نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۱، بهار ۱۴۰۰؛ ص ۲۵-۱

علمی – تخصصی

بررسی ادغام کاربردی بلاک‌چین و نقش آن در حوزهٔ اینترنت اشیا

احمد محمدی*

باشگاه پژوهشگران جوان و نخبگان، دانشگاه آزاد اسلامی واحد اردبیل، ایران

(دریافت: ۱۳۹۸/۱۲/۱۷، پذیرش: ۱۳۹۹/۱۱/۲۵)

چکیده

اینترنت اشیا یکی از عوامل تغییر زندگی انسان و کسب منافع عظیم اقتصادی است. به هر حال امنیت ناکافی داده‌ها و قابلیت اطمینان پایینِ اینترنت اشیا فعلی، به‌طور جدی استفاده از آن را محدود کرده‌اند. بلاک‌چین یک عامل توزیع شده و مقاوم در مقابل دست‌کاری است که شامل سوابق پایدار داده‌ها در موقعیت‌های مختلف بوده و توانایی رفع دغدغه‌های مربوط به امنیت داده‌ها در شبکه‌های اینترنت اشیا را دارد. بلاک‌چین درحالی‌که امنیت داده‌ها را برای اینترنت اشیا تضمین می‌کند، قابلیت رویارویی با برخی از چالش‌های اینترنتی نظیر بالا بودن تعداد دستگاه‌های اینترنت اشیا، ساختار ناهمگن شبکه، توان محدود رایانه، پهنای باند ارتباطی پایین و پیوندهای رادیوییِ مستعد خطا را دارد. این مقاله یک بررسی جامع بر روی فناوری‌های بلاک‌چین موجود انجام داده و نیز کاربردهای اینترنت اشیا را به‌صورت مفصل شرح می‌دهد. فناوری‌های بلاک‌چینی که توانایی پرداختن به چالش‌های مهمِ ناشی از اینترنت اشیا را داشته و به‌دنبال آن عملیات استفاده از کاربردهای اینترنت اشیا را ساده می‌کنند، با قابلیت‌های ممکن و پیشرفت‌های موجود در قراردادهای اجماعی بلاک‌چین و ساختارهای داده‌ها مورد شناسایی قرار گرفته‌اند.

کلیدواژه‌ها: بلاک‌چین، اینترنت اشیا، قرارداد اجماع، ساختار داده، ساختار ترکیبی، محدودیت‌های امنیت اینترنت اشیا

۱- مقدمه

سازوکارهای امنیتی سنتی نظیر شیوه‌های رمزنگاری به‌تنهایی برای حفظ یکپارچگی داده‌های عظیم کافی و مؤثر نیستند، از این‌رو، استفاده از فناوری اینترنت اشیا[1] در آینده را به‌طور جدی محدود می‌کنند. اینترنتی که اینترنت اشیا مبتنی بر آن است، به خودی‌خود محیطی ناامن بوده و همان‌طور که همیشه ثابت شده، امنیت داده‌ها در آن عاملی مهم است. علاوه‌بر این، اینترنت اشیا، معماری به‌طور کامل متفاوتی نسبت به اینترنت دارد و قابلیت اتصال به شبکه محاسبه را داشته، همچنین توانمندی اشیایی مثل حس‌گرها، وسایل بی‌مصرف را در عین محدودیت گسترش داده و این اشیا را قادر به تولید، تبادل و مصرف داده‌ها با کمترین میزان دخالت انسانی می‌سازد. در واقع استفاده از راهکارهای محاسباتی و هزینه‌بر در زمینهٔ امنیت اینترنت برای اینترنت اشیا نه اقتضایی و نه عملی است. از سرویس‌های ابری که در رأس اینترنت هستند به‌طور گسترده در پردازش و ذخیرهٔ داده‌های پرحجم اینترنت اشیا استفاده شده است. در بسیاری از موارد، داده‌های اینترنت اشیا می‌توانند در سرورهای مختلف در سرتاسر محیط ابری ذخیره شده و به‌صورت توزیع شده پردازش و مورد دسترسی قرار گیرند. با این‌حال سرویس‌های ابری می‌توانند به‌صورت ذاتی ناامن بوده و نسبت به حملات سایبری مثل، SQL injection و دست‌کاری داده‌های حساس که در مواقع خراب شدن یک گره آسیب‌پذیر باشند. به‌طورکلی، سرویس‌های ابری نمی‌توانند یکپارچگی و قابلیت دسترسی داده‌ها را تضمین کنند که همین مسئله در مورد برنامه‌های کاربردی اینترنت اشیا نیز صدق می‌کند. بلاک‌چین یک پایگاه دادهٔ فراگیر، انحراف ناپذیر و مقاوم در مقابل دست‌کاری بوده و توانایی بررسی مسائل امنیتی حیاتی اینترنت اشیا را دارد، به‌ویژه در زمینهٔ یکپارچگی و قابلیت اطمینان داده‌ها، بلاک‌چین برنامه‌های کاربردی نرم‌افزاری را قادر به ارسال و ذخیرهٔ تراکنش‌ها / رویدادها با استفاده از روش‌های قابل‌اعتماد و توزیع شده (نظیر به نظیر[2]) می‌سازد. بلاک‌چین به سرعت در حال افزایش محبوبیت خود بوده و از آن به‌طور گسترده در برنامه‌هایی کاربردی که شامل قراردادهای هوشمند، قابلیت ذخیره‌سازی توزیع شده و دارایی‌های دیجیتال می‌شوند استفاده شده است. کاربردهای بالقوهٔ بلاک‌چین در اینترنت اشیا شامل ذخیره‌سازی رویدادها (مثل تغییرات دما، رطوبت یا

* رایانامه نویسنده مسئول: ahmadmohammadi13641364@gmail.com

[1] Internet of Things(IOT)

[2] peer to peer

موقعیت) و ایجاد دفترکل‌های مقاوم در مقابل دست‌کاری می‌شود که این دفترها تنها توسط اشخاص خاص قابل خواندن می‌باشند؛ به‌عنوان مثال، شرکای خاص در یک زنجیرهٔ تأمین، نیازهای امنیتیِ اینترنت اشیا می‌توانند به‌واسطهٔ فناوری‌های بلاک‌چین برآورده شوند. ویژگی‌های برجستهٔ بلاک‌چین که در ادامه مطرح شده‌اند می‌توانند به یکپارچگی قابلیت‌های اینترنت اشیا کمک کنند و به‌دنبال آن امنیت اینترنت اشیا را بالا ببرند:

تمرکز زدایی: به‌طور ذاتی تنظیمات شبکهٔ نظیر به نظیر در بلاک‌چین برای شبکه‌های اینترنت اشیا مناسب است که به صورت معمولی توسعه یافته‌اند، برای مثال توسعهٔ بلاک‌چین در شبکه‌های اقتضایی خودرویی[1] بلاک‌چین‌ها می‌توانند تراکنش‌های موجود در بین بخش‌های مختلف را بدون نیاز به هماهنگی مرکزی ثبت کنند. این می‌تواند باعث منعطف‌تر شدن پیکربندی‌ها شده و خطر مربوط به خرابی‌های تک نقطه‌ای را کاهش دهد [۱].

یکپارچگی: بلاک‌چین‌ها می‌توانند تراکنش‌ها را به‌صورت دائمی با استفاده از یک روش قابل بازبینی حفظ کنند. به‌طور مشخص امضاء ارسال‌کنندگان در تراکنش‌ها می‌تواند تضمین کنندهٔ تمامیت و عدم‌انکار تراکنش‌ها شود. ساختار زنجیرهٔ درهم مربوط به بلاک‌چین‌ها این مسئله را تضمین می‌کند که هیچ دادهٔ ذخیره شده‌ای را نتوان تغییر داد، حتی به‌صورت جزئی. قراردادهای اجماع بلاک‌چین‌ها می‌توانند معتبر و سازگار بودن سوابق را تضمین کنند. همچنین قراردادها می‌توانند خرابی‌ها و حملات را تحمل کنند؛ برای مثال حملاتی که توانشان در قرارداد اثبات کار[2] کمتر از یک‌دوم یا در قرارداد اجماعی تحمل خطای بیزانس[3] عملی کمتر از یک‌سوم گره‌ها باشد. همهٔ این‌ها برای کاربردهای اینترنت اشیا حیاتی هستند، جایی که داده‌های اینترنت اشیا می‌توانند توسط دستگاه‌های ناهمگن یا در محیط‌های شبکه‌ای ناهمگن تولید و پردازش شوند [۲].

ناشناس بودن : بلاک‌چین‌ها می‌توانند برای حفظ ناشناسی و حریم خصوصی از کلیدهای عمومیِ قابل تغییر به‌عنوان هویت کاربران استفاده کنند. این برای بسیاری از خدمات و قابلیت‌های اینترنت اشیا جذاب است، به‌ویژه آن‌هایی که نیاز دارند هویت محرمانه و حریم خصوصی را حفظ کنند [۲].

در حال حاضر تمایلات به‌سمت استفاده از بلاک‌چین در شبکه‌های اینترنت اشیا در حوزهٔ دانشگاهی و صنعت با هدف بالا بردن امنیت در حال افزایش است. در همین راستا محیط ابری می‌تواند قابلیت ذخیره‌سازی توزیع شده را برای برنامه‌های کاربردی مبتنی بر اینترنت اشیا فراهم کند، این در حالی است که بلاک‌چین قابلیت تضمین یکپارچگی ذخیره‌سازی و جلوگیری از دست‌کاری داده‌ها را دارد. بلاک‌چین و ابر می‌توانند در هم ادغام و به‌صورت یک ابر توزیع شدهٔ مبتنی بر بلاک‌چین خدمت‌رسانی کنند. با این‌حال فناوری‌های بلاک‌چین موجود می‌توانند به واسطهٔ پیاده‌سازی هزینه‌بر دستگاه‌های اینترنت اشیا که پیش از این ذکر شد، ساختار ناهمگن شبکه با افرازبندی قوی و به‌دنبال آن داده‌های پرحجم حسگرها و تقاضا برای ظرفیت زیاد در بلاک چین برای قابلیت‌های اینترنت اشیا ناکارآمد باشند (به‌عنوان مثال، سرعت بالای تولید تراکنش‌ها یا بلوک‌ها). به‌طور مشخص ویژگی‌های فیزیکی دستگاه‌های اینترنت اشیا و شبکه‌ها مثل پهنای باند و قابلیت اتصال محدود، هم‌بندی غیرقطعی و تأخیرهای غیرقابل پیش‌بینی پیوندها می‌توانند باعث ایجاد اختلاف یا ناهماهنگی بین سوابق ذخیره شدهٔ توزیع شده در موقعیت‌های مختلف شوند. در واقع، سرعت تولید ثبت باید به واسطهٔ سرعت انتشار بلوک‌ها محدود شود، این بلوک‌ها همان بخش‌های دادهٔ بلاک‌چین‌ها هستند. فناوری‌های بلاک‌چین موجود که کمابیش به‌صورت غیرمنتظره در لایهٔ کاربردی کار می‌کنند و غافل از جنبه‌های فیزیکی شبکه‌ها و دستگاه‌ها هستند، می‌توانند سرعت تولید بلوک را بسیار کندتر از انتشار آن کنند، از این‌رو، این امر باعث استفادهٔ ناکارآمد از بلاک‌چین می‌شود. در این بررسی ما در مورد چالش‌های کلیدی و مزایای بلاک‌چین در کاربردهای اینترنت اشیا بحث می‌کنیم. شاخص‌ترین فناوری‌های بلاک‌چین از نظر قراردادهای اجماع و ساختارهای داده مورد تحلیل قرارگرفته‌اند. در اینجا محدودیت‌های فناوری‌های بلاک‌چین موجود برای کاربردهای اینترنت اشیا، همچنین مسیرهای تحقیقاتی بالقوهٔ آینده ذکر شده‌اند. شایان‌ذکر است که به‌تازگی نظرسنجی‌هایی به‌صورت کلی بر روی بلاک‌چین و نقش آن در اینترنت اشیا انجام شده است. این نظرسنجی تأکید زیادی بر روی طراحی و کاربرد دارند. در مقابل ما در این بررسی بر روی پیشینهٔ نظری بلاک‌چین متمرکز خواهیم شد. ما به‌طور مخصوص علاقه‌مند به شناسایی محدودیت‌ها و شکاف‌های نظریه‌های فعلی و درک تأثیرات آنها بر روی طراحی مقیاس‌پذیر بلاک‌چین برای کاربردهای اینترنت اشیا هستیم [۹-۳].

۲- روش تحقیق

این بررسی پیشرفت‌های تحقیقاتی اخیر بر روی بلاک‌چین و قابلیت‌های اینترنت اشیا که مبتنی بر بلاک‌چین هستند را به‌طور خلاصه بیان می‌کند. این بررسی روی هم مبتنی بر مراجع

[1] Vehicular ad hoc network(VANET)
[2] Proof of Work(POW)
[3] Byzantine Fault Tolerance(BFT)

تحقیقاتی است که از گوگل اسکولار[1]، وب‌آوساینس[2]، آی‌تریپل ای‌اکسپلور[3]، الزویر[4] و نیز مراجع برخطی مثل صفحات وب و جوامع توسعه‌دهنده در راستای ارائهٔ یک بررسی به‌هنگام بر روی فناوری‌های بلاک‌چین به‌دست آمده‌اند. مراجع به‌طور جامع مطابق با پنج خصوصیت مهم از فناوری‌های اینترنت اشیا بلاک چین دسته‌بندی شده‌اند. این بررسی ابتدا با هدف مسائل امنیتی اینترنت اشیا، مشخصه‌های اینترنت اشیا را به‌طور خلاصه بیان و در بخش (۳) تحلیل‌های امنیتی بر روی اینترنت اشیا انجام می‌دهد. در اینجا توجه ویژه به‌سمت ویژگی‌های منحصر به فرد شبکه‌ها و کاربردهای اینترنت اشیا مثل پویایی، هزینهٔ پایین، نیاز به توان بالا، دستگاه‌های پرتعداد، داده‌های پرحجم اینترنت اشیا، معماری غیرمتمرکز شبکه و اتصالات ناپایدار است. این مقاله با بررسی آخرین تحقیقات امنیتی انجام شده بر روی اینترنت اشیا، مسائل امنیتی در اینترنت اشیا نظیر حملاتی که به دستگاه‌های نهایی می‌شوند، حملات کانال‌های ارتباطی، حملات قراردادهای شبکه، حملات داده‌های حسگرها، حملات جلوگیری از سرویس‌دهی و حملات نرم‌افزاری را مورد شناسایی قرار می‌دهد. در بخش (۴) با در نظر گرفتن اولین برنامه کاربردی بلاک‌چین مثل بیت‌کوین[5]، مقدمات بلاک‌چین که شامل ساختار دادهٔ زنجیره‌ای، مسئله فرماندهان بیزانس[6] و قراردادهای اجماع می‌شوند، مورد بررسی قرار گرفته‌اند. این مقاله با بررسی مدل‌های حملات تئوریک و تحلیل حملات بلاک‌چین فعلی، بلاک‌چین را آنالیز می‌کند. حملات معمولی شامل حملهٔ دوبار خرج کردن، حملهٔ قرارداد اجماع، حملهٔ کسوف[7] و حملهٔ منع سرویس[8] می‌شوند. همان‌طور که در بخش (۵) گفته شده، بلاک‌چین نیز از فریب‌های برنامه‌نویسی، آسیب‌پذیری قراردادهای هوشمند و انتشار کلید خصوصی رنج می‌برد. در بخش (۶) کاربردها و پروژه‌های صنعتی اینترنت اشیا مبتنی بر بلاک‌چین با تأکید بر روی دو ساختار معمولی به نام‌های « بلاک‌چین ادغام شده با اینترنت اشیا» بلاک‌چین به‌عنوان یک سرویس برای اینترنت اشیا مورد بررسی قرارگرفته‌اند. چالش‌های حیاتی استفاده از بلاک‌چین در اینترنت اشیا به واسطهٔ مطالعهٔ کارایی بلاک‌چین و مقررات اینترنت اشیا مشخص شده‌اند. طرح‌ها و فناوری‌های بالقوهٔ بلاک‌چین که می‌توانند در کاربردهای اینترنت اشیا به کار گرفته شوند همراه با بحث‌های مربوط به حریم خصوصی هویت و کنترل دسترسی توضیح داده شده‌اند. این بررسی بیشتر به شرح سازگاری آخرین فناوری‌های بلاک‌چین در اینترنت اشیا از نظر ۳ دسته‌بندی غالب بلاک‌چین به نام‌های بلاک‌چین عمومی، بلاک‌چین خصوصی و بلاک‌چین ترکیبی می‌پردازد. ساز و کارهای محبوب اعتبارسنجی بلوک مثل مکانیسم اثبات کار، اثبات X و تحمل خطای بیزانس به‌طور مفصل شرح داده شده‌اند. علاوه‌بر ساختار زنجیره‌ای، دیگر ساختارهای داده‌ای که عملکرد بلاک‌چین را بهبود می‌بخشند و برای بلاک‌چین در اینترنت اشیا سودمند هستند (شامل DAG، GHOST و موارد دیگر می‌شوند) ارائه شده‌اند. پروژه‌ها و فناوری‌های تأثیرگذار از نظر ظرفیت، مقیاس و ویژگی‌های خاص با هم مقایسه شده‌اند. جزئیات را می‌توانید در بخش (۷) ببینید. این نظرسنجی اشاره به تعدادی از رویکردها و فرصت‌های تحقیقاتی در راستای پر کردن شکاف فعلی بین الزامات قابلیت‌های اینترنت اشیا و محدودیت‌های فناوری‌های بلاک‌چین موجود دارد [۱۰].

۳- محدودیت‌های امنیت اینترنت اشیا

شبکهٔ اینترنت اشیا به‌واسطهٔ توانایی‌اش در اتصال دستگاه‌های زیادی که قابلیت‌های محاسباتی و سنجشی مختلفی را در عین کمترین دخالت انسانی دارند، بر رقبای خود چیره شده است. بررسی و تحریک دستگاه‌ها باعث ایجاد شبکه‌های اینترنت اشیا ناهمگن در راستای ارائهٔ خدمات مختلف می‌شود. قابلیت‌های معمولی اینترنت اشیا شامل خانه‌های هوشمند، حمل و نقل هوشمند، شبکه‌های سلامت و شبکه‌های هوشمند می‌شود. یک معماری معمولی اینترنت اشیا از بالا به پایین شامل لایه‌های ادراکی، شبکه، سرویس و رابط می‌شود. لایهٔ ادراکی که در دیگر معماری‌های اینترنت اشیا به لایهٔ حسگر معروف است، شامل حسگرها و فعال‌کننده‌هایی می‌شود که اطلاعات محیطی را در راستای انجام عملیاتی مثل دریافت میزان دما، موقعیت، حرکت و شتاب جمع‌آوری و پردازش می‌کنند. لایهٔ ادراک یکی از بخش‌های ضروری نوعی از قابلیت‌های اینترنت اشیا است. از انواع دستگاه‌ها می‌توان در لایهٔ ادراکی در راستای ارتباط دنیای فیزیکی به دنیای دیجیتال استفاده کرد. دستگاه‌های نهایی معمولی شامل سامانه شناسایی فرکانس رادیویی[9]، حسگرها و فعال‌کننده‌های بی‌سیم، ارتباط میدانی نزدیک[10] و تلفن‌های سیار می‌شوند. برای مثال، برچسب RFID یک ریز تراشهٔ کوچک است که به یک آنتن متصل شده است [۱۱]. با اتصال برچسب‌های RFID به اشیا، می‌توان آنها را در عملیات منطقی، خرده‌فروشی‌ها و زنجیره‌های تأمین شناسایی، ردیابی و مورد نظارت قرارداد. لایهٔ شبکه مسئول ارتباط دیگر دستگاه‌های

[1] Google Scholar
[2] Web Of Science
[3] IEEE Xplore
[4] Elsevier
[5] Bitcoin
[6] Byzantine Generals Problem
[7] Eclipse Attack
[8] Denial of Service attack(DOS)
[9] Radio-Frequency Identification(RFID)
[10] Near Field Communication(NFC)

هوشمند، دستگاه‌های موجود در شبکه و سرورها است. لایهٔ سرویس دستگاه‌های مشخصی را به‌منظور ارائهٔ الزامات اینترنت اشیا ایجاد و مدیریت می‌کند. لایهٔ رابط فعل و انفعالات مربوط به استفاده از داده‌ها را با به‌کارگیری اشیایی که برای کاربردهای خاص در نظر می‌گیرد، تسهیل می‌کند [۴-۳].

