یک شبکه ی مشترک امن و یک شبکه ی اجماع اثبات اعتبار

خلاصه

این وایت پیپر[1] ارائه دهنده ی موارد استفاده, چهارچوب فنی و پیاده سازی جزئیات Deeper Networkو پروژه ی پولکادات[2]که متشکل از اتصال Deeperخط دستگاه ها و اکوسیستم Deeper Networkاست، می باشد.

Deeper Networkیک فناوری بلاک چین همه در یک راه حل[3] است که آزادی اینترنت واقعی با افزایش امنیت و تجربه کاربری بدون اصطکاک را فراهم می سازد .

دستگاه های اتصال Deeperاتصال همتا به همتا شبکه را به صورت خصوصی و امن فراهم می سازند. کاربران اتصال Deeperیک شبکه ی اجماع غیر متمرکز واقعی بر اساس ساز و کار اجماع (POC)اثبات اعتبار خاص Deeperرا تشکیل خواهند داد.

اتصالDeeper اولین در نوع خودش است که تکنولوژی یا فناوری امنیت سایبری را با فناوری بلاک چین که توسط اقتصاد تسهیمی آنلاینonline sharing economy هدایت می شود را ترکیب می‌کند.

اتصال Deeperکاربران را به طور یکپارچه به اکوسیستم شبکه ی Deeperکه از زنجیره ی Deeperتغذیه می شود ،هدایت می کند.

زنجیره یDeeper یک پلتفرم قرارداد هوشمند واقعاً غیر متمرکز است که بر اساس مکانیسم اجماع اثبات اعتبارPOC اجرا می شود.

زنجیره یDeeper با امنیت بالایش ،کارایی بالا و مصرف انرژی کم توصیف می‌شود.

نود های[4]اتصال Deeper به طور خودکار می توانند در استخراج زنجیره ی Deeperشرکت کنند.

زنجیره یDeeper بسیاری از وب سرویس های بنیادین را قادر می سازد تا درشبکه یDeeper به عنوان مثالdDNS وdCDN وغیره توسعه یابند.

راهی را برای انقلاب وب ۳.۰هموار می‌کند.

توسعه‌دهندگان همچنین می توانند برنامه‌های کاربردی خودشان را در زنجیره یِ Deeperتوسعه داده و توزیع کنند.

برنامه‌هایd Apps در زنجیره یDeeper برای حفظ حریم خصوصی و داده کاربر و اطمینان از حاکمیت داده‌های شخصی، مناسب‌تر خواهد بود.

[1] whitepaper
[2] polkadot
[3] All in one solution
[4] nodes

فهرست

[5] Trident protocol
[6] multiplexing
[7] Gateway
[8] Cross platform

[9] Rig
[10] Blockchain

[11] Toknomics
[12] staking system
[13] governance
[14] Treasury pool
[15] Road map
[16] Token

۱.مشکلات عصر وب ۲.۰

تکثیر اطلاعات زمانی آغاز شد که بی شنگ [17] اولین نوع متحرک را با استفاده از مواد چینی اختراع کرد. صد سال پیش، یوهانس گوتنبرگ[18] نوع متحرک دستگاه چاپ را در اروپا اختراع کرد. امروزه پس از هزار سال از اختراع بی شنگ, اینترنت تکامل یافته ترین فناوری برای اشتراک گذاری و ذخیره اطلاعات به صورتی که با نمایش یک شتاب غیر قابل باور در جریان اطلاعات آنها را به راحتی در اختیار میلیاردها نفر از مردم قرار می دهد. درست مانند دستگاه چاپ آن زمان، اینترنت انقلابی در انتشار دانش ایجاد کرده است که هیچ ویژگی منحصر به فرد از نخبگان نداشته اند. توسعه سریع فناوری اینترنت، ما را به سمت بحران نقطه عطف در تاریخ سوق داده است. دنیایی که ما در آن زندگی می کنیم عمیقا توسط داده ها تغییر می کند .با ظهور عصر وب۲.۰ ،داده ها همچون هویت های کاملاً دیجیتالی ساخته شده در اینترنت، شخصی تر شده است. بر اساس این حقیقت، در سال IBM,۲۰۱۳ اهمیت داده را برای قرن ۲۱ ،همچون قدرت بخار برای قرن ۱۸ ،برق برای قرن ۱۹ و هیدروکربن‌ها برای قرن بیست اعلام کرد. با وجود اهمیت داده، جمعیت تا حد زیادی از خطرات داده‌های شخصی که توسط تعداد کمی از افراد منتخب کنترل می‌شود ،قدرتی که اکنون بر ما دارند، بی اطلاع هستند.

جرائم سایبری ۱.۱

انتشار ویروس های شبکه یک تهدید بی حد و مرز است و سبب آسیب‌های اقتصادی جدی می‌شود. در سال ۲۰۱۷ ،۱.۶۵ میلیون کامپیوتر توسط ویروس های شبکه ربوده و مجبور به مشارکت در استخراج ارزهای دیجیتال(۳۷) شدند. با توسعه ی اینترنت(Things(IoT، محدوده ی مداخلات مخرب به گونه‌ای جهشی افزایش یافته است. ویروس‌های(IoT) می‌توانند کامپیوترهای شخصی، دوربین ها، لوازم هوشمند، قفل درهای هوشمند، روترها و دیگر دستگاه‌های قابل دسترس به اینترنت را بربایند. با شروع ویروسMirai(۳۳) در ژوئن سال ۲۰۱۸ بیش از ۶۰۰ هزار دستگاه شبکه ای هک شده است(۵۰). به علاوه ،حملات فیشینگ[19] توسط وبسایت های مخرب راه اندازی شده اند که می توانند اطلاعات شخصی حساس مانند نام کاربری گذرواژه ها و جزئیات کارت اعتباری از طریق پنهان شدن به عنوان اشخاص و سازمانهای مورد اعتماد(۴۰) به دست آورند. در سال ۲۰۱۷ ،سیستم ضد فیشینگ کسپرسکی [20]بیش از ۲۴۶ میلیون بار فعال شد و ۱۵.۹ درصد از کاربران آن برای سایت‌های فیشینگ (۱۶)هدف قرار گرفتند. درپی ضررهای مالی ناشی از وب سایت های فیشینگ از دسامبر سال ۲۰۱۳ تا دسامبر سال ۲۰۱۶ پلیس فدرال آمریکا[21] ۲۲۰۰۰ مورد کلاهبرداری فیشینگ را در ایالات متحده در مجموع بیش از۱.۶ میلیارد دلار آمریکا(۳۱) رسیدگی کرد. تخمین زده می شود که سال ۲۰۲۰ رکورد خسارت تقریباً یک تریلیون دلار دو برابر بیشتر از سال ۲۰۱۸ رقم می خورد(۴۳). این تا حدی ناشی از همه گیری ویروس‌کرونا است زیرا هکرها مشتریان ،مشاغل و جمعیت عظیمی که به کار از راه دور روی آوردند را قربانی می کنند. هکرها دیگر دستگاه‌های خاصی را هدف قرار نمی دهند بلکه هدف کل سازمان ها که با

