MANDALA: A scalable blockchain model with mesh-and-spoke network and H-PBFT consensus algorithm

نگارنده:

محمد قهری

استاد راهنما:

دکتر حسینی سنو

فهرست عناوین

فهرست تصاویر

فهرست جداول

1. چکیده

با توسعه سریع فناوری بلاک چین، مقیاس شرکت کنندگان آن همچنان در حال گسترش است. ساختار شبکه و الگوریتم اجماع PBFT زنجیره بلوکی دارای مشکلاتی مانند راندمان انتقال پایین و سربار ارتباط بالا است که در نتیجه مقیاس پذیری ضعیفی دارد. برای حل این مشکلات، هدف ما بهبود مقیاس پذیری بلاک چین است تا بتواند از گره های مقیاس بزرگ برای انتقال و ارتباطات کارآمد پشتیبانی کند. در این مطالعه، مدلی به نام MANDALA با شبکه مش و اسپوک و اجماع H-PBFT پیشنهاد می‌کنیم. شبکه Mesh-and-Spoke گره‌ها را در لایه‌های مختلف گروه‌بندی می‌کند و قوانین ارتباطی را بین گروه‌ها تنظیم می‌کند که کارایی انتقال شبکه را بهبود می‌بخشد. سپس، ما الگوریتم اجماع سلسله مراتبی عملی بیزانسی تحمل خطا (H-PBFT) را پیشنهاد می کنیم. اجماع کل شبکه را به چندین لایه فرعی تقسیم می کند که پیچیدگی ارتباط کمتری را به دست می آورد و تحمل خطا را بهبود می بخشد. ما مدل را برای اعتبارسنجی عملکرد و امنیت آن شبیه سازی کردیم. نتایج نشان داد که سربار ارتباط را کاهش داده و نرخ انتقال موثر و توان عملیاتی را با فرض تضمین امنیت بهبود می‌بخشد. در مقایسه با دیگر طرح‌های بهینه‌سازی بلاک چین، مدل ما دارای کارایی اجماع، امنیت و مقیاس‌پذیری بهتری است.

2. مقدمه

در چند سال اخیر تکنولوژی بلاکچین توجه خیلی زیادی رو از طرف صنعت و اکادمی دریافت کرده و در حال توسعه یافتن به سمت طیف گسترده تری از کاربردهاست. هوش مصنوعی، اینترت اشیا، پزشکی و شبکه‌های اجتماعی از سری مواردی هستند که میشه از بلاکچین در اونها استفاده کرد.عمده‌ی کاربرد بلاکچین مربوط میشه به بحث امینت و ماهیت غیرقابل تغییر بودن لِجرها که در کل باعث حفظ جامعیت داده میشه.همینطور غیرمتمرکز بودن یک موضوع کلیدی در بلاکچین هست که اون رو مناسب برای استفاده در مواردی مانند اینترت اشیا صنعتی میکنه[1].[1]

حالا علاوه بر مزایای ذاتی که بلاکچین به همراه خودش داره و در بخش‌های بعدی بیشتر در مورد صحبت خواهیم کرد، با یک سری چالش هم برای استفاده گسترده از این تکنولوژی مواجهیم که باید بهش اشاره بشه.

در حال حاضر پلتفرمهای بلاکچین مختلفی وجود دارند، مانند بیتکوین، اتریوم،میستیکو و هایپرلجر.با اینکه بلاکچین‌های عمومی مثل بیتکوین و اتریوم بیشتر در موارد مربوط به رمزارزها استفاده میشوند ولی در حال تکامل به سمت استفاده‌های تجاری دیگه هم هستند. میستیکو هم بیشتر برای کاریردهای مربوط به big data استفاده میشه.[2]

بحث اصلی این مقاله به کار گیری بلاکچین در کنار اپلیکیشن‌های دیوایس‌های با محدودیت منابع در اینترنت اشیا است که یک سری چالش رو در مقابل ما قرار میده که اجتناب ناپذیر هستند: (1) پلتفرم‌های بلاکچین موجود و الگوریتم‌های اجماع مربوط به اونها از لحاظ محاسباتی بسیار سنگین هستند و اجرای اونها روی دیوایس‌های اینترنت اشیا مشکل است.(2) بلاکچین‌های موجود توان عملیاتی تراکنش مناسب برای استفاده‌های اینترنت اشیا ندارند.(3) سرچ‌های تمام متنِ APIها رو نداریم در این پلتفرمها. این موارد برخی از چالشهای این حوزه است.[2]

[1] industrial internet of things

3. اینترنت اشیا[2]

اینترنت اشیا (IoT) مجموعه وسیعی از اشیاء را با دستگاه‌های حسگر و فعال که داده‌ها را در سایر اشیا، برنامه‌ها و پلتفرم‌ها جمع‌آوری، تجزیه و تحلیل و به اشتراک می‌گذارند، توصیف می‌کند. اینترنت اشیا در حال تبدیل شدن به گامی به سوی انقلاب در دنیای مدرن و تبدیل شدن به نقطه‌ی عطفی در زمینه‌ی هوش مصنوعی است[3].

تعریف جامع‌تری که میشه در مورد اینترت اشیا بیان کرد، یک زیرساخت جهانی برای جامعه‌ی اطلاعاتی،که سرویسهای پیشرفته رو با به هم پیوستگی اشیا[3](چه فیزیکی و چه مجازی) بر اساس تکنولوژی‌های ارتباطی و اطلاعاتیِ موجود و در حال پیشرفت فراهم میکند[4].

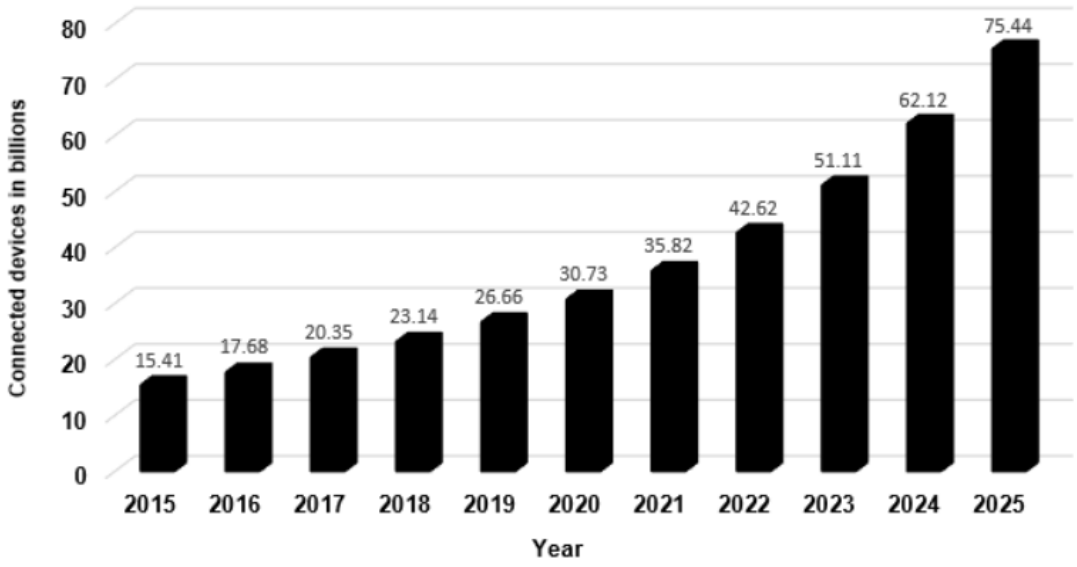
یک اکوسیستم IOT میتونه شامل دستگاه‌های هوشمندِ مبتنی بر وب باشند، که از سیستم‌های گنجانده شده مثل پردازنده‌ها، حسگرها و سخت‌افزارهای ارتباطی برای جمع‌آوری، ارسال و پردازش داده‌هایی که به دست آوردند استفاده میکنند. این دیوایس‌ها عمده کارها رو بدون دخالت انسان انجام میدهند ولی انسان‌ها میتونند با این دیوایسها تعامل داشته باشند، برای مثال انجام پیکربندی اونها یا دسترسی به داده‌های جمع‌آوری شده توسط این دیوایس‌ها .

سیستم‌های IOT در حال حاضر بر اساس مدلِ متمرکز سرور/کلاینت ساخته شدند، که این الزام رو ایجاد میکنه که تمام دیوایس‌ها به یک سرور مرکزی متصل بشوند و اهراز هویت رو هم از همین طریق انجام خواهند داد.که مشکلاتی را به وجود خواهد آورد که در بخش‌های بعدی بررسی خواهیم کرد.

تعداد اشیاء اینترنت اشیا در سال 2008 از جمعیت سراسر جهان پیشی گرفت. طبق آمار Statista ، پیش‌بینی میشد که تعداد اشیاء اینترنت اشیا تا پایان سال 2020 از مرز 31 میلیارد دستگاه در سراسر جهان بگذرد. انتظار می‌رود که این تعداد تا پایان سال 2025 به طور قابل توجهی افزایش یابد و به حدود 75 میلیارد دستگاه برسد، همانطور که در شکل 1 نشان داده شده است.

---

[2] Internet of things
[3] things



تصویر 1.رشد تعداد دستگاه‌های iot از سال 2015 تا 2025

علاوه بر این، بازار اینترنت اشیا تقریباً به طور تصاعدی در حال رشد است. طبق آمار Statista، درآمد تخمینی اینترنت اشیا در سال 2015، 743 میلیارد دلار بود. انتظار می رود این رقم به طور چشمگیری افزایش یابد و به 1742میلیارد دلار تا پایان سال 2030 برسد.

ویژگی‌های سیستم‌های IOT [5]

اینترنت اشیا خدمات و برنامه های دیجیتالی بی شماری را تولید می کند که مزایای متعددی را نسبت به راه حل های موجود ارائه می دهد. این برنامه ها و سرویس ها دارای ویژگی های مشترکی هستند که شامل موارد زیر میشوند:

- **توانایی‌های حسگری**: فناوری اصلی که پیشرفت‌ها را در حوزه‌های مختلف اینترنت اشیا ارتقا می‌دهد، شبکه حسگر بی‌سیم (WSN) است. WSN معمولاً شبکه ای از حسگرها است که اطلاعات پیرامون را حس می کند و این اطلاعات را از طریق یک رسانه ارتباطی برای پردازش ارسال می کند. حسگرها بلوک‌های سازنده اینترنت اشیا هستند که امکان جمع‌آوری تمام اطلاعات به صورت بلادرنگ و متنی[4] در مورد محیط اطراف را فراهم می‌کنند که به تصمیم‌گیرندگان اجازه می‌دهد تا تصمیمات دقیق و دقیق را به موقع بگیرند.

[4] contextual

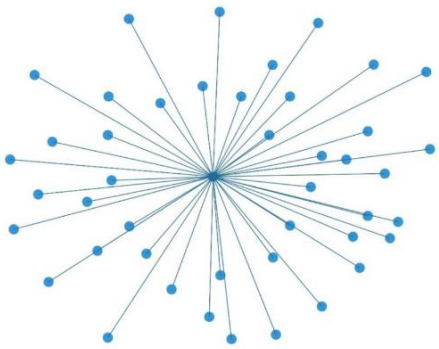
- **اتصال**[5]: یکی از ویژگی‌های کلیدی سیستم اینترنت اشیا است که میلیاردها دستگاه و شی را قادر می‌سازد از راه دور در دسترس باشند. علاوه بر این، به اشیاء مختلف در محیط ما اجازه می دهد تا از طریق اینترنت با یکدیگر متصل شوند و با یکدیگر ارتباط برقرار کنند، که امکان ایجاد برنامه ها و خدمات جدید را فراهم می کند.
- **شبکه‌ای در مقیاس بزرگ:** همانطور که قبلا گفته شد، IoT شامل میلیاردها دستگاه است که انتظار می رود تا پایان سال 2025 به 75 میلیارد دستگاه برسد .این تعداد زیاد دستگاه ها و اشیا شبکه ای در مقیاس بزرگ ایجاد می کنند که با روش های سنتی یا کلاسیک قابل مدیریت نیست
- **سیستم پویا:** اینترنت اشیا به طور ذاتی یک سیستم پویا است .یعنی می تواند اشیاء مختلف را در مکان های مختلف متصل کند .علاوه بر این، با حسگرهایی که اطلاعات مختلف را به طور بلادرنگ در مورد محیط اطراف جمع‌آوری کند، دستگاه‌های اینترنت اشیا را می‌توان به صورت پویا با شرایط و شرایط متغیر تطبیق داد.
- **قابلیت های هوشمند**[6]: دستگاه‌های اینترنت اشیا با سخت‌افزار، نرم‌افزار و قابلیت‌های حسگری پیشرفته که امکان جمع‌آوری حجم وسیعی از داده‌های زمینه‌ای را فراهم می‌کند، می‌توانند تصمیمات هوشمندانه‌ای را در شرایط مختلف اتخاذ کنند و به طور هوشمند با سایر اشیاء همکار همکاری کنند.
- **کلان داده:** میلیاردها دستگاه اینترنت اشیا وجود دارد که حجم وسیعی از داده ها را جمع‌آوری می‌کنند که با استفاده از روش های سنتی تجزیه و تحلیل داده ها قابل تجزیه و تحلیل نیستند. این به اصطلاح " کلان داده" اشاره دارد. اینترنت اشیا یکی از غنی‌ترین منابع داده‌های کلان است که حجم وسیعی از داده‌ها را ایجاد می‌کند که برای بهره‌مندی از مزایای کامل داده‌های اینترنت اشیا به روش‌های تحلیلی نوآورانه نیاز دارد.

[5] Connectivity
[6] Intelligence capabilities

- **ناهمگونی**: سیستم اینترنت اشیا به دستگاه ها و اشیاء مختلف امکان آدرس دهی و ارتباط با یکدیگر از طریق اینترنت را می دهد. این دستگاه‌ها دارای ویژگی‌های ناهمگونی از جمله پروتکل‌های ارتباطی، سیستم‌عامل‌ها، پلتفرم‌ها و سایر اجزای نرم‌افزاری و سخت‌افزاری هستند. با وجود این ویژگی‌های ناهمگون، سیستم اینترنت اشیا به همه این دستگاه‌ها اجازه می‌دهد تا به طور کارآمد و مؤثر با یکدیگر ارتباط برقرار کنند.

