بررسی روش‌های اجماع بلاک‌چین‌های مورد استفاده در اینترنت اشیا

حسین شعله‌رسا[۱]، محمدعلی آصف[۱]، کاظم فولادی قلعه[۲]

[۱]دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
{h.sholehrasa,maasef}@ut.ac.ir
[۲]استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛
سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده

با توسعه و فراگیری مفاهیم فناوری بلاک‌چین و ملموس شدن کاربردهای متنوع آن، فناوری‌های دیگر نظیر اینترنت اشیا نیز با آن آمیخته شده‌اند. بلاک‌چین، دفتر کل توزیع‌شده‌ای است که اغلب به‌صورت غیرمتمرکز توسط گره‌های متصل به شبکه اداره می‌شود. این سازوکار نیاز به الگوریتم‌هایی برای اثبات درستی پردازش‌ها و عدم تقلب دارد که اجماع نامیده می‌شود. روش‌های مختلفی برای اجماع وجود دارد، اما در فضای اینترنت اشیا علاوه بر اثبات درستی نقل و انتقالات داده‌های درون شبکه، مفاهیم جدیدی مانند اثبات و راستی‌آزمایی موقعیت جغرافیایی و وجود فیزیکی نیز مطرح است. در سالیان اخیر با رواج بیشتر رمزارزها، ایده‌ها و پروژه‌های زیادی برای ایجاد چنین بستری مطرح شده است که از پروژه مطرح بازار بنام «هلیوم» تا اجماع نوآورانه‌ای مانند G-PBFT و LH-Raft که از اجماع اختصاصی خود برای ایجاد یک شبکه بیسیم امن و اثبات وجود گره‌ها در موقعیت جغرافیایی‌شان استفاده می‌کنند تا خدمات مورد نیاز دستگاه‌های مبتنی بر اینترنت اشیا را فراهم کنند. در این مقاله روش‌های اجماع متمرکز بر اثبات مکان از جنبه‌های هدف، کاربردها، نحوه کارکرد و توزیع پاداش مورد بررسی و مقایسه قرار خواهند گرفت تا گزینه‌های بهینه شناسایی شوند.

کلمات کلیدی: بلاک‌چین، الگوریتم اجماع، اینترنت اشیا، رمزارز، زنجیره‌ی بلوکی، اثبات مکان.

۱ مقدمه

۱.۱ بلاک‌چین

بلاک‌چین فناوری نوظهوری برای ذخیره‌سازی غیرمتمرکز[۱] داده است که در سالیان اخیر با توجه به مزایای پرشمار آن مورد توجه حوزه‌های مختلف قرارگرفته است. بلاک‌چین دفترکل توزیع‌شده‌ای است که شبکه‌ای نظیر به نظیر[۲] تشکیل می‌دهد. داده‌ها در این شبکه که شامل تراکنش‌ها و قطعه کدهای قابل اجرا به‌نام «قرارداد هوشمند»[۳] هستند، به‌صورت تغییرناپذیر در بلوک‌هایی قرار می‌گیرند که هر یک هش[۴] منحصر به‌فردی دارند. نحوه ایجاد و تأیید هش در هر شبکه بر مبنای الگوریتم‌های متفاوتی می‌تواند باشد. معمولاً در طی استفاده از این سیستم‌ها، نیاز به اعتماد به شخص ثالثی نیست. همچنین مدیریت و تصمیم‌گیری در آنها معمولاً بر دوش یک تصمیم‌گیرنده‌ی مرکزی نیست، بلکه به‌صورت انجمن محور[۵] است.

این ویژگی‌ها که بخشی از مشخصه‌های زنجیره بلوک‌ها هستند، منجر به ادغام این فناوری با حوزه‌های مختلفی مثل برنامه‌های مالی غیرمتمرکز[۶]، آثار هنری، صنعت بازی‌های کامپیوتری، ذخیره داده‌های پزشکی، زنجیره تأمین و بسیاری موارد دیگر شده است. یکی از این حوزه‌ها، اینترنت اشیا است [۱].

۲.۱ اینترنت اشیا و بلاک‌چین

اینترنت اشیا[۷] سیستمی از دستگاه‌های مرتبط به یکدیگر است که قابلیت انتقال اطلاعات روی شبکه بدون نیاز به انسان را دارد. چیزها/ اشیا، برای مثال می‌تواند ماشینی باشد که سنسورهای درونی آن به راننده اخطار زیاد یا کم بودن فشار لاستیک می‌دهد. همین‌طور میتواند دستگاهی باشد که در قلب کاشته شده و وضعیت قلب را دریافت و پردازش می‌کند.

اینترنت اشیا در عصر کنونی به‌طور گسترده‌ای برای جمع‌آوری داده‌ها از حسگرها و انجام وظیفه خاص با توجه به نیازمندی‌های تعریف شده، در حال استفاده است. برای محقق‌سازی این امر نیاز به شبکه‌های متصل به‌هم برای تبادل داده‌ها وجود دارد. این شبکه باید امن و بلادرنگ[۸] باشد تا اطلاعات با تأخیر بسیار کم و در پروتکلی امن جابجا شود. در بعضی از حوزه‌ها مثل مراقبت‌های بهداشتی، اطلاعات ذخیره شده نیز باید از امنیت بالایی برخوردار باشد. از مشکلات بزرگ اینترنت اشیا حریم خصوصی و امنیت آن است. یکی از حمله‌های بزرگی که در این مورد رخ داده است، حمله بزرگ Mirai بود. برای حل این دو مشکل می‌توان از بلاک‌چین استفاده نمود. با این وجود، در طی پیاده‌سازی یک سیستم مبتنی بر بلاک‌چین برای اینترنت اشیا، محدودیت‌های ذخیره‌سازی، برق و توانایی محاسباتی دستگاه‌های اینترنت اشیا چالش برانگیز

[1] Decentralized
[2] Peer-to-peer
[3] Smart Contract
[4] Hash
[5] Community-based
[6] Decentralized Finance Applications (dApps)
[7] Internet of Things
[8] Real-time

است [۲]، [۳].

۳.۱ مکانیزم‌های اجماع

همان‌طور که پیش‌تر گفته شد، معمولاً مدیریت و تصمیم‌گیری پروژه‌های غیرمتمرکز بر عهده گروهی از تصمیم‌گیران دخیل در پروژه می‌باشد. معنای کلمه اجماع[۹] به‌صورت خلاصه توافق اعضای یک گروه برای تصمیم‌گیری است. اجماع از اجزای مهم یک سیستم غیرمتمرکز قدرت گرفته از زنجیره بلوکی است [۴].