---

[17] Bi sheng
[18] Johannes Gutenberg
[19] phishing
[20] kaspersky
[21] FBI

استفاده از اپراتور های انسانی به عنوان حلقه های ضعیف به خاطر دسترسی به کل شبکه ها می باشد.تراولکس[22](یک شرکت خدمات مالی بریتانیایی)یک شرکت تبادلات خارجی با فعالیت در ۷۰ کشور جهان نمونه‌ای از این وضعیت است .این شرکت باید برای پرداخت هزینه به منظور رمزگشایی فایل های حیاتی کامپیوتر پس از برخورد با sodinokibiیکی از پیچیده‌ترین حملات باج افزاری تا به امروز که حمله ای ویرانگر انجام داده است(۱۵) با مطالبات روبرو می‌شود. این ارقام و اشکال جای تعجب ندارد همانطور که تعداد کاربران اینترنت دائماً با نرخ یک میلیون در روز در حال افزایش است. تخمین زده می‌شود که تا سال ۲۰۳۰ هفت میلیارد کاربر در سراسر جهان با یک تریلیون سنسور شبکه تعبیه شده در جهان اطراف ما تا سال۲۰۲۲ و در مجموع ۴۵ میلیون در ۲۰ سال آینده وجود خواهد داشت(۲). جرایم سایبری, انگل غیرقابل اجتنابی است که در پی فعالیت‌های بشر صورت می‌گیرد به طوری که اکنون بیش از بلایای طبیعی هزینه در بر دارد و بیش از تجارت مواد مخدر قابل حمل تر است(۳۴) جرایم سایبری یکی از بزرگترین خطرات برای مشاغل و افراد خواهد بود.

۱.۲ سرکوب اطلاعات و سانسور اینترنت

سرکوب اطلاعات و سانسور اینترنتی به عمل نفی میزان آزادی بیان خاص که با محروم کردن کاربر از برخی حقوق در اینترنت به طوری که هویت کاربر یا آی پی[23] وی قادر به مرور وب یا ارسال پیام نباشد(۵) ،اطلاق می شود. بسیاری از کشورها در سراسر جهان تعداد زیادی از وب‌سایت‌ها را به دلایل مختلف(۲۵)،(۲۶)،(۵۴) از جمله ایالات متحده که طرفدار باسابقه آزادی بیان است ،مسدود کرده‌اند. ممنوعیت اخیر حسابهای رسانه های اجتماعی توسط دونالد ترامپ[24] بیانگر این است که حتی در سرزمین آزادی ,آزادی بیان در اینترنت تضمین نمی شود. رویداد سهام GMEیک نمونه ی کامل اخیر از سانسور به‌عنوان بسترهای معاملاتی است مانند رابین هود [25]وE مارکت که تمامی معاملات برای سهام مربوطه متوقف شد. حتی بستر دیسکورد[26] برای دوستداران بازی ,چت گروهی که بعدها به نامWSB شد را تعطیل کرد تا هماهنگی هر چه بیشتر این گروه تجاری را خنثی کند با توجه به این آزادی اینترنت جهانی برای دهمین سال متوالی کاهش یافته است همانطور که امتیاز ۲۶ کشور در طی دوره ی پوشش سال های ۲۰۱۹ ۲۰۲۰ کم شده است، امتیاز ایالات متحده برای چهارمین سال متوالی افول کرده است. با اینکه فیس‌بوک[27] توییتر[28] و سایر بسترهای رسانه های اجتماعی به عنوان ابزاری برای فعالیت‌های اجتماعی مورد استفاده قرار گرفتند، نظارت بر رسانه های اجتماعی توسط دستگاه‌های اجرایی محلی و فدرال[29] اثربخشی این ابزارها را خنثی می کند بعضی اشخاص آزار و اذیت هدفمند را تجربه می‌کنند یا اتهامات مجرمانه ای جعلی برای پست ها یا بازتوییت های(۴۷) خودشان مطرح می شود. در راستای این همه راحتی و تسهیلات امکانات برای سانسور و نظارت در اینترنت نیز ذاتی و طبیعی است. این مشکلات آن قدر رایج و گسترده است که مردم مجبورند در ازای سهولت در اینترنت(۵۶) حریم خصوصی را کنار

[22] Travelex
[23] IP
[24] Donald Trump
[25] Robinhood
[26] Discord
[27] Fasebook
[28] Twitter
[29] Federal&local enforcement agencies

بگذارند و اغلب ناآگاهانه از اطلاعات حقوق خصوصی محروم می شوند(۱۹) اغلب اطلاعات شخصی توسط ارائه دهندگان خدمات کنترل می‌شود و حتی برای سود و منفعت به شخص سوم (ثالث)فروخته می‌شوند(۲۲)(۲۴). این نقل قول قدیمی از دهه ۷۰ هرگز درست نبوده است "اگر هزینه محصول را نپردازید شما خود محصول هستید."

توجه: به خاطر سیاست های مختلف در مناطق و کشورهای مختلف شبکه یDeeper ویژگی های دسترسی برای نسخه های فروخته شده در مناطق مختلف را تنظیم و محدود می سازد و نسخه های متفاوتی برای کشورها راه اندازی می‌کند تا از سازگاری محصولاتDeeper با قوانین و مقررات آنها اطمینان حاصل کند. این لزوما به معنای این نیست که ما با چنین محدودیت هایی موافقیم در حالی که ما اینترنت بی حد و مرز و رایگان را در نظر داریم. در حالی که ما به قوانین محلی احترام می‌گذاریم، ما قدم‌های پیشگامانه ای به سمت فرایند جمعی و طولانی برای دموکراتیزه کردن[30] شبکه بر می داریم.