1-3. معماری متمرکز IOT

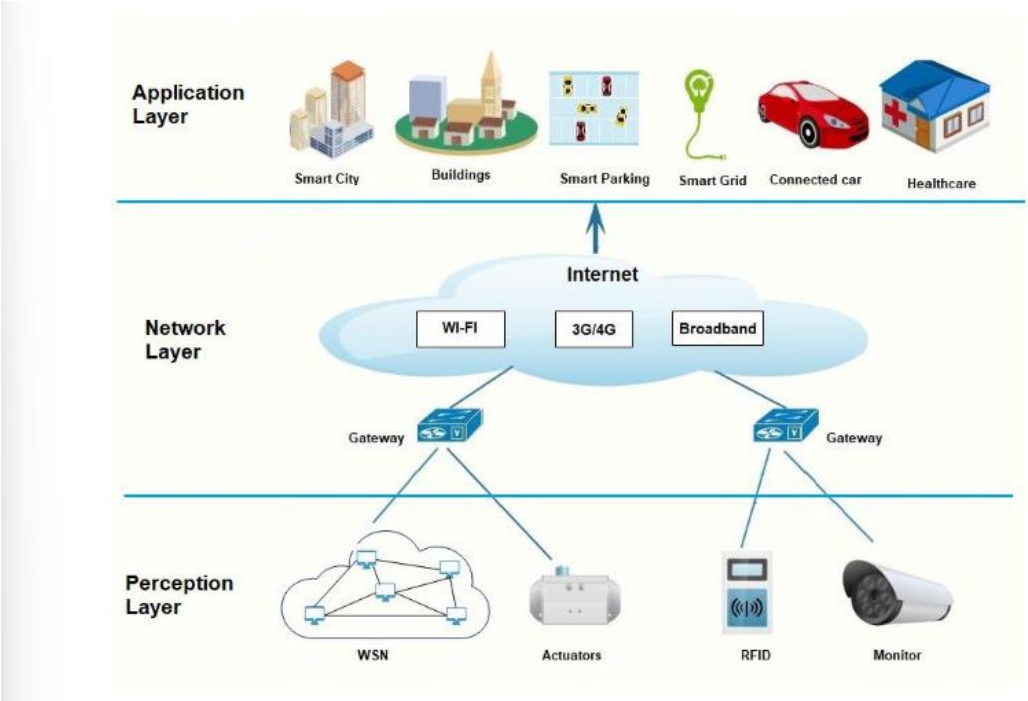
مدیریت مجموعه ای از گره ها برای کار با هم برای فرموله کردن یک سیستم نیاز به طراحی معماری خاصی دارد. از جمله طرح های محبوب، معماری متمرکز است که با استفاده از یک سرور متمرکز برای کنترل و مدیریت مجموعه ای از گره ها ساخته شده است. این گره ها از یک سیستم کامپیوتری پیشرفته، لپ تاپ، تلفن همراه و غیره متفاوت هستند که قادر به انجام انواع عملیات هستند. سرور متمرکز به‌عنوان مدیری عمل می‌کند که با تمام درخواست‌هایی که از گره‌های مختلف می‌آیند سروکار دارد و زمان‌بندی و تخصیص وظایف را در میان گره‌ها در شبکه مدیریت می‌کند. شکل ساده ای از یک معماری متمرکز در شکل 2 نشان داده شده است که در آن تمام گره ها در شبکه از طریق یک سرور مرکزی متصل می شوند.



تصویر 2. معماری متمرکز

سیستم اینترنت اشیا یکی از نمونه‌های رایج یک سیستم متمرکز است که به آن معماری مشتری-سرور نیز می‌گویند. در این رویکرد، تمام دستگاه‌ها و اشیاء اینترنت اشیا از طریق یک سرور متمرکز، که معمولاً یک سرور ابری است، متصل، مدیریت و احراز هویت می‌شوند.

ما در معماری مترکز سیستم‌های IOT شاهد مدل‌های مختلفی هستیم، که قابل فهم‌ترین مدل، مدل 3 لایه است که متشکل از سه لایه‌ی کابرد[7]، شبکه و لایه‌ی ادراکی[8] می‌باشد[6]. اگرچه چندین معماری متمرکز دیگر برای IOT وجود دارد که تا 6 لایه رو هم شامل میشوند که توسط محققان مختلف پیشنهاد شده‌اند، این مدل 3 لایه عملکرد سیستم IOT رو به خوبی نمایش میدهد.



تصویر 3. مدل 3 لایه برای معماری متمرکز سیستمهای IOT

اولین لایه معماری اینترنت اشیا، **لایه درک** است (که لایه حسگر نیز نامیده می شود). این لایه شامل انواع مختلفی از سنسورها، شناسه های فرکانس رادیویی (RFID)، محرک ها[9] و شبکه‌ی سنسورهای وایرلس[10] است. مسئولیت اصلی این لایه حس و درک محیط اطراف و جمع آوری داده های مربوطه قابل پردازش و

[7] application
[8] perception
[9] actutators
[10] WSN(wireless sensor network)

استخراج اطلاعات معنادار برای درک و کنترل دنیای فیزیکی اطراف ماست. بر اساس داده‌های جمع‌آوری‌شده، دستگاه‌های اینترنت اشیا می‌توانند با استفاده از محرک‌ها تصمیمات آگاهانه و مستقلی بگیرند.

لایه **شبکه** برای اتصال و ارتباط همه‌ی دستگاه های IoT از طریق اینترنت استفاده می شود، سرور مرکزی در این لایه قرار گرفته است. این لایه دارای دروازه هایی[11] است که نشان دهنده نقاط ارتباطی بین لایه ادراکی و شبکه است. در این لایه از فناوری‌ها و پروتکل‌های ارتباطی مختلفی مانند شبکه‌های سلولی نسل چهار و سه، ZigBee، Wi-Fi، Bluetooth و Broadband برای انتقال داده‌ها بین لایه ادراکی و کاربرد استفاده شده است. لایه **کاربرد** شامل برنامه های متنوع اینترنت اشیا است که از حجم عظیمی از داده های جمع آوری و پردازش شده به ترتیب در لایه ادراک و شبکه استفاده می کند و خدمات دیجیتالی را در حوزه های متنوعی مانند مراقبت های بهداشتی، پارکینگ هوشمند، خانه هوشمند، شهر هوشمند، پوشیدنی هاو شبکه برق هوشمند تولید می کند.

2-3. کاربردهای IOT

کاربردهای اینترنت اشیا بسیار طیف گسترده‌ای رو در بر میگیره که در اینجا مثال‌هایی در سه بخش مختلف را بیان میکنیم. بخش اول کابردهای مربوط به **خانه‌های هوشمند** است. خانه هوشمند احتمالاً محبوب‌ترین برنامه اینترنت اشیا در حال حاضر است زیرا بسیار مقرون به صرفه و به آسانی در دسترس مصرف‌کنندگان است. کاربردهایی مثل امنیت که با استفاده از دوربین‌ها و حسگرهای مختلف پیاده‌سازی میشه و امکان این رو داره که از راه دور کنترل بشه و به طور خودکار تصمیماتی مانند خبر کردن نیروهای پلیس رو انجام بده، و یا مصارفی مانند سیستمهای سرمایشی و گرمایشی خودکار که براساس ترجیحات کاربر به طور خودکار دما و شرایط محیط رو تنظیم میکنند.

[11] gateways

مثال دیگه‌ی اینترنت اشیا حول محور رانندگی هوشمند میچرخه. سیستم حمل و نقل هوشمند[12] یا ITS حال و آینده‌ی ارتباطات خودرویی است. کاربردهای گوناگون این مورد در زمینه‌های مختلفی مثل ماشین‌های خودران، سرویس‌های امنیتی خودروها مثل سیستم‌های ضد سرقت و یکی از موارد پرکاربرد که در زندگی روزمره ازش استفاده میکنیم برنامه‌های مسیریابی است.

مورد سوم مصارفِ مربوط به سلامت[13] است. ینترنت اشیا متخصصان مراقبت های بهداشتی را قادر می سازد بیشتر مراقب باشند و فعالانه با بیماران ارتباط برقرار کنند. داده‌های جمع‌آوری‌شده از دستگاه‌های IoT می‌تواند به پزشکان کمک کند تا بهترین فرآیند درمانی را برای بیماران شناسایی کنند و به نتایج مورد انتظار برسند. دستگاه‌هایی به شکل پوشیدنی‌هایی مانند نوارهای تناسب اندام و سایر دستگاه‌های متصل به‌صورت بی‌سیم مانند کاف‌های کنترل فشار خون و ضربان قلب، گلوکومتر و غیره به بیماران دسترسی شخصی به توجه را می‌دهند. این دستگاه ها را می توان برای یادآوری شمارش کالری، بررسی ورزش، قرار ملاقات ها، تغییرات فشار خون و موارد دیگر تنظیم کرد.

3-3. چالشهایی که در سیستم متمزکز IOT باهاش مواجهیم

مدل متمرکز موجود سیستم اینترنت اشیا چندین مزیت را برای اتصال و برقراری ارتباط با طیف گسترده‌ای از دستگاه‌هایی که توسط سرور متمرکز مدیریت می‌شوند، فراهم می‌کند. از این رو، کل شارژ شبکه اینترنت اشیا از طریق یک سرور مرکزی مدیریت می شود که مدیریت و نگهداری آن ساده تر است. علاوه بر این، هزینه‌های پیاده‌سازی چندین ایستگاه کاری کامل از سخت‌افزار و نرم‌افزار در شبکه را کاهش می‌دهد، که در آن بیشتر عملیات پردازش تنها توسط سرور متمرکز انجام می‌شود. بنابراین، بیشتر گره های شبکه می توانند مانند یک ترمینال برای اتصال به سرور مرکزی باشند. علاوه بر این، معماری متمرکز اینترنت اشیا امنیت فیزیکی بهتری را ارائه می‌کند، زیرا بیشتر داده‌های اینترنت اشیا در یک مکان واحد نگهداری

[12] Intelligent transport System
[13] healthcare

می‌شوند، که محافظت در برابر آسیب‌های فیزیکی ساده‌تر است. از سوی دیگر، معماری متمرکز اینترنت اشیا چالش‌های متعددی را در بر دارد. به عنوان مثال، با مشکلات مقیاس پذیری مواجه است زیرا نمی تواند با افزایش مداوم دستگاه های اینترنت اشیا وفق پیدا کند. علاوه بر این، چالش های امنیتی و حریم خصوصی متعددی را معرفی می کند[7]. در ادامه بررسی تعدادی از این چالش‌ها خواهیم پرداخت.

- **نقطه‌ی تکی خرابی**[14]: از آنجایی که سرور متمرکز تمام عملیات پردازش را انجام می دهد و ارتباطات بین دستگاه های مختلف را مدیریت می کند، این یک نقطه خرابی(SPF) ایجاد می کند که در صورت از کار افتادن سرور، کل شبکه دستگاه ها غیرقابل دسترسی خواهد بود.
- **امینت**: امنیت یکی از چالش‌های کلیدی در مدل متمرکز اینترنت اشیا است زیرا تمام عملیات پردازش داده و ذخیره‌سازی داده‌ها در یک مکان و از طریق یک سرور مرکزی انجام می‌شود که آن را در معرض انواع مختلف تهدیدات به‌ویژه انکار سرویس قرار می‌دهد.
- **محرمانگی**: انواع مختلفی از داده‌های بی‌درنگ از جمله اطلاعات حساس از دستگاه‌های اینترنت اشیا مانند عادت‌ها، گذرواژه‌ها، اطلاعات شخصی و مالی و غیره جمع‌آوری می‌شوند. این داده‌های جمع‌آوری‌شده در یک مکان تحت کنترل کامل سرور شخص ثالث متمرکز نگهداری می‌شوند که می‌تواند محرمانگی را نقض کند. حریم خصوصی داده ها به‌علاوه، ذخیره آن در یک مکان می‌تواند باعث سهولت نفوذ آن شود.
- **عدم انعطاف‌پذیری**: سرور متمرکز ارتباطات و عملیات پردازش بین تمام گره‌های متصل به شبکه اینترنت اشیا را کنترل می‌کند، که حجم کاری[15] زیادی ایجاد می‌کند. برای مدیریت این حجم کاری، سرور متمرکز بار را برای فرار از مشکلات اوج بار برنامه ریزی می کند. با این حال، این انعطاف پذیری کاربر را در حین انجام وظایف خود به دلیل دستور کار فشرده و تاخیر مرتبط با این فرآیند محدود می کند.

[14] Single Point of Failure
[15] workload

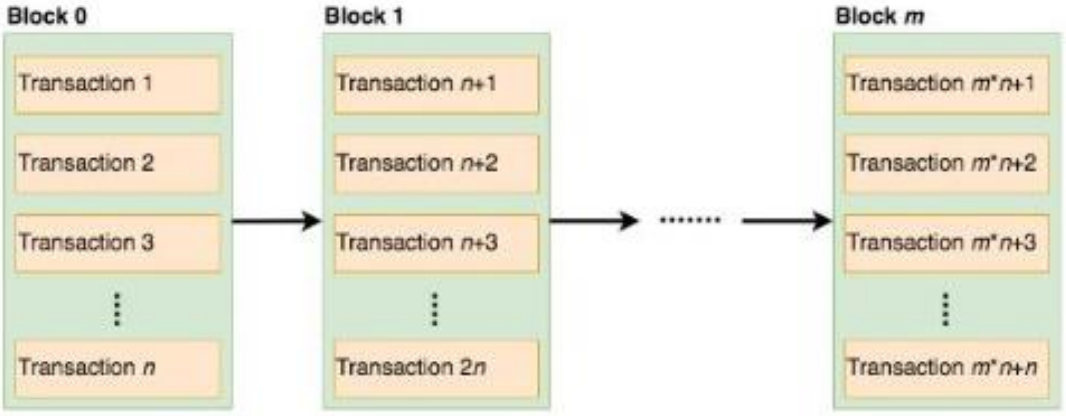
- **مقیاس پذیری:** یکی از بزرگترین چالش های مرتبط با مدل متمرکز، مقیاس پذیری است. مدیریت و کنترل تمام گره ها در شبکه توسط یک سرور مرکزی تنها در شبکه های کوچک می تواند به خوبی مقیاس شود. به کارگیری مفهوم یک سیستم متمرکز با سازمان های بزرگ سازمانی که چندین شعبه در حوزه های مختلف را درگیر می کند غیر منطقی خواهد بود. تعداد دستگاه های اینترنت اشیا به طور مداوم در حال افزایش است و این بدان معنی است که مدل متمرکز قادر به گسترش در مقیاس بالا و عملکرد کارآمد نیست.
- **دسترسی و تنوع**: ز جمله جنبه های مهم یک سیستم کارآمد، قابلیت دسترسی به تمامی کاربران با نیازهای متنوع است .با این حال، سیستم متمرکز کاربران خود را ملزم می کند تا با استفاده از فرآیندهای یکسان به اطلاعات به طور پیوسته دسترسی داشته باشند .علاوه بر این، اکثر سیستم‌های متمرکز از یک سیستم عامل خاص برای کل شبکه استفاده می‌کنند که تنوع درون شبکه را محدود می‌کند .برای سیستم اینترنت اشیا که شامل دستگاه‌های ناهمگن و متنوع است، این امر باعث ایجاد یک مشکل جدی می‌شود که نیاز به رسیدگی دارد.