۳-۱- مشخصات اینترنت اشیا

قابلیت‌های اینترنت اشیا توانایی تأثیرگذاری بر روی جنبه‌های مختلف زندگی روزمرهٔ انسان‌ها را دارند. آنها را می‌توان به چهار دستهٔ زیر تقسیم کرد: حمل و نقل و تدارکات، مراقبت‌های بهداشتی، محیط‌های هوشمند (شامل خانه‌های هوشمند) و برنامه‌های شخصی و اجتماعی. دستگاه‌های نهایی و فناوری‌های شبکه‌ای و ارتباطی بسته به اهداف و درخواست‌های مختلف با هم متفاوت‌اند. در ادامه دو جنبهٔ اصلی که در موقعیت‌های مختلف قابلیت‌های متفاوتی دارند را بررسی می‌کنیم [۱۲].

• قابلیت جابجایی در برابر هم‌بندی پایدار:

هم‌بندی اینترنت اشیا می‌تواند بسته به سرعت متغیر باشد. قابلیت‌های معمولی با هم‌بندی‌های پایدار و متحرک برای حمل و نقل به ترتیب عبارت‌اند از شبکه‌های مربوط به خانه‌های هوشمند و شبکه‌های اقتضایی خودرویی اکثر دستگاه‌های موجود در خانه‌های هوشمند پایدار بوده و حاوی هم‌بندی شبکهٔ پایدار می‌باشند، این در حالی است که وسایل نقلیه به سرعت جابه‌جا می‌شوند و این مستلزم هم‌بندی‌هایی است که بسته به زمان متغیر هستند. تحرک دستگاه‌های نهایی باعث می‌شود اتصال به شبکه غیرقابل پیش‌بینی و مدیریت نهادها چالش برانگیز شود [۱۳].

• هزینهٔ پایین در برابر عملکرد با ظرفیت بالا:

دستگاه‌های اینترنت اشیا به‌دلیل بسترهای سخت‌افزاری و قابلیت‌های متغیر، ناهمگن هستند. یکی از انواع دستگاه‌های اینترنت اشیا حسگرهای کوچک با منابع محدود برای پردازش، ارتباط و ذخیره‌سازی می‌باشند. یک‌چنین دستگاه‌هایی به‌طور معمول کم‌هزینه بوده و از این‌رو، می‌توانند برای اندازه‌گیری دما، فشار، رطوبت،علائم پزشکی بدن انسان، مواد شیمیایی و بیوشیمیایی در مقیاس‌های وسیع مورد استفاده قرار گیرند. آنها برحسب معمول در شبکه‌های بی‌سیم اقتضایی یا شبکه‌های بی‌سیم مِش[1] مثل زیگبی[2] ارتباط برقرار می‌کنند. یک‌چنین حسگرهایی اغلب با باتری‌های محدود تغذیه می‌شوند و انرژی جدید مثل اینترنت اشیاء کم پهنا[3] به‌منظور افزایش طول عمر حس‌گرها معرفی شده‌اند، اما حس‌گرها هنوز در قابلیت‌های پردازشی، ارتباطی و ذخیره‌سازی محدود هستند. یکی دیگر از انواع دستگاه‌های اینترنت اشیا که می‌توانند گران‌تر و قوی‌تر باشند عبارت‌اند از تلفن‌های همراه و خودروها. آنها باتری‌های بزرگ‌تر و قابلیت محاسباتی و ذخیره‌سازی قوی‌تری دارند. از این‌رو، یک چنین دستگاه‌هایی می‌توانند در بالا بردن ظرفیت نقش داشته باشند.

شبکه‌های اینترنت اشیا که با دستگاه‌های ناهمگن و قراردادهای مختلف پیاده‌سازی شده‌اند، ویژگی‌های مشترک مشخصی دارند که به شرح زیر هستند:

• تعداد زیاد گره‌ها و داده‌های حجیم اینترنت اشیا :

تعداد دستگاه‌های اینترنت اشیا پیوسته در حال افزایش خواهند بود. انتظار می‌رود تعداد دستگاه‌های متصل در اینترنت اشیا تا سال ۲۰۲۰ به بیش از ۲۰/۴ میلیارد عدد برسد. اینترنت اشیا نه تنها با گره‌های زیادی کار می‌کند، بلکه تقاضای رو به رشدی برای افزایش ظرفیت دارد، چون دستگاه‌های زیاد داده‌های زیادی را نیز جمع‌آوری می‌کنند.

• غیرمتمرکزسازی[4]:

غیرمتمرکزسازی و ناهمگونی دو ویژگی از اینترنت اشیا هستند. غیرمتمرکزسازی به‌طور کلی مربوط به بالا بودن تعداد گره‌های اینترنت اشیا است (به‌عنوان مثال، در شهرهای هوشمند)، چون داده‌هایی که باید در یک لحظه پردازش شوند بسیار زیاد هستند. دستگاه‌های اینترنت اشیا داده‌ها را به‌روش غیرمتمرکز جمع‌آوری، پردازش و ذخیره‌سازی می‌کنند. الگوریتم‌های غیرمتمرکز در اینترنت اشیا مثل الگوریتم‌های خوشه‌بندی در شبکهٔ حسگر بی‌سیم [5] و رایانش غیرمتمرکز می‌توانند به ظرفیت و مقیاس‌پذیری اینترنت اشیا کمک کنند.

• اتصالات ناپایدار و غیرقابل پیش‌بینی :

اتصالات ناپایدار و غیرپیش‌بینی دستگاه‌های اینترنت اشیا نه تنها ناشی از تحرک و حالت خواب/ بیکاریِ دستگاه‌های اینترنت اشیا هستند، بلکه پیوندهای بی‌سیم معمولی غیرقابل اعتماد مربوط به دستگاه‌های اینترنت اشیا نیز از دیگر عوامل آنها می‌باشند. در نتیجه یک شبکهٔ اینترنت اشیا ممکن است به افرازهای جدا تقسیم شده و این افرازها می‌توانند در طول زمان متغیر باشند.

۳-۲- تحلیل‌های امنیتی بر روی اینترنت اشیا

ویژگی خاص اینترنت اشیا باعث می‌شوند امنیت داده‌ها تبدیل به

[1] Wireless mesh network
[2] Zigbee
[3] Narrowband IoT(NB-IOT)
[4] Decentralized
[5] Wireless Sensor Network(WSN)

یک مشکل سخت در اینترنت اشیا شود. ابتدا اینکه اکثر دستگاه‌های اینترنت اشیا در مناطق انسانی غیردوستانه و بدون نظارت مستقر شده‌اند و نمی‌توان همیشه مراقب این همه دستگاه بود. این باعث می‌شود دستگاه‌ها در مقابل صدمات چند بعدی آسیب‌پذیر باشند. برای مثال دشمنان ممکن است به‌منظور حمله به شبکه‌های اینترنت اشیا، این دستگاه‌ها را به‌صورت فیزیکی تسخیر و کنترل کنند. سازوکارهای امنیتی سنتی مثل رمزنگاری نامتقارن از نظر محاسباتی خواستار دستگاه‌های اینترنت اشیا با توانایی محدود هستند. داده‌های حسگرها می‌توانند توسط بسیاری از دستگاه‌های واسط مختلف ذخیره، منتقل و پردازش شوند که این می‌تواند خطر دست‌کاری و جعل را افزایش دهد. کانال‌های بی‌سیم غیرقابل اعتماد و باز که ماهیت داده پراکنی دارند باعث ایجاد ضررهای اضافی برای امنیت داده‌ها می‌شوند. پیچیدگی سامانه اینترنت اشیا نیز آسیب‌پذیری‌های بالا را افزایش می‌دهد. در ادامه حملات فیزیکی به شبکه‌های اینترنت اشیا از لایهٔ پایین به بالا به‌صورت خلاصه بیان شده‌اند.

۳-۲-۱- حملاتی که به دستگاه‌های نهایی می‌شوند

دشمنان گره‌ها را از طریق حملات گرفتن گره به‌صورت فیزیکی اسیر و کنترل می‌کنند. اطلاعات محرمانهٔ ذخیره شده در گره‌های اسیر مثل کلیدها و گواهی‌ها برای دشمنان قابل رؤیت خواهند شد. دشمنان نیز می‌توانند از اطلاعات گرفته شده برای نشان دادن خود به‌عنوان گره‌های مشروع استفاده کرده و حملات دیگری مثل حملهٔ تزریق داده‌های کاذب را انجام دهند.

۳-۲-۲- حملات کانال‌های ارتباطی

ممکن است دشمنان از کانال‌های انتقال شنود کرده و در آنها دخالت کنند و از ماهیت پخش رادیویی بهره ببرند. اگر پیام‌ها رمزنگاری نشده باشند، دشمنان می‌توانند به‌سرعت اطلاعات را به‌دست آورند. حتی اگر پیام‌ها رمزنگاری شده باشند، دشمنان هنوز هم می‌توانند جریان‌های آنها را تحلیل و اطلاعات خصوصی مثل موقعیت منابع یا مقاصد را به‌دست آورند. دشمنان نیز می‌توانند با ارسال پیام‌های نویزدار در کانال‌های بی‌سیم دخالت و حتی آنها را مسدود کنند.

۳-۲-۳- حملات قراردادهای شبکه

دشمنان با استفاده از بخش‌های آسیب‌پذیر قراردادهای شبکه می‌توانند حملات سایبری، حملهٔ پاسخ، حملهٔ مردمیانی[1]، سیاه‌چاله[2]، حملات لانهٔ کرمی و غیره را اجرا کنند. برای مثال، یک حملهٔ سیبیل[3] چند هویت مشروع را در دستگاه‌های اینترنت اشیا جعل می‌کند. یک‌چنین حملاتی راندمان و دقت سازوکار رأی‌گیری و قراردادهای رأی‌گیری چند مسیره را به مخاطره می‌اندازند.

۳-۲-۴- حمله به داده‌های حسگرها

شبکه‌های اینترنت اشیا می‌توانند با استفاده از قراردادهای شبکه اقتضایی با هم ارتباط داشته باشند؛ برای مثال، پیام‌ها تا رسیدن به مقصدشان گام‌به‌گام منتقل می‌شوند. در اینجا فرصت دست‌کاری داده‌ها یا تزریق داده‌های کاذب برای دشمنان فراهم می‌شود. یک دشمن می‌تواند به‌عنوان یک انتقال‌دهنده پیام‌های را دست‌کاری و آنها را به دیگر گره‌ها انتقال دهد که به این کار دست‌کاری داده‌ها گفته می‌شود. الگوریتم‌های احراز هویت به منظور جلوگیری از دست‌کاری داده‌ها پیاده‌سازی شده‌اند. حملهٔ تزریق داده‌های کاذب به دشمنانی اشاره دارد که داده‌های کاذب را با استفاده از هویت‌های مشروع به سرتاسر شبکه ارسال می‌کنند. وقتی دادهٔ کاذب پذیرفته شد، برنامه‌های کاربردی اینترنت اشیا ممکن است دستورالعمل‌های اشتباهی را ایجاد یا سرویس‌های اشتباهی را ارائه دهند که دنبال آن برنامه‌های کاربردی و شبکه‌های IoT به خطر می‌افتند. برای مثال اگر وسایل نقلیه پیام‌های اشتباهی را از جاده دریافت کنند، تراکم ترافیک ممکن است شدت یابد. با استفاده از الگوریتم‌های احراز هویت می‌توان به خوبی از حملات تزریق داده‌های کاذب پیشگیری کرد.

۳-۲-۵- حملهٔ منع از سرویس[4]

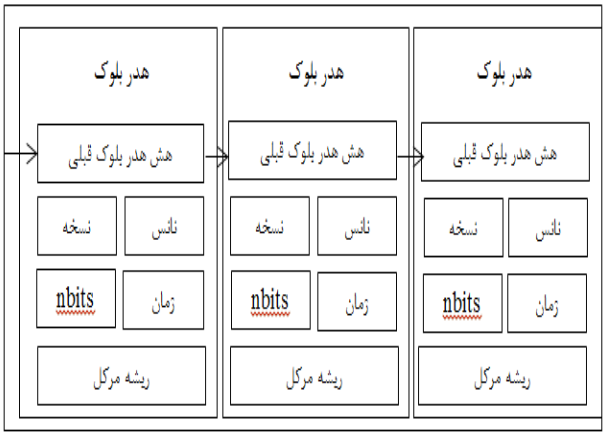
حملهٔ DoS نشان‌دهندهٔ مجموعه‌ای از حملات است که توانایی از پای درآوردن منابع و نارسایی سرویس‌های دستگاه‌های اینترنت اشیا را دارند. برای مثال حملهٔ محرومیت از خواب به وقفه انداختن در برنامهٔ خواب و بیدار نگه‌داشتن دستگاه‌ها یا گره‌ها به صورت دائمی تا زمان تمام شدن باتری‌شان اطلاق می‌شود. دستگاه‌های اینترنت اشیا منابع شبکه‌ای و ارتباطیِ محدودی دارند، از این‌رو، حملات DoS می‌توانند فاجعه‌بار باشند. یک چنین حملاتی انرژی محدود گره‌های حسگر را تمام، قابلیت اتصال شبکه را کاهش، کل شبکه را فلج و طول عمر شبکه را کاهش می‌دهند.

۳-۲-۶- حملات نرم‌افزاری

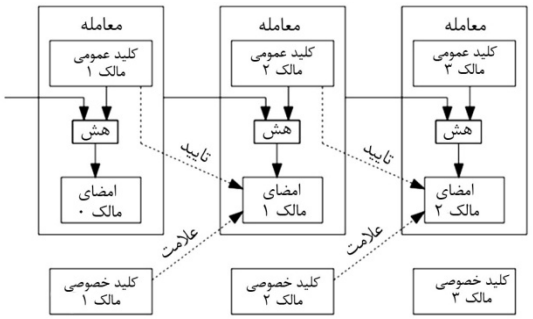
حملات نرم‌افزاری به یک سری از حملاتی گفته می‌شود که از بخش‌های پنهان نرم‌افزار برای تغییر آن و کنترل عملیات استفاده می‌کند. حملات نرم‌افزاری معمولی شامل ویروس‌ها / کرم‌ها / اسکریپت‌های مخرب می‌شوند. از سامانه تشخیص نفوذ[5] و دیگر

[1] Man-in-the-Middle(MITM)
[2] Packet drop attack
[3] sybil attack
[4] Denial of Service(DOS)
[5] Intrusion Detection System(IDS)

سازوکارهای سنتی امنیت اینترنت برای مقابله با حملات نرم‌افزاری استفاده شده است. امنیت یک دغدغهٔ مهم برای برنامه‌های کاربردی اینترنت اشیا است. به‌طور مشخص، ادغام داده‌ها و دستگاه‌های اینترنت اشیا، مثل داده‌های حسگرها و دستورات فعال‌کننده مهم‌ترین تضمین برای محفوظ نگه داشتن عملیات اینترنت اشیا است. به‌منظور محافظت از ارتباطات اینترنت اشیا و محرمانه بودن، ادغام، پیکربندی و عدم تکذیب جریان‌های اطلاعاتی سازوکارهای مؤثری باید طراحی شوند. برای اطمینان از یکپارچه بودن داده‌ها از مبدأ، دستگاه‌های اینترنت اشیا باید شناسایی شوند. از الگوریتم‌های پیکربندی و رمزنگاری برای تضمین محرمانه بودن و ادغام داده‌های اینترنت اشیا استفاده شده است. پس از اینکه داده‌های حسگر به محل ذخیره‌سازی داده‌ها ارسال شدند، مسئولیت امنیت داده‌ها بر عهدهٔ سرویس‌های ذخیره‌سازی داده‌ها خواهد بود.



ساختار داده بلوک‌ها (a)



ساختار داده معاملات (b)

شکل (۱): ساختار دادهٔ بلاک‌چین بیت‌کوین

۴- فناوری‌های بلاک‌چین فعلی

بلاک‌چین سرویس ذخیره‌سازی دادهٔ نامتمرکز را با یک دفترکل مقاوم در برابر دست‌کاری ارائه می‌کند که این دفترکل شامل بلوک‌هایی است که به‌صورت زنجیره در شبکه‌های توزیع شده به هم متصل شده‌اند. این می‌تواند تراکنش‌ها یا رویدادهای تراکنشی را با استفاده از رمزنگاری ذخیره‌سازی کند. اولین بلاک‌چین در سال ۲۰۰۸ توسط ساتوشی ناکاموتو[1] معرفی و در سال ۲۰۰۹ به عنوان فن فعال‌سازی برای توسعهٔ ارز مجازی بیت‌کوین پیاده‌سازی شد. بلاک‌چین داده‌ها را به‌صورت امن و توزیع شده ذخیره می‌کند. بخش اصلیِ سوابق در بلاک‌چین تراکنش (معامله) است. وقتی یک معاملهٔ جدید تولید می‌شود، در تمام شبکهٔ بلاک‌چین منتشر می‌شود. گره‌های دریافت‌کنندهٔ معامله می‌توانند با اعتبارسنجی امضاء ضمیمه شده به معامله آن را تائید و معاملات تائید شده‌ای را در بلوک‌های ایمن رمزنگاری شده استخراج کنند. یک‌چنین گره‌هایی به استخراج‌کنندهٔ بلوک (به صورت مختصر ماینر[2]) معروف هستند. به‌منظور اجازه دادن به یک ماینر برای ایجاد یک بلوک، یک مسئلهٔ اجماع باید یک روش توزیع شده حل شود. ماینرهایی که موفق به حل مسئلهٔ اجماع می‌شوند، بلوک‌های جدیدشان را در سرتاسر شبکه منتشر می‌کنند. به محض دریافت یک بلوک جدید، ماینرها هنوز هم قادر به حل مسئلهٔ اجماع ضمیمه شده به بلوک برای زنجیرهٔ خودشان هستند، پس از آن معاملات محصور در بلوک تائید شده و بلوک می‌تواند پاسخ صحیح مسئلهٔ اجماع را ارائه دهد. در زنجیره‌ها بلوک جدید حاوی یک پیوند متصل به بلوک قبلی است که این پیوند با استفاده از روش‌های رمزنگاری تولید شده است. همهٔ ماینرها می‌توانند زنجیره‌هایشان را به‌طور منظم باهم منطبق کنند. شرایط خاص برای اطمینان از نامتناقض بودن دفترکل در شبکهٔ توزیع شده تعریف می‌شوند؛ به‌عنوان مثال، درجایی که اختلاف بین زنجیره‌ها وجود دارد، بلاک‌چین بیت‌کوین تنها حاوی طولانی‌ترین زنجیر است. در ادامه توضیحات دقیق‌تری در مورد بخش‌های کلیدیِ بلاک‌چین (مثل ساختار داده، قرارداد اجماع، قراردادهای هوشمند و تحلیل‌های امنیتی بر روی بلاک‌چین) موجود است.

۵- تحلیل‌های امنیتی برروی بلاک‌چین

بلاک‌چین توجهات را به خاصیت ضد دست‌کاری‌اش در شبکه‌های غیرمتمرکز جلب می‌کند. به‌طور مشخص بلاک‌چین نیاز به این ندارد که گره‌ها به همدیگر اعتماد داشته باشند. با این‌حال بلاک‌چین هنوز آسیب‌پذیری‌هایی دارد. به‌طور معمول تهدیدات امنیتی برای بلاک‌چین به‌صورت زیر هستند:

• هزینه‌های مضاعف:

دشمنان سعی می‌کنند گیرنده‌های معاملات را با معاملات متناقض گمراه کنند؛ به‌عنوان مثال از کوین‌های مشابه در

[1] Satoshi Nakamoto
[2] Miner

بیت‌کوین استفاده می‌کنند. روش‌های تهاجمی شامل ارسال معاملات متناقض و استخراج قبل از موعد یک یا بیش از یک بلوک برای دریافت معاملات ناسازگار می‌شود.

