساده، با فیلترکردن پروتکل‌های غیرضروری جلوگیری کنند و بتوانند آدرس‌های IP نامعتبر را نیز متوقف کنند. اگرچه، چنین راهکاری بر پیچیدگی سیستم می‌افزاید اما با توجه به اولویت‌بندی صورت گرفته رفع نواقص امنیتی اهمیت بیشتری داد. همچنین پیکربندی مناسب برنامه‌های کاربردی سرویس‌دهنده، جهت ارتباط اینترنت اشیا در به حداقل رساندن تأثیر حمله منبع سرویس تأثیر بسیار مهمی دارند. با توجه به کاربرد گسترده فناوری اینترنت اشیا در حوزه پزشکی و سلامت جهت پژوهش‌های آینده پیشنهاد می‌گردد تا چالش‌های اینترنت اشیا در حوزه سلامت با خروجی‌های این پژوهش مقایسه شود.

منابع و مؤاخذ

[1]. Ronaghi, M. H., & Forouharfar, A. (2020). A contextualized study of the usage of the Internet of things (IoTs) in smart farming in a typical Middle Eastern country within the context of Unified Theory of Acceptance and Use of Technology model (UTAUT). Technology in Society, 63, 101415. https://doi.org/10.1016/j.techsoc.2020.101415

[2]. Atlam H., Walters R. and Wills G. (2018). Fog computing and the internet of things: a review. Big data cogn. comput. 2(10): 2-18.

[3]. Moin S., Karim A., Safdar Z., Safdar K., Ahmed E. and Imran M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues, Future Generation Computer Systems, 100: 325–343.

[4]. Ronaghi, M. H. (2022). Contextualizing the impact of blockchain technology on the performance of new firms: The role of corporate governance as an intermediate outcome. The Journal of High Technology Management Research, 33(2), 100438. https://doi.org/10.1016/j.hitech.2022.100438

[5]. Zhang Z., et al., (2014). IoT security: ongoing challenges and research opportunities, in: Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, IEEE, 2014.

[6]. Dinh T.N. and Thai M.T. (2018). Ai and blockchain: A disruptive integration, Computer 51(9): 48–53.

[7]. Biswas K. and Muthukkumarasamy V. (2016). securing smart cities using blockchain technology, in: High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on, IEEE.

[8]. Ronaghi, M. H. (2022). Blockchain Technology Acceptance in Iran's Banking Industry. Journal of Management Improvement, 16(1), 30-53. (In Persian)
[9]. Spearpoint M. (2017). A proposed currency system for academic peer review payments using the blockchain technology, Publications 5(3): 19-25.
[10]. Khan M.A. and Salah K. (2018). IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82: 395–411.
[11]. Underwood S. (2016). Blockchain beyond bitcoin, Commun. ACM 59 (11): 15–17.
[12]. Singh S., Jeong Y. and Park J.H. (2016). A survey on cloud computing security: Issues, threats, and solutions, J. Netw. Comput. Appl. 75: 200–222.
[13]. Xu T., Wendt J. and Potkonjak M. (2014). Security of IoT systems: Design challenges and opportunities, in: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press.
[14]. Lin I. and Liao T. (2017). A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 19 (5): 653–659.
[15]. Wortmann F. and Flüchter K. (2015). Internet of things, Bus. Inf. Syst. Eng. 57(3): 221–224.
[16]. Yeoh P. (2017). Regulatory issues in blockchain technology, J. Financ. Regul. Compliance 25 (2): 196–208.
[17]. Grosse R. (2012). Bank regulation, governance and the crisis: a behavioral finance view, J. Financ. Regul. Compliance 20 (1) (2012) 4–25.
[18]. Kewell B., Adams R. and Parry G. (2017). Blockchain for good? Strateg. Change 26 (5): 429–437.
[19]. Ronaghi, M. H. (2021). Open-source software migration under sanctions conditions. International Journal of System Assurance Engineering and Management, 12(6), 1132-1145. https://doi.org/10.1007/s13198-021-01329-y
[20]. Fabiano N. (2017) The internet of things ecosystem: The blockchain and privacy issues, The challenge for a global privacy standard, in: Internet of Things for the Global Community (IoTGC), 2017 International Conference on, IEEE.
[21]. Norta A. (2015). Creation of smart-contracting collaborations for decentralized autonomous organizations, in: International Conference on Business Informatics Research, Springer, 2015.
[22]. Pashaeizad H. (2008). Delphi method: a comprehensive approach. Peyk noor. 6(2): 63-80 (In Persian)
[23]. Mendel. J. M., (2007). Type-2 Fuzzy Sets and Systems: An Overview, Computational Intelligence Magazine, IEEE, 2:20-29.
[24]. Tasatanattakool P. and Techapanupreeda C. (2018). Blockchain: Challenges and applications, in: Information Networking (ICOIN), 2018 International Conference on, IEEE.
[25]. Rehiman K. and Veni S. (2015). Privacy and trust for smart mobile devices in internet of things—A literature study, Int. J. Adv. Res. Comput. Eng. Technol. 4(5): 1775–1779.
[26]. Ronaghi M. and Hosseini F. (2018). Identifying and Ranking IoT Services in Healthcare Sector, Journal of health administration, 21(73):29-41 (In Persian)

Science and Education

Critical Issues of IoTs in Distributed Blockchain in Iran

Mohammad Hossein Ronaghi[*,1]

Internet of Things (IoT) refers to the distributed smart sensor objects, sensor networks and wearable devices with the purpose of exchanging information and services through sensor networks are the key for creating smart environments. Present IoT data is not trustworthy in the external environment, as data manipulation is lacking when data is shared with other parties. To overcome the above-mentioned limitation of IoT, the emerging secure decentralized storage technology; the blockchain technology refers to the distributed database or ledger that preserve connected devices record sets as a new thing. Therefore, we aim to identify the essential implementation requirements of blockchain in the IoTs by content analysis. In the second phase evaluate interpretation of experts by Delphi method. Panel of information technology experts consists twelve members who work on IT sector. Finally, we use Analytic Hierarchy Process method under interval type 2 fuzzy logic for ranking codes. An important part of the results revealed the importance of Regulations and governance (0.31), Standards (0.21), Privacy (0.16), Security flaw (0.10), Scalable data management (0.08), Network speed (0.05), Complexity (0.03), Interoperability (0.03) and Fork (0.02) in security challenges of IoTs in Blockchain. According to the results of this study, the growing needs of the users for secure communication in IoT network infrastructures while adopting blockchain as a security solution. However, adopting blockchain in the IoT environment imposes certain security and trust issues/requirements.

Keywords: Internet of Things, Blockchain, Governance, Delphi Technique, Type-2 fuzzy set

[*] Corresponding Author, Associate Professor, Tel/Fax: (071)36276372, E-mail: mh_ronaghi@shirazu.ac.ir
[1] Department of Management, College of Economics, Management and Social sciences, Shiraz University, Shiraz, Iran

DOR: 20.1001.1.2008935.1401.13.1.8.1