در ادامه به بررسی راه‌حلهای موجود برای رفع تعدادی از این چالشها خواهیم پرداخت، به خصوص راه‌حل‌هایی که تکنولوژی بلاکچین در اخیار ما قرار میدهد

4. تکنولوژی بلاکچین و معماری غیرمتمرکز

در اواخر سال 1998 نیک سابو دانشمند کامپیوتر و رمز نگار معروف آمریکایی اولین رمزارز به اسم BitGold رو معرفی کرد که آغاز شروعِ عصرِ بلاکچین بود. بیت گلد یکی از اولین تلاش ها برای ایجاد یک ارز مجازی غیرمتمرکز بود. اگرچه پروژه بیت گلد هرگز اجرا نشد، تلاش سابو به طور گسترده به عنوان پیشروی پروتکل بیت کوین ساتوشی ناکاموتو در نظر گرفته می شود. در حقیقت، پروتکل‌های بیت‌کوین و بیتگلد آنقدر شباهت‌های نزدیک دارند که مردم حدس می‌زنند که سابو خالق ناشناس بیت‌کوین، ساتوشی ناکاموتو است.

یک بلاک چین مانند یک دفتر کل توزیع شده است که داده های آن بین شبکه ای از همتایان[۱۶] به اشتراک گذاشته می شود. فناوری بلاک چین روشی کارآمد برای ثبت تراکنش ها یا هر گونه تعامل دیجیتالی ارائه می دهد به گونه ای که آن را ایمن، شفاف، بسیار مقاوم در برابر قطعی ها و قابل بازرسی می کند. این فناوری هنوز جدید است و به سرعت در حال تغییر. در سال 2008، ساتوشی ناکاموتو مفهوم بیت کوین را معرفی کرد. این با انتشار مقاله محبوب "بیت کوین: یک سیستم نقدی الکترونیکی همتا به همتا[۱۷]" بود. این مقاله پیشنهادی را برای توزیع تراکنش های الکترونیکی به جای حفظ وابسته به موسسات متمرکز برای مبادله ارائه کرد.همانطور که در تصویر4 مشاهده میشه بلاکچین از دو بخش اصلی تشکیل شده[8]:



تصویر 4.ساختار بلاکچین

- معاملات: اقداماتی هستند که توسط مشارکت کنندگان در سیستم ایجاد می شوند. مانند تراکنش‌های مالی.
- بلاک‌ها: تراکنش ها را ثبت میکند و مطمئن میشود که به ترتیب صحیح هستند و دستکاری نشده اند. همچنین هر بلاک به توسط یک هش به بلاک قبلی خود زنجیر شده است.

4-1. ویژگی‌های بلاکچین

بلاک چین می تواند مزایای متعددی را برای زمینه ها و برنامه های مختلف ارائه دهد. این فناوری جدید دارای برخی از ویژگی های مشترک است:

[16] peers
[17] Peer to peer

- **تغییرناپذیری**[18]: ساخت دفاتر[19] غیرقابل تغییر یکی از ارزش های کلیدی بلاک چین است. همه پایگاه های داده متمرکز ممکن است خراب شوند و معمولاً برای حفظ یکپارچگی اطلاعات نیاز به اعتماد به شخص ثالث دارند. هنگامی که شما در مورد یک معامله به توافق رسیدید و آن را ثبت کردید، هرگز نمی توان آن را تغییر داد.
- **تمرکززدایی**: بلاک چین معمولاً یک محیط غیرمتمرکز و توزیع شده است که مبتنی بر ارتباط همتا به همتا بین گره های ارتباطی است. تمرکززدایی امکان استفاده از قدرت پردازش همه کاربران مشارکت کننده را فراهم می کند، که تأخیر را کاهش می دهد و نقطه تکی شکست را حذف می‌کند.
- **ناشناس بودن**: علیرغم بلاک چین که از یک دفتر کل استفاده می کند که بین همه کاربران توزیع شده است، بلاک چین یک هویت ناشناس برای محافظت از حریم خصوصی گره ها ارائه می دهد. از ویژگی ناشناس بودن می توان برای ارائه یک سیستم رای گیری امن و خصوصی استفاده کرد.
- **امنیت بهتر:** یکی از مزایای فناوری بلاک چین این است که امنیت بهتری نسبت به راه حل های موجود فراهم می کند. با استفاده از زیرساخت کلید عمومی، بلاک چین یک محیط امن در برابر انواع مختلف حملات فراهم می کند. علاوه بر این، مکانیسم اجماع یک روش قابل اعتماد را ارائه می دهد که امنیت بلاک چین را بهبود می بخشد. علاوه بر این، عدم وجود یک نقطه شکست در فناوری بلاک چین، که می تواند کل سیستم ها را تحت تاثیر قرار دهد، امنیت بهتری را نسبت به مدل متمرکز فراهم می کند.
- **افزایش ظرفیت**: یکی از نکات قابل توجه در مورد فناوری بلاک چین این است که می تواند ظرفیت کل شبکه را افزایش دهد. داشتن هزاران کامپیوتر که به طور کلی با هم کار می کنند می تواند قدرت بیشتری نسبت به چند سرور متمرکز داشته باشد.

[18] Immutability
[19] ledgers

4-2. انواع مختلف بلاکچین

بسته به داده‌های مدیریت‌شده، در دسترس بودن چنین داده‌هایی و اعمالی که کاربر می‌تواند انجام دهد، انواع مختلفی از بلاک چین‌ها وجود دارد. بنابراین، می توان آن را بین بلاک چین های عمومی و خصوصی [20]و مجاز و بدون مجوز[21] تقسیم‌بندی کرد. ذکر این نکته مهم است که برخی از نویسندگان از اصطلاحات عمومی/بدون مجوز و خصوصی/مجاز به عنوان مترادف استفاده می کنند، چیزی که ممکن است هنگام صحبت در مورد رمزارزها منسجم باشد، اما این مورد برای برنامه های اینترنت اشیاء صادق نیست، جایی که مهم است که بین احراز هویت (چه کسی می تواند به بلاک چین دسترسی داشته باشد؛ خصوصی در مقابل عمومی) و مجوز[22] (کاری که یک دستگاه IoT می تواند انجام دهد؛ بدون مجوز در مقابل مجاز). در بلاک چین های عمومی هر کسی می تواند بدون تایید شخص ثالث به بلاک چین بپیوندد و بتواند به عنوان یک گره ساده یا به عنوان ماینر/ اعتبارسنج عمل کند .ماینرها/ اعتبارسنج‌ها معمولاً در بلاک چین‌های عمومی مانند بیت‌کوین، اتریوم یا لایت‌کوین پاداش‌هایی تحت عنوان Fee دریافت می‌کنند.

در مورد بلاک چین های خصوصی، مالک دسترسی به شبکه را محدود می کند. بسیاری از بلاک چین های خصوصی نیز به منظور کنترل اینکه کدام کاربران می توانند تراکنش ها را انجام دهند، از قراردادهای هوشمند استفاده میکنند یا به عنوان ماینر در شبکه عمل کنند، اما توجه داشته باشید که همه بلاک چین های خصوصی لزوماً مجاز نیستند. به عنوان مثال، یک سازمان می تواند یک بلاک چین خصوصی مبتنی بر اتریوم را مستقر کند که بدون مجوز است. نمونه هایی از بلاک چین های مجاز، مواردی هستند که توسط Hyperledger Fabric یا Ripple استفاده می شود.

4-3. تعیین نیاز به استفاده از بلاک چین

قبل از پرداختن به جزئیات نحوه استفاده از بلاک چین برای کاربردهای اینترنت اشیا، ابتدا باید تاکید کرد که بلاکچین همیشه بهترین راه حل برای هر سناریوی اینترنت اشیا نیست. پایگاه‌های اطلاعاتی سنتی یا

[20] Public and private
[21] permissioned and permissionless
[22] authorization

دفتر کل مبتنی بر گراف جهت‌دار غیرمدور[۲۳] (DAG) ممکن است برای برخی از برنامه‌های کاربردی اینترنت اشیا مناسب‌تر باشند. به طور خاص، برای تعیین اینکه آیا استفاده از بلاک چین مناسب است یا خیر، یک توسعه دهنده باید تصمیم بگیرد که آیا ویژگی های زیر برای یک برنامه IoT ضروری است یا خیر[6].

- **تمرکززدایی**: زمانی که یک سیستم متمرکز قابل اعتماد وجود نداشته باشد، برنامه های IoT نیازمند تمرکززدایی هستند .با این حال، بسیاری از کاربران همچنان کورکورانه به برخی شرکت‌ها، سازمان‌های دولتی یا بانک‌ها اعتماد دارند، بنابراین اگر اعتماد متقابل وجود داشته باشد، نیازی به بلاک چین نیست.
- **مبادلات P2P**: در اینترنت اشیا، بیشتر ارتباطات از گره‌ها به دروازه‌هایی می‌روند که داده‌ها را به یک سرور راه دور یا ابر هدایت می‌کنند. ارتباطات بین همتایان در سطح گره در واقع چندان رایج نیست، به جز برای کاربردهای خاص، مانند swarms هوشمند یا در سیستم های محاسباتی مه . همچنین پارادایم های دیگری وجود دارند که ارتباطات بین گره ها را در همان سطح تقویت می کنند، همانطور که در محاسبات مه با دروازه های محلی اتفاق می افتد .
- **سیستم پرداخت**: برخی از برنامه های اینترنت اشیا ممکن است نیاز به انجام معاملات اقتصادی با اشخاص ثالث داشته باشند، اما بسیاری از برنامه ها اینطور نیستند. علاوه بر این، تراکنش‌های اقتصادی همچنان می‌توانند از طریق سیستم‌های پرداخت سنتی انجام شوند، اگرچه معمولاً مستلزم پرداخت کارمزد تراکنش هستند و اعتماد به بانک‌ها یا واسطه‌ها ضروری است.
- **ثبت تراکنش های متوالی عمومی**: بسیاری از شبکه‌های اینترنت اشیا داده‌هایی را جمع‌آوری می‌کنند که باید به‌طور متوالی مهر زمانی زده و ذخیره شوند. با این وجود، چنین نیازهایی ممکن است به راحتی با پایگاه های داده سنتی برآورده شوند، به ویژه در مواردی که امنیت تضمین شده است یا حملات نادر هستند.

[23] Directed Acyclic Graph

- **مجموعه معاملات خرد:** برخی از برنامه‌های اینترنت اشیا ممکن است برای حفظ قابلیت ردیابی، برای اهداف ممیزی یا به این دلیل که تکنیک‌های کلان داده بعداً به کار می‌روند، ممکن است نیاز به ثبت هر تراکنش داشته باشند. در این شرایط، یک زنجیره جانبی ممکن است مفید باشد. با این حال، سایر برنامه ها نیازی به ذخیره هر مقدار جمع آوری شده ندارند.

4-4. مزایا و چالشهای ادغام بلاک چین با اینترنت اشیا

ادغام بلاک چین و اینترنت اشیا (IoT) این پتانسیل را دارد که شیوه تعامل ما با فناوری را متحول کند. با ترکیب این دو فناوری، مشاغل می توانند از افزایش امنیت، بهبود حریم خصوصی داده ها و شفافیت بهتر بهره مند شوند. بلاک چین می تواند یک پلت فرم امن برای دستگاه های IoT برای برقراری ارتباط با یکدیگر فراهم کند و در عین حال به کاربران این امکان را می دهد که کنترل کاملی بر داده های خود داشته باشند. با راه‌حل‌های مبتنی بر بلاک چین، شرکت‌ها می‌توانند به طیف گسترده‌ای از مزایای مانند بهبود مقیاس‌پذیری، افزایش یکپارچگی داده‌ها و افزایش کارایی دسترسی داشته باشند.

شکی نیست که ادغام بلاک چین مزایای زیادی دارد. با این حال، فناوری بلاک چین یک مدل کامل نیست که دارای معایب و چالش های خاص خود باشد. این چالش ها را می توان به صورت زیر خلاصه کرد:

- **مقیاس پذیری**: مشکلات مقیاس پذیری در بلاک چین ممکن است در نهایت منجر به متمرکز شدن شود، که بر آینده ارز دیجیتال سایه می اندازد. با افزایش تعداد گره‌ها در شبکه، بلاکچین به طور ضعیفی گسترش پیدا میکند. این موضوع جدی است زیرا انتظار می‌رود شبکه‌های IoT حاوی تعداد زیادی گره باشند
- **قدرت پردازش و زمان**: قدرت پردازش و زمان مورد نیاز برای دستیابی به رمزگذاری برای تمام اشیاء موجود در یک سیستم بلاک چین. سیستم های اینترنت اشیا انواع مختلفی از دستگاه ها را دارند که قابلیت های محاسباتی بسیار متفاوتی دارند و همه آنها نمی توانند الگوریتم‌های رمزگذاری یکسانی را با سرعت مورد نیاز اجرا کنند.