• حملات مربوط به قراردادهای اجماع:

مهاجمان می‌توانند امنیت قراردادهای اجماع را با تصرف بخش بزرگی از توان محاسباتی کل شبکه به خطر بیندازند. یک‌چنین مهاجمانی می‌توانند زنجیره را کنترل و بازسازی کنند. یکی از نمونه‌های آن عبارت است از حملهٔ ۵۱٪ در بلاک‌چین‌های PoW؛ به‌عنوان مثال، بیت‌کوین. مهاجمانی که بیش از نیمی از قدرت هش را دارند می‌توانند بلاک‌چین را مجبور به پذیرش بلوک‌های نامشروع کنند؛ به این‌صورت که مسئلهٔ اجماع (به‌عنوان مثال، PoW در بیت‌کوین) را سریع‌تر از دیگر گره‌ها حل می‌کنند. در حال حاضر ثابت شده که ۳۳٪ از قدرت هش برای غلبه بر قدرت PoW کافی است.

• حملات Eclipse:

حملات Eclipse به حملات موجود در شبکهٔ نظیر به نظیر اطلاق می‌شود، جایی که دشمنان تمام نقاط اتصال به گره‌های مشروع را به انحصار خود درمی‌آورند و از اتصال این گره‌ها به گره‌های بی‌عیب و نقص جلوگیری می‌کنند. حملهٔ Eclipse در بلاک‌چین ابتدا از طریق یک قرارداد تصادفی بر روی بیت‌کوین انجام شد. در این قرارداد این‌طور تعریف می‌شود که یک گره در بیت‌کوین به تعداد مشخصی از همسایه‌های منتخب متصل می‌شود تا از این طریق ارتباط نظیر به نظیر و عملیات مربوط به بلاک‌چین حفظ شوند. گزارش شده که اتریوم از طریق قرارداد نظیر به نظیر Kademlia نیز در معرض حملات Eclipse قرارگرفته است [۱۴].

• آسیب‌پذیری قراردادهای هوشمند:

قراردادهای هوشمند به‌دلیل باز بودن و تغییرناپذیری بلاک‌چین حساس هستند. باگ‌ها و فریب‌ها برای عموم و نیز دشمنان مشخص هستند. همچنین به‌دلیل برگشت ناپذیری بلاک‌چین، ترکیب خطاها در قراردادهای هوشمند کار چالش برانگیزی است. یکی از نمونه‌های برجسته در این زمینه حمله به یک سازمان خود مختار غیرمتمرکز[1] در سال ۲۰۱۶ است که به حملهٔ DAO معروف است. این حمله باعث چند شاخه شدن بلاک‌چین اتریوم شد.

• فریب برنامه‌نویسی:

مهاجمان می‌توانند برای استخراج مشخصه‌های بلاک‌چین در برنامه‌نویسی از فریب استفاده کنند؛ مثل حملهٔ piracy که در سال ۲۰۱۸ گزارش شده است.

حملهٔ توزیع شدهٔ نقض سرویس[2]:

دشمنان منابع بلاک‌چین را با انجام یک حملهٔ مشترک از پای درمی‌آورند (به‌عنوان مثال، کل توانایی پردازش شبکه را به حداقل می‌رسانند). در سال ۲۰۱۶ دشمنان از دستورالعمل‌های کم ارزش EVM برای کم کردن سرعت پردازش بلوک‌ها استفاده کردند. تولید حساب‌های کاربری زیاد با توازن کم توسط دشمنان منجر به ایجاد یک حملهٔ DDoS می‌شود.

• انتشار کلید خصوصی:

مهاجمان می‌توانند کلید خصوصی یک حساب کاربری را برای گرفتن حساب به سرقت ببرند. این کار با حملات شبکه‌ای سنتی یا اسیر کردن گره‌های فیزیکی شدنی است.

۶- بلاک‌چین برای اینترنت اشیا: کاربردها

شبکه‌های اینترنت اشیا داده محور هستند و داده‌ها در آنها توسط دستگاه‌های نهایی زیادی آپلود می‌شود. این باعث می‌شود داده و دستگاه هر دو اهداف حملات در اینترنت اشیا باشند. داده‌های حس‌گرها در یک سامانه اینترنت اشیا می‌توانند شخصی یا حساس باشند؛ به‌عنوان مثال، اینترنت اشیا پزشکی یا مربوط به کاربردهای ملی باشند؛ به‌عنوان مثال، شبکهٔ هوشمند مبتنی بر اینترنت اشیا و کارخانهٔ هسته‌ای. تمامیت و حریم خصوصی داده‌ها امر مهمی است. یکپارچگی داده‌ها و تضمین آن در بلاک‌چین اهمیت زیادی را برای قابلیت‌های مختلف اینترنت اشیا دارد (به‌عنوان مثال، مدیریت زنجیره تأمین و شهرهای هوشمند). فناوری‌های بلاک‌چین با تهدیدهای امنیتی از جنبهٔ داده‌های حسگرها و دستگاه‌های نهایی مقابله می‌کنند. صحت داده‌های حسگرها، داده‌های موجود در شبکه‌های اینترنت اشیا مجهز به بلاک‌چین را می‌توان به داده‌های مربوط به بلاک‌چین (مثل حساب کاربری، توازن و هزینهٔ معامله) و داده‌های مربوط به اینترنت اشیا (مثل داده‌های حس‌گرها) تقسیم کرد. داده‌های مربوط به بلاک‌چین را می‌توان براساس معاملات قبلی تائید کرد؛ به‌عنوان مثال، هزینه باید کمتر از توازن یک حساب کاربری باشد (همان‌طور که در دیگر قابلیت‌های معمولی بلاک‌چین انجام شده است). داده‌های مربوط به اینترنت اشیا با استفاده از امضاء، محافظت می‌شوند. این کار تضمین می‌کند که فقط پیام‌های ارسال شده توسط دستگاه‌های اینترنت اشیا مجاز، ذخیره و مورد استفاده قرار گیرند. از سوی دیگر، صحت داده‌های مربوط به اینترنت اشیا می‌تواند توسط سرویس اوراکل که داده‌های معتبر را

[1] DecentralisedAutonomous Organisation(DAO)

[2] Distributed Denial of Service attack(DdoS)

ارائه می‌دهد، تضمین شود. ساختار هَش شدهٔ مرتبط با عناصر قبلی می‌تواند امنیت داده‌های حسی ثبت شده در دفترکل‌های بلاک‌چین اینترنت اشیا را تضمین کند.

رفتارهای مخرب دستگاه‌های اینترنت اشیا: رفتارهای مخرب دستگاه‌های نهایی در بلاک‌چین اینترنت اشیا را می‌توان به سه بخش خلاصه کرد:

(۱) ارسال معاملات با امضاهای جعلی که می‌تواند توسط سامانه بلاک‌چین کشف، مجازات و رد شود؛

(۲) ارسال معاملات با داده‌های جعلی اما امضاهای درست که می‌تواند توسط الگوریتم‌های تشخیص داده‌های جعلی حذف و گرهٔ منبع معامله مجازات شود؛

(۳) مصرف منابع؛ برای مثال DoS که می‌توان با استفاده از سازوکارهای هزینهٔ معاملات از این کار جلوگیری کرد.

۶-۱- برنامه‌های کاربردی و پروژه‌های اینترنت اشیا مبتنی بر بلاک‌چین

اکثر (اگر نه همه) فناوری‌های بلاک‌چین موجود بر روی لایهٔ کاربردی متمرکز هستند، جایی که شبکه‌ها به‌طور معمول به صورت نظیر به نظیر و به دور از محدودیت‌های فیزیکی شبکه، دستگاه‌ها و پهنای باند می‌باشند. برای مثال، Enigma یک شبکهٔ بلاک‌چین نظیر به نظیر است که به‌تازگی برای مدیریت داده‌های شخصیِ غیرمتمرکز توسعه یافته است. ارز دیجیتال آیوتا (IOTA)، ارز رمزنگاری شده‌ای است که هدفش ارائهٔ رویکردهای بلاک‌چین برای شبکه‌های اینترنت اشیا است. در سال ۲۰۱۵، پوپوف[1] سندی را ارائه داد که مشخصه فناوری موجود در Iota ارائه شده و اهداف آن را آشکار می‌کند [۳۶]. Tangle که از دفتر کل توزیع شدهٔ ضد دست‌کاری بلاک‌چین ارث می‌برد، به‌جای ساختارهای زنجیره‌ای (مانند بیت‌کوین) از یک ساختار گراف حلقوی جهت‌دار[2] استفاده می‌کند. معاملات تنها بخش‌های قابل ذخیره در IOTA هستند. هر معامله دو معاملهٔ منتشر شدهٔ قبلی را تائید می‌کند یک چنین ساختار انعطاف‌پذیری باعث ذخیره‌سازی انرژی شده و بر روی استخراج معاملات و انتقال آنها به بلوک‌ها کار می‌کند. معاملات به‌صورت موازی تائید شده و کم و بیش به‌صورت فوری توسط Tangle پذیرش می‌شوند، این کار باعث بالا رفتن ظرفیت IOTA از نظر نرخ معاملات می‌شود. IOTA هزینهٔ معاملات را کنار می‌گذارد، چون شرکت‌کنندگان اینترنت اشیا می‌توانند در مواردی که هزینهٔ معاملات مصرفی در مقایسه با مقدار ذخیره شده در معاملات بالاست دلسرد شوند.

[1] Popov
[2] Directed Acyclic Graph (DAG)

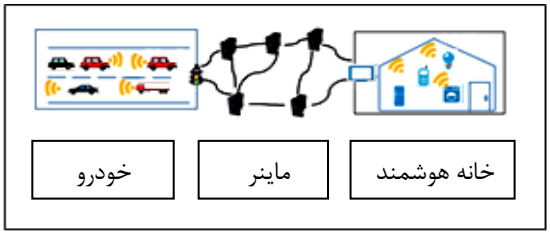
IOTA از چهار نوع گره پشتیبانی می‌کند؛ گرهٔ کامل، گرهٔ بدون سربرگ (به‌طور خاص گره‌های کاملی که در کنسول محلی کار می‌کنند)، کیف پول لایت[3] و کیف پول اندروید. IOTA در سال ۲۰۱۷ یک نسخهٔ بتا را برای پشتیبانی از کیف پول لایت منتشر کرد. کیف پول‌های لایت به سرورهایی وصل می‌شوند که برای دریافت وضعیت شبکه و انتشار معاملات، عملیات پیاده‌سازی مرجع IOTA (IRI) بر روی آنها اجرا می‌شود. با این حال حتی کیف پول‌های لایت هنوز هم باید محاسبات مورد نیاز برای تولید معاملات مجاز که ساختار DAG به آنها نیاز دارد را انجام دهند. دستگاه‌های اینترنت اشیا با توانایی محدود مثل گره‌های باتری دار مجبورند کیف پول‌های لایت را در IOTA اجرا کنند. بسترهای اینترنت اشیا مبتنی بر بلاک‌چین دیگری برای اهداف خاص وجود دارند. آی‌بی‌ام[4] با همکاری سامسونگ یک پروژهٔ مبتنی بر بلاک‌چین به نام سامانه دورسنجی نقطه به نقطه نامتمرکز مستقل[5] را معرفی‌کرده است [۵۲]. علاوه‌بر این، یک سرویس اشتراک دادهٔ مبتنی بر بلاک‌چین توسط IBM برای مشاغل و صنایع معرفی شده است. در این سرویس داده‌های اینترنت اشیا می‌توانند از طریق دفترکل‌های بلاک‌چین شخصی اشتراک‌گذاری شوند تا از ایجاد اختلاف بین شرکای تجاری جلوگیری شود.

۶-۲- ساختار برنامه‌های کاربردی اینترنت اشیا مبتنی بر بلاک‌چین

در برنامه‌های کاربردی بلاک‌چین اینترنت اشیا از دو ساختار مختلف بسته به قابلیت‌های متفاوت دستگاه‌های اینترنت اشیا می‌توان استفاده کرد.

۶-۲-۱- بلاک‌چین ادغام شده در اینترنت اشیا

دستگاه‌های اینترنت اشیا می‌توانند به شبکهٔ بلاک‌چین متصل شده و بخشی از قابلیت‌های اصلی بلاک‌چین (مثل تولید معاملات مربوط به داده‌های خام حسگرها، تائید معاملات و حتی استخراج بلوک‌ها) شوند.



شکل (۲): ساختار شبکهٔ اینترنت اشیا مبتنی بر بلاک‌چین [۴۷]

[3] Light Wallet
[4] InternationalBusinessMachines Corporation (IBM)
[5] AutonomousDecentralized Peer-to-Peer Telemetry (ADEPT)

در شبکه‌های بلاک‌چین اینترنت اشیا سه نقش مجازی نظیر گرهٔ سبک[۱]، گرهٔ کامل[۲] و ماینر باید پشتیبانی شوند.

شبکهٔ خودرویی اقتضایی که در سمت چپ شکل (۲) قرار دارد یک برنامه کاربردی بالقوه است که در این ساختار اجرا می‌شود. ماینرها معاملات را در بلوک‌ها استخراج و همهٔ بلوک‌ها را ذخیره می‌کنند. این بلوک‌ها بالاترین میزان درخواست ذخیره‌سازی و محاسبه را دارند. گره‌های کامل تمام بلوک‌ها را ذخیره می‌کنند که این بلوک‌ها حاوی سرآیند و بدنهٔ بلوک هستند، اما عملیات استخراج بلوک را انجام نمی‌دهند. گره‌های کامل نیاز به حجم ذخیره‌سازی بالا و سطح مشخصی از محاسبات دارند. دستگاه‌های نهایی اینترنت اشیا در شبکه‌های بلاک‌چین به‌صورت گره‌های سبک عمل می‌کنند. دستگاه‌های اینترنت اشیا می‌توانند کلیدهای خصوصی را به‌صورت مستقل تولید کنند یا برای کنترل دسترسی و حسابرسی احراز هویت شوند. گره‌های سبک سر بلوک‌ها را ذخیره و معاملات را تولید می‌کنند اما بلوک‌ها را استخراج نمی‌کنند، آنها می‌توانند توسط فناوری تائید پرداخت ساده[۳] پشتیبانی شوند که توضیح داده خواهد شد. گره‌های سبک می‌توانند در مقایسه با گره‌های کامل و ماینرها با فضای ذخیره‌سازی و توان کمتری کار کنند. کیف پول[۴] نوع خاصی از گره‌های سبک است و به کمترین میزان فضا و توان محاسباتی نیاز دارد. در کیف پول تنها عملیات اصلی را می‌توان روی معاملات انجام داد و برای بازیابی داده‌های استخراج شده در بلوک‌ها به کمک گره‌های کامل نیاز دارد. برای مثال، در هایپرلجرفابریک[۵] گره‌های جدید مثل دستگاه‌های اینترنت اشیا باید ابتدا در احراز هویت ثبت شده تا کلیدهای خصوصی آنها نگهداری شوند. در اینجا از کلیدهای خصوصی مربوط به مشتریان (گره‌های سبک) برای تولید امضاهای معاملات استفاده شده تا بدین وسیله بتوان صاحبان معاملات را تائید هویت کرد. مشتریان فقط معاملات را تولید و منتشر می‌کنند.

۶-۲-۲- بلاک‌چین سرویسی برای اینترنت اشیا

بلاک‌چین یک لایهٔ سرویس را به‌منظور ادغام با ساختار معمولیِ اینترنت اشیا مثل معماری چهار سطحی که در بخش (۳) ارائه شده، فراهم کرده است. به‌طور معمول این ساختار شامل سه وظیفهٔ اساسی است؛ حسگر، عامل و ماینر. خانهٔ هوشمندی که در سمت راست شکل (۲) قرار دارد یک افراز معمولی اینترنت اشیا است که بر روی این زیرساخت اجرا شده است. حسگرهای اینترنت اشیا داده‌ها را جمع‌آوری کرده و از طریق عاملان بلاک چین با سرویس‌های بلاک‌چین ارتباط برقرار می‌کنند. حس‌گرها در عملیات بلاک‌چین دخالت ندارند. عاملان می‌توانند داده‌های جمع‌آوری شدهٔ حسگرها را مانند معاملات تفسیر و معاملات در شبکهٔ بلاک‌چین منتشر کنند. عاملان نیز می‌توانند مسئولیت امنیت معاملات را با استفاده از کلیدهای خصوصی بپذیرند، این در حالی است که دستگاه‌های اینترنت اشیا کلید ندارند و در بلاک‌چین دخالتی ندارند. ماینرها که یک شبکهٔ نظیر به نظیر را تشکیل می‌دهند، عملیات هسته‌ای بلاک‌چین را انجام می‌دهند؛ عملیاتی مثل تائید معاملات و استخراج معاملات در بلوک‌ها.

۷- مقایسه نرم‌افزارهای کاربردی برای اینترنت اشیا

ساختار بلاک‌چینی که شامل اینترنت اشیا می‌شود، با استقرار مستقیم بلاک‌چین برروی دستگاه‌ها امنیت و قابلیت ادغام داده‌ها را خواهد داشت. دستگاه‌های اینترنت اشیا که گرهٔ لایت بر رویشان اجرا می‌شود، می‌توانند با کمک فناوری تائید پرداخت ساده پیام‌ها را به شکل معاملات تولید و تائید کنند. براساس این حقیقت که عاملان به‌عنوان نمایندگانی بین دستگاه‌های اینترنت اشیا و شبکهٔ بلاک‌چین عمل می‌کنند، عامل می‌تواند حملات مردمیانی[۶] مثل تزریق دست‌کاری و جعل را انجام دهد. در اینجا عاملان خطر شکست تک نقطه‌ای را افزایش می‌دهند. عملیات استقرار و پیاده‌سازی ساختار «بلاک‌چین به‌عنوان سرویس» آسان و قابل انعطاف است. ماژول اینترنت اشیا با کمک عاملان مشخصه‌های خودش را تا حدی حفظ می‌کند، بنابراین، در راستای همکاری با بلاک‌چین نیاز به تغییرات محدودی بر روی سامانه فعلی دارد. برای مثال مسئلهٔ افزونگی داده‌های حسی را می‌توان با استفاده از الگوریتم‌های تجمع حل کرد. نتایج جمع‌آوری شده می‌توانند حجم داده‌های حسی را کاهش داده و نیاز بالای برنامه‌های کاربردی اینترنت اشیا به ظرفیت معاملاتی را رفع کنند. در مقابل در یک بلاک‌چین حاویِ اینترنت اشیا، دستگاه‌های اینترنت اشیا باید برای اجرای برنامه‌های کاربردی بلاک‌چین برنامه‌ریزی شوند. عملیات بلاک‌چین می‌توانند مصرف‌کنندهٔ منابع باشند؛ همچنین می‌توانند محاسبه و اتصال را بر روی دستگاه‌های مشخصی انجام شوند.

۸- چالش‌های مربوط به استفاده از بلاک‌چین در عملیات اینترنت اشیا

بلاک‌چین‌های فعلی برای اجرا در شبکه‌های همگن نظیر به نظیر

[1] Light node
[2] Full node
[3] Simplified Payment Verification(SPV)
[3] Wallet.
[5] Fabric Hyperledger

[6] man-in-the-middle

طراحی‌شده‌اند. با این‌حال ویژگی‌های اینترنت اشیا (برای مثال، منابع محدود دستگاه‌های نهایی در مقایسه با سرورهای سطح بالا یا دستگاه‌های رایانه‌ی رومیزی) به‌صورت مستقیم از توسعهٔ بلاک‌چین برای اینترنت اشیا جلوگیری می‌کنند. به کارگیری بلاک‌چین در دستگاه‌های اینترنت اشیا چالش‌های زیر را به همراه دارد.

محاسبه: فعالیت بلاک‌چین برای دستگاه‌های خفیف اینترنت اشیا غیرقابل‌کنترل است. برخی از الگوریتم‌های رمزنگاری پیشرفته مثل دانش صفر[1] و الگوریتم رمزنگاری بر اساس ویژگی[2] که در بلاک‌چین‌های حفظ حریم خصوصی مورد استفاده قرارگرفته‌اند برای دستگاه‌های اینترنت اشیا بسیار سنگین هستند. یک گرهٔ کامل در بلاک‌چین باید تائید شود و به دنبال همهٔ بلوک‌ها و معاملات باشد. این‌گره نیز می‌تواند یکبار سنگین برای دستگاه‌های اینترنت اشیا با منابع محدود باشد. قراردادهای اجماع شبیه به PoW نمی‌توانند بر روی دستگاه‌های اینترنت اشیا اجرا شوند. در مورد بیت‌کوین، کل شبکه می‌تواند با قدرت در حدود 10^{1}H/s کار کند. پردازنده‌های گرافیکی مدرن می‌توانند به قدرت حدودی 10^{7}H/s برسند. با این‌حال حتی یک دستگاه اینترنت اشیا قوی مثل Raspberry pi ۳ می‌تواند تنها به 10^{4}H/s برسد. در نتیجه دستگاه‌های اینترنت اشیا نمی‌توانند به اندازه کافی در منابع محاسباتی مشارکت داشته باشند و از عهدهٔ وظایف PoW بر نمی‌آیند.