۴.۱ اهمیت استفاده از اجماع بهینه

با استفاده از پروتکل‌های اجماع کلاسیک‌تر احتمال آسیب‌پذیری به حمله سیبیل[۱۰] [۵]، هزینه زیاد محاسباتی و مقیاس پذیری وجود دارد. الگوریتم‌های اجماع که به موقعیت جغرافیایی دستگاه‌ها توجه می‌کنند تا حد خوبی مشکل مقیاس‌پذیری و هزینه زیاد محاسبات را حل کرده‌اند. بعضی از این الگوریتم‌ها به‌جای استفاده از تمامی دستگاه‌های اینترنت اشیا، از منتخبی از آنها برای الگوریتم اجماع خود استفاده می‌کنند.

در ادامه این مقاله، موضوعات زیر را مورد بررسی قرار می‌دهیم:

- سیر تکاملی و جزئیات روش‌های اجماع مورد استفاده در بلاک‌چین ها را مرور می‌کنیم.
- به بررسی دقیق‌تر اجماع‌های بهینه می‌پردازیم.
- و مشخصه‌هایی برای سنجش روش‌های اجماعی که موقعیت مکانی را مد نظر دارند تعریف می‌کنیم.

۲ الگوریتم‌های اجماع

۱.۲ پیش‌نیاز: مفهوم اجماع

در یک سیستم متمرکز مثل شرکت، کارمندان در زمان مشخصی حاضر و در دسترس هستند اما در سیستم‌های غیرمتمرکز بدین شکل نیست. در نتیجه، الگوریتم‌های اجماع باید دارای یک حداقل برای تصویب یک تغییر باشند. به‌طور مثال اگر ۵۱٪ از گره‌های یک شبکه در الگوریتم اجماع بلاک‌چین به توافق برسند که اطلاعات را آپدیت و به‌روزرسانی کنند، این اتفاق خواهد افتاد. الگوریتم اجماع یک روش است که از طریق آن، تمام افراد فعال در شبکه بلاک‌چین به یک توافق مشترک درباره وضعیت حال حاضر دفترکل توزیع‌شده دست می‌یابند. بدین ترتیب، الگوریتم‌های اجماع، اعتبار را در شبکه بلاک‌چین و اعتماد را بین گره‌ها یا همتایان ناشناس در محیط محاسباتی توزیع‌شده ایجاد می‌کنند. اساساً پروتکل اجماع اطمینان حاصل می‌کند هر بلاک جدید که به بلاک‌چین اضافه می‌شود، تنها نسخه واقعی است که توسط تمام گره‌ها مورد توافق واقع شده است. پروتکل اجماع بلاک‌چین شامل اهداف خاصی نظیر دست‌یابی به توافق، همکاری، حق مساوی

[9] Consensus
[10] sybil

هر گره و حضور اجباری هر گره در فرایند اجماع است. در نتیجه، الگوریتم اجماع در صدد دستیابی به توافق مشترکی است که توسط کل شبکه حاصل شده باشد. الگوریتم‌های اجماع کاربردهای دیگری هم دارند، مانند:

- تصمیم‌گیری در مورد اینکه آیا یک تراکنش صلاحیت تأیید و ذخیره روی دفترکل توزیع‌شده را دارد یا خیر؛
- انتخاب گره‌ها برای مدیریت امور روی دفترکل توزیع‌شده؛
- تضمین یک‌دست‌سازی اطلاعات روی سیستم‌های سرویس‌دهنده به شبکه.

۲.۲ پیش نیاز: روش‌های اجماع متداول مورد استفاده در شبکه‌های بلاک‌چین

در این بخش به بررسی اجمالی تعدادی از روش‌های اجماع متداول می‌پردازیم.

اثبات کار (Proof-of-work). اجماع مورد استفاده در اولین شبکه بلاک‌چین بود که در سال ۲۰۰۹ در رمزارز بیت‌کوین[11] [۶] استفاده شد. در این مدل، داده‌هایی به کمک تابع هش SHA-۲۵۶ در بلاک‌ها ذخیره می‌شوند. در میان گره‌های حاضر در شبکه، عضوی که هش با مشخصه‌های مورد نیاز و تعریف شده را بیابد، برای گرفتن تأیید، آن را به همه شبکه ارسال می‌کند. در صورتی که بیشتر از نیمی از شبکه آن را تأیید کنند، بلاک معتبر شناخته می‌شود و با هش پیدا شده بسته می‌شود. سپس گره‌ای که هش را پیدا کرده است، پاداش دریافت می‌کند. لازم به ذکر است که این عملیات به‌وسیله پردازش سخت‌افزارهای متصل به شبکه انجام می‌شود. از معایب آن می‌توان به مصرف برق و حمله ٪۵۱ اشاره کرد.

اثبات سهام (Proof-of-stake). کارکرد این مدل اجماع نیازی به دستگاه سخت‌افزاری ندارد، چرا که گره‌های حاضر در شبکه، طبق تعداد سهامشان به‌صورت تصادفی (تعداد توکن یا همان سهام بیشتر باعث افزایش شانس و قدرت می‌شود) در بستن بلاک معتبر ایفای نقش می‌کنند. در واقع با اختصاص رمزارز به یک شبکه، در یک مسابقه شرکت داده می‌شویم. همانند قرعه‌کشی بانکی که به‌عنوان مثال هر ۲۰ دلار یک امتیاز برای شما محاسبه می‌شود و هرچه امتیاز شما بیشتر باشد قاعدتاً شانس بیشتری هم برای برنده شدن خواهید داشت.

اثبات فعالیت (Proof-of-activity). درواقع ترکیبی از الگوریتم اجماع اثبات کار و اثبات سهام است. مرحله ابتدایی که استخراج است، از الگوریتمی مشابه گواه اثبات کار استفاده می‌شود و سپس با رفتن به بلوک بعدی از الگوریتمی شبیه به الگوریتم گواه اثبات سهام کمک می‌گیرد [۷].