- **خیره سازی**: یکی از مزایای اصلی بلوک چین است که نیاز به سرور مرکزی برای ذخیره تراکنش ها و شناسه های دستگاه را از می برد، اما دفتر کل باید در خود گره ها ذخیره شود. دفتر کل توزیع شده با گذشت زمان و با افزایش تعداد گره ها در شبکه، اندازه آن افزایش می یابد. آنچه قبلاً گفته شد، دستگاه های IoT منابع محاسباتی کم و ظرفیت ذخیره سازی بسیار پایینی دارند

5-4. کاربردهای اینترنت اشیاءِ مبتنی بر بلاکچین(BIOT)[24]

فناوری بلاک چین را می توان در بسیاری از زمینه ها و موارد استفاده کرد. ملانی سوآن در کتاب بلاکچین: نقشه‌ای برای آینده‌ی اقتصاد پیشنهاد کرد که تکامل کاربرد بلاک چین با بیت کوین (بلاک چین 1.0) آغاز شد، سپس به سمت قراردادهای هوشمند (بلاک چین 2.0) تکامل یافت و بعداً به سمت عدالت، کارایی و برنامه های کاربردی هماهنگی (بلاک چین 3.0) رفت. در رابطه با قراردادهای هوشمند، آنها به عنوان قطعاتی از کدهای غیرمتمرکز خودکفا تعریف می شوند که در صورت تحقق شرایط خاص، به طور مستقل اجرا می شوند. قراردادهای هوشمند را می توان در بسیاری از موارد عملی، از جمله نقل و انتقالات بین المللی، وام مسکن یا تامین مالی جمعی به کار برد.

فراتر از ارزهای دیجیتال و قراردادهای هوشمند، فناوری‌های بلاک چین را می‌توان در حوزه‌های مختلفی که برنامه‌های اینترنت اشیاء درگیر هستند مانند سنجش، ذخیره‌سازی داده، مدیریت هویت، نشان زمانی[25]،برنامه های کاربردی زندگی هوشمند، سیستم های حمل و نقل هوشمند، پوشیدنی ها ، مدیریت زنجیره تامین، سنجش جمعی سیار[26] و قوانین سایبری استفاده کرد.

5. سیستم پیشنهادی[9]

اگرچه فناوری بلاک چین قابلیت اطمینان داده ها را بهبود می بخشد، اما از مقیاس پذیری ضعیف در استفاده عملی، عمدتاً در کارایی و گسترش گره رنج می برد . با افزایش سریع تعداد تراکنش ها در زنجیره،

[24] Blockchain-based IoT
[25] timestamping
[26] mobile crowd sensing

کارایی بلاک چین نمی تواند با عملیات با فرکانس بالا همگام شود. برای مثال، توان عملیاتی بیت کوین حدود 7 تراکنش در ثانیه (tps) است و اتریوم 10 تا 30 تراکنش در ثانیه است . چنین عملکردی نمی تواند تقاضا برای تأیید به موقع تعداد زیادی از معاملات را برآورده کند. در همین حال، مشکلات انتقال داده های اضافی و راندمان انتقال پایین نیز به طور گسترده در شبکه بلاک چین وجود دارد که تراکم شبکه را تشدید می کند و به طور جدی عملکرد بلاکچین را کاهش می دهد. علاوه بر این، با افزایش تعداد گره‌ها، کارایی الگوریتم اجماع[۲۷] به سرعت کاهش می‌یابد و کاربرد آن را در مقیاس‌های بزرگ‌تر محدود می‌کند. به عنوان مثال، الگوریتم بیزانتین تحمل خطا[۲۸] (BFT) در سیستم هایی با گره های مقیاس بزرگ ناکارآمد است. بنابراین، عمدتاً در زنجیره های کنسرسیومی با گره های کمتر استفاده می شود.

1-5. ساختار شبکه ای که توسط بلاک چین استفاده میشود

شبکه پذیرفته شده توسط بلاک چین عمدتاً دارای چهار ساختار است: متمرکز[۲۹]، بدون ساختار[۳۰]، ساختار یافته[۳۱] و ترکیبی[۳۲]. **شبکه متمرکز** از توپولوژی Hub-and-Spoke استفاده می کند که نگهداری آن آسان است و کارایی کوئری گرفتن بالایی دارد. اما مستعد یک نقطه شکست است و شبکه فاقد مقیاس پذیری است. مثال‌هایی از این مدل عبارتند از Napster، Fastpass و IMS. **شبکه بدون ساختار** از روش سازماندهی گراف تصادفی برای تشکیل یک شبکه مش استفاده می کند که قوی است اما سربار شبکه بالایی دارد. بیت‌کوین ،R2Trust و ColChain از این نمونه هستند. **شبکه ساختاریافته** از جدول هش توزیع شده برای مدیریت گره ها استفاده می کند و طرح های مرتبط شامل اتریوم ، مدل مقیاس پذیر اینترنت اشیا[۳۳] ، گراف درختی است. تأخیر پرس و جو را کاهش داده و شبکه را پایدارتر می کند، اما هزینه نگهداری ساختار را افزایش می دهد که بر استفاده از شبکه تأثیر می گذارد. شبکه **ترکیبی**، گره هایی با عملکرد بالاتر را به

[27] consensus
[28] Byzantine Fault Tolerant
[29] centralized
[30] unstructured
[31] structured
[32] hybrid
[33] IoT Scalable Model

عنوان ابرگره برای انجام وظایف جستجو انتخاب می کند. برنامه های کاربردی مرتبط شامل EOS، RCANE است. این ساختار شبکه بیشتر به ابرگره ها وابسته است که بر کارایی و امنیت انتقال تأثیر می گذارد.

اکثر ساختارهای شبکه فوق از راندمان انتقال پایین رنج می برند. گره ها در برابر حملات آسیب پذیر هستند و امنیت آنها تحت تأثیر قرار می گیرد. ساختار شبکه بلاک چین بر کارایی انتقال شبکه تأثیر می گذارد که یکی از دلایل مشکل مقیاس پذیری است. بیت کوین از یک شبکه بدون ساختار استفاده می کند. مکانیسم سیل[۳۴] به راحتی می تواند مشکلاتی مانند طوفان پخش[۳۵] و افزونگی اطلاعات را ایجاد کند که باعث کاهش کارایی انتقال شبکه می شود. اتریوم از یک شبکه ساختاریافته استفاده می کند و نوسانات شبکه ناشی از تغییرات مکرر گره، هزینه نگهداری را به شدت افزایش می دهد.

2-5. مروری بر الگوریتم‌های اجماع مورد استفاده در بلاکچین

علاوه بر این، الگوریتم اجماع بخشی اساسی از بلاک چین است که تأثیر زیادی بر مقیاس پذیری بلاک چین دارد. الگوریتم‌های اجماع رایج عبارتند از: اثبات کار (PoW)، اثبات سهام (PoS) ، تحمل خطای بیزانسی عملی[۳۶] (PBFT) . در یک بلاک چین با اجماع PoW، اعضا از قدرت محاسباتی خود برای رقابت برای عملیات هش استفاده می کنند، اما منابع محاسباتی زیادی مصرف می کند و به طور کلی توان عملیاتی پایینی دارد . اجماع PoS به نفع شرکت کنندگان با توکن های بیشتر است که خطر انحصار و تمرکز را افزایش می دهد [19]. PBFT عملکرد بیشتری دارد و منابع محاسباتی زیادی مصرف نمی کند، اما پیچیدگی ارتباطی آن به اندازه $O(N^2)$ است. با گسترش مقیاس گره، سربار ارتباط آن به سرعت افزایش می یابد و عملکردی مانند راندمان و توان عملیاتی به طور قابل توجهی بدتر می شود.

[34] flood
[35] Broadcast storm
[36] Practical BFT

3-5. بررسی مدل پیشنهادیِ mandala

با توجه به تحلیل‌های فوق، ساختار شبکه و الگوریتم اجماع، عملکرد و مقیاس‌پذیریِ گره‌های بلاک چین را محدود می‌کند. در مقاله‌ای که بررسی خواهد شد، مدلی به نام **MANDALA** را برای بهبود مقیاس پذیری بلاک چین پیشنهاد شده است. این مدل دو بخش اصلی دارد،بخش اول یک شبکه با ساختار mesh-and-spoke که شبکه بلاک چین را به چندین لایه تقسیم می کند. مزیت این است که می تواند مقیاس پذیری و کارایی انتقال داده گره ها را بهبود بخشد. علاوه بر این، مکانیسم انزوا، مکانیسم افزونگی، مکانیسم سازماندهی مجدد، مکانیسم تشویق و تنبیه را راه اندازی کردیم. اینها امنیت را بهبود می بخشد و از انحصار اجماع توسط چند گره جلوگیری می کند. بخش دوم شامل الگوریتم اجماع است، این الگورتیم پیشنهادی کاملا مناسبِ ساختار mesh-and-spoke بوده و H-BFT نامگذاری شده است. این الگوریتم اجماع شبکه را بر اساس شبکه Mesh-andSpoke به چندین لایه فرعی تقسیم می کند که پیچیدگی ارتباط را کاهش می دهد و تحمل خطا را بهبود می بخشد. با افزایش تعداد گره های معمولی، کارایی ارتباط و توان عملیاتی H-PBFT به سرعت PBFT کاهش نمی یابد. در ادامه به طور کامل در مورد الگوریتم‌های اجماع صحبت خواهیم کرد.

4-5. الگوریتم‌های اجماع در بلاکچین[10]

پروتکل‌های اجماع تشکیل دهنده‌ی هسته بلاک چین با تضمین مهم برای امنیت سیستم هستند. ترتیب تراکنش های دریافت شده توسط گره ها در شبکه به دلیل تاخیر شبکه ناسازگار است. برخی از پروتکل‌های اجماع پیشنهاد شده‌اند تا همه گره‌ها در شبکه در یک زمان معین به یک اجماع برسند. آنها را می توان به Proof-of-X (PoX) و Bizantine Fault Tolerant (BFT) تقسیم کرد.

اجماع PoX به طور گسترده ای برای بلاک چین عمومی مناسب است که به ترتیب شامل اثبات کار (PoW)، اثبات سهام (PoS) و اثبات شهرت (PoR) می شود. این پروتکل های اجماع با مقیاس پذیری عالی گره از

طریق رقابت گره طراحی شده اند. با این حال، آنها تا حد زیادی انرژی مصرف می کنند و تاخیر طولانی در تایید تراکنش دارند.

اجماع BFT در بلاک چین‌های کنسرسیوم استفاده می شود که عمدتاً شامل PBFT ، BFTمقیاس پذیر و HoneyBadgerBFT است. این پروتکل ها در مصرف انرژی صرفه جویی می کنند و می توانند توان عملیاتی بالاتری نسبت به پروتکل های اجماع PoX داشته باشند. با این حال، اکثر آنها مقیاس پذیری ضعیف دارند. ما اجماع PBFT را به عنوان مثال در نظر می گیریم. از آنجایی که PBFT انرژی زیادی مصرف نمی کند و می تواند به توان عملیاتی بسیار بالاتری دست یابد، به طور گسترده در بلاک چین های خصوصی و کنسرسیومی مورد استفاده قرار می گیرد. با این حال، مقیاس پذیری گره که نشان دهنده ظرفیت شبکه برای پردازش رشد گره است، یک گلوگاه برای PBFT است . به دلیل پیچیدگی ارتباطی بالا، تنها می تواند به چند ده گره برسد. هنگامی که تعداد گره‌ها در شبکه از این آستانه فراتر رود، تأخیر تأیید تراکنش PBFT بسیار افزایش می‌یابد و توان عملیاتی تا حد زیادی کاهش می‌یابد. بعلاوه، زمانی که گره اصلی یک گره مخرب یا خراب باشد، فرآیند تغییر نما راه اندازی می شود. با ظهور سیستم بلاک چین در مقیاس بزرگ، اجماع PBFT به دلیل مقیاس پذیری ضعیف و کارایی پایین مانع از کاربرد بیشتر آن می شود[11]. بسیاری از پروتکل های اجماع بهبود یافته بر اساس PBFT با تنظیم ساختار ارتباطی آن توسعه یافته اند. HoneyBadgerBFT پیشنهاد شده است که می تواند در شبکه ناهمزمان[۳۷] به یک اجماع برسد. با این حال، باعث پیچیدگی بزرگ ارتباطی می شود. HotStuff فرآیند را در توپولوژی ستاره ای سازماندهی می کند تا پیچیدگی پیام را کاهش دهد. و مفهوم بهینه‌سازی خط لوله را معرفی می‌کند که می‌تواند دورهای مختلف موارد اجماع مختلف را همپوشانی کند. متأسفانه، شبکه به قابلیت اطمینان رهبر حساس است. یک روش مقیاس پذیر تحمل خطا بیزانسی[۳۸] (SBFT) برای کاهش ارتباطات در جمع کننده ها و امضاهای آستانه پیشنهاد شده است. یک توافق PBFT چند لایه مقیاس‌پذیر با گروه‌بندی گره‌ها در لایه‌های مختلف و محدود کردن ارتباطات درون گروه برای کاهش پیچیدگی ارتباطات معرفی شد. یک اجماع بهینه

[37] asynchronous
[38] scalable Byzantine fault tolerant

در معرفی شد که یک ساختار سلسله مراتبی طراحی می کند و PBFT و RAFT را با هم ترکیب می کند تا مقیاس پذیری را افزایش دهد. نوآوری ساختار سلسله مراتبی را می توان برای بهبود مقیاس پذیری بلاک چین به کار برد. با این حال، مشکل این است که هرچه لایه‌های بیشتری وجود داشته باشد، تحمل خطا برای گره‌های بیزانسی کمتر است و عملکرد ایمنی تا حدی کاهش می یابد.

در حوزه بلاک چین و ارزهای دیجیتال هم از این مسئله الهام گرفته شده و راهکار تحمل خطای بیزانس کاربردی یا عملی برای حل آن پیشنهاد شده است. در واقع بر اساس منطق این مسئله، همه شرکت‌کنندگان در یک شبکه باید برای جلوگیری از شکست سیستم و ایجاد بحران، بر سر یک راهبرد مستحکم و درست به توافق برسند.