ذخیره‌سازی: محل‌های ذخیره‌سازی که بلاک‌چین به آنها نیاز دارد، می‌تواند برای دستگاه‌های اینترنت اشیا گران قیمت باشد. در حدود 5×10^{5} بلوک بیت‌کوین در سال ۹ ماین شده است. سایز کل بلاک‌چین بیت‌کوین در حدود ۱۵۰ GB است. این رقم برای اتریوم در حدود 5×10^{6} بلوک است. سایز کل بلاک‌چین اتریوم درحدود ۴۰۰GB است. باید تمام بلوک‌ها ذخیره شوند. بدون وجود این داده‌های حجیم، دستگاه‌های اینترنت اشیا نمی‌توانند معاملات تولید شده توسط بقیه را تائید کنند. همچنین ارسال‌کنندهٔ معامله به داده‌های قبلی نیاز دارد (تراز و شاخص معاملات) تا بتواند معاملات جدیدی را ایجاد کند. در نتیجه دستگاه‌های اینترنت اشیا باید به خودشان تکیه کنند و بار ذخیره‌سازی به‌دوش خودشان باشد اینکه متکی‌بر سرورهای راه دور باشند که این کار مستلزم تحمیل بار محاسباتی اضافی و ارتباط ایمن بین دستگاه‌های اینترنت اشیا و سرورهای مورد اعتماد است. همهٔ سرشاخه‌ها به ترتیب در بلاک‌چین بیت‌کوین و بلاک‌چین اتریوم در حدود ۳۸ gb و ۲ gb فضا اشغال می‌کنند.

حتی با فناوری پیشرفتهٔ بلاک‌چین (به‌عنوان مثال، فناوری تأیید پرداخت ساده[3]) اندازه سرتیتر می‌تواند به حدود ۸۰ b برای بلوک بیت‌کوین و ۵۰۰ b برای بلوک اتریوم برسد. علاوه‌بر این، ذخیرهٔ داده در بلاک‌چین هزینه‌بر است. برای مثال، هزینه به ازای ذخیرهٔ هر گیگابایت داده در اتریوم در حدود 2×10^{5} دلار آمریکا است. یک دادهٔ ۳۲ b غیر صفر ۲۰ kgwei/gas هزینه دارد و ۱ اتریوم در حدود ۱۲/۹۰ دلار است. هزینهٔ عملی شدن کار در برنامه‌های کاربردی اینترنت اشیا بسیار بالاست. اینترنت اشیا پشتیبانی از داده‌های حجم بالا را تضمین می‌کند. سایز کلیِ داده‌ها در اینترنت اشیا مجهز به بلاک‌چین می‌تواند بسیار زیاد شود، چون امکان دارد هر بلوک n بار در یک شبکهٔ بلاک‌چین n گره‌ای تکثیر شود.

ارتباط: گره‌های موجود در بلاک‌چین نیاز به انتقال و تبادل داده‌ها به‌صورت مکرر دارند. دلیلش این است که بلاک‌چین بر روی یک شبکهٔ نظیر به نظیر اجرا می‌شود و به‌منظور حفظ سوابق تبادل داده‌ها را ادامه می‌دهد؛ به‌عنوان مثال برای آخرین معاملات و بلوک‌ها. فناوری‌های ارتباط بی‌سیم که از آنها به‌طور گسترده برای اتصال دستگاه‌های اینترنت اشیا استفاده شده از عواملی مثل سایه، محوشدگی و دخالت رنج می‌برند و در پروژه‌های معمولیِ بلاک‌چین مثل بیت‌کوین بسیار قابل اطمینان‌تر از اتصالات سیم‌دار هستند. ظرفیت فناوری‌های بی‌سیم بسیار کمتر از آن چیزی است که بلاک‌چین انتظار دارد. برای مثال، بلوتوث (IEEE ۸۰۲.۱۵.۳) نرخ دادهٔ ۷۲۰ kbps؛ ZigBee(IEEE ۸۰۲.۱۵.۳) نرخ‌دادهٔ ۲۵۰Kbps؛ Ultra-wideband (UWB,IEEE ۸۰۲.۱۵.۳) نرخ دادهٔ Mbps ۱۱۰ و Wi-Fi (۸۰۲.۱۱ a/b/g) نرخ دادهٔ ۵۴Mbps را می‌توانند ارائه کنند. NB-IoT نرخ علامت تقریبی ۱۰۰kbps دارد.

انرژی: برخی از دستگاه‌های اینترنت اشیا برای کار در دراز مدت با استفاده از انرژی باتری طراحی شده‌اند. برای مثال یک دستگاه اینترنت اشیا برای مصرف روزانه ۰/۳ mWh طراحی شده و حداقل ۵ روز با استفاده از یک باتری CR2032 با ظرفیت ۶۰۰ mWh کار می‌کند. دستگاه‌های اینترنت اشیا از راهبردهای ذخیرهٔ انرژی (مثل حالت خواب) و فناوری‌های ارتباطیِ با بازدهی بالا (مثلNB-IoT) استفاده می‌کنند. با این‌حال محاسبات و ارتباطات مورد نیاز توسط عملیات بلاک‌چین معمولی گرسنهٔ انرژی هستند. برای مثال SHA-۲۵۶ در حدود به ۹۰ nJ/B انرژی نیاز دارد. مصرف انرژیِ نرمال بلوتوث در حدود ۱۴۰mJ/Mb؛ ZigBee در حدود ۳۰۰ mJ/Mb؛ UWB در حدود ۷ mJ/Mb و Wi-Fi در حدود ۱۳ mJ/Mb است. در نتیجه ذخیرهٔ انرژی

[1] zero-knowledgement
[2] Attribute-based encryption(ABE)
[3] Simplified Payment Verification(SPV)

۰/۳ mWh در یک روز، تنها می‌تواند پاسخگوی پردازش و انتقالِ در حدود ۰/۵MB داده (نیمی از یک بلوک بیت‌کوین) با استفاده از قرارداد ZigBee باشد.

پویایی و تقسیم‌بندی اینترنت اشیا: شبکهٔ بی‌سیم را می‌توان به یک حالت زیرساختی که در آن همهٔ بسته‌ها توسط زیرساخت‌های شبکه (ایستگاه‌های پایه) منتقل می‌شوند و یک حالت شبکه اقتضایی که در آن شبکه متکی‌بر زیرساخت‌های قبلی نبوده و هر گره داده‌ها را برای دیگر گره‌ها انتقال می‌دهد، تقسیم‌بندی کرد. پویایی‌دستگاه‌های اینترنت اشیا می‌تواند موجب تضعیف بهره‌وری بلاک‌چین شود. در شبکهٔ بی‌سیم مبتنی بر زیرساخت، پویایی‌دستگاه‌ها می‌تواند منجر به تقویت علامت‌دهی و کنترل پیام‌ها شود. در مقابل در شبکه‌های بی‌سیم اقتضایی، عملیات بخش‌بندی شبکه باعث می‌شود شبکه به بخش‌های غیر مرتبط تقسیم شود (این مربوط به زمانی است که گره‌های سیار با الگوهای متنوع جابه‌جا می‌شوند).

تأخیر و ظرفیت: از تأخیر بالای بلاک‌چین برای حصول اطمینان از ثبات در شبکه‌های غیرمتمرکز بلاک‌چین استفاده شده است. تأخیری که به‌طور معمول به بلاک‌چین تحمیل می‌شود برای بسیاری از برنامه‌های کاربردی اینترنت اشیا غیرقابل پذیرش است. برای مثال، زمان تائید بلوک ۱۰ دقیقه‌ای در بیت کوین برای برنامه‌های‌کاربردی اینترنت اشیا مثل شبکه‌های خودرویی بسیار زیاد است. در واقع تأخیر بالای بلاک‌چین منجر به محدود شدن ظرفیت بلاک‌چین می‌شود. ظرفیت بلاک‌چین‌ها (به‌عنوان مثال، 1Mb در ۱۰ دقیقه برای بیت‌کوین) بسیار پایین‌تر از چیزی است که برنامه‌های کاربردی اینترنت اشیا به آن نیاز دارند. ظرفیت مورد نیاز اینترنت اشیا با توجه به افرازهای مختلف متفاوت است. برای مثال، در افراز شهر هوشمند مبتنی‌بر اینترنت اشیا، ردیابی ۷۰۰ خودرو در ۲۴ ساعت برابر با ۴/۰۳ Gb (در حدود ۰/۲۴ mb/h به ازای هر ماشین) است. در ضمن داده‌های اینترنت اشیا مربوط به پارک متعلق به ۵۵ نقطه برابر با ۲۴۹ kb درحدود ۵ ماه است (۳۶ b به ازای هر نقطه در هر روز). فضای مورد نیاز برنامه‌های‌کاربردی اینترنت اشیا با زیاد شدن تعداد دستگاه‌های اینترنت اشیا پیوسته در حال افزایش است.

۹- طرح‌های بالقوه‌ی بلاک‌چین در برنامه‌های‌کاربردی اینترنت اشیا

۹-۱- قالب معاملات

جدا از معاملات بیت‌کوین، معاملات مربوط به برنامه‌های‌کاربردی اینترنت اشیا باید از ساختارهای دادهٔ تعریف شده به‌وسیلهٔ کاربر پشتیبانی‌کنند. یکی از نمونه‌های عملی عبارت است از معاملات مربوط به برنامه‌های کاربردی اینترنت اشیا که برای اتریوم ایجاد شده‌اند. فارغ از معاملات بیت‌کوین، یک معاملهٔ اتریوم حاوی یک رشته داده است که این رشته نشان‌دهندهٔ داده‌هایی است که باید منتقل شوند. رشته داده طول متغیری دارد و ارسال‌کننده می‌تواند هزینهٔ بالاتری را برای رشته‌های دادهٔ بزرگ‌تر پرداخت کند. باید توجه داشت که در اتریوم هزینهٔ معامله باید کمتر از محدودهٔ gas در بلوک باشد؛ به‌عبارت دیگر رشته داده نمی‌تواند به‌صورت نامحدود افزایش یابد. تأخیر تائید معاملات می‌تواند تحت تأثیر سایز معاملات باشد، به‌خصوص در شبکه‌های اینترنت اشیا با کانال‌های بی‌سیم غیرقابل اعتماد. معاملات کوچک می‌توانند به نرخ موفقیت بالا در انتقال و تأخیر انتقال‌کم دست یابند. قرارداد بسته داده کاربر[1] کاربرد بالایی را در اینترنت اشیا به عنوان یک قرارداد کم‌حجم دارد. براساس این حقیقت که UDP قابلیت تصحیح خطا را ندارد، بهتر است که سایز معامله کمتر از بارهای خطای قراردادهای شبکه (به‌عنوان مثال، UDP و IP) باشد تا بدین وسیله از تکه شدن جلوگیری شده و نرخ انتقال موفقیت‌آمیز افزایش یابد. در نتیجه انتظار می‌رود معاملات کوچک‌تر توسط تعداد زیادی از ماینرها قابل مشاهده باشند و همچنین احتمال اینکه این معاملات در بلوک‌های استخراج شوند از معاملات بزرگ بیشتر است. تأخیر می‌تواند با عاملانی که به صورت بی‌سیم دستگاه‌های اینترنت اشیا و به‌صورت سیم‌دار ماینرها را به‌هم متصل کرده‌اند، کاهش یابد. عاملان به‌صورت برابر معاملات با سایزهای مختلف را برای ماینرها منتشر می‌کنند.

۹-۱-۱- تشویق و توکن

دستمزد معامله برای توازن هزینهٔ معامله و تعدیل مصرف منابع در بلاک‌چین امر مهمی است. برای مثال، از دستمزد معامله برای سنجش پیچیدگی معاملات در اتریوم استفاده شده است. معاملاتی که منابع بیشتری مصرف می‌کنند، دستمزد بیشتری را برای معامله متحمل می‌شوند. از سوی دیگر دستمزد معامله نیز راهی را برای اختصاص مجدد معاملات ارائه می‌دهد، به‌خصوص در بلاک‌چین‌های عمومی با ظرفیت محدود. درصورتی که تعداد معاملات در یک لحظه زیاد شود، زمان تائید نیز طولانی می‌شود و ارسال‌کنندگان معاملات می‌توانند دستمزد بیشتری را به ماینرهای اولویت‌دار پرداخت کنند (به‌عنوان مثال، آنهایی که زمان تأییدشان کوتاه‌تر است). از یک سامانه توکن در بلاک‌چین می‌توان به‌عنوان یک سامانه معتبر و قابل اعتماد استفاده کرد. دستمزد معامله می‌تواند هزینهٔ حملات را در مقایسه با حملات سنتی اینترنت اشیا (برای مثال، حملات پیام جعلی و DoS) افزایش داده و از این‌رو، عاملان رفتارهای مخرب را از انجام

[1] User Datagram Protocol (UDP)

این‌گونه رفتارها دلسرد کند. دستگاه‌های اینترنت اشیا ممکن است به‌دلیل منابع محدود و پیوندهای اساسی ضعیف (بی‌سیم) نتوانند بلوک‌ها را در راستای به‌دست آوردن توکن‌ها برای دستمزد معاملات استخراج کنند. دستگاه‌های اینترنت اشیا می‌توانند سرویس‌هایشان را «بفروشند»؛ به‌عنوان مثال، سرویس انرژی تجدیدپذیر برای توکن‌ها. درنتیجه کاربران سرویس (به عنوان مثال، مدیر اینترنت اشیا یا سرشاخه) دستگاه‌های اینترنت اشیا را دوباره شارژ می‌کنند. انتظار می‌رود دستگاه‌های اینترنت اشیا، حضور فعالی در بلاک‌چین داشته باشند و از الگوهای رفتاریِ مناسب پیروی کنند، با اینکه مستعد انجام حملات خودخواهانه با استفاده از پهنای باند و انرژی و منابع محاسباتی محدود هستند. دستگاه‌های اینترنت اشیا با استفاده از فناوری قرارداد هوشمند می‌توانند منابع (به‌عنوان مثال، انرژی یا بسته‌های داده) را خریداری کنند. این می‌تواند انگیزه‌ای برای دستگاه‌های اینترنت اشیا مبنی بر دریافت توکن‌ها باشد.

۹-۱-۲- قرارداد هوشمند

یک قرارداد هوشمند[1] بخشی از «کد اجرا شده با روش رمزنگاری اقتصادی امن» است که در پایهٔ بلاک‌چین اجرا می‌شود. وقتی شرط تعریف شده برقرار می‌شود، قرارداد هوشمند خودش و بدون کمک هیچ بخشی بند مربوطه را اجرا می‌کند. علاوه‌بر این، عملیات حسابرسی بلادرنگ را انجام می‌دهد؛ چون تمام عملیات به‌صورت معامله در یک دفترکل غیرمتمرکز بلاک‌چین ثبت و تائید شده‌اند. این معاملات قابل ردیابی و غیرقابل انکار هستند، از این‌رو، امنیت اجرایی دستگاه را بالا می‌برند. قرارداد هوشمند عوامل مختلف مثل دستگاه‌های اینترنت اشیا و دارایی‌های دیجیتال را به نهادهای مجازی در بلاک‌چین تبدیل می‌کند و آنها را قادر می‌سازد با دیگر عوامل تعامل داشته باشند. کد مربوط به قرارداد هوشمند در بلاک‌چین ذخیره شده و با استفاده از یک آدرس یکتا قابل شناسایی است. یک قرارداد هوشمند را می‌توان به دو صورت فراخوانی کرد: روش اول با استفاده از معاملات معتبر و واردکردن آدرس قرارداد هوشمند در محدوده دریافت کننده؛ روش دوم اجرای داخلی کد؛ بنابراین تمام سوابق‌اجرایی را می‌توان با استفاده از دفترکل بلاک‌چین ردیابی‌کرد. قرارداد هوشمند به‌طور مستقل و خودکار بر روی تمامی گره‌های موجود در شبکهٔ بلاک‌چین اجرا می‌شود. چند پروژهٔ بلاک‌چین شامل اتریوم و بیت‌کوین قرارداد هوشمند را پیاده‌سازی کرده‌اند. با توجه به اینکه اینترنت اشیا از حس‌گرهای موجود در نواحی بدون سرنشین انتظار دارد به‌صورت خودکار و با استفاده از قوانین تعریف‌شده و نامتمرکز اجرا شوند، قرارداد هوشمند توانایی بهبود بهره‌وری و امنیت برنامه‌های کاربردی اینترنت اشیا را دارد. دستگاه‌های اینترنت اشیا می‌توانند معاملات خود مختار را از طریق قراردادهای هوشمند انجام دهند. از بلاک‌چین برای جایگزینی ساختار حمل و نقل هوشمند[2] و به روزرسانی قابل اعتماد دستگاه‌های اینترنت اشیا استفاده شده است.

۹-۱-۳- ذخیره‌سازی غیر زنجیره‌ای

ذخیره‌سازی غیر زنجیره‌ای یک راه حل مؤثر برای کاهش هزینه‌های ذخیره‌سازی است. داده‌ها می‌توانند به‌صورت جداگانه در مکانی دیگر ذخیره و از یک اشاره‌گر برای ارجاع به بلاک‌چین استفاده کنند. در مرجع [۳]، دو نوع جدید از معاملات (معامله برای مدیریت کنترل دسترسی و معامله برای ذخیره و بازیابی داده‌ها) در راستای انجام عملیات ذخیره‌سازی غیر زنجیره‌ای ارائه شده است. ذخیره‌سازی غیر زنجیره‌ای مقدار کلید نمونه‌ای از Kademilia (یک جدول هش توزیع شده[3]) است. DHT در شبکه‌ای از گره‌ها است که این گره‌ها مستقل از بلاک‌چین هستند. برای اطمینان از قابلیت دسترسی، داده‌ها درگره‌ها به صورت تصادفی ثبت و تکرار می‌شوند.

۹-۲- مباحث امنیتی بر روی برنامه‌های‌کاربردی اینترنت اشیا مبتنی بر بلاک‌چین

اگرچه فناوری بلاک‌چین به بردباری در مقابل خطای بیزانس معروف است، اما این فناوری هنوز نتوانسته مسائل امنیتی که مربوط به ادامهٔ حیات شبکه‌های اینترنت اشیا مبتنی بر بلاک‌چین است را حل کند.

۹-۲-۱- حریم خصوصی

براساس این حقیقت که معاملات به گونه‌ای طراحی شده‌اند که به‌صورت عمومی در دسترس باشند و توسط تمام گره‌ها تائید شوند، بلاک‌چین می‌تواند از مسائل مربوط به حریم خصوصی آسیب ببیند که شامل حریم خصوصی کاربران و محرمانه بودن داده‌ها می‌شود.