1.3بحران اعتماد اینترنت

از زمانی که ارائه دهندگان خدمات اینترنتی و دیگر شرکت‌های بزرگ آنلاین توانستند اطلاعات کاربران را نظاره، ذخیره و بفروشند بدیهی است که اینترنت فاقد حریم خصوصی اطلاعات می باشد. این واقعیت ناگفته نماند همچنین آنها می توانند مشخصات شما را داشته باشند و این اطلاعات را با سازمان‌های دولتی به اشتراک بگذارند وسعت این نظارت عمیق و بسیار مزاحم است .از ژانویه سال ۲۰۰۵ تا مه سال ۲۰۰۸ بیش از ۲۰۰ میلیون مورد مشکوک به پرونده های حساس شخصی که نقض کرده‌اند (۱۰)وجود داشته است. در نتیجه، موسسات پزشکی ۶.۲ میلیارد دلار در سال ۲۰۱۴ و ۲۰۱۵ ضرر کرده اند.درسال۲۰۱۸،داده های فیس بوک و کمبریج(۴۹) نقض شد و بار دیگر توجه جهانی را به سمت تهدید نشت داده ها جلب کردند. در حقیقت، مسئله ی نقض داده ها در سراسر جهان رایج است (۲۷). این هراس القاء نقض داده ها ناشی از ماهیت بسیار متمرکز اینترنت و اثرات جانبی تجارت اطلاعات(۵۱) می باشد. با توجه به مشکلات فوق، جای تعجب نیست که اینترنت امروزی به طور کامل مورد اعتماد باشد، عدم شفافیت و زیرساخت‌های قابل اعتماد، بحران اعتماد را ایجاد کرده است. در حقیقت، سرکوب ،سانسور، فریب و دیگر انواع فعالیتهای مخرب معمول نیستند. بیت کوین [31]در سال ۲۰۱۹ در نتیجه بحران مالی سال ۲۰۰۸ پدید آمد. یک رویداد در زمانی که تعداد زیادی از بانکها و سایر موسسات مالی در سراسر جهان شکست خوردند و از طریق دولت با هزینه مالیات دهندگان شان باید وثیقه می‌گذاشتند. این وضعیت منجر به از دست دادن اعتماد کامل و اعتماد به سیستم مالی شد. بیت‌کوین یک شکل غیرمتمرکز پول نقد دیجیتال در نظر گرفته شد و هدف آن از بین بردن نیاز به واسطه های سنتی مانند بانک‌ها و دولت‌ها برای انجام معاملات مالی بود. دیدگاه اصلی مال ساتوشی [32]بود که هر رایانه با یک رای در روند استخراج مشارکت کند. متاسفانه، این دیدگاه خیلی زود از بین رفت .تا سال ۲۰۱۲ ،دستگاه‌های سخت افزار استخراج تخصصی پدید آمدند که تحول به سمت صنعتی شدن را آغاز کردند .به زودی مزار صنعتی وسیع ماینرهای سرگرم کننده معمولی را از بازی خارج کردند. این موضوع به طور ناعادلانه توجه عرضه درچند دست را به عنوان متمرکز سازی استخراج معرفی کرده است. اگر یک گروه ماینرها ۵۱

[30] democratizing
[31] Bitcoin
[32] Satoshi

درصد از کل عرضه را کنترل کنند ،شبکه در آن لحظه متمرکز می شود. شبکه Deeperمعتقد است دیدگاه ساتوشی قابل دستیابی است و می‌خواهد در این زمینه با معرفی الگوریتم اجماع اثبات اعتبار(POC) در بین کاربران خود نفوذ کند به طوری که همه هر یک بتوانند شرکت کنند. ما معتقدیم دیدگاه ما از طریق توسعه ی فناوری و تجربه‌ای که تیم ما در طی سال ها در زمینه طراحی سخت افزار، سیستم عامل ها، امنیت سایبری و بلاکچین ها جمع آوری کرده اند،امکان پذیر است.

۱.۴ عقائد هسته یِDeeper

عقاید هسته ی Deeperعبارتند از:

1.آزادی:دموکراتیزه کردن شبکه

رفع محدودیت های شدید اعمال شده توسط سیاست ها و سانسور بر جریان اطلاعات به منظور دستیابی به تبادل داده بدون اصطکاک بین کل نژاد بشر می باشد.

۲.عدالت:بلاکچین برای همه

نفوذ به ارزش واقعی فناوری بلاک چین برای توانمند سازی مردم عادی به جای اینکه یکی از مکانیسم بسیار را از طریق درصد کمی از افراد ممتاز ایجاد کند. یک شبکه اجتماعی غیرمتمرکز واقعی باید بستری باشد جایی که هم مجاز به شرکت و هم بهره مندی از آن هستند .این باید در خدمت جامعه به طور کامل باشد به جای اینکه یک سازمان متمرکز یا یک گروه از افراد قدرتمند خدمت کنند.

۳.اعتماد

اطلاعات قدرتمندند و به مردم تعلق دارند.

مشابه خانه ها،زمین و پس اندازها،داده های شخصی نوعی مالکیت خصوصی هستند و به طوری که اهمیت حفاظت از آن شایستگی دارد. ماموریت نهاییDeeper ترکیب امنیت و فناوری بلاک چین برای ایجاد یک اینترنت قابل اعتماد که حاکمیت داده‌های شخصی را تضمین می‌کند.