[11] Bitcoin

۳.۲ اجماع‌های متمرکز بر موقعیت مکانی

۱.۳.۲ PoC (Proof of Coverage)

شبکه هلیوم. PoC الگوریتم اجماع مورد استفاده در رمزارز هلیوم[۱۲] [۷] است. در ادامه به بررسی اجماع مورد استفاده در این شبکه می‌پردازیم. این شبکه توسط تیم باتجربه‌ای با هدف فراهم کردن ارتباط دستگاه‌های اینترنت اشیا در شبکه‌ای غیرمتمرکز و برطرف کردن کمبودها و نقص‌های فعلی زیرساخت‌های موجود راه اندازی شده است. هلیوم یک شبکه بی‌سیم گسترده و غیرمتمرکز قدرت گرفته از بلاک‌چین برای اینترنت اشیا است که در سال ۲۰۱۹ راه‌اندازی شد. گره‌های شبکه دارای هات‌اسپات[۱۳]هایی هستند که ترکیبی از دستگاه‌های مودم روتر بی‌سیم و ماینر بلاک‌چین می‌باشند. ماینرهای متصل به شبکه با توکن HNT با توجه به پارامترهای مختلفی پاداش خود را دریافت می‌کنند. هلیوم شبکه خودش را «شبکه مردم»[۱۴] نامیده است. برای تبدیل شدن به یک ماینر می‌توان یکی از دستگاه‌های برندهای ارائه دهنده آن را خریداری کرد و یا به‌دست خود ساخت. هر دستگاه می‌تواند تا محدوده‌ای بالغ بر ۱۰ کیلومتر (محدوده فرکانسی تحت پروتکل Lora WAN [۸]) را پوشش دهد. این محدوده فرکانسی معمولاً طبق قانون‌گذاری مقررات رادیویی کشورها مشکلی ندارد و برای عموم آزاد است.

در این شبکه هر چند بلاک یک بار، وضعیت هات‌اسپات‌ها به‌صورت مداوم با سازوکاری به‌نام PoC Challenge مورد بررسی قرار می‌گیرد. داده‌های اثبات‌ها در بلاک‌ها ذخیره می‌شود که تأیید قطعی از پوشش وایرلسی است که توسط گره‌های شبکه ساخته شده است. تا به امروز میلیون‌ها چالش صادر و پردازش شده است.

نحوه دقیق کارکرد چالش‌ها بدین شکل است [۷]:

- چالشگر[۱۵]: هات‌اسپاتی که چالش را می‌سازد و ارسال می‌کند. هات اسپات‌ها به‌طور متوسط یک بار در هر ۳۰۰ بلاک چالش ارسال می‌کنند.
- انتقال‌دهنده[۱۶]: مخابره‌کننده یا چالش‌شونده نیز می‌تواند نامیده شود. این هات‌اسپات هدف چالش می‌باشد و مسئول انتقال داده‌ی چالش به هات اسپات‌های مجاور (شاهدها) برای ثبت شاهد می‌باشد.
- شاهد[۱۷]: هات اسپات‌هایی که از لحاظ جغرافیایی به چالش‌شونده نزدیک هستند و وجود هات‌اسپات چالش‌شونده در فرایند چالش را بعد از اینکه به آنها منتقل شد گزارش می‌کنند و در واقع شهادت می‌دهند.

[12] Helium
[13] Hotspot
[14] The People's Network
[15] Challenger
[16] Transmitter or Challengee
[17] Witness

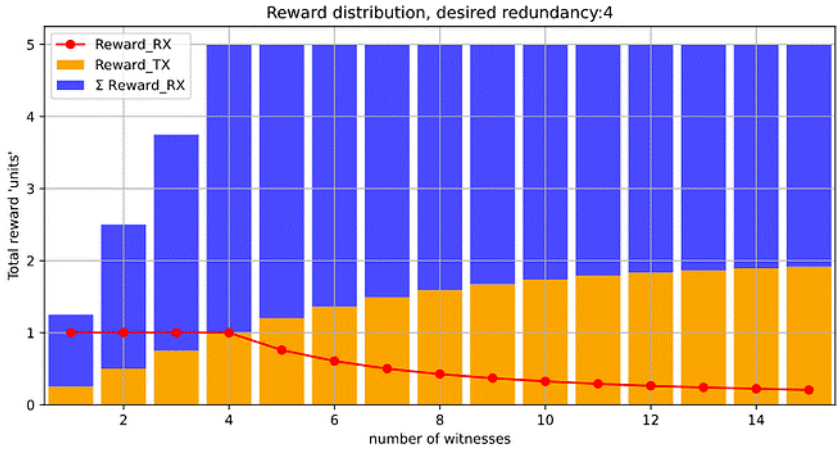
جزئیات عملیات چالش. هات‌اسپات‌ها پس از انجام چالش مقداری توکن HNT (توکن شبکه هلیوم) را به عنوان پاداش دریافت می‌کنند. چالشگر ابتدا یک کلید عمومی و خصوصی زودگذر می‌سازد تا در چالش استفاده شود. کلید عمومی و خصوصی SHA256 هر دو همراه با هش بلاک فعلی به عنوان یک درخواست PoC ذخیره می‌شوند. اگر درخواست معتبر باشد و توسط بلاک‌چین تأیید شود، هش بلاکی که رسید در آن ظاهر می‌شود با هش کلید عمومی زودگذر و هویت و اطلاعات چالشگر برای ایجاد آنتروپی قابل تأیید ترکیب می‌شود. سپس یک عدد رندوم از طریق این آنتروپی ایجاد می‌شود و برای انتخاب یک هات‌اسپات تصادفی از کل شبکه (نه لزوماً مودم‌های نزدیک چالش‌شونده) استفاده می‌شود. وقتی بسته چالش ساخته شد، به انتقال‌دهنده از طریق شبکه همتا به همتا هلیوم منتقل می‌شود. چالش‌شونده مورد هدف، بسته چالش را دریافت می‌کند و بیرونی‌ترین لایه را به‌وسیله کلید خصوصی و کلید عمومی زودگذر این چالش رمزگشایی می‌کند. کلید عمومی زودگذر در بسته PoC نمایش داده می‌شود و هات‌اسپات دریافت‌کننده بلاک‌چین را برای دریافت PoC فعال، SHA256 مربوطه کلید عمومی بررسی می‌کند و سریعاً نتیجه را به بسته در شبکه هلیوم منتقل می‌کند. هر تعداد از هات‌اسپات‌های نزدیک به چالشگر از لحاظ جغرافیایی، این داده را دریافت می‌کنند و به‌عنوان شاهد، وجود چالش‌شونده را اثبات خواهند کرد.

پاداش‌دهی در فرایند PoC. به‌صورت کلی دو متغیر برای پاداشدهی وجود دارد: تعداد شاهدین در مدل HIP15 و تعداد هات‌اسپات‌ها در هر فضای ۶ضلعی تعریف‌شده در HIP17.

در مدل HIP15 برای هر چرخه چالش، هر پاداش بین هات‌اسپات‌هایی که در فرایند نقش داشته‌اند تقسیم می‌شود. اگر هات اسپاتی در این چرخه به‌عنوان شاهد نقش داشته باشد، سهم ۳۱٪.۵ از پاداشی که به انتقال‌دهنده‌ها داده می‌شود خواهد داشت. برای مثال اگر ۵ هات‌اسپات شاهد در یک چالش موفق، شرکت داشته باشند، هر هات‌اسپات یک پنجم از ۳۱٪.۵ از پاداش در نظر گرفته شده برای چالش را می‌گیرد. برای هر انتقال‌دهنده، هرچه تعداد شاهدان بیشتر باشد، پاداش انتقال‌دهنده بیشتر خواهد بود.