• حریم خصوصی کاربران:

با اینکه کاربر می‌تواند چند هویت مجازی را به‌طور مستقل در بلاک‌چین ایجاد کند، نقشه‌برداری یک به چند بین یک کاربر فیزیکی و نهادهای مجازی را می‌توان براساس یک گراف معاملاتی ایجاد کرد و وضعیت شناسایی یک کاربر فیزیکی را می‌توان حدس زد. یک پول الکترونیک به‌طور کامل ناشناس باید غیرقابل کشف (به‌عبارت دیگر برای هر معاملهٔ ورودی، تمامی

[1] Smart Contract

[2] Intelligent Transportation Systems(ITS)

[3] distributed hash table(DHT)

ارسال‌کنندگان هم احتمال باشند) و غیرقابل پیوند شدن باشد (به‌عبارت دیگر در مورد هر دو معاملهٔ خروجی، نتوان ثابت کرد که این دو برای یک نفر ارسال شده‌اند). بیت‌کوین ناشناس نیست اما شبه ناشناس است. این کار به سه روش انجام می‌شود: ثبت یک کاربر فیزیکی در غالب یک نهاد مجازی تنها توسط کاربر انجام می‌شود؛ نهادهای مجازی مجاز هستند به تعداد مورد نیاز و به‌طور مستقل تولید شوند؛ سرویس ادغام برای ترکیب منابع تعدادی از نهادهای مجازی در راستای سردرگم کردن و جلوگیری از بازگشت به منابع اصلی ارائه شده است. در بلاک‌چین‌های اخیر حریم خصوصی کاربر توسط فناوری‌های رمزنگاری پیشرفته محافظت شده است [۴۷]. در راستای حل مسئلهٔ حریم خصوصی قراردادهای هوشمند در بلاک‌چین عمومی تلاش‌هایی را انجام داده که در آن یک قرارداد رمزنگاری مؤثر به نام اثبات دانش صفر با استفاده از اصول اولیهٔ رمزنگاری به‌صورت خودکار تولید می‌شود. اثبات دانش صفر شرایطی را ایجاد می‌کند که در آن امکان اثبات یک حالت بدون وجود هیچ اطلاعاتی به جز حالت خودش فراهم می‌شود. از روش اثبات دانش صفر نیز در Zerocoin، Zerocash، Provisions و غیره استفاده شده است تا به جای امضاهای مبتنی برکلید عمومی، مدیریت به‌صورت ناشناس اثبات شود. ارزهای رمزنگاری‌شدهٔ با قابلیت حفظ حریم خصوصی و دانش صفر نیاز به منابع بیشتری دارند که همین امر باعث محدودسازی قابلیت‌های آنها شده است. برای مثال، یک معاملهٔ Zerocoin بزرگ‌تراز ۴۵ kb بوده و برای تائید به ۴۵۰ ms زمان نیاز دارد. عملیات تولید یک معاملهٔ Zerocash درحدود ۳/۲ gb افظه و ۵۰s زمان می‌برد. یکی دیگر از فناوری‌های کلیدیِ حفظ حریم خصوصی کاربران امضاء حلقوی است که با استفاده از کلید خصوصی‌اش و کلیدهای عمومیِ دیگر، توسط تمامی اعضای گروه انجام می‌شود. در امضاء حلقوی یک بیانیه توسط اعضاء موجود در یک گروه خاص از افراد مورد تائید قرار می‌گیرد. برای مثال، مونرو[1] یک بلاک‌چین غیرقابل ردیابی براساس امضاء حلقوی است که پیوند موجود در بین ارسال‌کننده و معامله را قطع می‌کند. امضاء حلقوی عدم پیوندگذاری معامله و دریافت‌کننده را تضمین نمی‌کند، چون معاملات نیازی به این ندارند که آدرس دریافت‌کننده تحویل داده شود. فناوری کریپتونوت[2] با اجرای عملیات تبادل دیفی هلمن[3] می‌توانند به شرایط قابلیت عدم پیوندگذاری با یک آدرس یکتا در راستای ایجاد یک رمز مشترک بین ارسال‌کننده و دریافت‌کننده فعالیت کند. سپس کلید مقصد یک‌بار مصرف توسط ارسال‌کننده تولید شده و از آن به‌عنوان آدرس موقت دریافت‌کنندهٔ معامله استفاده می‌شود. وقتی معامله با بررسی معاملات در حال عبور شناسایی شد، دریافت‌کنندهٔ واقعی می‌تواند کلید یکبار مصرف مربوطه را بازیابی و سرمایهٔ مربوطه را خرج کند. باید توجه داشت که یک رابطهٔ پایاپای بین حریم خصوصی و ظرفیت وجود دارد، چون سایز معامله می‌تواند با افزایش سایز گروه بیشتر شود.

• حریم خصوصی داده‌ها:

قابلیت عدم‌کشف و عدم‌پیوند گذاری با محرمانه بودن داده‌ها تعاملی ندارد. بلاک‌چین اینترنت اشیا نیز باید داده‌ها را به‌صورت محرمانه نگهداری کند. محرمانه بودن بلاک‌چین را می‌توان با فناوری‌های معاملهٔ محرمانه حفظ کرد. برای مثال، Elementsproject و مونرو محتوای معاملات‌را نگه می‌دارند؛ به‌عنوان مثال، مبلغ قابل انتقال تنها برای شرکت‌کنندگان مشخصی قابل‌رؤیت است. درضمن محتوا باید تائید شود، به‌صورتی که هیچ کوینی از کوین‌های قابل‌دسترس را نمی‌توان به‌صورت رمزنگاری‌شده خرج کرد. در معاملات محرمانه از چند فناوری رمزنگاری استفاده می‌شود؛ به‌عنوان مثال، امضاهای حلقوی Borromean و طرح‌های تعهدی Pedersen.

یکی دیگر از رویکردهای امکان‌پذیر برای حفظ حریم خصوصی رمزنگاری مبتنی بر ویژگی (ABE) است که در آن کلیدهای رمزی براساس ویژگی‌های همتاها تولید می‌شوند. در صورت استفاده از ABE، داده‌های حسگرها می‌توانند (که مربوط به مسئولین مربوطه است) در معاملات رمزنگاری و با استفاده از اعتبارنامه‌های رمز گشایی توسط کاربران و ماینرها رمز گشایی شوند، اگر و تنها اگر ویژگی‌های ماینرها یا کاربران مورد پذیرش ساختار دسترسی باشد. رمزنگاری به‌طور کامل همگن[4] که با استفاده از آن می‌توان محاسبات را بر روی داده‌های رمزی انجام داد، روش دیگری را پیشنهاد می‌دهد.

۹-۲-۲- هویت و مدیریت دستگاه

درکاربردهای اینترنت اشیا، صاحبان باید از ویژگی‌های دستگاهشان باخبر باشند و بالعکس. با این‌حال در بلاک‌چین‌های عمومیِ فعلی (به‌عنوان مثال، بیت‌کوین و اتریوم)، همتاها با آدرس‌های عمومی‌شان تعریف شده‌اند که این آدرس را می‌توان به‌صورت مستقل و بدون اطلاع قبلی به دیگران ایجاد کرد. یک سرویس نام‌گذاری مبتنی بر مدل پرس‌وجو در مرجع معرفی شده، جایی که هویت مجازی دستگاه‌های اینترنت اشیا براساس آخرین فعالیت‌هایشان تائید می‌شود. براساس مرجع [۱۸]، در بلاک‌چین یک گرهٔ فیزیکی را می‌توان به‌صورت چندین گرهٔ مجازی در نظر گرفت. در بلاک‌چین‌های خصوصی، همتاها باید

[1] Monero
[2] CryptoNote
[3] Diffie-Hellman exchanges
[4] Completely homogeneous cryptography

برای ورود به شبکهٔ بلاک‌چین تائید هویت شوند. در نتیجه مدیریت هویت یکی از الزامات اساسی بلاک‌چین‌های خصوصی هستند. برای مثال، در هایپرلجرفابریک می‌توان عملیات مدیریت هویت را برای تائید نام‌نویسی و معاملات انجام داد.

۹-۲-۳- کنترل دسترسی

بلاک‌چین به‌عنوان یک سامانه توزیع شده این امکان را به دستگاه‌های اینترنت اشیا می‌دهد تا سیاست‌های کنترل دسترسی‌شان را تنظیم کرده و کنترل کاملی بر روی داده‌هایشان داشته باشند و دستیابی به دستگاه عادلانه باشد. یکی از فناوری‌های مربوط به کنترل دسترسی قراردادهای هوشمند قابل برنامه‌ریزی است. قراردادهای هوشمندی که سیاست‌های کنترل دسترسی را پیاده‌سازی می‌کنند می‌توانند منوط به شناسایی کنترل‌کنندهٔ داده‌ها یا داده‌های مشخص براساس داده‌ها پیاده‌سازی شوند؛ یا اینکه براساس کنترل‌کنندهٔ داده برای چند موضوع داده پیاده‌سازی شوند. روش دیگر برای کنترل دسترسی استفاده از بلاک‌چین به‌عنوان یک پایگاه داده به‌منظور ذخیرهٔ تمام سیاست‌های کنترل دسترسی برای منابع داده و درخواست‌کننده‌ها به شکل معاملات است. اگر یک درخواست دسترسی پذیرفته شود، معاملهٔ اعطای دسترسی می‌تواند در بلاک‌چین ثبت و به شبکهٔ بلاک‌چین منتشر شود. در غیر این صورت معاملهٔ درخواست دسترسی رد شده و به اطلاع ارسال‌کنندهٔ آن خواهد رسید.

۱۰- بلاک‌چین برای اینترنت اشیا: فناوری‌ها

در این بخش ما در مورد فناوری‌های بلاک‌چین که می‌توانند در برنامه‌های کاربردی اینترنت اشیا مورد استفاده قرار گیرند بحث می‌کنیم. ما ابتدا سه بخش از شبکه‌های بلاک‌چین فعلی را توضیح داده و سپس برنامه‌های‌کاربردی اینترنت اشیا را در دسته‌های مناسب قرار می‌دهیم. سپس بخش اصلی بلاک‌چین (قرارداد اجماع) از دو دیدگاه کلیدی مورد بررسی قرار می‌گیرد. براساس کنترل‌های دسترسیِ شبکه‌های بلاک‌چین، بهترین بلاک‌چین‌ها را می‌توان به بلاک‌چین عمومی، بلاک‌چین خصوصی و بلاک‌چین ترکیبی (که ترکیبی از دو مورد قبلی است) دسته‌بندی کرد.

۱) **بلاک‌چین عمومی:** نوع برجستهٔ بلاک‌چین، بلاک‌چین عمومی است که در آن بدون وجود کنترل دسترسی تمام گره‌های غیرقابل اعتماد و غیرقابل اطمینان می‌توانند معاملات را خوانده و ذخیره کنند و در استخراج بلوک‌ها و عملیات بلاک‌چین شرکت کنند. بلاک‌چین‌های عمومی برای شبکه‌های توزیع شدهٔ عمومی با دسترسی باز طراحی شده‌اند و مقیاس‌پذیری بالایی دارند. با این‌حال حفظ سوابق مداومِ بلاک‌چین عمومی سخت‌تر می‌شود، چون مقیاس شبکه بالا می‌رود و در نتیجه نرخ تولید بلوک در بلاک‌چین عمومی بالا می‌رود. دلیل آن این است که شبکه‌های عمومی بدون وجود کنترل دسترسی، سیاست کنترل استواری برای شناسایی و احراز هویت شرکت‌کنندگان ندارند و بنابراین قراردادهای اجماعِ اجرا شده باید از نرخ تولید به سختی انتقاد کنند. به طور نرمال از PoW و PoX به‌عنوان قراردادهای اجماع در بلاک‌چین‌های عمومی استفاده شده است و در مقایسه با الگوریتم PBTF که در بلاک‌چین خصوصی از آن استفاده شده به نرخ تولید بلوک کمتری می‌رسد. در بخش‌های بعدی در مورد الگوریتم PBTF به‌طور مفصل بحث خواهیم کرد. پروژه‌های بلاک‌چین عمومی فعلی که شامل بیت‌کوین و اتریشم می‌شوند نیز باز هستند و ظرفیت محدودی دارند. بلاک‌چین عمومی برای برنامه‌های‌کاربردی اینترنت اشیا مناسب است که قابلیت دسترسی باز داشته یا در صورت بالا بودن مقیاس همتاهای انعطاف‌پذیری دارند؛ مثل ونت و زنجیرهٔ تأمین.

۲) **بلاک‌چین خصوصی:** یک‌دستهٔ محبوب دیگر از بلاک‌چین‌ها، بلاک‌چین خصوصی است که در شبکه‌های خصوصی بسته با کنترل دسترسی سخت‌گیرانه و با مجوز خواندن/ نوشتن و نیز شناسایی و تائید هویت شرکت‌کنندگان مستقر است. بلاک‌چین‌های خصوصی می‌توانند نیازهای مربوط به حریم خصوصی را رفع کنند. همچنین توجه مؤسسات مالی را به طرز قابل توجهی جلب کرده‌اند. شبکه‌های اختصاصی که بلاک‌چین خصوصی در آنها کار می‌کند، می‌توانند برای بالا بردن سرعت و تأخیر پایین بهینه‌سازی شوند. بلاک‌چین خصوصی از قراردادهای BFT استفاده می‌کند. قابلیت کنترل دسترسی که توسط بلاک‌چین ارائه شده، برنامه‌های کاربردی اینترنت اشیا را در مقابل مخالفان خارجی محافظت می‌کند. به‌طور کلی بلک‌چین خصوصی برای برنامه‌کاربردی اینترنت اشیا با تعداد ماینرهای کم مناسب است، چون پیچیدگی ارتباطی و سرریز قراردادهای BFT در آنها بالا است. وقتی سایز شبکه فراتر از بیست می‌رود، ظرفیت بلاک‌چین خصوصی به‌طور چشمگیری کم می‌شود. بلاک‌چین خصوصی جدا از قراردادهای اجماع BFT مختلف، می‌تواند از دیگر قراردادهای اجماع مثل Paxos و Raft در پاسخ به انواع خاص خطاها استفاده کند.

۳) **بلاک‌چین ترکیبی:** دسته‌ای دیگر از بلاک‌چین‌ها، بلاک‌چین ترکیبی است که برای استفاده از مزایای بلاک‌چین‌های عمومی و خصوصی، یا به طور خاص‌تر، برای

استفاده از نرخ تولید بلوک بلاک‌چین خصوصی و مقیاس‌پذیری بلاک‌چین عمومی ارائه شده است. برای مثال، لیو و همکارانش یک قرارداد اجماعی بیزانتین که از نظر محاسباتی مقیاس‌پذیر است را برای بلاک‌چین‌ها معرفی کرده‌اند، جایی که ظرفیت بلاک‌چین می‌تواند از نظر خطی $o\left(\frac{n}{logn}\right) or(\frac{n}{lognlogn})$ با قابلیت محاسبه برابری کند. در اینجا یک شبکهٔ توزیع شدهٔ با کمترین مجوز به‌صورت یکنواخت به بخش‌های کوچک‌تر تقسیم شده است. در ابتدا جفت‌های موجود در شبکه باید پازل PoW را برای اثبات هویتشان و اجتناب از حملات سایبیل حل کنند. سپس جفت‌ها براساس قدرت محاسباتی‌شان که مربوط به زمان مورد نیاز برای حل پازل PoW است، به‌صورت یک شکل به بخش‌های کوچک‌تری تقسیم می‌شوند. هر بخش مجموعه‌ای گسسته از معاملات را پردازش می‌کند. با استفاده از قراردادهای اجماع بیزانس مثل تحمل خطای بیزانس عملی[1] بین بخش‌ها اجماع به‌وجود می‌آید. اجماع نهایی در بین بخش‌ها توسط قرارداد اجماع بیزانتین حاصل و در تمام شبکه منتشر می‌شود. این طرح ترکیبی قابلیت مقیاس‌پذیری بالا در حد شبکه‌های بزرگ (به عنوان مثال، در حد ۱۶۰۰ گره) دارد. یکی دیگر از مثال‌های اخیر در مورد بلاک‌چین ترکیبی بیزانس است که به شکل پویا گروه‌های هش اجماعی متناسب با قدرت را در راستای جمع‌آوری ماینرهای پایانی موفق ایجاد می‌کند. برای بهینه‌سازی تعهدات مربوط به معاملات و تائید تحت عملکرد عادی می‌توان از درخت‌های ارتباطی استفاده کرد. مثال‌های دیگر از بلاک‌چین ترکیبی شامل یک الگوریتم انعطاف‌پذیر و بهینهٔ اجماع بیزانس می‌شود که [۴۸]، برای بلاک‌چین کنسرسیوم معرفی کرده‌اند. این الگوریتم متکی‌بر رهبر یا امضاء یا عملیات تصادفی نیست. قرارداد اجماع معرفی شده، مستلزم حذف اجماع بیزانس چند متغیره است تا بدین‌وسیله اجماع بیزانس باینری بتواند ویژگی اعتبار را به ارمغان بیاورد. این ویژگی به این صورت است که اگر تمام فرایندهای غیر معیوب یک مقدار را برگردانند، هیچ مقدار دیگری را نمی‌توان در نظر گرفت. بلاک‌چین ترکیبی به‌دلیل پیچیده و ناهمگن بودن شبکه‌های اینترنت اشیا برای برنامه‌های کاربردی اینترنت اشیا جذاب است. یک ساختار بلاک‌چین سلسله مراتبی برای کاربردهای خانگی معرفی‌شده، جایی که یک بلاک‌چین خصوصی در اختیار «ماینرهای» منبع‌دار است. سه نوع بلاک‌چینی که نام برده شد برای کاربردهای مختلفی مناسب هستند. قرارداد اجماع برای اطمینان از کارکرد بلاک‌چین می‌باشد. در شبکهٔ بلاک‌چین، گره‌ها معاملات را در کل شبکه منتشر کرده و با دنبال کردن قرارداد اجماع در مورد معاملات پذیرفته شده به توافق می‌رسند. قرارداد اجماع با دو مشکل عمده رو به‌رو است: اصل اعتبارسنجی داده‌های واحد چیست؟ و ساختار داده‌های واحد در دفترکل بلاک‌چین به چه صورت است؟

۱۰-۱- اصل اعتبارسنجی داده‌های واحد

۱۰-۱-۱- اثبات کار (PoW)

الگوریتم اثبات کار یک ابزار عملی برای رسیدن به اجماع در زنجیرهٔ بلوک‌های تولید شدهٔ توزیعی ارائه می‌دهد، این در حالی است که می‌تواند دست‌کاری یا خراب کردن زنجیره‌ها توسط شرکت‌کنندگان غیرقابل اعتماد جلوگیری کند. PoW چالش‌هایی را ایجاد می‌کند که انجامشان سخت اما تأییدشان آسان است؛ به عنوان مثال، استفاده از توابع هش که توابعی یک‌طرفه بوده و محاسبه‌شان با یک ورودی داده شده آسان است، اما به‌دست آوردن ورودی از روی خروجی کار سختی است. برای مثال، بلاک‌چین بیت‌کوین را در نظر می‌گیریم. هر بلوک در بیت‌کوین درحدود ۱۰ دقیقه زمان می‌برد تا از کل شبکه استخراج شود.

$$0x181bc330 \rightarrow \quad 0x1bc330 * 256 \wedge (0x18 -$$
$$Bi \qquad B_i^l \qquad 2^8 \qquad B_i^u$$

Target: 0x1bc330000000000000000000000000000000000000000000

شکل(۳): تبدیل قسمت " nBits "به یک هدف

از سوی دیگر پاسخ مربوط به PoW به راحتی می‌تواند با یک عملیات هَش سنجیده شود. در همین راستا بیت‌کوین می‌تواند با استفاده از یک راهبرد پردازندهٔ تک رای[2] برای جلوگیری از حملهٔ سایبری جلوگیری کند، جایی که یک موجودی واحد می‌تواند وانمود کند هویتی چندگانه در یک فرایند اجماع دارد. همان‌طور که در شکل (۳) نشان داده شده، PoW بیت‌کوین بر روی یک هدف سراسری در i مین دوره تنظیم شده که با Ti نشان داده شده و یک عدد صحیح ۲۵۶ Bit بدون علامت است. با تنظیم رشته ۳۲Bit «nonce»، هش مربوط به یک سرتیتر معتبر در بلوک، تمامی رشته‌های موجود در سرآیند که شامل نسخه، هش سر پیام بلوک قبلی، هش ریشهٔ مرکل، زمان و تعداد بیت‌ها می‌شود را با هم ترکیب می‌کند. هرچه T_i کوچک‌تر باشد هدف دقیق‌تر است و پیدا کردن یک خروجی هش برابر یا کمتر از یک Ti کوچک از طریق تنظیم رشته «nonce» سخت‌تر است. بیت کوین از SHA-۲۵۶ به‌عنوان تابع‌هش استفاده می‌کند. SHA۲۵۶ داده‌هایی با سایزهای مختلف را به ۲۵۶ Bit تغییر می‌دهد.

[1] Practical Byzantine Fault Tolerance (PBFT)

[2] CPU-one-vote

ماینرها باید مقادیر مختلفی را برای رشته «nonce» در نظر بگیرند تا به یک مقدار هش معتبر برسند. ماینرها باید از مجموعه از قوانین مشترک در مورد معاملات پیروی کنند. برای مثال، هیچ‌کدام از معاملات جدیدی که استخراج می‌شوند نباید با معاملاتی که پیش از این استخراج شده‌اند یکی باشد. براساس قوانین، ماینرها می‌توانند معاملاتی را انتخاب کنند که باید در بلوک‌های جدید استخراج شود.