۲.بررسی اجمالی پروژه

۲.۱اتصال Deeper

۲.۱.۱معرفی و فلسفه ی طرح

اتصالDeeper یک بلاک چین که همه را در یک راه حل کار می‌کند که آزادی اینترنت واقعی را با امنیت بالا و تجربه کاربری بدون اصطکاک را ایجاد می‌کند .فلسفه طرح اتصال Deeperهمزمان با وصل کردن به برق بدون هیچ ترتیبی اجرا می شود کاربران می توانند از امنیت شبکه حفاظت شده بدون نیاز به پرش از طریق هیچ حلقه ای[33] لذت ببرند. نه دانش فنی و نه راهنمای کاربر پیچیده مورد نیاز است. تنها کاری که باید انجام داد این است که دستگاه را بین مودم و روتر به برق وصل کنید و آن را روشن کنید و از همه مزایای آن لذت ببرید: دور زدن سانسور، محافظت در برابر حملات سایبری، تنظیم کنترل والدین، مشارکت در اشتراک گذاری پهنای باند شبکه و استخراج بلاک چین از مزایای آن است.

شکل۱(تعاملات محصولات)←شکل در فایل اصلی موجود است

[33] hoops

نسل های تعاملات متنوع را از۱←Deeper connect Lite تا ۲← Deeper Connect Miniتا۳←Deeper Connect Nanoو حالا ۴←Deeper Connect Picoبا هر نسخه ابعاد کوچکتر مشاهده کرده است. چشم انداز اتصال Deeperهمیشه این بوده که خود را به کابل شبکه محلی تا جایی که ممکن است نزدیک نماید با این باور که فناوری عالی در پس‌زمینه ترکیب می‌شود و از سر راه کاربران برداشته می‌شود.Deeper Connect Pico نشان دهنده ی آخرین تجسم از این اخلاق است. طیف دستگاه‌های اتصال Deeper از بدو تاسیس با هزاران مورد فروش در سراسر جهان، استقبال عظیم کاربران را مشاهده کرده است. یکی از برترین محصولات ایندی گوگو[34] است.

۲.۱.۲راه حلی برای اینترنت با امنیت بیشتر،خصوصی و عادلانه

اتصال Deeperنسل هایی از تکرار اعم از۱←Deeper Connect Lite تا ۲← Deeper Connectکه هم به عنوان یک نود در شبکه ی خصوصی غیرمتمرکز و هم نسل بعدی فایروال[35]را در شبکه خانگی ارائه می دهد، را مشاهده کرده است. شبکه ی خصوصی غیرمتمرکز بدون سرور و توزیع شده اند. اطلاعات کاربران هرگز نمی توان وارد شد، لوداد ،هک کرد، یا احضار کرد. فایروال های درجه یک 7 لایه ای ,کل شبکه ی خانگی کاربران را ایمن می کند .تبلیغات را مسدود می‌کند، ترافیک وب را نظارت می کند وNSFWوNSFC در کل دستگاه‌های اینترنتی فیلتر می نماید.

۲.۱.۳ تور فنی deForceوAtomOS ،پروتکل سه گانه و IPچندگانه

Atom OS

هسته امنیت شبکه ی اتصالDeeper ها در ارتباط با AtomOSکه یک سیستم عملیاتی شبکه طراحی شده و توسعه یافته توسط Deeperاست ،استعداد نهفته است. AtomOSاولین قفل رایگان سیستم عامل شبکه در جهان است. ویژگیهای سیستم دسترسی بالا ،عملکرد بالا و مقیاس پذیری بالا که همگی به طراحی بدون قفل در وضعیت هنری‌اش بستگی دارد.

پروتکل سه گانه

Deeperپروتکل سه گانه ی خود را توسعه داد که یک پروتکل ارتباطات مشترک و غیر متمرکز است و مبتنی است بر بلاک چین با تونل زنی تطبیقی و فناوری های مسیریابی هوشمند که با حفاظت امنیتی عمیق به علاوه بهبود تجربه کاربر را ایجاد می‌کند. این سانسور شبکه را دور می‌زند، انتقال داده ها را ایمن می کند، استفاده از پهنای باند شبکه را به حداکثر می رساند و تاخیر در فرایند انتقال بسته داده را کاهش می دهد. این به لطف ادغام موثر فناوری‌های شبکه همچون نفوذ اینترانت، رمزگذاری داده، پروتکل پوشش و کنترل تراکم لایه تونلی به دست می آید .جزئیات بیشتر در بخش5.1 است.

IPچندگانه

[34] Indiegogo
[35] Firewall

فناوریIP چندگانه ثبت شده درDeeper ترتیب آدرسIP صفر و سازگاری هوشمند آدرسIP روتر برای ارتباط خودکار از طریق وصل واقعی دستگاه های اتصال Deeperبه برق و داشتن تجربه واقعی دسترسی به اینترنت را دارد.

۲.۲شبکه یDeeper

۲.۲.۱ پایه گذاری اساس و بنیاد وب ۳.۰

Deeperبرای غیر متمرکز سازی واقعی و دموکراسی اینترنت تلاش می‌کند .غیر متمرکز سازی واقعی به معنای این است که نه سازمان واحدی می تواند به تمام سطوح شبکه تسلط داشته باشد و نه هیچ نقطه واحدی از خرابی بر کل شبکه تاثیر خواهد گذاشت. زنجیره های chainعمومی غیر متمرکز، برنامه های غیر متمرکز و گیت وی های[36] غیر متمرکز ضروری هستند. به عنوان مثال، شبکه اتریوم[37] فعلی هنوز در سطح گیت وی متمرکز می شود و بیش از حد به خدمات رابط APIایجاد شده از طریقInfura برای برنامه هایdApps اصلی وابسته است.Infuraخودش به خدمات ابری (AWS(cloud servicesتوسط آمازون[38] متکی است. این بدان معناست که اکوسیستم اتریوم نمی‌تواند به طور واقعی ساختار شبکه متمرکز را تشخیص دهد و به طور طبیعی معایب ساختار شبکه متمرکز باقی می ماند. Infuraاخیر این را در زمان خرابی مجدداً تایید می کند به این منظور که این منجر به ناکارآمدی اکثر برنامه‌های dAppsاتریوم شده است. شبکه ی Deeperدر حال ایجاد غیر متمرکز سازی در هر سطح از پشته[39] از یک زنجیره ی عمومی غیر متمرکز در زنجیره ی Deeperبه سمت گیت وی (دروازه) غیرمتمرکز دراتصالDeeper است. Deeperدر حال پایه گذاری زمینه ای برای نسل بعدی اینترنت است.