در مدل HIP17 اگر تعداد هات‌اسپات‌های هر منطقه از هدف تراکمی مورد نظر بیشتر شود، شاهد کمتر پاداش می‌گیرد. هر محدوده‌ی جغرافیایی هدف تراکمی خود را دارد و با بیشتر شدن تعداد ماینرها و در واقع شاهدها از تعداد مشخصی، درآمد چالش‌شونده افزایش پیدا نمی‌کند و درآمد شاهدها کم می‌شود.

تایید اثبات. زمانی که چالشگر مجموعه کامل رسید شاهدها و انتقال‌دهنده‌های فرآیند را دریافت کرد یا زمان سپری شده از زمان صدور چالش، از زمان تعیین شده بالاتر رفت چالش PoC کامل در نظر گرفته می‌شود. در این مرحله چالشگر رسید اثبات را به عنوان یک تراکنش به بلاک‌چین ارائه می‌کند تا توسط گروه اجماع فعلی تأیید شود. به‌دلیل آنکه مراحل انجام شده توسط چالشگر برای ساخت و کامل کردن اثبات به‌راحتی قابل انجام مجدد هستند، اعضای گروه اجماع می‌توانند مشروعیت اثبات را تأیید کنند. به طور مشخص، چالشگر کلید زودگذر سری را که برای به انجام درخواست اصلی PoC و رمزگذاری هر لایه از بسته چالش استفاده می‌کند را فاش می‌کند. این اطلاعات مهم، که تا زمان انتشار رسید پنهان بوده است، امکان ایجاد مجدد آنتروپی قطعی را می‌دهد.



شکل ۱: میزان پاداش به‌ازای تعداد هات‌اسپات‌های فعال در یک منطقه [۷]

هلیوم از پروتکل اجماع نوآورانه و اختصاصی خود استفاده می‌کند. این پروتکل به‌منظور اهمیت بخشیدن به ویژگی‌های کلیدی زیر ایجاد شده است:

- بدون نیاز به اجازه: هر هات اسپات مطابق با قوانین اجماع و مشخصه‌های شبکه باید بتواند به‌صورت آزادانه در شبکه هلیوم شرکت کند.
- طراحی کاملا غیرمتمرکز: هیچ مشوق و انگیزه‌ای برای استفاده از عواملی مثل مصرف کم انرژی برای استقرار سخت‌افزار بیشر از حد نیاز و متمرکز شدن در یک نقطه وجود ندارد.
- بر اساس کار مفید: دستیابی به اجماع شبکه باید مفید و قابل استفاده مجدد برای شبکه باشد. در سیستم‌های مبتنی بر توافق مثل بیت‌کوین، کارهایی که برای دستیابی به اجماع انجام می‌شود فقط برای یک بلوک خاص معتبر است. در مقابل، در سیستم اجماع هلیوم باید کارهایی انجام شود که علاوه بر ایمن‌سازی شبکه بلاک‌چین، برای شبکه مفید و قابل استفاده باشد.
- نرخ بالای تراکنش‌های تأییدشده: پروتکل باید بتواند به تعداد زیادی تراکنش در ثانیه دست یابد و هنگامی که تراکنش توسط بلاک‌چین مشاهده شد، تأیید شده منظور می‌گردد. کاربرانی که داده‌های دستگاه را از طریق شبکه هلیوم ارسال می‌کنند، نمی‌توانند زمان‌های طولانی حل و فصل بلاک را که معمولاً در سایر بلاک‌چین‌ها وجود دارد را متحمل شوند.

Honey Badger BTF. پروتکل اجماع هلیوم بر اساس توزیعی از پروتکل Honey Badger BFT (HBBFT) [۹] نوشته شده است. HBBFT بر اساس مجموعه‌ای از تحقیقات است که در ابتدا توسط اندرومیلر در دانشگاه Illinois آغاز شد. پروتکل HBBFT یک پروتکل پخش اتمی با زمان غیریکسان است که برای ایجاد گروهی از گره‌های شناخته‌شده برای دستیابی به اجماع در مورد پیوندهای غیرقابل اعتماد

طراحی شده است. در هلیوم، یک گروه اجماعی از اعتبارسنج‌های منتخب، تراکنش‌های رمزگذاری شده را به‌عنوان ورودی دریافت می‌کنند و قبل از تشکیل یک بلاک و افزودن آن به بلاک‌چین به توافق مشترک در مورد ترتیب این تراکنش‌ها می‌رسند.

پروتکل HBBFT متکی بر طرحی است که به‌عنوان Threshold encryption شناخته می‌شود. با استفاده از این طرح، معاملات با استفاده از یک کلید عمومی مشترک رمزگذاری می‌شوند و تنها زمانی رمزگشایی می‌شوند که گروه اجماع انتخاب شده برای رمزگشایی آنها باهم همکاری کنند. استفاده از Threshold encryption هلیوم را قادر می‌سازد تا به تراکنش‌های غیرقابل سانسور دست یابد.

انتخابات گروه اجماع و سوددهی یک گروه اجماع جدید، یکبار در هر دوره انتخاب می‌شود. در حال حاضر ۴۰ عضو برای هر گروه اجماعی انتخاب شده‌اند، همان‌طور که در متغیر زنجیره‌ای num_consensus_members تعریف شده است. با توجه به پارامترهایی که پیش‌تر توضیح داده شد، می‌توان برآورد کلی از درآمد تخمینی یک هات‌اسپات با درنظرگیری تعداد هات‌اسپات‌های اطراف صفر، کمی و تعدادی زیادی را بیان کرد که در این لحظه در حدود 12 HNT به‌ازای هر دستگاه به‌صورت ماهیانه می‌باشد.

۲.۳.۲ LH-Raft

این الگوریتم از پروتکل اصلی Raft [۱۰] الهام گرفته‌است. الگوریتم Raft از نظر کارایی و تحمل خطا[18] همانند الگوریتم Paxos [۱۱] می‌باشد و ساده شده این الگوریتم است. Raft، Paxos و PBFT [۱۲] از نظر توان عملیاتی[19] توانایی رسیدگی به هزاران درخواست، زمان پردازش کم و هزینه محاسبات کم را دارا هستند. این ویژگی‌ها، این الگوریتمها را برای استفاده در اینترنت اشیا مناسب می‌کنند. همچنین مقیاس‌پذیری آن‌ها کم است به‌همین خاطر بهتر است در بلاک‌چین‌های خصوصی که اهراز هویت دارند مورد استفاده قرار گیرند.