هدف PoW در بیت‌کوین اثبات نرخ تولید بلوک است. ماینرها باید روند تجدید هدف را دنبال کنند، در غیراین صورت بلوک‌های تازه استخراج شده توسط شبکهٔ بیت‌کوین پذیرش نخواهند شد. هدف Ti برای بلوک‌های جدیدی که باید در i مین دوره استخراج شوند به ۳۲Bit فشرده شده که با Bi نشان داده شده و در یک رشته "nBits" ۳۲Bit در سربلوک ذخیره شده است. تبدیل B_i به هدف T_i به‌صورت زیر است:

$$T_i = B_i^l \times 2^{8\times(B_i^u-3)} \quad (۱)$$

در اینجا B_i^l مقدار مربوط به ۲۴ بیت پایین از B_i و B_i^u مقدار مربوط به ۸ بیت بالای B_i است. فرایند تبدیل در شکل (۳) نشان داده شده است.

سختی تولید یک مقدار هش معتبر با رابطهٔ موجود بین هدف ماکزیمم و هدف فعلی مشخص شده است که رابطهٔ آن به‌صورت زیر می‌باشد:

$$D_i = \frac{T_{\max}}{T_i} \quad (۲)$$

که در اینجا T_{max} هدف بیشینه بوده و کما بیش برابر با $2^{۲۵۶-۳۲}$ است. برای مثال، سختی کار بیت کوین در ۱۲ ژوئن ۲۰۱۷ برابر با ۶۷۸۷۶۰۱۱۰۰۸۲ بوده است. با در نظر گرفتن سختیِ D_i میانگین زمان استخراج یک بلوک که با E(t) نشان داده شده، به‌صورت زیر محاسبه می‌شود:

$$E(t) = \frac{D_i \times 2^{۳۲}}{r} \quad (۳)$$

که در اینجا r نرخ هش ماینر (تعداد عملیات هشی که در یک ثانیه انجام می‌شود) است.

وقتی یک بلوک جدید تولید می‌شود، این بلوک با استفاده از الگوریتم‌های غرقابی به کل شبکه ارسال می‌شود (برای مثال، کل بسته‌های ورودی از طریق پیوندهای خروجی ارسال می‌شوند). وقتی یک گره در شبکهٔ بیت‌کوین یک بلوک جدید را دریافت می‌کند، چک می‌کند که آیا مقدار «nBits» با فرایند تجدید هدف مطابقت دارد یا خیر. سپس هش مربوط به سر بلوک را برای چک شدن محاسبه می‌کند. سپس رسیدن هش سرآیند به هدف مورد نظر در رشته «nBits »را مورد بررسی قرار می‌دهد. دریافت‌کننده نیز مابقی محتوای بلوک را برای اعتبارسنجی چک می‌کند. جفت‌ها می‌توانند به‌منظور از بین بردن تضادهای موجود در بینشان، به‌صورت مشارکتی با هم کار کنند. به این عملیات استخراج ائتلافی گفته می‌شود. با این‌حال استخراج ائتلافی نمی‌تواند نرخ توسعهٔ بلاک‌چین را به میزان قابل توجهی بالا ببرد، چون سختی کار می‌تواند در پاسخ به تغییر نرخ تولید بلوک به صورت پویا تنظیم شود. علاوه‌بر این، استخراج ائتلافی هدفش انتقال بلاک‌چین توزیع شده به یک سامانه متمرکز است. این می‌تواند برای جلوگیری از دست‌کاری بلاک‌چین مضر باشد. به منظور جلوگیری از مشارکتی کار کردنِ گره‌ها، [۵۱]، پازل‌های غیرقابل برون‌سپاری را معرفی کردند. استخراج ائتلافی براساس این حقیقت انجام می‌شود که اعضاء یک ائتلاف به یکدیگر اعتماد ندارند و عملیات اثبات رمزنگاری را به دیگر اعضاء ائتلاف می‌سپارند تا نشان دهند به سود ائتلاف کار می‌کنند. در استخراج ائتلافی، کارفرما می‌تواند ماینرهایی را برای استخراج بلوک به کار گیرد. کارفرما از بلوک‌های استخراجی پاداش دریافت خواهد کرد و این پاداش را براساس مدارک ماینرها بین آنها تقسیم می‌کند. پازل غیرقابل برون‌سپاری برای غیرفعال‌سازی رابطه طراحی شده است، به این صورت که به ماینر واقعی اجازه می‌دهد پاداش را بدون جایگذاری ردی از کارفرما سرقت کند. به‌طورکلی از PoW تنها برای پیدا کردن هدف فعلی استفاده شده و در ارائهٔ خدمات مفید نقشی ندارد. یکی از موارد استثنا این است که Permacoin از PoW برای ارائهٔ خدمات حفظ داده‌ها استفاده می‌کند. Permacoin به گره‌ها برای ذخیرهٔ پرونده‌ها و به منابع محاسباتی برای انجام روند اثبات و ارائهٔ سرویس نیاز دارد.

۱۰-۱-۲- اثبات x

می‌توان هویت‌های موجود را از سایر شیوه‌ها نیز مورد تأیید و اثبات قرارداد. این روش‌ها جایگزین روش‌هایی شده که روی شناسایی نانس[1] (یک عدد خاص بلاک‌چین) تمرکز می‌کنند (برای مثال روش اثبات کار). یکی دیگر از روش‌های اثباتی محبوب، همان روش اثبات سهام (سرمایه)[2] است [۱۹]، این روش از نظر صرفه‌جویی در انرژی مصرفی در موقعیت بهتری نسبت به روش اثبات کار (POW) قرار می‌گیرد. در این روش به‌جای اینکه از هویت‌ها خواسته شود تا یک نانس را پیدا بکنند، از آن‌ها خواسته می‌شود تا مالکیت خود بر ارز دیجیتالی را به اثبات برسانند، به موازات این فرایند، این فرض مطرح می‌شود که اعضایی با ارز دیجیتالی بیشتر با احتمال ضعیف‌تری نسبت به حمله به شبکه و اخلال در تمامیت آن اقدام می‌کنند. برای تایید

[1] Nonce
[2] Proof of Stake(POS)

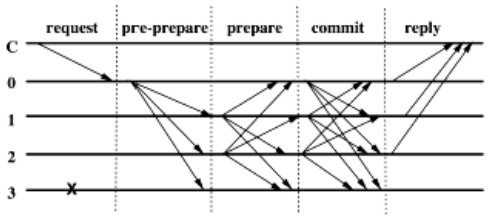
بلوک‌ها از رویکرد پیشنهادی [۲۵]، استفاده شده است، روش پیشنهادی براساس انتخاب ترازنامهٔ حساب کاربری عمل می‌کند. توجه داشته باشید که چنین انتخابی به‌صورت ذاتی غیرعادلانه است چرا که هویتی با بیشترین ثروت (موجودی حساب) بر کلیهٔ عملیات شبکه‌ای تسلط خواهد داشت. اثبات فعالیت[1] [۱۳]، با ادغام اثبات کار و اثبات سهام عمل می‌کند. در گام نخست، ماینرها (استخراج‌کننده بیت‌کوین) تلاش می‌کنند سربرگ‌های خالی بلوک‌ها را تولید کنند. این داده‌های سربرگی شامل ترکیبی از بلوک‌های قبلی، آدرس عمومی ماینر، شاخص بلوک و نانس است که با حل پازل هشی همچون POW به‌دست می‌آیند. در گام بعدی، سربرگ‌های خالی بلوک به شبکه مخابره می‌شوند (پخش گسترده). N ذینفع خوش‌شانس برای امضاء سربرگ بلوک انتخاب می‌شوند. N امین ذینفع به ترکیب سربرگ‌های خالی بلوک تأیید شده توسط N-۱ ذینفع و تراکنش‌ها می‌پردازد و آن‌ها را در یک بلوک جدید قرار می‌دهد. پاداش بین N ذینفع و ماینر به اشتراک گذاشته می‌شود. برخلاف POW، حملات باقدرت هش بالاتر از ۵۰٪ در POA قادر به سلطه بر بلاک‌چین فعلی یا تعیین شرایط گسترش آن نیستند. این در حالی است که POA نیازمند این است که سربرگ خالی بلوک N بار امضاء و مخابره بشود، بنابراین پیچیدگی سامانه افزایش و ظرفیت آن کاهش می‌یابند. راهکارهای متعدد دیگری نیز برای استفادهٔ ترکیبی با اندازهٔ سهام پیشنهاد شده‌اند تا راجع به مبنای تعریف بلوک بعدی تصمیم‌گیری نمایند. برای مثال، بلک‌کوین [۴۴]، از تصادفی سازی جهت پیش‌بینی مولد بعدی استفاده می‌کند، درحالی‌که پیرکوین[2] انتخاب مبتنی بر طول عمر سکه را ترجیح می‌دهد [۱۹]. در مقایسه با POW، POS از بهره‌وری مصرف انرژی بهتری برخوردار است. متأسفانه هزینهٔ استخراج بلوک‌ها در POS پایین و نزدیک به صفر است، POS در برابر حملاتی همچون حملهٔ محدودهٔ وسیع، حملهٔ سهام صفر، حملهٔ توزیع اولیه، حملهٔ عروس، حملهٔ انباشت سن سکه و حملات پیش محاسبه‌ای آسیب‌پذیر است [۲۶]. برای مثال، مهاجمی که از سهام کافی برخوردار است قادر به بازنویسی بلاک‌چین از روی پاره‌ای از بلوک‌های موجود است. حتی افراد خرابکاری با حداقل سهام در بلاک‌چین مبتنی بر POS نیز قادر به ایجاد بلاک‌چین جایگزین و معتبر از روی بلوک اولیه هستند (هر بلوک به اندازهٔ کافی قدیمی). از این وضعیت تحت عنوان حملهٔ محدودهٔ وسیع یاد می‌شود. گره‌های جدیدی که به شبکهٔ بلاک‌چین می‌پیوندند از قدرت تمایزدهی صحیح بلاک‌چین واقعی و جعلی بی‌بهره هستند. از سوی دیگر، با بالا رفتن چشمگیر قدرت محاسباتی/ زمان مورد نیاز برای بازسازی POW در بلاک‌چین هم از چنین حملاتی جلوگیری می‌شود. سایر رویکردهای POX پیشنهادی در بلاک‌چین عمومی عبارت‌اند از اثبات ذخیره (POD) [۲۸]، اثبات سوخت (POB) [۲۸]، اثبات زمان سپری شده (POET) [۲۹]. در POD، از شرکت‌کنندگان در استخراج خواسته شده تا سکه‌های خود را در حساب قرضه با قفل زمانی ذخیره کنند. در این حالت امکان جابه‌جایی سکه‌ها از بین می‌رود. هر ماینر دارای قدرت رأی‌دهی متناسب با میزان سکه‌های قفل شده است. یک بلوک معتبر است، اگر ۲/۳ کل قدرت رأی‌دهی را به خود اختصاص بدهد. کل فرایند رأی‌دهی مشابه PBFT است، قرارداد اجماع چند مرحله‌ای در آن پیاده‌سازی می‌شود. فرایند رأی‌گیری شامل سه مرحله است: ۱- پیشنهاددهی، ۲- پیش پردازش، ۳- پیش تعهد. پس از اینکه هر هویت بیش از ۲/۳ پیش تعهدها را دریافت نمود، نسبت به گسترش زنجیره اقدام می‌کند. POD قادر است سکه‌های قرضی هویت حاضر در تراکنش‌های مشکل‌ساز را حذف بکند و لذا از حملهٔ مصرف دوگانه جلوگیری می‌شود [۲۸]. در POB، ماینر سکه‌ها را به آدرس غیرقابل مصرفی می‌فرستد. به عنوان مثال، با سوزاندن سکه‌ها نسبت به استخراج از بلوک‌ها اقدام می‌کند. سکه‌های موجود در آدرس‌های غیرقابل مصرف بین ماینرهایی که به‌عنوان پاداش در بلوک‌ها ماین کرده به اشتراک گذاشته می‌شوند. توجه داشته باشید که سوخت سکه غیرقابل کنترل است و ممکن است کُل سکه‌ها کاهش یابد [۲۸]. Sawtooth با همکاری اینتل از POET به‌عنوان الگوریتم اجماعی استفاده می‌کند [۲۹]. در POET، زمان تصادفی قابل اطمینانی به هر سکه داده می‌شود. پس از انقضای فرصت زمانی، گرهٔ متناظر به تولید بلوک اقدام می‌کند. POET بر پایهٔ افزونه‌های امنیت نرم‌افزاری مورد اعتماد اینتل بنا شده است (SGX) [۳۰].

۱۰-۱-۳- تحمل خطای بیزانس

تحمل خطای بیزانس (BFT) [۵]، اغلب در بلاک‌چین‌های خصوصی برای فرمول‌بندی قرارداد اجماع و تضمین پیوستگی به‌کار می‌رود. بدین منظور از راه‌حل‌های مسائل ژنرال‌های بیزانسی (مسائل توافقی توصیف شده در بخش (۱۰)) استفاده می‌شود. الگوریتم‌های PBFT [۲]، به‌شکل اختصاصی برای حذف خطاهای بیزانسی به‌کار می‌روند. در ۱۹۹۹، کاسترو و لیسکوف[3] نخستین الگوریتم تکرار حالت ماشین مقاومت در برابر خطای بیزانسی (تحمل خطای بیزانسی کاربردی PBFT) را پیشنهاد دادند [۲]، این روش با سربار ارتباطی $O(n^2)$ در شبکه‌ای با n عضو همراه می‌شود. PBFT به‌عنوان یک الگوریتم BFT رهبر دارای یک گرهٔ اصلی و n-۱ گرهٔ پشتیبان در شبکه‌ای n گره‌ای

[1] Proof-of-Activity(POA)
[2] Peercoin
[3] Castro & Liskov

است. ممکن است گره‌های پشتیبان دچار خرابی بشوند. گرهٔ اصلی مسئول دریافت درخواست از کلاینت‌ها و راه‌اندازی الگوریتم است [۱۸].



شکل (۴): عملیات PBFT در صورت عدم‌وجود خطای

PBFT با الهام‌گیری از تکرار با برچسب‌های نمایشی [۱۸] و مطابق شکل (۴) شامل ۴ مرحله است: ۱- ارسال درخواست خدمات به گرهٔ اصلی توسط کلاینت ۲- ارسال چندگانهٔ درخواست توسط گرهٔ اصلی به گره‌های پشتیبان، گرهٔ اصلی (تکرار ۰) شناسهٔ توالی را به درخواست m کلاینت اختصاص می‌دهد و پیام PRE-PREPARE با تعیین وظایف را مالتی کست می‌کند. ۳- تکرارها درخواست را اجرا کرده و به کلاینت پاسخ می‌دهند. در صورتی‌که یکی از گره‌های پشتیبان نسبت به فرایند تخصیصی موافقت نماید (پارامترهای صحیح و معتبر)، یک پیام PREPARE را مالتی کست می‌کند. هنگامی‌که پشتیبان پیامی را دریافت و نسبت به وظیفهٔ مربوطه و تفکیکی موافقت داشته باشد (۲f پیام PREPARE پیوسته و تأیید شده از پشتیبان‌های مختلف)، آنگاه یک پیام COMMIT به‌صورت گروهی مخابره می‌شود. گرهٔ پشتیبان درخواست m را اجرا می‌کند و پس از دریافت ۲f پیام COMMIT معتبر و پیوسته به کلاینت پاسخ می‌دهد. ۴- کلاینت منتظر f+۱ پاسخ از گره‌های پاسخ دهندهٔ مختلف مانده و نتیجهٔ یکسان تلورانس عملیاتی تا حداکثر f خطا حاصل می‌شود. الگوریتم PBFT از پایداری و مقاومت بالایی برخوردار است. اثبات شده که الگوریتم PBFT قادر به تضمین اجماع برای n هویت شبکه‌ای در شبکه‌ای مطمئن و هم‌زمان است تا زمانی که تعداد هویت‌های خائن از n-۱/۳ فراتر نرود [۵]. به‌طور دقیق‌تر، الگوریتم تنها نیازمند $n > 3f+1$ پاسخ است تا f پاسخ خطا را تحمل کرده و خروجی صحیح و بدون خطا برای کلاینت را تضمین نماید [۱۴]. در واقع ۳f +۱ پیام PREPARE در هر گرهٔ پشتیبان، از جمله خودش در مرحلهٔ دوم برای ایجاد پشتیبانی دائمی و صحیح و تولید پیام COMMIT صحیح کافی هستند. مراحل سوم و چهارم تضمین‌کنندهٔ دریافت پاسخ‌های پیوسته در حدی بیشتر از f پاسخ غلط در هر گرهٔ پشتیبان یا کارفرما هستند. الگوریتم PBFT کارایی خوبی دارد و قادر به پردازش هزاران درخواست در ثانیه با تأخیر پردازی در حد ۱۰ ms است [۱۵]. به جزء سربار $O(n^2)$، PBFT نیازمند این است که تمامی گره‌ها به‌درستی شناسایی، تأیید و احراز هویت شده باشند. با توجه به این دلایل، PBFT گزینهٔ مناسبی برای بلاک‌چین‌های خصوصی در مقیاسی کوچک و کنترل‌پذیر است. الگوریتم PBFT در برابر افرازبندی شبکه‌ها آسیب‌پذیر است. یک افراز قادر به گسترش زنجیرهٔ خود نیست، مگر اینکه تعداد گره‌های مطمئن افراز npb در شرط npb>n- (n- ۱/۳) -قرار بگیرند. n تعداد کل گره‌های شبکه است. در واقع PBFT قادر به تحمل حداکثر n-۱/۳ پاسخ غلط از مجموع n پاسخ است [۲].

۱۰-۱-۴- انواع مختلف PBFT

در مرجع [۱۴] یک قرارداد BFT غیرهمزمان با نام BFT گورکن را توسعه دادند که دسترسی‌پذیری بدون هم‌زمانی را تضمین می‌کند. این سامانه قرارداد مخابرهٔ اتمی برای زیر مجموعهٔ مشترک و غیرهمزمان[1] را حذف می‌کند و بازدهی را افزایش می‌دهد. گره اصلی ACS به هر گره این امکان را داده تا مقداری را پیشنهاد داده و تضمین بکند هر گره بردار مشترک با مقادیر ورودی حداقل n-۲f گرهٔ صحیح در شبکه‌ای با n عضو و f خطا در خروجی تولید نماید. BFT گورکن با هزینهٔ ارتباطی O(n) در شبکهٔ n عضوی همراه می‌شود. الگوریتم جدید از شبکه‌های بزرگ‌تر پشتیبانی کرده و در شبکهٔ ۱۰۴ عضوی قادر به ثبت ۱۵۰۰TPS است. یک پروژهٔ فراگیر بین‌المللی و جدید در حوزهٔ بلاک‌چین با نام دفترکل فراگیر روی فن‌های عملیاتی بلاک‌چین و پیاده‌سازی الگوریتم‌های BFT در بلاک‌چین تمرکز نموده است [۳۱]. دفترکل فراگیر یک پروژهٔ تعاملی متن باز است که موجبات ارتقاء مصرف بین حوزه‌ای (چند صنعتی) بلاک‌چین را فراهم می‌سازد. میزبانی از داده‌های پروژه توسط بنیاد لینوکس صورت گرفته است. برترین شرکت‌های جهان در حوزه‌های مالی، بانکداری، اینترنت اشیا، زنجیره تأمین و فناوری در این پروژه مشارکت دارند. دفترکل فراگیر خود از چندین پروژهٔ بلاک‌چینی مستقل تشکیل شده است،[[۲۱] ، [۳۲]، [۳۳] [۳۴]]. فابریک پروژهٔ پیشروی این طرح محسوب می‌شود و با همکاری شرکت‌های Digitalasset و IBM برگزار شده است. فابریک از معماری ماژولی سود می‌برد و به‌صورت دینامیک از ماژول‌های بارگذاری پشتیبانی می‌کند (قراردادهای اجماع و خدمات عضویت). فابریک از PBFT به‌عنوان قرارداد اجماع پیش‌فرض خود استفاده می‌کند. برای حفظ قابلیت برنامه‌ریزی، قراردادهای هوشمند واقع‌شده در محفظه‌های فناوری طراحی شده‌اند که از آن‌ها تحت عنوان زنجیره کد[2] یاد می‌شود. بورو حالت تعمیم یافتهٔ اتریوم است و تمرکز آن روی خدمات قراردادی هوشمند مجاز قرارگرفته است. برای بلاک‌چین از میدلور BFT به‌نام تندرمینت

[1] - asynchronous common subset(ACS)
[2] - Chaincode

[۲۸] به‌عنوان قرارداد اجماعی استفاده می‌شود. ایروها مؤلفه‌های داخلی C++ را برای سایر پروژه‌ها در دسترس قرار می‌دهد. ایروها نیز از PBFT به‌عنوان قرارداد اجماعی خود سود می‌برد.