۲.۲.۲شبکه ی خصوصی غیرمتمرکز(DPN)

شبکه خصوصی غیرمتمرکز یک شبکه اشتراک گذاری پهنای باند غیر متمرکزP2P برای دور زدن سانسورها و اطمینان از حفظ حریم خصوصی است. شبکه بدون سرور و توزیع شده است؛ هرگز نمی توان اطلاعات کاربران ثبت، نشت،هک و احضار کرد .هر یک از عاملان[40] گره (نود)هم قدرت مشتری و هم سرور را دارند ؛ عوامل گره(نود) پاداش استخراج برای مشارکت پهنای باند به شبکه را دریافت می‌کنند. مشوق استخراج، قدرت شبکه را در مقایسه با مدل‌های شبکه ی سنتیP2Pتضمین می کند.

۲.۲.۳وب غیرمتمرکز(DWEB)

هر کس می‌تواند وبسایت خودش را بسازد و در شبکه ی Deeperآن را به ثبت برساند. در شبکه ی Deeperآدرس IPسرور وب پنهان است که وب سایت ها را در برابر سانسور ها و حملات DDoSمقاوم می سازد. شبکه ی Deeperهمچنین خدمات زیر ساخت بنیادین برای وب۳.۰ با DNS(dDNS)غیر متمرکزDeeperوCDN(dCDN)غیر متمرکزDeeper ایجاد می کند. DNSمعماری برای برطرف سازی آدرس IPو پرس جو از اینترنت است.داشتن زیر ساخت متمرکزDNS اینترنت را بسیار ضعیف

---

[36] Gateways
[37] Ethereum
[38] Amazon
[39] stack
[40] operator

می سازد و مستعد سانسور و حملات می کند. خدمات DNSغیر متمرکز کمک به ایجاد اینترنت دموکراتیک تر می کند. CDNتجربه ی مرور وب را از طریق ذخیره سازی محتوا در ابر[41] تسریع می کند .CDNغیرمتمرکز اجازه دسترسی سریعتر edgeبه محتویات ذخیره شده را می دهد .

۲.۲.۴گیت وی(دروازه)غیرمتمرکز(DGATE)

اتصال Deeperیک گیت وی(دروازه) غیر متمرکز به سمت وب.۰ ۳ است کاربران اتصال Deeperنه تنها می‌توانند به خدمات شبکه غیرمتمرکز متنوع از طریق شبکه Deeperبه طور ایمن دسترسی داشته باشند، بلکه آنها می‌توانند همچنین به طور یکپارچه به برنامه‌های متنوع dApps شخص سوم همچون خدمات ذخیره سازی غیر متمرکز در اکوسیستم پولکادات یا خدمات DeFiدسترسی پیدا کنند. دروازه های غیر متمرکز به عنوان نود ها(گره ها) تضمین می کند که اکوسیستم Deeper در برابر مسائلی مانند زمان خرابی Infuraمعروف که اکو سیستم اتریوم را لرزاند و در نتیجه دروازه ی متمرکز به اکثر خدمات در شبکه ی اتریوم دسترسی پیدا کردند، مقاوم است.

۳.سخت افزار

هدف اتصال Deeperارائه ی راه حل سخت افزاریplug and playرا برای امنیت، به اشتراک گذاری اقتصاد و بلاک چین همه در یک راه حل است. نکات برجسته سخت افزاراتصالDeeper در زیر توضیح داده شده است.

۳.۱چند سکویی

اتصال Deeperطوری طراحی شده است که با پلتفرم های سخت افزاری مختلف سازگار است. AtomOSبه طور موفقیت آمیزی بر روی هر دو پردازنده ی اینتل[42] وARM64اجرا می شود که Deeperاز مزایای هر دو پلتفرم بهره ببرد (سیستم عامل اینتل به اندازه کافی قدرتمند هستند تا انواع سناریوهای عالی اضافه بار شبکه کهDeeperرا قادر می سازد نه تنها موارد استفاده پیچیده از شبکه‌های خانگی را پوشش دهد ،بلکه همچنین سطح نیازمندی‌های(الزامات) پروژه را برآورده می‌کند.)

از سوی دیگر پلتفرم ARMبه دلیل مصرف کم انرژی و قیمت ارزان مشهور است که این برای نیازهای معمولی شبکه ی خانگی و انواع مختلف موارد استفاده از موبایل شایسته است. در آینده ,Deeperهم چنین برای محصولات ARM32که هزینه سخت افزار را به کمتر از ۱۰ دلار کاهش می‌دهد، برنامه‌هایی دارد.

۳.۲مصرف انرژی پائین

طبق ارزیابی متخصصان اقتصادی(۴) کل مصرف انباشته سالانه انرژی از استخراج بیت کوین در سراسر جهان ۶۸.۸۱ میلیارد کیلووات بر ساعت رسیده است ؛شش برابر انرژی مصرفی در مه سال ۲۰۱۷ که ۱۱.۵۷ میلیارد کیلووات بر ساعت بوده است. مصرف انرژی تمام ماینرهای بیت کوین در سراسر جهان مشابه جمهوری چک است که استخراج ها معادل ۰.۳۱درصد از

[41] Cloud
[42] Intel

مصرف انرژی جهان بوده است.میانگین مصرف انرژی برای هر تراکنش بیت کوین برابر با ۹۶۸ کیلو وات بر ساعت است یعنی مصرف انرژی ۳۲ خانواده آمریکایی در یک روز است. در حال حاضر، میزان انتشار کربن سالانه بیتکوین ۳۳،۸۵ میلیون تن یا ۱۳۰۰ کیلو گرم کربن در هر بیت کوین(۳۰) است .طراحی منحصر به فرد و الگوریتم اجماع POC Deeperاین مشکل را با استفاده از ریگ های استخراج[43] که در شبکه ی اجماع با منابع محاسباتی بسیار کم شرکت می کنند، حل می کند. اتصالDeeper از پردازنده های تعبیه شده کم مصرف برای ساخت یک شبکه ی اجماع و اشتراک گذاری شبکه، استفاده می کند. حداکثر انرژی مصرفی یک دستگاه اتصال 15,Deeper وات است. حداکثر انرژی مصرفی اتصالDeeper Mini ۵ وات است. همانطور که در جدول ۱ مشاهده می کنید ،اتصالDeeper یکی از پر انرژی ترین محصولات در بازار است(تقریباً سه مرتبه قدر مصرف انرژی کمتری نسبت به ریگ های استخراج ASIC/GPUدارند) و پتانسیل تبدیل شدن به سوداورترین ریگ استخراج بلاک چین را دارند.