الگوریتم LH-Raft [۱۳] با استفاده از پروتکل اجماع سلسله‌مراتبی و آگاه از مکان[20] مشکل مقیاس‌پذیری را حل کرده است. برای جلوگیری از حمله‌های مختلف و تشکیل یک گره اجماع داخلی، اطلاعات جغرافیایی دستگاه شامل طول و عرض جغرافیایی و برچسب زمانی[21] جمع‌آوری می‌شوند. این الگوریتم کارایی بهتری دارد و همچنین هزینه ارتباط و تأخیر اجرای الگوریتم آن نیز کم است. زمانی که تعداد گره‌های در شبکه زیاد شود، اختلاف زیادی در هزینه ارتباط و تأخیر اجرای الگوریتم با دیگر الگوریتم‌ها ایجاد می‌شود که نشان‌دهنده مقیاس‌پذیری بالا این الگوریتم می‌باشد.

الگوریتم LH-Raft ابتدا گره‌های داوطلبی را انتخاب می‌کند که در هر زیرلایه شامل لایه برگ[22]، لایه وسطی (میانی)[23] و لایه بالایی شبکه بلاک‌چینی، به اجماع کمتری نیاز دارد. سپس یک گروه محلی از کاندیداها بر اساس امتیاز فاصله و شهرت گره‌ها تشکیل می‌دهد. وظیفه‌ی این گره‌ها انتخاب رهبران محلی

[18] Fault-tolerance
[19] Throughput
[20] Location-aware
[21] Timestamp
[22] Leaf layer
[23] Middle layer

جدول ۱: مقایسه نتایج Raft و LH-Raft؛ n تعداد تمام دستگاه‌های اینترنت اشیا و c تعداد گروه‌های منتخب است.

الگوریتم	سربار ارتباط	هزینه ارتباط
Raft	$O(n^2)$	n^2
LH-Raft	$O(c^2)$	n^2/c^2

می‌باشد. در مرحله بعد، تمام رهبران محلی از چند لایه برگ و بقیه گره‌های کاندیدا دوباره رهبر بالاتر را انتخاب می‌کنند. برای اجماع لایه بالاتر از طرح امضای آستانه[۲۴] استفاده می‌شود. در آخر رهبر اصلی انتخاب می‌شود. این طرح شبکه بلاک‌چینی، یک سلسله‌مراتبی است که بر اساس اطلاعات منطقه‌ای دستگاه‌های اینترنت اشیا و استفاده از رونوشت‌های محلی و جهانی است. این امر سبب حفظ ثبات برای تمام تراکنش‌های بلاک‌چینی در تمام لایه‌ها است.

اگر گره‌های متقلب در الگوریتم PoW بیشتر از ٪۵۰ تعداد، الگوریتم PBFT بیشتر از ٪۳۳.۳ تعداد و الگوریتم LH-Raft در حالت غیر بیزانسی (خرابی گره، تأخیر شبکه، گم شدن بسته) بیشتر از ٪۵۰ تعداد و در حالت بیزانسی بیشتر از ٪۳۳.۳ تعداد باشد می‌توانند دفترکل تراکنش‌ها را عوض کنند. دو مورد مهم از نتایج تئوری این الگوریتم می توان به جدول ۱ اشاره کرد [۱۳].

۳.۳.۲ GPBFT

این الگوریتم از الگوریتم اجماع PBFT بهره برده است. الگوریتم G-PBFT [۱۴] به اطلاعات جغرافیایی دستگاه‌های اینترنت اشیا ارزش بیشتری می‌دهد. این امر سبب محافظت در مقابل حمله سیبیل می‌شود. الگوریتم PBFT [۱۲] پروتکلی مناسب برای اینترنت اشیا با شبکه‌ای با اندازه کوچک است. گره‌های شرکت کننده به‌راحتی نمی‌توانند به شبکه اضافه یا حذف شوند. ترافیک بالا سربار شبکه ($O(n^2)$) و پویا نبودن سبب این می‌شود که برای شبکه اینترنت اشیای با گره‌های زیاد و پویا مناسب نباشد. الگوریتم G-PBFT این دو مشکل را حل می‌کند. دستگاه‌های اینترنت اشیا که به‌صورت ثابت هستند معمولاً از قدرت پردازشی بیشتری نسبت به بقیه دستگاه‌های اینترنت اشیا مثل موبایل دارند. لامپ هوشمند خیابان یک نمونه از دستگاه‌های ثابت می‌باشد. از جهتی دیگر، معمولاً شرکت‌ها صاحب این دستگاه‌ها هستند پس احتمال اینکه یک گره مخرب باشد کمتر است. به‌همین خاطر G-PFBT از دستگاه‌های ثابت استفاده می‌کند و برای بلاک‌چین‌های خصوصی و کنسرسیومی[۲۵] مناسب است.

در این الگوریتم دو نوع گره مشتری و تأییدکننده وجود دارد. تمام تأییدکننده‌ها باهم یک کمیته اجماع تشکیل می‌دهند. تراکنش‌هایی که توسط مشتری ساخته می‌شود را بین خود جابه‌جا می‌کنند تا سربار ارتباطات کم شود. علاوه بر اینکه اطلاعات جغرافیایی دستگاه‌ها توی هر تراکنش هست، باید به‌صورت دوره‌ای نیز موقعیت و پرچسب زمانی خود را بفرستند. برای این کار از Crypto Spatial Coordiantes (CSC)

[24] Threshold Signature Scheme
[25] consortium

جدول ۲: جدول انتخابات [۱۴]: چند نمونه CSC به همراه برچسب زمانی و تایمر جغرافیایی در الگوریتم G-PBFT

	CSC	برچسب زمانی	تایمر جغرافیایی
۱	5AH71r9wTRp9eHsqR	29/8/2022 18:00:00	0
۲	5AH71r9wTRp9eHsqR	29/8/2022 18:56:04	56:04
۳	5AH71r9wTRp9eHsqR	30/8/2022 00:00:00	06:56:04
۴	5AH71r9wTRp9eHsqR	30/8/2022 06:00:00	12:56:04
۵	5AH71r9wTRp9eHsqR	30/8/2022 12:00:00	18:56:04

استفاده می‌شود. قبل از اینکه انتخابات تأییدکننده اجرایی شود، یک سری گره وجود دارند که به‌عنوان تأییدکننده هستند. این گره‌ها اطلاعات دستگاه‌های اینترنت اشیاء که شامل CSC و برچسب زمانی‌شان می‌باشد را اعتبارسنجی می‌کنند.