تحمل خطای بیزانسی عملی یک الگوریتم اجماع است که در اواخر دهه 90 توسط باربارا لیسکوف و میگل کاسترو معرفی شد. pBFT به گونه‌ای طراحی شده است که در سیستم‌های ناهمزمان (بدون محدودیت بالایی در زمان دریافت پاسخ به درخواست) کارآمد باشد و برای زمان سربار کم بهینه شده است. هدف آن حل بسیاری از مشکلات مرتبط با راه‌حل‌های تحمل خطای بیزانسی بود. حوزه های کاربردی شامل محاسبات توزیع شده و بلاک چین است. تحمل خطا بیزانس (BFT) ویژگی یک شبکه توزیع شده برای دستیابی به اجماع (توافق در مورد مقدار یکسان) است، حتی زمانی که برخی از گره های شبکه قادر به پاسخگویی نیستند یا با اطلاعات نادرست پاسخ می دهند(برای مثال در pBFT مقدار این نودها اگر کمتر از یک سوم تعداد کل نود ها باشد هم مشکلی پیش نخواهد آمد). هدف مکانیزم BFT محافظت در برابر خرابی سیستم با استفاده از تصمیم گیری جمعی (هر دو گره صحیح و معیوب) است که هدف آن کاهش تأثیر گره های معیوب است. BFT از مسئله ژنرال های بیزانسی گرفته شده است. این مسئله در مقاله ای توسط لسلی لمپورت، رابرت شوستاک و مارشال پیز در تحقیقات مایکروسافت در سال 1982 به درستی توضیح داده شد:

تصور کنید که چندین لشکر از ارتش بیزانس در خارج از یک شهر دشمن اردو زده اند و هر لشکر توسط ژنرال خود فرماندهی می شود. ژنرال ها فقط از طریق پیام رسان می توانند با یکدیگر ارتباط برقرار کنند. پس از مشاهده دشمن، آنها باید در مورد یک برنامه اقدام مشترک تصمیم بگیرند. با این حال، برخی از

ژنرال ها ممکن است خائن باشند و سعی کنند از دستیابی ژنرال های وفادار به توافق جلوگیری کنند. ژنرال ها باید در مورد زمان حمله به شهر تصمیم بگیرند، اما برای حمله همزمان به اکثریت قوی ارتش خود نیاز دارند. ژنرال‌ها باید الگوریتمی داشته باشند تا تضمین کند که (الف) همه ژنرال‌های وفادار در مورد یک برنامه عمل تصمیم می‌گیرند، و (ب) تعداد کمی از خائنان نمی‌توانند باعث شوند ژنرال‌های وفادار برنامه بدی اتخاذ کنند. ژنرال‌های وفادار همه آنچه را که الگوریتم می‌گوید انجام می‌دهند، اما خائنان ممکن است هر کاری که بخواهند انجام دهند. الگوریتم باید شرط (الف) را بدون توجه به کاری که خائنان انجام می دهند تضمین کند. ژنرال های وفادار نه تنها باید به توافق برسند، بلکه باید بر روی یک برنامه معقول توافق کنند.

تحمل خطا بیزانسی را می توان در صورتی به دست آورد که گره های به درستی کار در شبکه بر روی مقادیر خود به توافق برسند. ممکن است یک مقدار رأی پیش‌فرض به پیام‌های از دست رفته داده شود، به‌عنوان مثال، می‌توانیم فرض کنیم که پیام از یک گره خاص «عیب» است اگر پیام در یک محدودیت زمانی مشخص دریافت نشود. علاوه بر این، اگر اکثر گره ها با یک مقدار صحیح پاسخ دهند، می توانیم یک پاسخ پیش فرض را نیز اختصاص دهیم.لزلی لمپورت ثابت کرد که اگر پردازنده‌های $1+3m$ داشته باشیم، می‌توان به اجماع (توافق در مورد همان حالت) دست یافت، اگر بیش از m پردازنده‌ها معیوب باشند، به این معنی که بیش از دو سوم از تعداد کل پردازنده‌ها باید درست رفتار کنند.

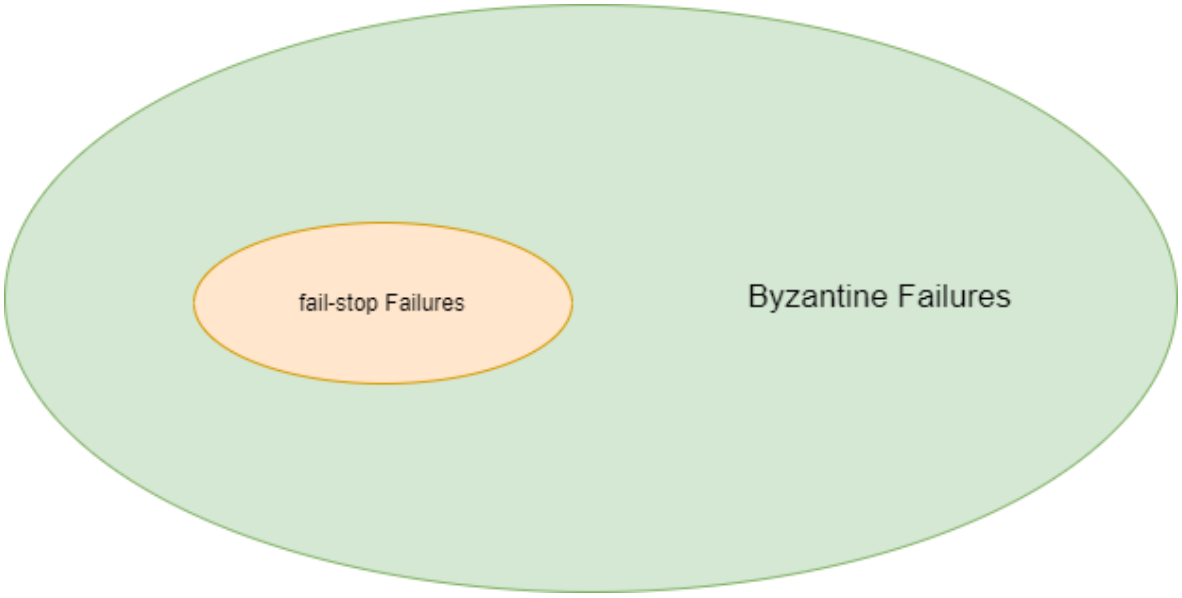
انواع شکست های بیزانسی:

دو دسته از شکست ها در نظر گرفته می شوند. یکی Fail-stop (که در آن گره از کار می افتد و دیگر کار نمیکند) و دیگری شکست دلخواه گره است. برخی از خرابی های گره دلخواه[۳۹] در زیر آورده شده است:

- عدم بازگشت نتیجه
- با نتیجه نادرست پاسخ میدهد
- با نتیجه ای عمدا گمراه کننده پاسخ میدهد

[39] arbitrary-node failure

- به قسمت های مختلف سیستم با نتایج متفاوتی پاسخ میدهد



تصویر 5. دیاگرام خطاهایی که BFT رو شامل میشه

مزایای pBFT :

- بهره وری انرژی pBFT :می تواند بدون انجام محاسبات پیچیده ریاضی(مانندPOW به اجماع توزیع شده دست یابد) .
- **نهایی بودن تراکنش**: تراکنش ها تراکنش ها پس از نهایی شدن و توافق (برخلاف مکانیزم PoW در بیت کوین که در آن هر گره به طور جداگانه تمام تراکنش ها را قبل از افزودن بلوک جدید به بلاک چین تایید می کند؛ تایید می تواند بین 10 تا 60 دقیقه بسته به تعداد موجودیت‌هایی که کار تایید را انجام میدهند طول بکشد) نیازی به تایید چندگانه ندارند.

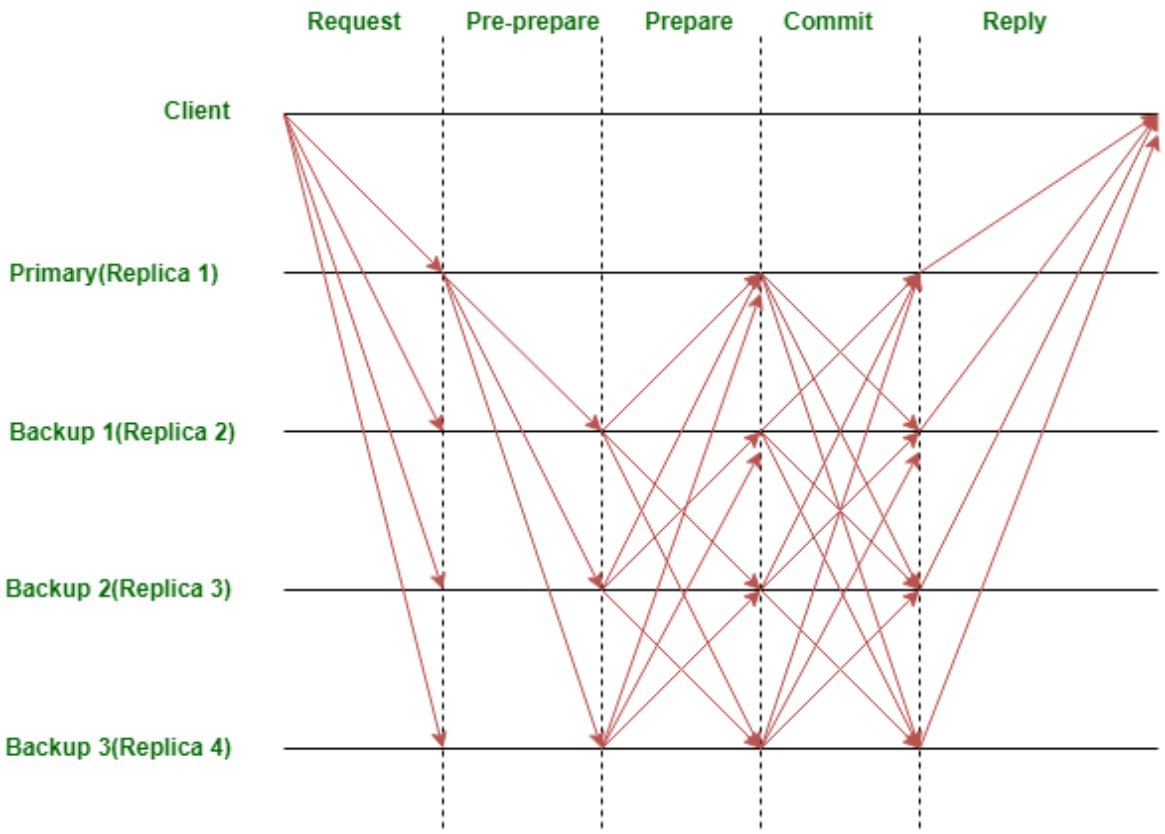
- **اختلاف کم در پاداش‌ها**[40]: چون هر گره در شبکه در پاسخ به درخواست مشتری شرکت می کند، از این رو به هر گره میتوان پاداشی را اختصاص داد که منجر به واریانس پایین در پاداش دادن به گره هایی می شود که در تصمیم گیری کمک می کنند.

5-5. نحوه‌ی عملکرد pBFT

pBFT سعی می‌کند یک شبیه‌سازی عملی ماشین حالت بیزانسی را ارائه دهد که می‌تواند حتی زمانی که گره‌های مخرب در سیستم کار می‌کنند، کار کند. گره‌ها در یک سیستم توزیع‌شده با قابلیت pBFT به‌طور متوالی مرتب می‌شوند که یک گره اصلی (یا گره رهبر) است و سایر گره‌ها به عنوان ثانویه (یا گره‌های پشتیبان) شناخته می‌شوند. در اینجا نکته‌ی قابل توجه این است که هر گره واجد شرایط در سیستم می تواند با انتقال از ثانویه به اولیه (معمولاً در صورت خرابی گره اولیه) به عنوان اصلی تبدیل شود. هدف این است که همه گره‌های صادقانه با استفاده از قانون اکثریت[41] به اجماع در مورد وضعیت سیستم کمک کنند. هر دورِ اجماع pBFT به 4 مرحله تقسیم می شود (تصویر):

- مشتری درخواستی را به گره اصلی (رهبر) ارسال می کند.
- گره اصلی (رهبر) درخواست را به تمام گره های ثانویه (پشتیبان) ارسال می کند.
- گره ها (اولیه و ثانویه) سرویس درخواستی را انجام می دهند و سپس یک پاسخ را برای مشتری ارسال می کنند.
- درخواست زمانی با موفقیت ارائه می شود که مشتری پاسخ های 'm+1' را از گره های مختلف در شبکه با نتیجه یکسان دریافت کند، جایی که m حداکثر تعداد مجاز گره های معیوب است.

[40] Low reward variance
[41] majority rule



تصویر 6

گره اصلی (رهبر) در طول هر نما[۴۲] تغییر می کند (دورهای اجماع pBFT) و می تواند با **پروتکل تغییر نما**[۴۳] جایگزین شود اگر مدت زمان از پیش تعریف شده ای سپری شده باشد بدون اینکه گره پیشرو درخواستی را برای پشتیبان ها ارسال کند (ثانویه). در صورت نیاز، اکثریت گره های صادق می توانند به مشروعیت گره اصلی فعلی رأی دهند و آن را با گره پیشرو بعدی در ردیف جایگزین کنند.

محدودیت‌های pBFT:

مدل اجماع pBFT تنها زمانی کارآمد عمل می کند که تعداد گره ها در شبکه توزیع شده به دلیل سربار ارتباطی بالا که به طور تصاعدی با هر گره اضافی در شبکه افزایش می یابد، کم باشد.

- **حملات Sybil**: مکانیسم‌های pBFT مستعد حملات Sybil هستند، جایی که یک نهاد (طرف) هویت‌های[۴۴] زیادی را کنترل می‌کند. با افزایش تعداد گره ها در شبکه، انجام حملات سیبیل به

[42] view
[43] view change protocol
[44] identities

طور فزاینده ای دشوار می شود. اما از آنجایی که مکانیسم‌های pBFT دارای مشکلات مقیاس‌پذیری نیز هستند، مکانیسم pBFT در ترکیب با مکانیسم(مکانیسم‌های) دیگر استفاده می‌شود.

- **مقیاس‌بندی**[۴۵]: pBFT به دلیل سربار بالا (به خاطر ارتباط آن با تمام گره های دیگر در هر مرحله) مقیاس‌پذیری خوبی ندارد. با افزایش تعداد گره ها در شبکه (به اندازه $O(n^{\wedge k})$ افزایش می یابد، که در آن n پیام ها و k تعداد گره ها است)، زمان صرف شده برای پاسخ به درخواست نیز افزایش می یابد.