انرژی مصرفی	انواع سخت افزار
w۵_۱۵	Deeper connect
w۲۰۰۰_۳۰۰۰	ریگ استخراجASIC
w۱۰۰۰_۲۰۰۰	ریگ استخراج_GPU

جدول ۱ :مقایسه ی انرژی مصرفی ریگ های استخراج

کیف پول سخت افزاری

سخت افزار امنیتیDeeper همچنین یک ویژگی کیف پول ارز رمزنگاری شده را برای ایجاد کاربرانی با بالاترین سطح امنیت ارز رمزنگاری شده بدون نیاز به هیچگونه دانش و بلاک چین یا امنیت شبکه از سوی کاربران،ادغام می کند.

اتصالDeeper چندین ضمانت امنیتی با AtomOSارایه می‌دهد که باعث می‌شود این برای خرابکاران(دزدان اینترنتی) و سازمانهای مخرب که کنترل سخت افزار را از دور به دست می‌آورند، غیرممکن شود. در نتیجه، اطلاعات کلیدی ذخیره شده در دستگاه غیر قابل دسترسی برای خرابکاران است. به علاوه ،حملات مخرب شناسایی خواهند شد و برای کمک به دستگیری خرابکاران ضبط می‌شوند.

شکل۲ :دستیابی مخرب متوقف وضبط خواهد شد←شکل در فایل اصلی موجود است

اتصال Deeperاز فناوری رمزگذاری سه گانه برای تضمین امنیت دستگاه های ذخیره سازی استفاده می کند. حتی اگر یک دستگاه سخت‌افزاری از بین برود، هیچ کس نمی تواند به داده ها ذخیره شده در دستگاه نفوذ کند. فناوری رمزگذاری سه گانه شامل رمزگذاری دستگاه بلوک ای، رمزگذاری فایل سیستم و رمزگذاری فایل هاست.

۳.۳.۱رمزگذاری دستگاه بلوکه ای

[43] Rig mining

اگر دستگاه ذخیره سازی از بین برود، خرابکاران کراکر[44] می توانند فایل های مهم را از طریق تجزیه و تحلیل داده در دستگاه بلوک ای بخوانند. برای مقابله با آنها، هر بلوکه در اتصالDeeper با-AES CBC(14)(شکل۳) رمزگذاری شده است که این باعث میشود دزدی داده بسیار مشکل شود به خاطر اینکه خرابکاران فقط می‌توانند به داده‌های رمزگذاری شده دسترسی داشته باشند.

۳.۳.۲رمز گذاری فایل های سیستم

حقیقتاً به کارگیری رمزگذاری دستگاه بلوکه ای برای اطمینان از امنیت دستگاه کافی نیست .برای محافظت بیشتر و ذخیره سازی رسانه‌های اجتماعی مان، اتصالDeeper ساختار داده های کلیدی از فایل های سیستم کلی به هم ریخت(شکل ۴) .

شکل۳:کل داده دیسک در اتصالDeeper توسط AES-CBCرمز گذاری شده است.

با توجه به رازداری سختگیرانه از ساختار داده های DeeperFSو خرابکاران نمی توانند هر گونه اطلاعات دستگاه بلوک ای مربوط به ساختار فایل های سیستم را بازیابی کنند و بنابراین نمی توانند به هرگونه فایل مهم ذخیره شده در فایل های سیستم دسترسی پیدا کنند.

***شکل۴:*فایل های سیستم رمز گذاری شده، خرابکاران را گیج می‌کند.**

۳.۳.۳رمز گذاری فایل

تمامی فایل های مهم ذخیره شده در فایلهای سیستم اتصالDeeper باید از طریق AES-CBCرمز گذاری شوند. کلید رمز گشایی برای تمامی فایل ها فقط در کد برنامه کامپایل [45]است این بدین معناست که فقط برنامه ی Deeperمی‌تواند در صورت نیاز به اطلاعات متن ساده دسترسی پیدا کند(شکل ۵).

شکل۵:فناوری رمزگذاری سه گانه امنیت داده اتصال Deeperرا تضمین می کند.

۳.۴ریگ استخراج با امنیت شبکه

در ۲۸ مه سال ۲۰۱۸ "بسته مرگ "در اتریوم (CVE2018-12018)کشف شد (۳۹)جایی که حمله کنندگان می توانستند نودهای گت[46] از طریق ارسال به بسته ی مرگ مسدود کنند.گت مشتری اصلی اتریوم است که برای پروژه ی اتریوم بسیار مهم هستند ؛حدود ۷۰ درصد از نودهای در حال اجرای گت شامل نود های کلیدی برای تبادل عمومی و استخرهای استخراج هستند .با این باگ(اشکال)[47]یک حمله کننده می‌تواند اتریوم را خراب کند و با یک زمین لرزه در بازار اتریوم رها شود. پس از ارایه خدمات اشتراک گذاری شبکه ،اتصال Deeperبه خوبی ریگ های استخراج زنجیره عمیق تر خواهد شد. در حال حاضر، مسئله ی امنیت ریگ های استخراج نادیده گرفته شده است؛ با این حال، اگر یک خرابکار باگ های(اشکالات) نرم‌افزاری استخراج یا ضعف های سخت افزاری استخراج را مورد هدف قرار دهد همچون یک حمله که به طور طبیعی تأثیر قابل توجهی بر روی ارزش مربوط به ارز رمزگذاری شده

[44] Crackers
[45] Compiled program code
[46] Geth nodes
[47] Bug

دارد . تمامی محصولات ژن های امنیت شبکه را به ارث می برند و تمامی آنها دقیق طراحی شده و کاملا آزمایش شده اند. دستگاه های امنیت در حال اجرا امن ترین ریگ های استخراج در جهان خواهند بود که حداکثر محافظت از زنجیره ی و منافع تمامی ماینر هایش را دارد.