الگوریتم G-PBFT همانند الگوریتم PBFT از Views و Phases یکسانی استفاده می‌کند ولی در الگوریتم G-PBFT لفظ جدید era معرفی شده است که می‌توان به‌عنوان یک اتصال چند PBFT متوالی در نظر گرفت. اگر زنجیره ثابت PBFTها عوض شود زنجیره از era آن به یک era جدید می‌رود.

۳ تحلیل مشخصه‌ها و خروجی اجماع‌های مبتنی بر موقعیت مکانی

۱.۳ مقایسه پروژه‌های کاربردی در اینترنت اشیا و بلاک‌چین

در جدول ۳ مقایسه بین چند پروژه کاربردی که به منظور همگام‌سازی بلاک‌چین و اینترنت اشیا طراحی شده‌اند انجام شده است. در این جدول اجماع اختصاصی هر پروژه، جزئیات هدف و سرویس اصلی و سخت‌افزار مرتبط با اینترنت اشیا بررسی شده است. بعضی از پروژه‌ها مانند هلیوم بخش بزرگی از بازار را تصاحب کرده‌اند، در حالی که بعضی دیگر در مراحل ابتدایی هستند و حتی به‌طور کامل برای استفاده عموم عرضه نشده‌اند. همچنین برخی پروژه‌ها از اجماع اختصاصی خود استفاده می‌کنند و برخی دیگر از الگوریتم‌های کلاسیک نظیر PoS بهره می‌گیرند. در بخش سخت‌افزاری نیز شاهد طیف قابل توجهی از دستگاه‌های گوناگون با اهداف مختلف هستیم.

۲.۳ مقایسه الگوریتم‌های اجماع

در جدول ۴ مقایسه‌ای بین الگوریتم‌های اجماع متداول و الگوریتم‌های جدیدتر و کاربردی در اینترنت اشیا انجام شده‌است. نمونه‌های با مدل بلاک‌چین بدون اجازه رویکرد غیرمتمرکزی را دنبال می‌کنند در حالی که نمونه‌های بااجازه کاربردی اغلب سازمانی دارند. الگوریتم‌های جدیدتر معمولاً از سرعت و مقیاس پذیری بیشتری برخوردار هستند و سربار محاسباتی را کاهش داده‌اند. الگوریتم‌های بررسی شده در این مقاله با

جدول ۳: مقایسه مشخصه‌های بلاک‌چین‌های مورد استفاده در حوزه اینترنت اشیا

پروژه	بلاک‌چین	الگوریتم اجماع	سرویس	دستگاه‌های اینترنت اشیا
Helium [7]	Helium	Proof of Coverage	شبکه غیر متمرکز	دستگاه‌های اینترنت اشیا
Slock.it [15]	Ethereum	PoW	فروشگاه کمیسیون	قفل الکترونیکی
ElectriCChain [16]	SolarCoin	PoS	پردازش اطلاعات پنل‌های خورشیدی	پنل خورشیدی
Filament [17]	Hardware-based Consortium Blockchain	PoS PoW	سرویس تراکنش برای اینترنت اشیاء تعبیه شده (embedded)	تراشه بلوک
JD.com [18]	BFT Blockchain	BFT	پلتفرم بلاک‌چین	دستگاه‌های اینترنت اشیا
LeewayHertz [19]	Public Blockchain	PoW	راه حل‌های اینترنت اشیاء-بلاک‌چین	ربات‌ها و دستگاه‌های صوتی
LO3 Energy [20]	Public Blockchain Solution	PoW	بازارگاه انرژی خورشیدی	پنل خورشیدی
Atonomi [21]	Atonomi	Atonomi	راه حل‌های اینترنت اشیاء-بلاک‌چین	دستگاه و خانه‌های هوشمند
UniquID [22]	Litecoin	PoW	خدمات یکپارچه در اینترنت اشیاء و بلاک‌چین	سنسورها, عملگرها و لوازم خانگی
Xage [23]	Fabric	PBFT	سرویس امنیتی	دلال‌های اقتصادی (brokers)

علامت * مشخص شده‌اند. به‌صورت کلی می‌توان گفت الگوریتم‌های G-PBFT و Proof Of Coverage و LH-Raft سرعت تراکنش و مقیاس‌پذیری بالا، سربار کم شبکه و محاسبات را به نسبت بقیه مکانیزم‌های اجماع دارا هستند.

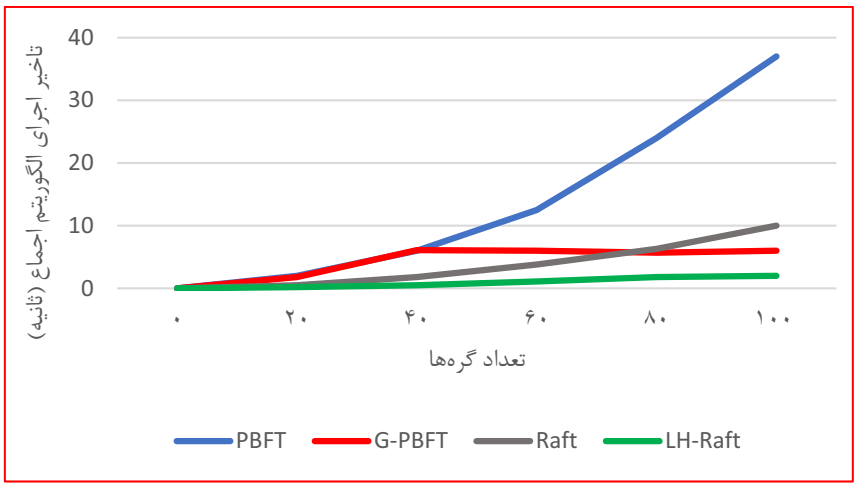
۳.۳ مقایسه کارایی الگوریتم‌های اجماع مورد بررسی

در شکل ۲ به بررسی کارایی الگوریتم‌های اجماع مورد بررسی پرداخته‌ایم. برای محاسبه کارایی الگوریتم‌ها، به‌جای معیار تراکنش بر ثانیه (TPS) از معیار تأخیر اجرا الگوریتم اجماع استفاده می‌کنیم. در واقع تأخیر را از زمانی که تراکنش به گره فرستاده می‌شود و بعد از اجرای الگوریتم اجماع در دفتر توزیع کل نوشته می‌شود، محاسبه می‌گردد. طبق نمودار، رشد الگوریتم PBFT به‌صورت نمایی می‌باشد. الگوریتم G-PBFT در تعداد گره کمتر، مثلاً ۴۰ عدد، به‌دلیل این که تأییدکنندگان به کمیته اضافه می‌شوند، رفتاری همچون

PBFT دارد .این در حالی است که از زمانی که انتخاب‌کنندگان جدید به کمیته اضافه نمی‌شوند مقدار تأخیر اجرای الگوریتم اجماع آن بیشتر نمی‌شود [۱۴]. الگوریتم Raft با افزایش گره، تأخیر اجماع آن افزایش می‌یابد. در بعضی قسمت‌ها با شیب ملایم این افزایش صورت می‌گیرد. در مقابل، الگوریتم LH-Raft تعداد کاندیداها کمتر است، چرا که با توجه به موقعیت مکانی گره‌ها انتخاب می‌شوند و این امر سبب تأخیر کم‌تر است. می‌توان گفت از گره ۱ تا ۱۰۰، تأخیر الگوریتم LH-Raft ٪۷۲ کمتر از Raft است [۱۳].