پلتفرم‌هایی که از pBFT استفاده میکنند:

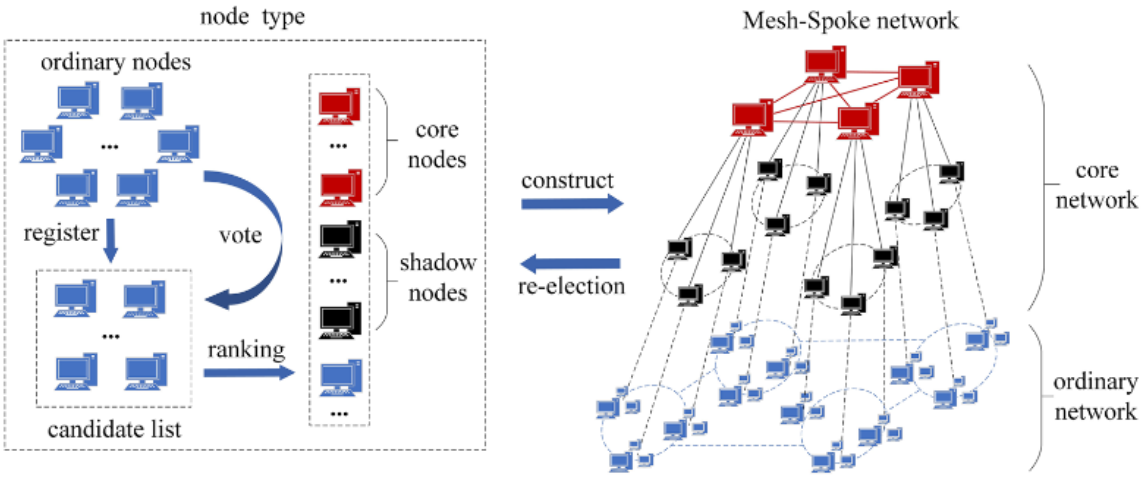
- زیلیکا[۴۶] - استفاده از pBFT و ترکیب اون با الگوریتم اجماع PoW
- هایپرلجر فابریک - ورژنِ مجوز دار[۴۷] pBFT
- تندرمینت[۴۸] - pBFT + DPoS(Delegated Proof-of-Stake)

برای افزایش کیفیت و عملکرد pBFT برای موارد و شرایط استفاده خاص، تغییرات زیادی پیشنهاد و به کار گرفته شده و مدل‌های مختفی از اون مثل RBFT[49] ارائه شده‌اند. در این مقاله به همراه مدل ماندالا نوع بهبود یافته‌ای از pBFT استفاده میشودبه اسم H-pBFT که در ادامه معرفی خواهد شد.

6. معماری مدل mesh-and-spoke به اسم ماندالا[9]

MANDALA عمدتاً از شبکه Mesh-and-Spoke و الگوریتم اجماع H-PBFT تشکیل شده است و معماری کلی آن در شکل 7 نشان داده شده است.

[45] scaling
[46] Zilliqa
[47] permissioned
[48] Tendermint
[49] Redundant BFT



تصویر 7.معماری مدل ماندالا

مقیاس پذیری ضعیف یک مشکل جهانی و برجسته در شبکه های بلاک چین فعلی است. هر خطایی که در گره های اجماع رخ دهد، تأثیر زیادی بر کل سیستم خواهد داشت. بنابراین، قابلیت اطمینان گره های شرکت کننده در اجماع باید بهبود یابد. در این مدل، قابلیت اطمینان گره ها با رای گیری ارزیابی می شود و گره ها به سه نوع گره هسته[۵۰]، گره سایه[۵۱] و گره معمولی[۵۲] تقسیم می شوند که همگی شبکه Mesh-and-Spoke را تشکیل می دهند. گره های سایه و گره های هسته شبکه اصلی[۵۳] را تشکیل می دهند که H-PBFT را برای تولید بلوک ها و رسیدن به اجماع اجرا می کند. گره‌های معمولی شبکه معمولی را تشکیل می‌دهند که وظیفه ارسال تراکنش‌ها به شبکه اصلی و دریافت بلوک‌های جدید که به توافق رسیده‌اند را بر عهده دارد.H-PBFT وظایف اجماع گسترده شبکه را به زیرشبکه های دو لایه بر اساس شبکه Mesh-and-Spoke تقسیم می کند. پیچیدگی ارتباط را تا حد زیادی کاهش می دهد و مشکل سازگاری داده گره ها در شبکه را به طور موثر حل می کند.

[50] core
[51] shadow
[52] ordinary
[53] Core network

1-6. نمادهای استفاده شده در این مدل

نماد	توضیحات
$M_{Request}$	پیام درخواست
$M_{PRE-PREPARE}$	پیام پیش-آماده‌سازی
$M_{PREPARE}$	پیام آماده سازی
M_{COMMIT}	پیام اعزام
M_{REPLY}	پیام ریپلای
$M_{VIEW-CHANGE}$	پیام تغییر نما
<M>	امضای پیام M
O	تراکنش کامیت شده
t	timestamp
c	آیدی کلاینت
d	بلاکِ دیتا
v	شماره‌ی نما
T	فاصله زمانی برای تولید بلاک

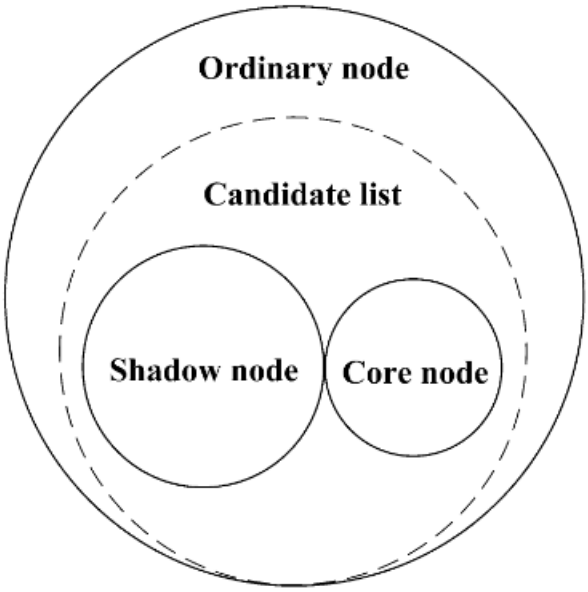
جدول 1 .نمادهای الگوریتم اجماع H-PBFT

نماد	توضیحات
N	تعداد گره‌های شبکه‌ی هسته
K	تعداد گره‌های شبکه‌ی معمولی
y	تعداد نودهای هسته
x	تعداد گره‌های سایه در هر گروه هسته
C_i	نود هسته با اندیس i
G_i	گروه هسته با اندیس i
S_{ij}	گره سایه با اندیس j در گروه G با اندیس i
N_{ij}	گره معمولی با اندیس j در گروه G با اندیس i
F_1	حد بالایی گره های بیزانسی در گره های هسته
L_1	لیست گره‌های سایه در G_i

جدول 2.نمادهای شبکه Mesh-and-Spoke

2-6. شبکه‌ی mesh-and-spoke

همانطور که گفته شد گره‌ها در این سیستمِ بلاک چین با رأی گیری به سه نوع تقسیم می شوند: گره های معمولی، گره های سایه و گره های هسته. رابطه منطقی بین انواع مختلف رابطه منطقی بین انواع مختلف گره ها در شکل 8 نشان داده شده است و تعاریف و توابع خاص به شرح زیر است:



تصویر 8. نمایش رابطه‌ی منطقی بین نودها

گره های معمولی: در شبکه Mesh-and-Spoke، به جز گره های هسته و گره های سایه، سایر گره ها گره های معمولی هستند که در اجماع شرکت نمی کنند، اما نیاز به پذیرش نتیجه‌ی اجماع دارند. هنگامی که یک گره معمولی به شبکه Mesh-and-Spoke می‌پیوندد، ابتدا شاخص i از گروه هسته‌ای را که باید به هم متصل شود، بر اساسفرمول $i = y \bmod id$ محاسبه می‌کند، جایی که id شماره هویت یکتای گره معمولی است. سپس، چندین گره سایه را در G_i متصل می کند (تعداد خاص هنوز قابل تنظیم است). این روش

می تواند اطمینان حاصل کند که گره های معمولی به طور نسبی در هر گروه هسته توزیع شده اند و بار شبکه را متعادل می کند. همانطور که در شکل 9 نشان داده شده است .

$\{N_{1i} \mid i=1,2,3,\ldots,K\}$ نودهای معمولیِ متعلق به G_1 هستند. وظایف اصلی گره های معمولی به شرح زیر است:

1. تراکنش را به گروه اصلی مربوطه ارسال میکند.
2. پس از دریافت آخرین بلوک، آن را به سایر گره های معمولی فوروارد میکند.

گره های سایه: هر گره هسته دارای x گره سایه است که می تواند مستقیما با آن گره هسته ارتباط برقرار کند. همانطور که در شکل 9 نشان داده شده است. $\{S_{1i} \mid i=1,2,3,\ldots,x\}$ گره‌های سایه‌ی متعلق به گره هسته‌ی C_1 هستند. وظایف اصلی گره های سایه به شرح زیر است:

1. پیام ها را بین گره های اصلی و گره های معمولی ارسال میکند. گره‌های سایه، تراکنش‌ها را از گره‌های معمولی جمع‌آوری می‌کنند و آن‌ها را به گره‌های اصلی ارسال می‌کنند، و همچنین بلوک‌هایی را که در شبکه اصلی به توافق رسیده‌اند، به گره‌های معمولی منتشر[۵۴] می‌کنند.
2. در اجماع شرکت میکند و همچنین به عنوان کاندیدای گره اصلی عمل میکند. در طی فرآیند اجماع، اگر یک گره هسته یک گره بیزانسی باشد، که پروتکل تغییر نما[۵۵] را راه اندازی می کند، با یک گره سایه واجد شرایط به عنوان گره هسته جدید جایگزین می شود.

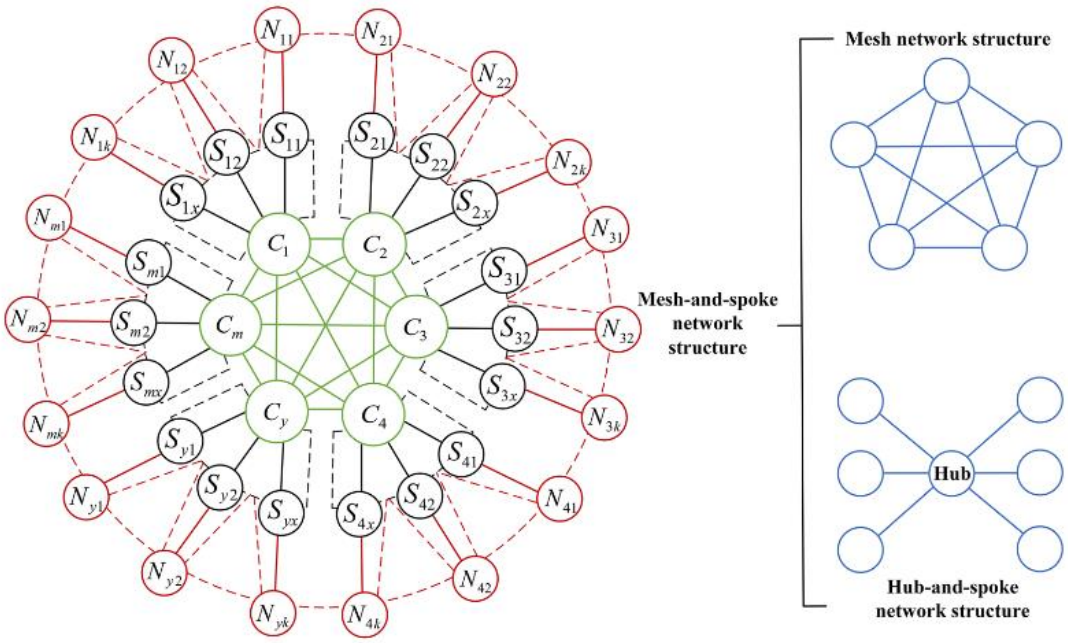
گره های اصلی: yگره با بیشترین تعداد رای[۵۶]. مجموعه گره‌های $\{C_i \mid i=1,2,3,\ldots,y\}$ همانطور که در شکل 9 میبینیم. وظایف اصلی گره های هسته به شرح زیر است:

1. تراکنش ها را از گره های سایه دریافت و تأیید میکند.
2. الگوریتم اجماع H-PBFT را برای تولید بلوک ها و رسیدن به اجماع اجرا میکنند.

[54] propagate
[55] view-change protocol
[56] vote

گروه هسته: گره هسته و گره های سایه متناظر آن گروه هسته را تشکیل می دهند که با G_i نشان داده می شود و i اندیسِ گره هسته است. برای مثال G_1 گروه هسته‌ی متناظر با گره هسته‌ی C_1 و گره‌های سایه‌ی متصل به اون رو نمایش میده. گروه‌های اصلی مستقل از یکدیگر هستند و تحت تأثیر گروه‌های دیگر قرار نمی‌گیرند، که می‌تواند به انزوای حریم خصوصی بهتری دست یابد. اگر یک گروه اصلی رفتار غیرعادی داشته باشد، تأثیری بر سایر گروه ها نخواهد داشت. گره های هسته به یکدیگر متصل هستند و گره های سایه فقط به گره های گروه متصل می شوند

شبکه معمولی: از گره های معمولی تشکیل شده است. گره های معمولی متصل به گره های سایه و رابطه اصلی اتصال بین گره های معمولی شبکه معمولی را تشکیل می دهند.همانطور که در شکل 9 مشاهده میشه گره‌ها معمولیِ $\{N_{1i} \mid i=1,2,3,\ldots,K\}$ از G_1 یک شبکه معمولی محلی را تشکیل می دهد و هر شبکه معمولی محلی با توجه به اتصال بین گره های معمولی شبکه معمولی را تشکیل می دهد.



تصویر 9.ساختار شبکه mesh-and-Spoke، که شبیه برخی از تصاویر گل ماندالا است، از این رو نام این مدل هم ماندالا گذاشته شده.

ساختار شبکه Mesh-and-Spoke یک ساختار منطقی مجازی است و ساختار واقعی شبکه را تغییر نمی‌دهد. همانطور که در شکل 9 نشان داده شده است، ساختار شبکه بلاک چین را به دو لایه تقسیم می کند: شبکه

اصلی از گره های هسته و گره های سایه تشکیل شده است، و شبکه معمولی از گره های معمولی تشکیل شده است. علاوه بر این یک سری مکانیزم ، مکانیسم انزوا، مکانیسم افزونگی، مکانیسم سازماندهی مجدد و مکانیسم تشویق و مجازات در شبکه پیاده سازی شده است که تعاریف آنها در ادامه خواهیم دید.