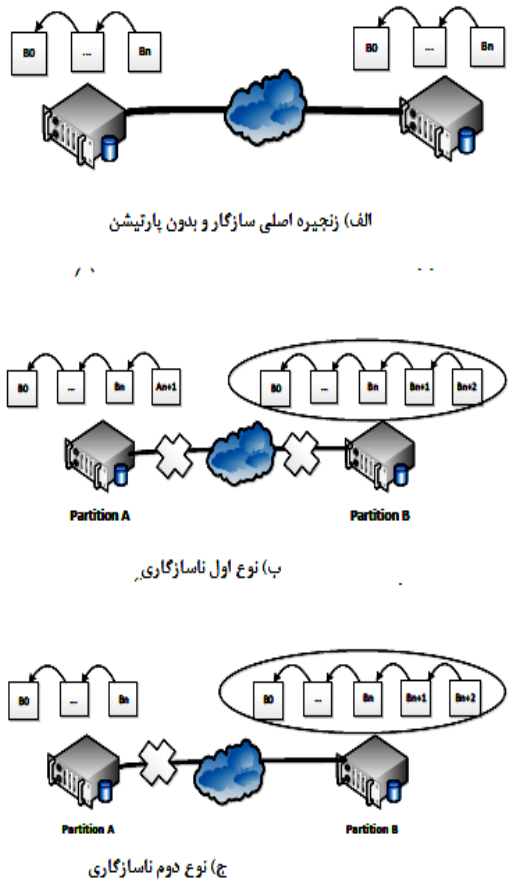
۱۰-۲- ساختار داده‌های واحد

ساختار تعیین‌کنندهٔ نحوهٔ ذخیرهٔ داده‌های واحد و تصمیم‌گیری راجع به دفترکل اصلی است. بررسی متمرکز روی حالتی است که بیش از یک دفترکُل به‌صورت توأمان روی شبکهٔ توزیعی وجود دارد. درصورتی‌که دفترکل‌های مختلف همگی پذیرفته بشوند، ظرفیت شبکهٔ بلاک‌چین افزایش می‌یابد، اما خطر دو برابر شدن سکه‌های مصرفی نیز وجود خواهد داشت. حملات مصرف دوگانه اشاره به خطاهایی دارد که یک سکه با موفقیت بیش از یکبار مصرف می‌شود [۴]. در حالت کُلی، حملهٔ مصرف دوگانه با ایجاد اسناد متضادی در سامانه توزیعی همراه می‌شود. بلاک‌چین تنها می‌تواند تضمین بکند که تمامی اسناد در پایان پیوسته هستند. اسناد قبل از پذیرش نهایی، به‌صورت موقت تأیید و سپس رد می‌شوند. بدین ترتیب امکان حملهٔ مصرف دوگانه پدید می‌آید.

۱۰-۲-۱- بلوک‌های زنجیر شده

در بلاک‌چینی با ساختار داده‌های زنجیر شده، همچون بیت کوین، تنها یک زنجیر برای کُل سامانه مورد تأیید قرار می‌گیرد، از این زنجیر تحت عنوان زنجیر اصلی یاد می‌شود [۱۹]. هر بلوک شامل هش رمزنگاری شده‌ای از سربرگ‌های بلوک قبلی است و با اعمال الگوریتم ترکیبی SHA-۲۵۶ بلوک فعلی به بعدی متصل می‌شود شکل (۱). این احتمال وجود دارد که زنجیرهای قرارگرفته در بخش‌های مختلف شبکه دارای ناپیوستگی باشند، چرا که هر قسمت نمای محدودی را نسبت به سایر قسمت‌های شبکه درپی‌خواهد داشت. به‌عبارتی دیگر، افرازی شدن شبکه در نسل‌های آتی شبکه‌های اینترنت اشیا محتمل است. برای رفع این مشکل، بیت‌کوین از قاعدهٔ ساده‌ای استفاده کرده که در آن سامانه فقط طولانی‌ترین زنجیره را به‌عنوان زنجیرهٔ اصلی در نظر می‌گیرد و بقیه را نادیده می‌گیرد [۴]. در کاربردهای اجرایی، هر عضو بلاک‌چین به طولانی‌ترین زنجیره انتقال یافته یا به حالت قبلی برمی‌گردد. زنجیره‌ها با توجه به اینکه بلوک‌ها به‌صورت محلی نگهداری و سپس حذف شده برای تهیهٔ اسناد پیوسته با یکدیگر سنکرون می‌شوند [۳۲].

برای شکل (۵) شامل دو نوع ناپیوستگی هستیم. اولین دسته از ناپیوستگی‌ها به‌دلیل استخراج افراز روی یک یا چند بلوک پس از آخرین بلاک‌چین پیوسته پدید می‌آیند. سایر افرازها با پذیرش بلوک‌های جدید به اجماع می‌رسند. در حین همگام‌سازی هیچ بلوکی حذف نمی‌شود [۳۳]، شکل (۵، ب) را ببینید. دومین نوع



شکل (۵): دو نوع ناسازگاری در بلاک‌چین با افرازها [۴۷]

ناپیوستگی حالتی است که طی آن یک افراز به الحاق بلوک‌هایی از آخرین حالت پیوسته (صحیح) اقدام می‌نماید. تنها طولانی‌ترین زنجیره باقی می‌ماند، درحالی‌که بقیه لغو می‌شوند. بلوک‌های فراخوانی شده به‌عنوان بلوک قدیمی شناخته می‌شوند [۳۴]، شکل (۵، ج) را ببینید. واضح است که ماینر با ارجاع به نوع اول از ناپیوستگی‌ها و پذیرش آخرین بلوک‌ها قادر به سوء استفاده از این شرایط است. راجع به ناپیوستگی‌های نوع ۲، ماینر باید بخشی از بلوک‌های خود را حذف نماید و به زنجیرهٔ اصلی طولانی‌تری منتقل بشود. نوع دوم از ناپیوستگی‌ها منجر به از دست رفتن تراکنش در بلوک قدیمی می‌شود. در مجموع، خطر از دست رفتن تراکنش به دو دلیل پایین است. علت اول اینکه تراکنش‌های موجود در بلوک قدیمی ممکن است در بلوک مورد تأیید باشند، تراکنش‌ها برای بسیاری از بخش‌های شبکه قابل رؤیت هستند و در بلوک‌های مختلف مشاهده و در گره‌های مختلف استخراج می‌شوند. علت دوم اینکه در صورت لغو تراکنش در بلوک قدیمی، به حالت تراکنش تأیید نشده برگشت می‌کند و در انتظار ورود به بلوک جدید می‌ماند. در صورت وجود تراکنش‌ها/ بلوک‌های ناسازگار در افرازهای مختلف، در نوع دوم از

ناپیوستگی‌ها شاهد وقوع حملهٔ مصرف دوگانه هستیم. بیت‌کوین به دریافت‌کنندگان سکه توصیه کرده به اندازهٔ ۶ بلوک برای تأیید منتظر بمانند [۴] تا بدین وسیله از حملات مصرف دوگانه جلوگیری بشود. استفاده از قراردادهای اجماع امکان اجرای این حملات در بلاک‌چین‌های زنجیره‌ای را ممکن می‌سازد. حملهٔ ۵۱٪ در مثال POW را در نظر بگیرید [۲۰]. درصورتی‌که یک گرهٔ قوی بیش از ۵۰٪ منابع محاسباتی شبکه را در اختیار داشته باشد، آنگاه قادر به تولید سریع بلوک‌ها و ربودن زنجیرهٔ اصلی است و قاعدهٔ طولانی‌ترین زنجیره اعمال می‌شود؛ بنابراین، مهاجم بر زنجیره‌ای با طول دلخواه تسلط خواهد داشت. در جولای ۲۰۱۸، نرخ هش شبکه در حد H/s ۱۰۸۱۹*۴ قرار دارد [۲۴]. حملات ۵۱٪ در عمل غیرممکن هستند. همچنین، بیت‌کوین نرخ تولید بلوک را به یک بلوک در هر ۱۰ دقیقه محدود می‌سازد. برای این منظور دشواری POW مطابق اطلاعات توصیف شده در بخش قبلی تنظیم می‌شود.

۱۰-۲-۲- قرارداد اجماع

سایر راهکارهای مرتبط با قرارداد اجماع از این واقعیت سود می‌برند که برخی بلوک‌های رها شده، تحت قرارداد اجماعی استخراج شده‌اند اما با توجه به فورک‌ها[1] از زنجیرهٔ اصلی کنار گذاشته می‌شوند. می‌توان از این بلوک‌ها برای ارتقای ظرفیت استفاده نمود. بدین منظور نیازمند تنظیم ساختار شبکه هستیم. یکی از قراردادهای اجماعی تحت عنوان tangle [۳۶]، از گراف غیر چرخه‌ای جهت‌دار برای سازمان‌دهی بلوک‌های، بجای زنجیره‌ها سود می‌برد، از سوی دیگر DAG یک گراف جهت‌دار محدود بدون چرخه‌های جهت‌دار است. در tangle هر تراکنش باید دو تراکنش قبلی را تأیید نماید. در نهایت یکی از اسناد متضاد تأییدیهٔ رقابت را دریافت کرده و مورد پذیرش قرار می‌گیرد. برخلاف حالت تک کپی در ساختار زنجیره‌ای، tangle تراکنش‌های متضاد را حذف نکرده و در شاخه‌های مختلف DAG نگهداری می‌کند. ساختار DAG با ایجاد ظرفیت مطلوب‌تری همراه است.

۱۰-۲-۳- سنگین‌ترین زیر درخت مشاهده شده حریصانه

قرارداد دیگری به‌نام سنگین‌ترین زیر درخت مشاهده شده حریصانه[2] بلوک‌ها را در ساختار درختی قرار می‌دهد [۳۶-۳۷]. مسیر اصلی از بلوک پایه، اولین بلوک بلاک‌چین شروع می‌شود و تا سنگین‌ترین زیر درخت با حداکثر تعداد بلوک‌ها ادامه می‌یابد. به‌عبارتی‌دیگر سنگین‌ترین محاسبهٔ به‌عنوان زنجیرهٔ اصلی عمومی با بیشترین تعداد بلوک پذیرفته می‌شود. GHOST سرعت بلوک از ۱۰ دقیقه برای هر بلوک در بلاک‌چین را به ۱۲s برای تولید هر بلوک در اتریوم افزایش می‌دهد [۲۳،۳۷]؛ بنابراین ظرفیت بلاک‌چین افزایش می‌یابد.

۱۰-۲-۴- ساختار ترکیبی

نسل بعدی بیت‌کوین [۱۶]، یک قرارداد عمومی بلاک‌چین است که وظیفهٔ تولید بلاک‌چین را به قدرت محاسباتی رهبران جهت تسریع تأیید تراکنش وابسته می‌کند. نسل بعدی بلاک‌چین با تفکیک عملیات بلاک‌چینی به دو مرحلهٔ انتخاب رهبر و سریالی کردن/ توالی‌دهی تراکنش‌ها تقسیم می‌شود. انتخاب رهبر با توجه به‌سرعت حل پازل‌های دشوار محاسباتی همچون POW صورت می‌گیرد. رهبر انتخابی در بلوک‌های کلیدی ثبت می‌شود. یک میکرو بلوک شامل تراکنش‌ها و یک سربرگ است که به بلوک قبلی اشاره دارد. میکرو بلاک فاقد نانس است و لذا می‌توان به تولید آن با نرخ از پیش تعیین شده اقدام نمود. این نرخ به مراتب بیشتر از نرخ تولید بلوک‌های کلیدی است. بلوک‌های کلیدی و میکرو بلوک همانند بیت کوین به هم زنجیر می‌شوند. هر بلوک شامل سربرگی است که مرجع خاص به بلوک‌های قبلی را در پی دارد.

۱۰-۳- بلاک‌چین شاردینگ

بلاک‌چین شاردینگ[3] [۴۰]، سازوکار جدیدی است که امکان پردازش موازی تراکنش‌ها را ممکن می‌سازد. بدین‌ترتیب، نرخ تولید بلوک بلاک‌چین به شکل عمده‌ای ارتقا می‌یابد. نخستین شاردینگ‌های پیشنهادی، [۱۷ یک نمونه] تنها پردازش تراکنش‌ها را به اشتراک گذاشته‌اند و یک بلاک‌چین عمومی را حفظ می‌کنند. انتظار می‌رود شبکه‌های فراگیر اینترنت اشیا با تولید داده‌های فراوانی در محدوده‌های وسیع همراه بشوند. از طرفی دیگر، داده‌های اینترنت اشیا از ناهمگنی و محلی بودن بالایی رنج می‌برند و تنها برای نواحی محلی کاربرد دارند. بدین ترتیب فرصت توسعهٔ بلاک‌چین‌های شاردینگ در محیط‌های اینترنت اشیا پدید می‌آید. یک زنجیرهٔ آغازین با هدف دریافت رخدادهای مهم و غیر رایج روی شبکه‌های عظیم اینترنت اشیا بکار می‌رود. زنجیره‌های ثانویه برای ثبت رخدادهای محلی در شبکه‌های مربوطه طراحی شده‌اند. دو بلاک‌چین فوق‌الذکر در مقیاس‌های زمانی متفاوتی عمل می‌کنند. مقادیر ترکیبی زنجیره‌های ثانویه به شکل تراکنشی در زنجیرهٔ اصلی ایمن‌سازی می‌شوند. به‌طور دقیق‌تر، زنجیرهٔ اصلی که ثبت رخدادهای عمومی کم تکرارتر را ممکن می‌سازد با پایین‌ترین سرعت‌های ممکن تحت هم‌زمان‌سازی (همگام سازی) قرار می‌گیرد؛ بنابراین

[1] Fork
[2] Greedy Heaviest-Observed Sub-Tree(GHOST)
[3] Sharding

ملزومات ظرفیتی مورد نیاز برای حفظ پیوستگی در مقیاس وسیع شبکه‌ای کاهش می‌یابند. لازم است دو دسته از بلاک‌چین‌ها به هم متصل بشوند تا درستی تمامی اسناد تضمین بشود (در سطوح محلی و جهانی). با تأکید بر پیاده‌سازی، برخی تحقیقات اولیه در [۸] گزارش‌شده‌اند.

۱۰-۴- زنجیره‌های جانبی

فارغ از فراگیری شبکه‌های اینترنت اشیا، برخی دستگاه‌های اینترنت اشیا از قدرت جابه‌جایی در فواصل طولانی برخوردارند. برای مثال دستگاه‌های نصب شده در هواپیماها، قطارها و کشتی‌ها [۸]. تمامیت داده‌های تولید شده توسط این دستگاه‌ها (برای مثال میزان خوردگی قطعات هواپیما)، اگر مهم‌تر از داده‌های تولیدی در دستگاه‌های اینترنت اشیا ثابت نباشند، حداقل به همان اندازه مهم هستند. توجه داشته باشید که امکان استخراج داده‌های دستگاه‌های سیار در صورت دور بودن از شبکه‌های اصلی یا افرازهای شبکه، واقع در بلاک‌چین‌های مختلف وجود دارد. جابه‌جایی و ادغام خود نوعی دست‌کاری در بلاک‌چین محسوب می‌شود. انتقال و مهاجرت بلوک‌ها و بخش‌ها و برگشت به شبکه‌های اصلی برای حفظ پیوستگی اطلاعات ثبت شده در دستگاه‌های متحرک به‌طورکامل حیاتی و حائز اهمیت است. با توجه به ماهیت ذاتی بلاک‌چین و مقاومت در برابر دست‌کاری با چالش‌هایی رو به‌رو می‌شویم. فناوری زنجیرهٔ جانبی [۱۲،۴۱] راه‌حلی را برای انتقال دارایی‌ها بین بلاک‌چین‌های مختلف ارائه می‌دهد. فناوری زنجیرهٔ جانبی امکان توکن‌ها بین بلاک‌چین‌های مختلف به شکل غیرمتمرکز را فراهم می‌سازد. فرایند انتقال دارایی مشابه تبادل ارز است [۴۱]. برخی چالش‌های مربوط به زنجیرهٔ جانبی نیازمند بررسی‌های دقیق‌تر هستند، برای مثال، گسترش زنجیره‌ها در شبکه‌ی اصلی و ایمپلنت کردن زنجیره‌ها داخل زنجیرهٔ اصلی.

۱۱- قراردادهای اجماع مخصوص اینترنت اشیا

قراردادهای اجماع با طراحی تخصصی و کاربردهای منحصربه‌فرد برای سودرسانی به برنامه‌های بلاک‌چین اینترنت اشیا داده محور مهم هستند. می‌توان قراردادهای اجماع را به گونه‌ای طراحی کرد که با تأیید داده‌های اجماع، بجای ترکیب مطلق تراکنش‌ها به اجماع دست یابند. توجه داشته باشید که مشاهدات حس‌گر به شدت به محدودهٔ مکانی مربوط هستند چرا که هم بندی شبکه از چگالی بالایی برخوردار می‌باشد. از طرفی دیگر، ماهیت فیزیکی در تعامل زمانی بین مشاهدات متوالی یک گره حس‌گر برقرار می‌باشد. همبستگی‌های مکانی و زمانی، در کنار ماهیت تعاملی اینترنت اشیا پتانسیل تولید قراردادهای اجماع محتوی محور را افزایش می‌دهند [۹]. درست بودن داده‌های حسگرها به کمک داده‌های حس‌گرهای مجاور و داده‌های تاریخی به‌صورت متقابل مورد تأیید قرار می‌گیرند [۱۰].

۱۱-۱- تأیید پرداخت ساده سازی شده (SPV)

وظایف استخراج بلوک فشار بالایی را به سامانه وارد می‌کنند و ممکن است حجم داده‌های بلاک‌چینی نیز بسیار بزرگ باشد، به گونه‌ای که پیاده‌سازی آن‌ها روی دستگاه‌های اینترنت اشیا غیرممکن باشد. فناوری تأیید پرداخت ساده‌سازی شده (SPV) امکان تأیید تراکنش‌ها، بدون اجرای فرایند استخراج و ذخیره‌سازی تمامی بلوک‌های قبلی را فراهم می‌سازد. گره‌های بلاک‌چینی مجهز به SPV تنها به منابع بسیار جزئی نیاز دارند و به راحتی روی دستگاه‌های اینترنت اشیا پیاده سازی می‌شوند. در SPV هر گره فقط سربرگ‌های بلوک زنجیره شده را نگهداری می‌کند و اتصال شاخهٔ مرکل نسبت به تراکنش‌ها مورد تأیید قرار می‌گیرد. هرچند گرهٔ SPV به تنهایی قادر به تأیید تراکنش‌ها نیست، اما به بررسی این موضوع پرداخته که آیا شبکهٔ بلاک‌چین تراکنش را پذیرفته است یا خیر؟ بدین منظور ارتباط شاخهٔ مرکل با تراکنش مورد ارزیابی قرار می‌گیرد. برای مثال، گره‌های SPV اتریوم برای دوچرخه‌های کوچک به‌کار رفته‌اند [۱۱]. گرهٔ سبک (اسم سامانه) یک حالت خاص پیاده‌سازی SPV در اتریوم محسوب می‌شود [۲۳]. گره‌های سبک داده‌های بلاک‌چین را از گره‌های حاوی تمامی بلوک‌ها دریافت می‌کنند (قرارداد جزئی در سرور سبک اتریوم، LES) [۲۳].