جدول ۴: مقایسه مشخصه‌های روش‌های اجماع متداول و روش‌های مورد استفاده در بلاک‌چین‌های مرتبط با اینترنت اشیا

الگوریتم	نوع بلاک‌چین	سرعت	مقیاس پذیری	سربار شبکه	سربار محاسباتی	تحمل تقلب	مثال استفاده شده
PoW	بدون اجازه	کم	کم	زیاد	زیاد	25%> قدرت محاسبات	BTC
PoS	بدون اجاره	کم	کم	زیاد	کم	50% > سهام	Peercoin
DPoS [24]	بدون اجازه	زیاد	کم	کم	کم	50% > اعتبارسنج‌ها	BitShares
PoA	بدون اجازه	کم	زیاد	کم	کم	50% > سهام آنلاین	Decred
PoSpace [25]	بدون اجازه	کم	کم	زیاد	کم	50% > فضا	SpaceMint
PoI [26]	بدون اجازه	کم	کم	زیاد	کم	50% > سهام	NEM
PoB [27]	بدون اجازه	کم	کم	زیاد	کم	50% > سکه‌ها	XCP
Proof of Coverage *	بدون اجازه	زیاد	زیاد	کم	کم	33.3% > کپی‌ها	Helium
G-PBFT*	بدون اجازه	زیاد	زیاد	کم	کم	33.3% > تأیید	
BFT	با اجازه	زیاد	کم	زیاد	کم	33.3% > کپی‌ها	Tendermint
PBFT*	با اجازه	زیاد	کم	زیاد	کم	33.3% > کپی‌های معیوب	Hyperledger
dBFT [28]	با اجازه	کم	زیاد	زیاد	کم	33.3% > کپی‌های معیوب	NEO
Hot Stuff [29]	با اجازه	زیاد	کم	کم	کم	33.3% > کپی‌ها	Libra
RAFT	با اجازه	زیاد	کم	کم	کم	50% > کپی‌ها	IPFS
LH-RAFT*	بدون اجازه	زیاد	زیاد	کم	کم	33.3% > گره‌ها	



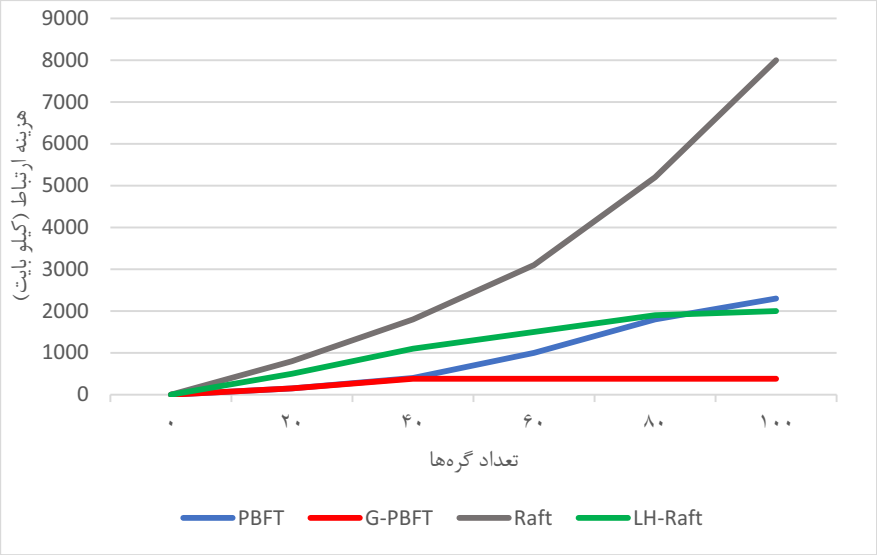
شکل ۲: مقایسه کارایی الگوریتم های اجماع موردبررسی [۱۳]، [۱۴]

۴.۳ مقایسه هزینه‌های ارتباطی در الگوریتم‌های اجماع موردبررسی

در شکل ۳ به بررسی هزینه‌های ارتباطی در اجماع‌های موردبررسی پرداخته‌ایم. برای محاسبه هزینه‌ی ارتباط از معیار هزینه ارتباط تمام گره‌ها که فقط یک تراکنش بلاک‌چینی انجام می‌شود، استفاده‌شده است. در الگوریتم PBFT با افزایش تعداد گره‌ها هزینه ارتباط با شیبی ملایمی در حال افزایش است ولی در G-PBFT بعد از حدود ۴۰ گره مقداری نزدیک به ۴۰۰ کیلوبایت را دارد و این روند به صورت تقریباً ثابت ادامه دارد [۱۴]. همچنان در حدود ۴۰ گره مقدار هزینه این دو الگوریتم یکسان است. در الگوریتم LH-Raft مقدار گره‌های زیر لایه‌ی برگ، میانی و بالایی به ترتیب ۲۰، ۴۰ و ۸۰ گره در حداکثر تعداد در نظر گرفته‌شده است [۱۳]. از گره ۱ تا ۲۰ به‌صورت رشد خطی به حدود ۵۰۰ کیلوبایت می‌رسد. به طور مشابه می‌توان گفت از گره ۱ تا ۸۰ نیز به‌صورت خطی رشد می‌کند و به نزدیک ۱۸۵۰ کیلوبایت می‌رسد. در مقابل، الگوریتم Raftبا افزایش گره‌ها هزینه ارتباط نیز با شیب بسیار افزایش می‌یابد.