- **مکانیسم جداسازی**[۵۷]: گره های هسته از گره های معمولی جدا شده اند و نمی توانند با یکدیگر ارتباط برقرار کنند .این دو نوع گره تعامل غیرمستقیم داده را از طریق گره های سایه انجام می دهند. به عنوان مثال، گره هسته C_1 می تواند با گره های سایه در G_1 و سایر گره های هسته ارتباط برقرار کند، اما نمی تواند با گره های معمولیِ خارج از G_1 ارتباط برقرار کند. این مکانیسم می تواند از حمله مستقیم گره های معمولی مخرب به گره های هسته جلوگیری کند و در نتیجه امنیت گره های هسته را تضمین کند.
- **مکانیسم افزونگی**[۵۸]: ارتباطات اضافی متقابل بین گره های معمولی و گره های سایه. برای مثال گره معمولیِ N_{mj} تعداد r نود سایه در G_m به همدیگه متصل میکنه($r<=x$) . این مکانیسم انتقال داده های پایدار بین شبکه اصلی و شبکه معمولی را تضمین می کند و درجه همزمانی ارتباط را بهبود می بخشد.
- **مکانیسم سازماندهی مجدد**: برای جلوگیری از انحصار[۵۹] گره های اصلی، مکانیزم سازماندهی مجدد طراحی شده است. در طول هر دوره اجماع، گره های انتخاب شده برای شبکه اصلی نمی توانند از لیست نامزد[۶۰] خارج شوند. سایر گره ها می توانند با پرداخت سپرده[۶۱] به لیست نامزدها بپیوندند یا می توانند برداشت[۶۲] کنند و سپرده خود را پس بگیرند. علاوه بر این، گره ها می توانند انتخاب های رای خود را در هر زمان تغییر دهند، بنابراین لیست نامزدها و رتبه بندی آرا به صورت پویا تغییر می کند. قبل از شروع هر دوره اجماع، سیستم گره های اصلی و گره های سایه را بر اساس آخرین رتبه بندی آرا در لیست نامزدها مجدداً تعیین می کند و سپس دوره اجماع را آغاز می کند.

---

[57] Isolation mechanism
[58] Redundancy mechanism
[59] monopoly
[60] candidate list
[61] deposit
[62] withdraw

تحت این مکانیسم، شبکه اصلی به طور دوره‌ای سازماندهی می‌شود و گره‌ها به نوبت بلاک‌ها را تولید می‌کنند که امنیت و عدالت را بهبود می‌بخشد.

- **مکانیزم تشویق و جریمه**: در اینجا درجات مختلفی از پاداش را به اعضای شبکه اصلی و گره‌های شرکت‌کننده در رای‌گیری داده خواهد شد تا گره‌های بیشتری تشویق بشوند تا فعالانه در اجماع و رای‌گیری شرکت کنند. اگر یکی از اعضای شبکه اصلی نتواند کار را انجام دهد، سپرده آن کسر می شود و نمی تواند در دوره اجماع بعدی به لیست نامزدها بپیوندد، که هزینه و دشواری اعمال مخرب را بسیار افزایش می دهد. با این حال اکثر گره ها در شبکه منطقی هستند و درست رفتار میکنند. آنها فعالانه به لیست نامزدها می پیوندند و برای دریافت غرامت[۶۳] بیشتر رای می دهند و بدخواهانه عمل نمی کنند. با این حال، هنوز تعداد کمی از گره های مخرب، یا گره های غیر طبیعی به دلیل خطاهای سخت افزاری، قطع اتصال و غیره وجود دارد که به این گره ها، گره های بیزانسی می گویند.

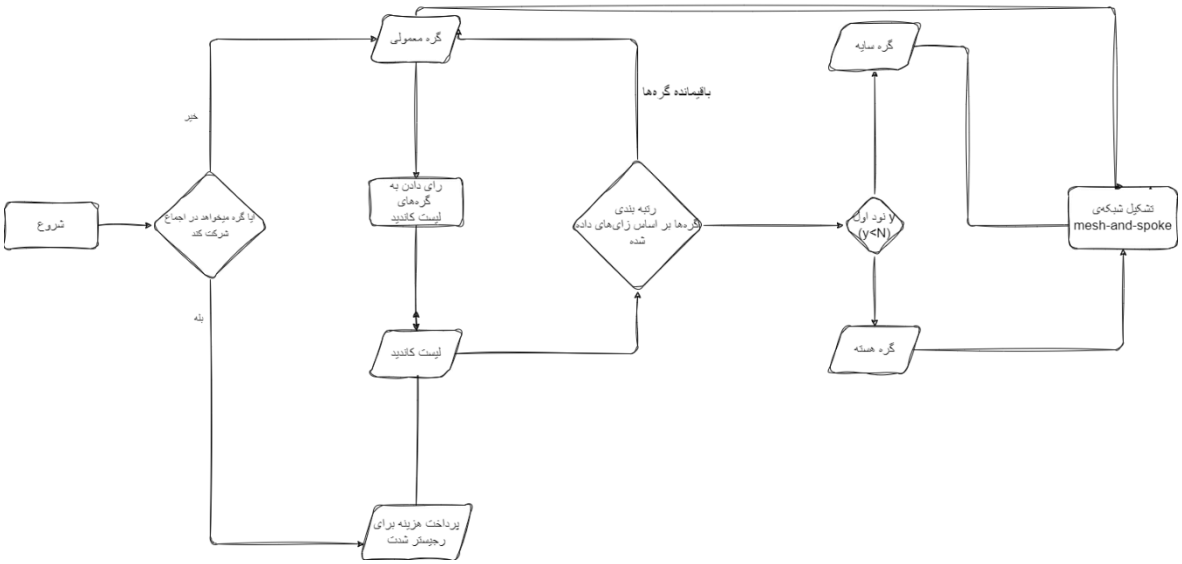
3-6. نحوه‌ی شکل گیری ساختار شبکه‌ی mesh-and-spoke

همانطور که در تصویر فلوپارت 10 نشان داده شده است، گره‌هایی در بلاک چین که مایل به شرکت در اجماع هستند، می‌توانند با پرداخت مبلغی به لیست نامزدها بپیوندند و سایر گره‌ها گره‌های معمولی باقی میمانند. گره های معمولی به گره های موجود در لیست نامزدها رأی می دهند و آنها را بر اساس تعداد آرای دریافتی رتبه بندی می کنند. N گره در اجماع شرکت می کنند و این گره ها را از لیست نامزد انتخاب می‌شوند. گره هایی که در بازه [1,y] رتبه بندی می شوند به عنوان گره های هسته انتخاب می شوند و گره هایی که در بازه [y+1,N] رتبه بندی می شوند به عنوان گره های سایه انتخاب می شوند. به هر گره هسته ابه طور تصادفی x گره سایه اختصاص داده می شود و گره های باقی مانده در لیست کاندید همچنان گره‌های معمولی باقی میمانند. N در ابتدا روی 10٪ از تعداد کل گره ها در لیست نامزد تنظیم می شود و

[63] compensation

باید شرط (x>2,y>3) را برآورده بکند. متعاقباً، گره‌ها می‌توانند پیشنهاداتی ارائه دهند و به تنظیم N رأی دهند.

پس از تقسیم انواع گره ها، شبکه اصلی و شبکه معمولی طبق قوانینی که در بخش قبلی گفته شد تشکیل می شوند. . ابتدا، گره های هسته یک شبکه مش را تشکیل می دهند. سپس هر گره هسته و گره سایه y یک شبکه hub-and-spoke را تشکیل می دهند. شبکه مش به عنوان یک هاب و گره های سایه مربوطه به عنوان گره های اسپیکر استفاده می شوند. این شبکه اصلی را تشکیل می دهد که یک ساختار شبکه Mesh-and-Spoke است. به طور مشابه، شبکه اصلی شبیه یک هاب است و گره های معمولی شبیه به گره های *spoke* هستند. علاوه بر اتصال گره های سایه متناظر، گره های معمولی رابطه اصلی را نیز حفظ می کنند که یک شبکه معمولی را تشکیل می دهد. در نهایت، شبکه اصلی و شبکه معمولی شبکه Mesh-and-Spoke نهایی را تشکیل می دهند.



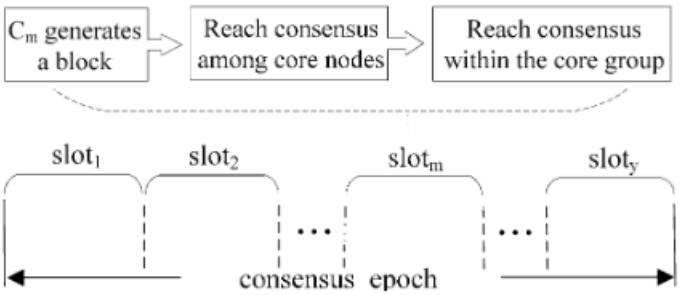
تصویر 10. پروسه‌ی تشکیل شبکه‌ی ماندالا

7. الگوریتم اجماع H-pBFT

PBFT سهم بزرگی در حل مسئله ژنرال های بیزانس دارد، اما پیچیدگی ارتباطی آن $O(N^2)$ کارایی اجماع را محدود می کند. با افزایش تعداد گره ها، ترافیک شبکه آن به سرعت رشد می کند که باعث فشار زیادی بر پهنای باند می شود. علاوه بر این، با شبکه Mesh-and-Spoke سازگار نیست. برای مقابله با مشکلات فوق، الگوریتم اجماع H-PBFT را پیشنهاد شده است که پیچیدگی ارتباط را کاهش می‌دهد و مقیاس‌پذیری، کارایی اجماع و تحمل خطای گره‌ها را بهبود می‌بخشد. یکی سری توضیحات و تعاریف در مورد این الگوریتم هست که ابتدا آنها بررسی خواهد شد:

دوره‌ی اجماع[۶۴]:

زمانی که y گره‌ی هسته به نوبت بلوک‌ها را تولید می‌کنند و به یک اجماع در شبکه اصلی می‌رسند، دوره‌ی اجماع نامیده می‌شود که به y بازه‌ی زمانی تقسیم می‌شود و هر بازه را یک اسلات می‌گویند. همانطور که در شکل 11 نشان داده شده است، یک بلوک توسط گره هسته در طول هر دوره‌ی اسلات تولید می شود. پس از اینکه بلوک در لایه گره هسته و لایه های داخلی هر گروه هسته به اجماع رسید،اسلات به پایان می‌رسد. زمانی که y اسلات اجرا شوند، دوره اجماع به پایان می رسد.



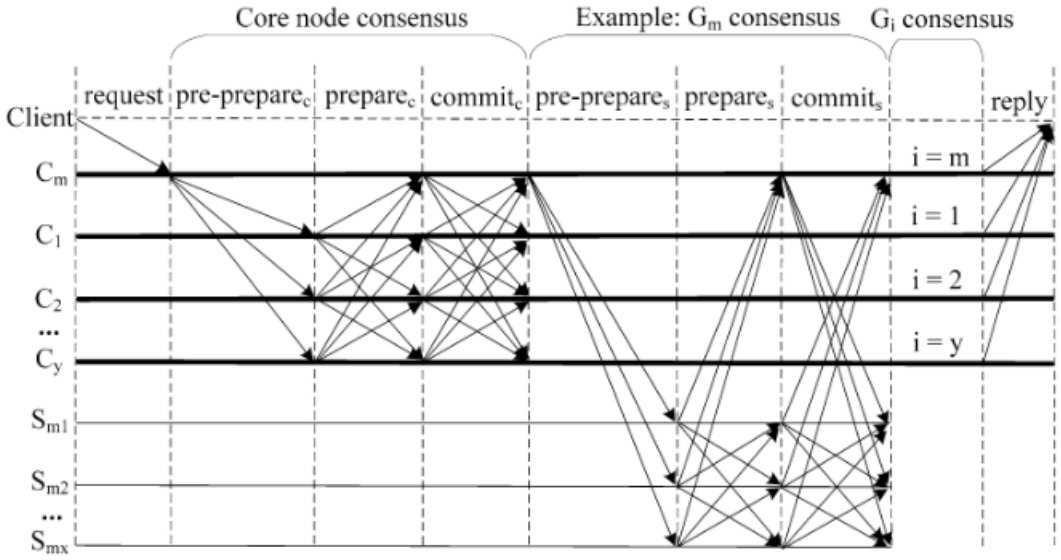
تصویر 11. ترکیب بندیِ هر دوره‌ی اجماع

7-1. فرایندِ انجام H-pBFT

H-PBFT مسئول سازماندهی گروه های مختلف در داخل شبکه اصلی است، به طوری که گره ها می توانند در مورد بلوکی که باید تولید شود به اجماع برسند. در طول هر دوره اسلات، تعداد معینی از تراکنش ها

[64] Consensus epoch

توسط گره اولیه به بلوک بسته می شود و صحت و سازگاری بلوک از طریق یک پروتکل اجماع دو لایه تضمین می شود. همانطور که در شکل 12 نشان داده شده است، روند اجماع ($1 < m < y$) $slot_m$ در یک دوره اجماع شرح داده شده است.



تصویر 12

1. **پروتکل گره لایه‌ی هسته**[65]؛ C_m به عنوان گره اولیه[66] عمل می کند، $y - 1$ گره هسته $\{C_i \mid i=1,2,\ldots,m-1,m+1,..,y\}$ به عنوان گره های مشابه[67] عمل می کنند، و حد بالایی گره بیزانسی f_1 است ($f_1 < y\ 3$). این فرایند به شرح زیر است، نمادها در جداول 1 و 2 شرح داده شده است.
   a. **درخواست**[68]؛ همانطور که در مرحله درخواست PBFT داشتیم، کلاینت $M_{REQUEST}$ را به C_m ارسال می کند و قالب پیام <REQUEST, o, t, c> است.
   b. **پیش آماده سازیِ c**[69]: C_m تراکنش صحیح رو در یک بلاک قرار میده و پیامِ زیر رو به گره‌های *replica* به صورت برادکست ارسال میکنه:

$$<<PRE\text{-}PREPARE,v,n,s,e_m>,d,l_m>$$

[65] Core node layer protocol
[66] primary
[67] replica
[68] Request
[69] **Pre-prepare$_c$**

c. **آماده سازیِ c[70]:** پس از دریافت پیام $M_{Pre\text{-}Prepare}$ گره C_i یک بررسی اعتبار انجام می دهد: بررسی میکند که آیا خلاصه دریافتی s, e_m با خلاصه تولید شده به صورت محلی برای d, l_m مطابقت دارد یا خیر. بررسی میکند که آیا v با نمای فعلی مطابقت دارد یا خیر. بررسی میکند که آیا پیام‌هایی با d و n یکسان اما خلاصه‌های متفاوت دریافت شده‌اند یا خیر. و در آخر بررسی میکند که همه‌ی تراکنش های موجود در بلوک ، معتبر هستند یا نه.

d. **اعزام C:**[71] بعد از اینکه گره $2f_1+1$ پیغام تایید شده $M_{PREPARE}$ را دریافت کرد، وارد فاز $commit_c$ می شود و سپس <COMMIT, v, n, s, ei, i> را به گره های اصلی برادکست می کند. به همین ترتیب، گره پیام را دریافت و تأیید می کند و پس از دریافت $2f_1+1$ پیغام تأیید شده M_{COMMIT}، در نظر می گیرد که بلوک در لایه گره هسته به اجماع رسیده است.