شکل۶:اتصال با ژن های امنیتی شبکه به ارث برده اش محافظت بیشتری برای زنجیره ی ایجاد می کند.

۴.سیستم عامل

معماری نرم افزار Deeperشامل یک صفحه داده، صفحه مدیریت و یک صفحه کنترل است. صفحه داده یا AtomOSپیشرفته به طور مستقل Deeperاجرا می شود که وظیفه رسیدگی به انتقال بسته داده کاربران، دریافت و بازرسی عمیق را برعهده دارد. صفحه مدیریت یک رابطه ی کاربر پسند برای نظارت بر روی عملیات سیستم یا تغییر تنظیمات سیستم، ارائه می دهد. صفحه ی کنترل ارتباط بین دستگاه و بلاکچین و ارتباط بین دستگاه‌ها را کنترل می‌کند و مکانیسم اجماع بلاک چین را پشتیبانی می کند . نمای لایه ای از معماری نرم‌افزار در شکل ۷ نشان داده شده است.

شکل۷:نمای لایه ای نرم افزار

کلید نرم‌افزارAtomOS,Deeper است(یک سیستم عامل شبکه ای که به صورت سفارشی برای امنیت عمیق ساخته شده است). همچنین اولین سیستم عامل شبکه بدون قفل در جهان است .طراحی پیشرفتهAtomOS پایه ای برای قابل اعتماد بودن، کارآمدی و امنیت کل سیستم است. ما به طور خلاصه سه صورتAtomOS را معرفی خواهیم کرد ؛ بسته یI/O، برنامه ریزی بسته و بازرسی عمیق بسته

۴.۱ بسته یI/O

بسته ورودی و خروجیI/O [48]بر لایه ی ورودی و خروجی AtomOS,I/Oمی افتد. این یکی از فناوری‌های کلیدی است که تاخیر جریان داده‌های کاربر و توان پهنای باند را تعیین می کند. سیستم عامل های سنتی(قدیمی) از یک پشته شبکه هسته[49] برای انتقال و دریافت داده استفاده می‌کنند .معایب اصلی این روش, تاخیر زیاد و توان پایین است. پس از پیمایش شبکه به یک دستگاه شبکه ای، بسته با یکسری موانع پردازشی واسطه‌ای همچون کارت رابط شبکه ،درایور دستگاه شبکه، پشته شبکه هسته و سوکت پیش از انجام آخرین پردازش(شکل ۸ را ببینید)، مواجه می‌شود. به علاوه این روش می تواند موجب تغییر زمینه به صورت مکرر و وقفه های سخت افزاری، تأخیر داده افزایشی بعدی و کاهش توان عملیاتی شود.

شکل۸:فرستنده و گیرنده داده در سیستم عامل سنتی

AtomOSفناوری بدون کپی [50]را برای دسترسی مستقیم به بسته ها از دستگاه شبکه‌ای به کار می گیرد(شکل ۹ را ببینید).

این فناوری نه تنها پشته شبکه هسته سنگین لینوکس[51] را دور می‌زند بلکه از تغییر(تعویض)مکرر زمینه و وقفه های سخت افزاری اجتناب می‌کند. این تاخیر بسته داده را بسیار کاهش می دهد و توان عملیاتی را

[48] Packet I/O
[49] Kernel
[50] zero-copy

بالا می برد.AtomOS فناوری بدون کپی را با (12)DPDKطراحی شده توسط اینتل اجرا می‌کند .داده های آزمایشی ارائه شده توسط اینتل نشان می دهد که DPDKتوان عملیاتی را ده برابر افزایش می دهد(۱۳).

شکل۹:گیرنده و فرستنده ی دادهDPDK

۴.۲برنامه ریزی بسته

AtomOSاولین سیستم عامل شبکه بدون قفل در جهان است که ساختار داده منحصر به فردHIPE را اجرا می کند. تمامی مشکلات سیستم عامل شبکه را می توان در ساختار مبتنی برHIPE حل کرد؛ این اجزا فلسفه ی طراحی ما را ساده و کارآمد و تحت کنترل تجسم می کند. پیش از نمایش اجرای دقیق HIPE,اجازه دهید نگاهی به محدودیت‌های کلی سیستم عامل های شبکه ی فعلی بیاندازیم.

۱.عملکرد بالا و مقیاس پذیری بالا

با کاهش اندازه ترانزیستورهایCPU و طبق قانون مقیاس گذاری دنارد [52](۱۱)به تدریج شکسته می‌شوند .کاهش اندازه ی ترانزیستورها باعث افزایش مصرف برق استاتیک[53] و تبدیل انرژی حرارتی را به صورت جدی منفجر می کند .علاوه بر این، گرمای انباشته شده بین ترانزیستورها قابل توجه است و خنک کردن CPUبه یک مسئله ی فوری تبدیل می‌شود. حقیقتاً ،افزایش فرکانسCPU به دلیل مشکل خنک کننده ،دیگر امکان پذیر نیست .بنابراین ،تولیدکنندگان بزرگ تراشه تحقیق درباره ی تراشه ی فرکانس بالا را به طور محسوس متوقف کرده‌اند. در عوض، آنها شروع به تحقیق در مورد معماری چند هسته ای فرکانس پایین کرده اند.کاویوم[54](شرکت سخت افزار آمریکایی)،یک تولید کننده معروف پردازنده، یک پردازنده ی شبکه ۴۸ هسته‌ای پیش از سال ۲۰۱۲(۹) راه اندازی کرد. AMDقصد دارد پردازنده ی چند هسته‌ای ۱۲۸ رشته ای را در سال ۲۰۱۹ منتشر کند(۲۳). توسعه پردازنده های چند هسته ای همچنین چالش‌هایی برای طراحی سیستم عامل های شبکه به همراه دارد. سیستم عامل های شبکه سنتی معمولاً بر اساس Vx works,Free BSD,لینوکس و سایر سیستم عامل های کلاسیک هستند. Vx worksبه عنوان یک سیستم عامل به موقع تعبیه شده ی تک هسته ای طراحی شده است که در دهه های اخیر توسط فروشندگان دستگاه شبکه به تدریج حذف شده است. هم لینوکس و هم Free BSDاز یونیکس[55] گرفته شده‌اند در حالی که یونیکس در اصل برای سیستم های کنترل به جای سیستم های ارسال داده طراحی شده بود .جریان طراحی ارثی این سیستم عامل های کلاسیک لذت بردن از مزایای پردازنده هایmulti core و حتی many coreرا برای آنها مشکل می سازد.