۱۲- بلاک‌چین قابل‌ویرایش

ذخیره‌سازی دستگاه‌های اینترنت اشیا برای حجم عمده‌ای از دفتر کل‌های بلاک‌چینی بسیار محدود است. در واقع بسیاری از دستگاه‌های اینترنت اشیا به ذخیره‌سازی تعداد زیادی از رخدادها در بلندمدت اقدام می‌کنند. حتی برای ثبت داده‌های مالی در بیت‌کوین، حجم کل از بلوک پایهٔ سال ۲۰۰۹ به GB ۱۴۹در دسامبر ۲۰۱۷ افزایش یافته است [۴۲]. لازم به ذکر است که داده‌های برخی برنامه‌های اینترنت اشیا پس از گذشت زمان ثابتی بی‌معنی می‌شوند. برای مثال، ثبت تغذیه، پس از مصرف آن بی‌معنی است؛ بنابراین می‌توان نسبت به حذف این داده‌ها از بلاک‌چین و کاهش ملزومات ذخیره‌سازی مورد نیاز بلاک‌چین اقدام نمود. اقدامات مجرمانه و اطلاعات ثبتی برای بلاک‌چین‌های اینترنت اشیا تقاضا برای فناوری بلاک‌چین قابل ویرایش، بدون از بین رفتن اعتماد داده‌های ذخیره‌سازی را افزایش داده‌اند. بلاک‌چین قابل ویرایش امکان حذف و ویرایش برخی بلوک‌ها را فراهم می‌سازد و درشرایط بخصوصی تکمیل می‌شوند. با توجه به اینکه ویرایش‌پذیری به نحوی در تضاد با ماهیت تغییرناپذیری بلاک‌چین قرار می‌گیرد، لازم است در بلاک‌چین قابل ویرایش

امنیت و سطح تمامی ویرایش‌های صورت گرفته تضمین بشود. در حال حاضر بلاک‌چین‌های قابل ویرایش برای الگوریتم‌های رمزنگاری همچون انواع توابع ترکیبی چند حالتی طراحی شده‌اند [۱۸]. در جدول (۱) مرور مقایسه‌ای از فناوری‌های فعلی بلاک‌چین در کاربردهای اینترنت اشیا نمایش داده شده است.

جدول(۱): مقایسه عملکرد بلاک‌چین در کاربردهای اینترنت اشیاء

نام	نوع	قرارداد اجماع	ظرفیت	مقیاس	کاربرد	مزایا	معایب
بیت‌کوین [۵۴]	عمومی	PoW+ طولانی‌ترین زنجیره	7 tps^{-}	$10^{5\#}$	ارز رمزنگاری شده	قابلیت بالای تحمل افراز مقاوم در برابر مداخله	ظرفیت محدود پیچیدگی محاسباتی بالا
اتریوم [۵۳]	عمومی	PoW+ گوست	۱۲ ثانیه/بلوک$^{\circ}$	$10^{5\#}$	ارز رمزنگاری شده قرارداد هوشمند بستربلاک‌چین	قابل برنامه‌ریزی قابلیت بالای تحمل افراز	پیچیدگی محاسباتی بالا
IOTA [۲۳]	عمومی	PoW+ تنگل	$> 800\ tps^{*}$	10^{3*}	بستر بلاک‌چین اینترنت اشیاء	ظرفیت بالا معامله‌ی بدون هزینه تحمل افراز	غیر قابل برنامه‌ریزی
فابریک [۲۰]	خصوصی	PBFT	10^{5} tps*	20^{*}	قرارداد هوشمند بستر بلاک‌چین	ظرفیت بالا بدون انشعاب معماری ماژولار	قابلیت پایین تحمل افراز سربار ارتباطی بالا مقیاس پذیری محدود نیاز به مرکز احراز هویت
بورا [۵۵]	خصوصی	تندرمینت	10^{5} tps*	tens*	قرارداد هوشمند	پشتیبانی از قرارداد هوشمند	نیاز به مرکز احراز هویت
ساوتوث [۵۵]	عمومی	PoET	در دسترس نمی‌باشد	در دسترس نمی‌باشد	بستر بلاک‌چین	پیچیدگی محاسباتی پایین	تنها با پردازنده‌ی اینتل کار می‌کند
پیرکوین [۵۷]	عمومی	PoS	0.1 tps$^{\#}$	$10^{3\#}$	ارز رمزنگاری شده	پیچیدگی محاسباتی پایین	خطر حمله از سوی ثروتمندان
بیت کوین-NG [۵۶]	عمومی	PoW	tens tps$^{\#}$	10^{3*}	بلاک‌چین	پیچیدگی محاسباتی پایین	خطر رهبر مخرب
اسکوین [۵۸]	عمومی	SCP	$> 22\ tps^{*}$	80^{*}	ارز رمزنگاری شده	ساختار کمیته‌ای	پیچیدگی محاسباتی بالا
اسلیم کوین [۵۹]	عمومی	PoB	در دسترس نمی‌باشد	در دسترس نمی‌باشد	ارز رمزنگاری شده	پیچیدگی محاسباتی پایین	خطر از دست دادن کوین

۱۳- نتیجه‌گیری

در این مقاله به مرور جامع کاربرد بلاک‌چین، برای برطرف سازی بسیاری از دغدغه‌های ایمنی داده‌ها در قلمروی اینترنت اشیا پرداخته‌ایم. تأثیر دستگاه‌های گستردهٔ اینترنت اشیا، قدرت محاسباتی محدود، پهنای باند ارتباطی ناچیز و پیوندهای رادیویی با نرخ خطای بالابر عملکرد بلاک‌چین مورد مطالعه قرارگرفته‌اند.

جدیدترین فناوری‌های بلاک‌چین با جزئیات فراگیر مورد تجزیه و تحلیل قرار گرفته‌اند، سپس این فناوری‌ها از نظر کارایی نسبت به سناریوهای اینترنت اشیا مورد مقایسه قرارگرفته‌اند. برخی جهت‌گیری‌های تحقیقات آتی عبارت‌اند از افزایش ظرفیت، امنیت و مقیاس‌پذیری بلاک‌چین‌ها برای ادغام مؤثرتر بلاک‌چین و اینترنت اشیا در آیندهٔ نزدیک.

تأکید اصلی روی سازگاری با شبکه‌های اینترنت اشیا قرارگرفته است. تمامی دستگاه‌های اینترنت اشیا از قدرت

به‌کارگیری خدمات بلاک‌چین برخوردار هستند. دستگاه‌های اینترنت اشیا با منابع کافی با توان محاسباتی بالا، تأمین برق دائمی، ذخیره‌سازی کافی و اتصالات شبکه‌ای پُرسرعت همچون وسایل نقلیه [۱]، به‌عنوان استخراج‌کننده یا گره‌های کامل در بلاک‌چین عمل می‌کنند. دستگاه‌های اینترنت اشیا با قدرت محاسباتی کمتر، همچون تلویزیون‌های هوشمند، به‌منزلهٔ گره‌های کم‌حجم بلاک‌چینی تلقی می‌شوند و خدمات را از گره‌های کامل یا ماینرها دریافت می‌کنند. دستگاه‌های اینترنت اشیا با قدرت ذخیره‌سازی، محاسبه و ارتباط محدود از طریق عوامل با کارکردهای اساسی بلاک‌چین ارتباط برقرار می‌کنند. قراردادهای اجماع به منزلهٔ کارکردهای هسته‌ای هستند که تصمیم‌گیری نسبت به عملکرد اینترنت اشیا مبتنی‌بر بلاک‌چین همچون نرخ بلوک‌ها، پیوستگی، مقیاس‌پذیری و امنیت را به همراه دارند. قراردادهای اجماع مبتنی بر POW در شبکه‌های آزاد از بالاترین امنیت برخوردار هستند [۳۸]. از سوی دیگر، POW توانایی استخراج بلوک در دستگاه‌های اینترنت اشیا را نابود می‌سازد چرا که ملزومات محاسباتی سنگینی را به همراه خواهد داشت. قراردادهای اجماع مبتنی بر POS با کاهش چشمگیر مصرف انرژی در مقایسه با POW همراه می‌شوند. POS این شانس را به دستگاه‌های اینترنت اشیا داده تا در استخراج بلوک مشارکت نمایند. لازم به ذکر است که نرخ تولید بلوک هر الگوریتم اجماعی POS و POW محدود می‌باشد. قراردادهای اجماع مبتنی بر PBFT برای بلاک‌چین‌های خصوصی محدودیت‌هایی را نسبت به تعداد ماینرهای حاضر به همراه خواهند داشت [۶]. علاوه‌بر، الگوریتم‌های اجماعی همچون POW، POS و PBFT، ظرفیت و مقیاس‌پذیری هم به محیط اجرا و پیکربندی بستگی دارند (سرعت، اندازهٔ شبکه و غیره). بالا وندهای ~، * و # نشان‌دهندهٔ منابع مختلف داده‌های نمایش‌دهی شده هستند:

- بالاوند ~ نشان‌دهندهٔ تحلیل عملی است. برای مثال، بیت کوین دارای کران بالای ۷ tbps برای نرخ تراکنش‌هاست که برحسب نرخ تولید بلوک و اندازه متفاوت است.
- بالاوند * نشان‌دهندهٔ نتایج تأیید شده در فرمت تجربی است.
- بالاوند # نشان‌دهندهٔ اطلاعات ثبت‌شدهٔ تاریخی است.

برای مثال، شبکهٔ اتریوم دارای بیش از ۳۰ هزار گره در کل جهان تا تاریخ ژوئن ۲۰۱۷ بوده است. از این منظر، نتایج قبلی به دلیل عدم وجود آزمون‌های تنشی غیرواقعی هستند.

از بین پروژه‌های بلاک‌چینی فوق‌الذکر، اتریوم برای بسیاری از کاربردهای اینترنت اشیا با تعداد زیادی از این دستگاه‌ها و ساختار شبکه‌ای همگن مناسب‌تر است. اتریوم به‌عنوان یک بلاک‌چین عمومی از مقیاس‌پذیری خوبی برخوردار است و به خوبی از دستگاه‌های غیر همگن پشتیبانی می‌کند. مهم‌ترین عیب اتریوم (نسخهٔ جدید در ۲۰۱۶ راه اندازی شده است) در کاربردهای اینترنت اشیا به پیچیدگی محاسباتی بالا و ظرفیت محدود برمی‌گردد. در مجموع، اتریوم با بهره‌گیری از قراردادهای اجماع POS بهینه برحسب معیارهای نوین در مسیر پیشرفت و تکامل قرار دارد [۳۹]. در واقع اتریوم سازگاری خوبی با اینترنت اشیا دارد. از طرفی دیگر، فابریک برای شبکه‌های اینترنت اشیا با داده‌های انبوه کاربرد دارد. فابریک بلاک‌چین را در مدل خدمات کلاینت ادغام کرده و ظرفیت بالایی تا TPS ۱۰۰۰۰ را پوشش می‌دهد. از طرفی دیگر، فابریک به محیط شبکه‌ای کنترل‌شده‌ای نیاز دارد و همانند اتریوم از دسترسی‌پذیری عمومی برخوردار نیست.

۱۴- مراجع

[1] P. K. Sharma, S. Y. Moon, and J. H. Park, "A Distri-buted Blockchain Based Vehicular Network Architecture in Smart City," Journal of Information Proces-sing Systems, vol. 13, no. 1, pp. 184-195, 2017.

[2] M. Castro and B. Liskov, " Practical Byzantine Fault Tolerance," Proc. Third Symp. Operating Systems Design and Implementation (OSDI '99), pp. 173-186, 1999.

[3] G. Zyskind, O. Nathan and A.S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," Proc. IEEE Security Privacy Workshops, pp. 180-184, 2015.

[4] C. Li and G. Chen, " On the security a class of image encryption schemes," in 2008 IEEE International Symposium on Circuits and Systems. pp. 3290–3293, 2008.

[5] S. Nakamoto, Bitcoin: "A Peer-to-Peer Electronic Cash System," 2008.

[6] L .Lamport, R.Shostak, and M. Pease, "The Byzantine generals problem," In Concurrency: the Works of Leslie Lamport , pp. 203-226,2019.

[7] M. Fitzi, U. Maurer, F. Matthias, and U. Maurer. "Efficient Byzantine agreement secure against general adversaries," International Symposium on Distributed Computing, pp. 134-148. Springer, Heidelberg, 1998.

[8] L. Tan, N. Tan, and N. Wang. " Future internet: The internet of things," In 2010 3rd international conference on advanced computer theory and engineering (ICACTE), vol. 5, IEEE, pp. V5-376, 2010.

[9] A. S. d. P. Crespo and L. I. C. Garc´ıa, "Stampery blockchain timestamping architecture," (bta)-version6, arXiv preprint arXiv:1711.04709.

[10] M. C. Vuran, O. B. Akan and I. F. Akyildiz, "Spatio-temporal correlation: Theory and applications for wireless sensor networks," Comput. Netw., vol. 45, no. 3, pp. 245, 2004.

[11] D. Romero, V. N. Ioannidis, and G. B. Giannakis, "Kernel-based reconstruction of space-time functions

[27] Proof of Stake Versus Proof of Work, Sep. 2015, [online]Available:https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf.

[28] J. Kwon, "Tendermint: Consensus without mining," 2014Available:http://tendermint.com/docs/tendermint{_}v04.pdf.

[29] M. B. Mollah and et. al., "Blockchain for Future Smart Grid: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 8, no. 1, pp. 18-43,1Jan.1,2021.

[30] G.D. Thackray, D.W .Rodgers, and D. Streutker – Geology. "Holocene scarp on the Sawtooth fault, central Idaho, USA, documented through lidar topographic analysis," Geology 41, no.6 , pp.639-642,2013.

[31] P. Mendki, "Blockchain enabled IoT edge computing" Proc. Int. Conf. Blockchain Technol., pp. 66-69, Marc. 2019.

[32] A. Chepurnoy, M. Larangeira and A. Ojiganov, "Rollerchain a blockchain with safely pruneable full blocks," arXiv preprint arXiv:1603.07926, 2016.

[33] C. Decker, J. Seidel and R. Wattenhofer, " Bitcoin meets strong consistency," Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN), pp. 13, 2016.

[34] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397-413, 2016.

[35] P. Mendki, "Blockchain enabled IoT edge computing, " Proc. Int. Conf. Blockchain Technol., pp. 66-69, Marc. 2019.

[36] A. Chepurnoy, M. Larangeira and A. Ojiganov, " Rollerchaina Blockchain With Safely Pruneable Full Blocks," White paper, 2016.

[37] S. Popov, "The tangle," Cit. On, vol. 2017, p. 131,Oct.2016.

[38] V. Buterin, "Toward a. 12-second block time," Ethereum. Blog, 2014.

[39] M. A. Khan, F. Algarni and M. T. Quasim, " Decentralised Internet of Things," in Decentralised Internet of Things. Studies in Big Data, Cham, Switzerland:Springer, vol. 71, 2020.

[40] ethdocs, "Ethereum Homestead documentation," Available: http://www.ethdocs.org/en/latest/.

[41] Q. Lin, H. Wang, X. Pei and J. Wang, " Food safety traceability system based on blockchain and EPCIS, " IEEE Access, vol. 7, pp. 20698-20707, 2019.

[42] A. Back and et. al., " Enabling blockchain innovations with pegged sidechains," Oct. 2014.

[43] X. Wang and et. al., " Survey on blockchain for Internet of Things," Comput. Commun., vol. 136, pp. 10-29, Feb. 2019.

[44] A. Miller, Y. Xia, K. Croman, E. Shi and D. Song, "The honeybadger of BFT protocols," Proc. 23rd ACM SIGSAC Conf. Comput. Commun. Security, pp. 31-42, 2016

[45] M. Neuder, D.J Moroz, R. Rao and D.C. Parkes. "Selfish behavior in the tezos proof-of-stake protocol," arXiv preprint arXiv:1912.02954 ,2019.

[46] S. Popov, O. Saa and P. Finardi, "Equilibria in the Tangle," https://arxiv.org/abs/1712.05385.2017.

on dynamic graphs," IEEE J. Sel. Topics Signal Process., vol. 11, no. 6, pp. 856-869, Sep. 2017.

[12] C. Jaffe, C. Mata and S. Kamvar, "Motivating urban cycling through a blockchain-based financial incentives system," Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. ACM Int. Symp. Wearable Comput. (UBICOMP/ISWC), pp. 81-84, 2017.

[13] Pilkington, "Blockchain Technology: Principles And Applications," in Research Handbook On Digital Transformations, pp. 225, 2016.

[14] C.Del-Valle-Soto, A. Rossa-Sierra. Cryptocurrencies: "A Futuristic Perspective or a Technological Strategy," In International Conference on Applied Human Factors and Ergonomics ,Springer, Cham .pp. 504-509, 2020.

[15] G. Bracha and S. Toueg, "Asynchronous consensus and broadcast protocols," Journal of the ACM (JACM), vol. 32, no. 4, pp. 824–840, 1985.

[16] P. L. Aublin, R. Guerraoui, N. Knežević, V. Quéma, and M. Vukolić, "The next 700 BFT protocols," ACM Trans. Comput. Syst., vol. 32, Jan. 2015.

[17] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in , Oct. 2015.

[18] T. Wu and X. Liang, "Exploration and practice of inter-bank application based on blockchain," 2017 12th International Conference on Computer Science and Education (ICCSE), pp. 219-224,2017.

[19] V. Daza, R. Di Pietro, I. Klimek and M. Signorini, CONNECT: "CONtextual NamE disCovery for blockchain-based services in the IoT," 2017 IEEE International Conference on Communications (ICC), pp. 1-6, 2017.

[20] S. King and S. Nadal, pcoin: "Peer-to-peer crypto-currency with proof-of-stake," Self-Published Paper, vol. 19, August 2012.

[21] M. Bastiaan, "Preventing the 51%-attack: A stochastic analysis of two phase proof of work in Bitcoin," Proc. 22nd Student Conf. IT, Jan. 2015, [online] Available: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventing-the-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf.

[22] S. Motepalli, P. Vilain, and H. A. Jacobsen, "Fabric Unit: A Framework for Faster Execution of Unit Tests on Hyperledger Fabric," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-3. 2020.

[23] G. Wood, "Ethereum: A secure decentralised gen-eralised transaction ledger," Ethereum Project ellow Paper, 2014.

[24] J. McKinney, "Light client protocol," in github .com /ethereum /wiki/wiki/Light-client-protocol, November 2017.

[25] A. M. Antonopoulus, "Mastering Bitcoin in Program the Open Blockchain," O'Reilly Media Inc., ISBN 978-1-491-95438-6.2017.

[26] N. Szabo, " The idea of smart contracts," 1997.

[47] S. Nakamoto, Bitcoin: “A Peer-to-Peer Electronic Cash System Bitcoin: A Peer-to-Peer Electronic Cash System,” Nov 2008.

[48] H. N. Dai, Z. Zheng and Y. Zhang, “ Blockchain for Internet of Things: A Survey,” in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076-8094, Oct. 2019.

[49] T. Crain, V. Gramoli, M. Larrea and M. Raynal, DBFT: “Efficient byzantine consensus with a weak coordinator and its application to consortium blockchains,” 2017.

[50] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” 2016 IEEE Symposium on Security and Privacy (SP), pp. 839-858, 2016.

[51] D. Demirel, J .Lancrenon. “ How to Securely Prolong the Computational Bindingness of Pedersen Commitments,” IACR Cryptol. ePrint Arch. P.584, 2015.

[52] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, ” Proceedings of IEEE Symposium on Security and Privacy (SP), pp. 839-858, 2016.

[53] T. M. Fernández-Caramés and P. Fraga-Lamas, “A review on the use of blockchain for the Internet of Things,” IEEE Access, vol. 6, pp. 32979-33001, 2018.

[54] R. Michaelis, “Evaluierung und Implementierung von Orakeln zur Bereitstellung von externen Daten für Smart Contracts in Ethereum.”

[55] D. Johnson. “Blockchain-Based Voting in the US and EU Constitutional Orders,” A Digital Technology to Secure Democratic Values?. European Journal of Risk Regulation, vol. 12, no. 2, 330-358,2019.

[56] P. Lade, R. Ghosh and S. Srinivasan, “Manufacturing analytics and industrial Internet of Things,” IEEE Intell. Syst., vol. 32, no. 3, pp. 74-79, May/Jun. 2017.

[57] L.J .Riley, G. Kotsialou, A. Dhillon, T. Mahmoodi P.J. McBurney and R. Pearce. “Deploying a shareholder rights management system onto a distributed ledger,” International Conference on Autonomous Agents and International Systems (AAMAS). 2019.

[58] S. King, S. Nadal, Ppcoin: “Peer-to-peer crypto-currency with proof-of-stake, Self-Published Paper,” vol. 19, August 2012.

[59] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), pp. 618-623, Mar. 2017.

[60] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert and P. Saxena, “A secure sharding protocol for open blockchains,” Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), pp. 17-30, 2016.

[61] M. Macdonald, L. Liu-Thorrold and R. Julien: “The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin,” 2017.

[62] Y. Marcus, E. Heilman and S .Goldberg. “Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network,” IACR Cryptol. ePrint Arch., vol. 236, 2018.