2. پروتکلِ لایه‌ی گروهِ هسته:[72] بعد از اینکه C_i تعدادِ $2f_1+1$ پیامِ M_{Commit} تایید شدخ دریافت کرد،مشخص می کند که لایه گره هسته به یک اجماع رسیده است. G_i داخل گروه اجماع را شروع می‌کند. با در نظر گرفتن G_m در تصویر 12 که C_m نقش گره اولیه را دارد و گره‌های سایه‌ی اختصاص یافته به اون نقش replica را دارند.

3. پروتکل تغییر نما در لایه گره هسته: پروتکل تغییر نما، وظیفه‌ی این رو داره که یک گره اولیه جدید رو تایید کنه، تا زمانی که گره اولیه‌ی فعلی با مشکل رو به رو شد، بتواند ادامه به کار سیستم رو تضمین کند. شماره نمایش لایه گره هسته v است. هنگامی که کپی ها نتوانند پس از بازه زمانی $2^{v+1} * T$ به یک اجماع برسند یا بلوک اشتباهی دریافت کنند، یک تغییر نما ایجاد می شود. نمای اصلی v همچنان تا زمانی که تغییر نما کامل شود معتبر است، بنابراین از تغییرات غیرضروری نمای به دلیل تاخیرهای گاه به گاه شبکه جلوگیری می شود.

---

[70] **Prepare$_c$**
[71] *Commit$_c$*
[72] *Core group layer protocol*

8. ارزیابی راهکار پیشنهادی

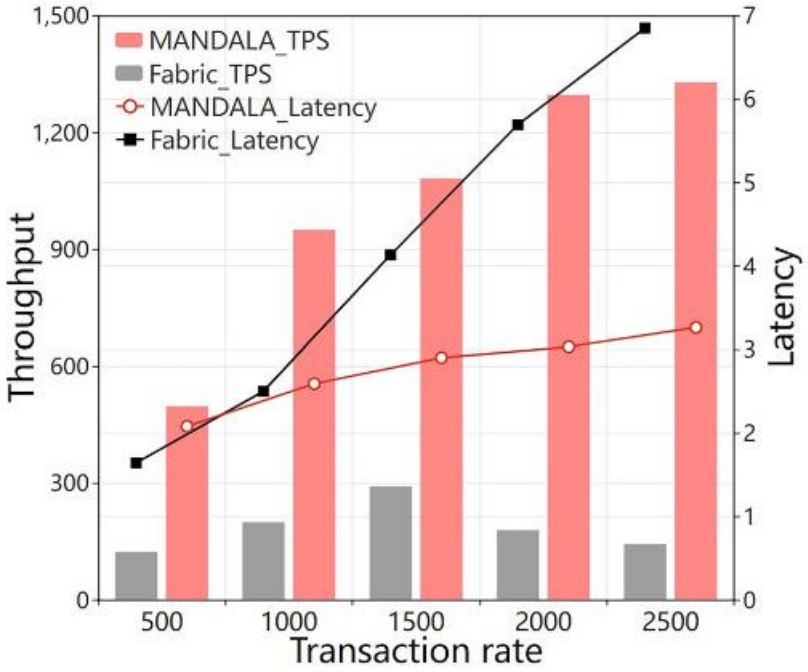
این مدل از جنبه‌های توان عملیاتی، تاخیر، زمان‌های ارتباط، نرخ انتقال موثر و امنیت با ترکیب اثبات نظری و آزمایش شبیه‌سازی آزمایش[۷۳] ارزیابی می‌شود. ین آزمایش بر روی پروژه بلاک چین Hyperledger Fabric ساخته شده است که یک سیستم متن باز ماژولار و قابل توسعه است.

- **توان عملیاتی و تاخیر**[۷۴]: توان عملیاتی و تأخیر معیارهای مهمی برای اندازه گیری عملکرد بلاک چین هستند. توان عملیاتی به تعداد تراکنش هایی اشاره دارد که سیستم بلاک چین می تواند در واحد زمان پردازش کند و تأخیر به مدت زمانی که طول می کشد تا یک تراکنش برای تکمیل ارسال شود، اشاره دارد. در این مقاله، تحت همان محیط شبکه، 16 گره شرکت‌کننده در اجماع راه‌اندازی شده‌اند، تعداد کل تراکنش‌ها 10000 تراکنش ثابت شده است و نرخ تراکنش (تعداد تراکنش‌های ارسال شده در هر ثانیه) 500 تا 2500 است. مقایسه مدل با Fabric، نتایج خروجی و تأخیر در شکل 13 نشان داده شده است. از نظر توان عملیاتی، با افزایش نرخ تراکنش، توان عملیاتی Fabric و MANDALA هر دو روند صعودی را در ظرفیت پردازش گره نشان می‌دهند، اما توان عملیاتی این مدل بالاتر است. با ادامه افزایش نرخ تراکنش، Fabric ابتدا به گلوگاه می رسد و سپس توان عملیاتی به طور قابل توجهی کاهش می یابد، در حالی که توان عملیاتی مدل ما همچنان در حال رشد است و به بیش از 1000 tps می رسد. بنابراین، ماندالا می تواند سطح بالایی از توان عملیاتی را حفظ کند و مقیاس پذیری بهتری را نشان دهد.

از نظر تأخیر، تأخیر فابریک با افزایش نرخ تراکنش به شدت افزایش می‌یابد که ناشی از پیچیدگی زیاد ارتباطی است. با افزایش نرخ تراکنش، تعداد پیام‌هایی که گره‌ها پخش و پردازش می‌کنند نیز افزایش می‌یابد که زمان زیادی می‌برد. ماندالا پیچیدگی ارتباط بهتری دارد و زمان ارتباط را تا حد

[73] theoretical proof and simulation experiment
[74] Throughput and latency

زیادی کاهش می دهد. اگرچه اجماع سلسله مراتبی و چند مرحله‌ای آن باعث می‌شود تاخیر اولیه بیشتر از Fabric باشد، اما با افزایش تعداد تراکنش‌ها، تاخیر اساساً ثابت می‌ماند. بنابراین MANDALA مقیاس پذیری بهتری دارد و برای شبکه های بزرگ مقیاس مناسب تر است.



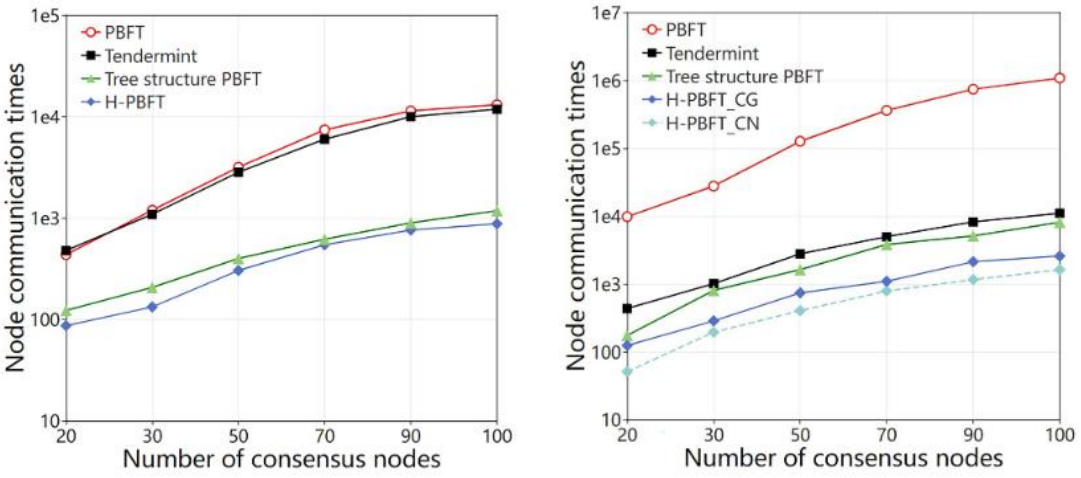
تصویر 13.توان عملیاتی و تاخیر

- **زمان ارتباط**[۷۵]:زمان‌های ارتباطی نشان‌دهنده ترافیک تولید شده توسط گره‌ها در فرآیند اجماع است [41]. مشکل اصلی PBFT و مکانیزم اجماع ناشی از آن پیچیدگی ارتباطی بالا است که باعث کاهش کارایی سیستم خواهد شد. هدف اصلی در طراحی H-PBFT کاهش پیچیدگی ارتباطات است.

شکل 14 زمان‌های ارتباط PBFT، Tendermint ، ساختار درختی PBFT و H-PBFT را نشان می‌دهد. PBFT معروف ترین الگوریتم عملی BFT است، Tendermint یک فرآیند ساده شده الگوریتم BFT مقیاس پذیر است، ساختار درختی PBFT یک الگوریتم BFT کارآمد بر اساس

[75] Communication times

ساختار شبکه درختی است. همانطور که در شکل 14 نشان داده شده است، با ادامه افزایش تعداد گره ها، PBFT و Tendermint باید اجماع را از طریق حجم ارتباطات با پیچیدگی $O(N^2)$ تکمیل کنند، که مقیاس پذیری افزایش تعداد گره‌ها را محدود می کند. هنگامی که تعداد گره ها خیلی زیاد است، PBFT به دلیل سربار ارتباط بیش از حد عملاً قابل استقرار نیست. هدف اصلی ساختار درختی PBFT و H-PBFT کاهش پیچیدگی ارتباطات است. هر دو به طور قابل توجهی ترافیک شبکه را کاهش می دهند، در حالی که H-PBFT پیچیدگی ارتباط را بیشتر بهینه می کند و ارتباطات کمتری ایجاد می کند. علاوه بر این، سربار ارتباطی H-PBFT هیچ ارتباطی با مقیاس گره های معمولی ندارد. تا زمانی که تعداد گره‌ها در شبکه اصلی نسبتاً ثابت باقی بماند، کارایی اجماع H-PBFT به سرعت با گسترش مقیاس گره کاهش نخواهد یافت. بنابراین، H-PBFT را می توان برای سناریوهایی با مقیاس گره بزرگتر اعمال کرد و به طور موثر مقیاس پذیری را بهبود بخشید.



9. نتیجه‌گیری

بعد بررسی‌های مختلفی که در بخش‌های مختلف در مورد اینترنت اشیا و بلاکچین انجام دادیم، ویژگی‌های هرکدوم رو لیست کردیم و به معایب و مزایای اون پرداختیم. گفتیم که میشه با ترکیب بلاکچین با اینترنت

اشیا، به مشکلاتی مانند امنیت تمرکززدایی و ... پرداخت، اما خود بلاکچین از مشکلاتی مانند کم بودم تعداد تراکنش در ثانیه و مقایس‌پذیری پایین رنج میبره.

این مقاله یک مدل بلاک چین مقیاس پذیر به نام MANDALA را پیشنهاد می کند که می تواند در سناریوهای مختلف بلاک چین مانند زنجیره های بدون مجوز یا دارای مجوز در مقیاس بزرگ استفاده شود. این مدل از الگوریتم H-PBFT برای دستیابی به اجماع بر اساس شبکه Mesh-and-Spoke پیشنهادی استفاده می کند. نتایج شبیه‌سازی نشان می‌دهد که این مدل می‌تواند سربار ارتباط را کاهش داده و بازده و بازده انتقال را بهبود بخشد. علاوه بر این، کارایی اجماع را از مقیاس گره های معمولی جدا می کند که به طور موثر مقیاس پذیری بلاک چین را بهبود می بخشد. بدون کاهش امنیت، استحکام الگوریتم اجماع تضمین می شود و توانایی مدل برای مقاومت در برابر حملات مخرب تضمین می شود. در مقایسه با دیگر طرح‌های بهینه‌سازی بلاک چین، ماندالا عملکرد، امنیت و مقیاس‌پذیری بهتری دارد.

10. ارجاعات

[1] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah, and R. Jayaraman, "Scalable blockchains — A systematic review," *Future Gener. Comput. Syst.*, vol. 126, pp. 136–162, Jan. 2022, doi: 10.1016/j.future.2021.07.035.

[2] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Tikiri—Towards a lightweight blockchain for IoT," *Future Gener. Comput. Syst.*, vol. 119, pp. 154–165, Jun. 2021, doi: 10.1016/j.future.2021.02.006.

[3] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A Review and State of Art of Internet of Things (IoT)," *Arch. Comput. Methods Eng.*, vol. 29, no. 3, pp. 1395–1413, May 2022, doi: 10.1007/s11831-021-09622-6.

[4] "ITU-T Recommendation database," *ITU*. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (accessed Dec. 17, 2022).

[5] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data Cogn. Comput.*, vol. 4, no. 4, Art. no. 4, Dec. 2020, doi: 10.3390/bdcc4040028.

[6] T. 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, May 2018, doi: 10.1109/ACCESS.2018.2842685.

[7] "Intelligence of things: opportunities & challenges - ePrints Soton." https://eprints.soton.ac.uk/422292/ (accessed Feb. 05, 2023).

[8] H. Atlam, A. Alenezi, M. Alassafi, and G. Wills, "Blockchain with Internet of Things: Benefits, Challenges and Future Directions," *Int. J. Intell. Syst. Appl.*, vol. 10, Jun. 2018, doi: 10.5815/ijisa.2018.06.05.

[9] J. Li *et al.*, "MANDALA: A scalable blockchain model with mesh-and-spoke network and H-PBFT consensus algorithm," *Peer--Peer Netw. Appl.*, Oct. 2022, doi: 10.1007/s12083-022-01373-w.

[10] J. Qi and Y. Guan, "Practical Byzantine fault tolerance consensus based on comprehensive reputation," *Peer--Peer Netw. Appl.*, Dec. 2022, doi: 10.1007/s12083-022-01408-2.

[11] “Practical byzantine fault tolerance and proactive recovery | ACM Transactions on Computer Systems.” https://dl.acm.org/doi/10.1145/571637.571640 (accessed Feb. 06, 2023).