۵.۳ ویژگی‌های مقایسه‌های انجام شده

در مقایسه‌های انجام شده به‌صورت مرحله به مرحله طیف گسترده‌ای از متغیرهای کیفی و کمی را در پروژه‌های این حوزه، الگوریتم‌های اجماع این حوزه و در نهایت جزئیات مشخصه‌های هر یک از الگوریتم‌های اجماع مورد توجه در این مقاله را بررسی و مقایسه نمودیم. در اغلب بررسی‌های ترویجی انجام‌شده در این حوزه، تنها مشخصه‌های مرسوم که در همه اجماع‌ها وجود دارد به عنوان متغیر در نظر گرفته شده‌اند، و در مدل‌های مبتنی بر موقعیت مکانی هم صرفاً مشخصه‌های مرتبط با راستی‌آزمایی داده‌ها مورد توجه قرار گرفته بود؛ اما در بررسی‌های انجام شده تلاش کردیم تا ویژگی‌های خاصی و تعیین‌کننده برای این رسته از اجماع‌های متمرکز بر اثبات موقعیت مکانی نیز در نظر گرفته شود تا روش بهینه مشخص شود. همچنین در اغلب بررسی‌های پیشین، مشخصه‌های فنی پروژه و الگوریتم محصولات برجسته در بازار همانند پروژه هلیوم،



شکل ۳: مقایسه هزینه ارتباط نمودارهای مورد بررسی [۱۳]، [۱۴]

در کنار روش‌های نوین، قرار نگرفته بود اما در این مقاله تلاش کردیم تا با کنار هم قراردادن و مقایسه‌ی آنها، به دید کلی جامع‌تر و بهتری دست یابیم.

۴ نتیجه‌گیری

الگوریتم‌های اجماع با به‌کارگیری در شبکه‌های بلاک‌چین در سالیان اخیر، به جایگاه بسیار مورد توجهی دست یافته‌اند. متخصصین تلاش می‌کنند تا با تحلیل مدل‌های پیشین و در نظر گرفتن تقاضاهای فعلی این حوزه، آنها را بهبود بخشند و روش‌های نوینی ابداع کنند. در این مقاله تلاش کردیم تا با انجام تحلیل‌های چند جانبه در خصوص الگوریتم‌های اجماع مورد استفاده در بلاک‌چین های توسعه داده شده برای ارتباط با اینترنت اشیا، بهینگی آنها را در زمینه‌های مختلف بسنجیم. در پایان می‌توان گفت با توجه به داده‌های به‌دست آمده، در صورت اولویت داشتن سرعت LH-Raft می‌تواند گزینه مناسب‌تری باشد. در صورت اهمیت بالاتر هزینه کم و پهنای باند بیشتر الگوریتم G-PBFT می‌تواند مورد استفاده قرار گیرد، و در حالتی که پیاده‌سازی در مقیاس انبوه و عرضه در بازار به‌مدت طولانی‌تر مهم باشد، الگوریتم Proof-of-Coverage مورد استفاده در هلیوم می‌تواند شبیه‌سازی شود.

الگوریتم‌های اجماع در سالیان اخیر دچار دگرگونی‌های بسیاری شده‌اند و همچنان فضای بسیاری برای رشد و به بلوغ رسیدن این حوزه‌ی نوظهور وجود دارد. الگوریتم‌های جدیدتر و مقایسه جنبه‌های دیگر این روش‌ها به‌عنوان سنجه تحلیل‌ها، و مقایسه و دسته‌بندی الگوریتم‌های کاربردی در موضوعات دیگر مثل ذخیره‌سازی داده‌های پزشکی و یا زنجیره تأمین می‌تواند موضوعات جالب توجه دیگر به‌عنوان موضوع پژوهش بیشتر علاقه‌مندان به این فضا قرار گیرد.

مراجع

[1] Zheng, Zibin, et al. “Blockchain challenges and opportunities: A survey”. International journal of web and grid services 14.4 (2018): 352-375.

[2] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, “Trust-based blockchain authorization for iot,” IEEE Transactions on Network and Service Management, 2021.

[3] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, “Controllable and trustworthy blockchain-based cloud data management,” Future Generation Computer Systems, V. 91, pp. 527-535, 2019.

[4] Bach, Leo Maxim, Branko Mihaljevic, and Mario Zagar. ”Comparative analysis of blockchain consensus algorithms”. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Ieee, 2018.

[5] J. R. Douceur, “The sybil attack,” International workshop on peer-to-peer systems, pp. 251-260, 2002.

[6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[7] Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, Rahul Garg, “Helium A Decentralized Wireless Network,” 2018.

[8] LoRa Alliance, “LoRaWAN - LoRa Alliance Technology,” 2014.

[9] Andrew Miller and Yu Xia and Kyle Croman and Elaine Shi and Dawn Song, “The Honey Badger of BFT Protocols,” 2016.

[10] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” Annual Technical Conference, p. 305–319, 2014.

[11] L. Lamport et al, “Paxos made simple,” ACM Sigact News, V. 32, pp. 18-25, 2001.

[12] M. Castro, B. Liskov et al, “Practical byzantine fault tolerance,” OSDL, V. 99, pp. 173-186, 1999.

[13] W. L. M. N. Hao Guo, “A Hierarchical and Location-aware Consensus Protocol for IoT-Blockchain Applications,” IEEE Transactions on Network and Service Management, 2020.

[14] L. Lao, X. Dai, B. Xiao and S. Guo, “G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications,” IEEE International Parallel and Distributed Processing Symposium, pp. 664-673, 2020.

[15] SlockIt, http://slock.it, (accessed: 2022/09/10).

[16] ElectriCChain, “Electricchain the solar energy blockchain project for climate change and beyond,” https://www.crunchbase.com/organization/electricchain, (accessed: 2022/09/10).

[17] Filament, “Filament’s industrial internet of things blockchain solution wins 2018 IoT innovator award,” 2018, https://www.crunchbase.com/organization/filamenthq, (accessed: 2022/09/10).

[18] JDChain, "JD enterprise blockchain service," https://blockchain.jd.com, (accessed: 2022/09/10).

[19] LeewayHertz, "Blockchain development for startups and enterprises," 2019.

[20] LO3, "LO3 energy the future of energy," https://lo3energy.com, (accessed: 2022/09/10).

[21] Atonomi, "Atonomi - bringing trust and security to IoT," https://atonomi.io, (accessed: 2022/09/10).

[22] UniquID, "UniquID incorporation blockchain identity access management," http://uniquid.com, (accessed: 2022/09/10).

[23] Xage, "Xage security," https://xage.com, (accessed: 2022/09/10).

[24] D. Larimer, "Delegated proof-of-stake (DPoS)," Bitshare whitepaper, 2014, https://www.geeksforgeeks.org/delegated-proof-of-stake/.

[25] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," Advances in Cryptology, p. 585–605, 2015.

[26] NEM, "NEM whitepaper," https://www.crunchbase.com/organization/nem, (accessed: 2022/09/10).

[27] J. Frankenfield, "Proof of burn," https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp, (accessed: 2022/09/10).

[28] NeoDocsBuilder, "NEO consensus mechanism," https://docs.neo.org/docs/en-us/basic/consensus/dbft.html, (accessed: 2022/09/10).

[29] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus with linearity and responsiveness," Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, p. 347–356, 2019.