۲.دسترسی بالا

سیستم عامل های شبکه معمولاً در محدوده ی یک مجموعه از دستگاه‌های شبکه مستقر می‌شوند به این معناست که اگر یک دستگاه شبکه خاموش باشد، اتصال تمامی دستگاه‌های موجود در شبکه که به آن

---

[51] Linux
[52] Dennard'scaling law
[53] static
[54] Cavium
[55] Unix

دستگاه متکی هستند، از بین می‌رود .بنابراین ،مشتریان به طور کلی تقاضای بسیار زیادی برای دسترسی دستگاه به شبکه را دارند .به طور کلی، دسترسی تجهیزات شبکه نیازمند رسیدن به ۹۹،۹۹۹ درصد است که این یعنی تنها ۵ دقیقه خرابی یا وقفه در سال قابل قبول است. در حال حاضر ،دستگاههای شبکه(به ویژه دستگاههای امنیتی شبکه) باید توان ترافیک بیشتر و ویژگی‌های بیشتری را به کار گیرد تا موجب حفظ دسترسی بالا که یک چالش فزاینده ای است، شود.

۳.ترتیب بسته

هنگامی که یک کاربر به یک وبسایت دسترسی پیدا می کند ممکن است ده ها دستگاه شبکه ای درگیر شوند .اگر این دستگاه ها ترتیب بسته را حفظ نکنند، بسته‌های داده کاربر ارسالی ممکن است به صورت کاملاً تصادفی به کاربر دریافت کننده تحویل داده شود .اختلال بسته الگوریتم کنترل ازدحام (۲۱)از پروتکل TCPتریگر می کند تا باعث کاهش اندازه ی پنجره انتقال TCPو در نتیجه کاهش جدی توان جریان داده و تاثیر بر روی تجربه کاربر می شود. همانطور که در بالا اشاره شد، پردازنده ی چند هسته ای multi coreو حتی many coreاکنون جریان اصلی هستند. اگرچه پردازنده‌های چند هسته ای می توانند بسته های داده را در برابر مسائل بی نظم و جدی که ممکن است بدون توجه و ملاحظات مناسب رخ دهند، پردازش می کنند. بهره برداری از پتانسیل پردازنده‌های چند هسته‌ای در حالیکه نظم بسته حفظ شود یک مهره سخت برای کرک[56] سیستم عامل های شبکه تبدیل شده است .در حال حاضر، تمامی سیستم عاملهای باید از قفل ها (۲۹)برای حل این مشکلات استفاده کنند. هرچند، طراحی قفل به نوبه خود به یک مسئله در سیستم عامل های شبکه تبدیل شده است. اگر دانه بندی[57] قفل بیش از حد بزرگ باشد, این قفل های بزرگ تنگنای کل سیستم برای پردازنده هایی با هسته های بیشتر و بیشتر می‌شود. اگر دانه بندی قفل بسیار کوچک باشد ممکن است منجر به بن بست ها و مشکلات وضعیت رقابتی[58] شود با اینکه عملکرد سیستم‌عامل ممکن است بهبود یابد. در صورت عدم رسیدگی مناسب، این مشکلات به طور قابل توجهی بر روی ثبات سیستم تاثیر خواهند گذاشت. به منظور برآوردن نیازهای کلی سیستم عامل ها و حل مشکلات مربوط به سیستم عامل های سنتی، AtomOSساختار داده HIPEرا برای رسیدگی به برنامه‌ریزی جهانی منابع مشترک در سیستم عامل شبکه استفاده می‌کند این صحت سیستم در حالی که کل مزایای عملکرد چند هسته ای بهره می برد، تضمین می کند. در ادامه اجرایHIPE به طور مختصر معرفی می شود.

1.منابع مشترک مختلف از سیستم‌عامل در گروه‌های Nطبقه‌بندی می‌شود . منابع مشترک بزرگ ممکن است شامل چندین گروه و منابع مشترک کوچک باشد که مربوط به یک گروه تک(واحد) است(شکل ۱۰ زیر را ببینید).

شکل۱۰:منابع مشترک طبقه بندی شده در گروه هایN

2.دسترسی به هر گروه منابع توسط رویدادها تریگر می شود. هر رویداد لازم است به یک منبع مشترک که در صف بدون قفل برای گروه منبع مربوطه قرار گرفته شده است، دسترسی پیدا کند هنگامی که یک رویداد در صف ظاهر شد، یک هسته CPUبه طور خودکار برای پردازش آن اختصاص می یابد . از

[56] Crack
[57] granularity
[58] Race condition

آنجایی کهHIPE تمام رویدادها را در صف بدون قفل مربوطه از هر گروه منابع نگه می دارد، آنها باید به ترتیب پردازش شوند و نمی توانند به طور همزمان پردازش شوند، بنابراین از منابع مشترک محافظت می کنند.

شکل۱۱ :دسترسی به هر گروه منابع توسط رویدادها در صف بدون قفل تریگر می شود.

۳.از آنجایی که تعداد گروه های منابع در سیستم بسیار بیشتر از تعداد هسته های CPUاست ،یک جریان مداوم داده ها برای هر CPUبرای پردازش به طور مداوم در دسترس است تا باعث افزایش عملکرد کل سیستم با تعداد هسته های CPUشود.

شکل۱۲ :گروه های منابع که به صورت موازی از طریق ها CPUها پردازش می شوند.

۴.طراحی بدون قفل نه تنها باعث توسعه ی بسیار بسته در حال پردازش می‌شود بلکه همچنین از مشکلات وضعیت رقابتی مختلف زمانی که پردازش ها به صورت موازی،تولید مثل می کنند مانند مگس ها اجتناب می کند.علاوه براین،از آنجایی که بسته های داده به ترتیب از خط لوله[59] ی HIPEعبور می کنند، این نظم بسته را در یک جریان داده خاص پس از پردازشAtomOS که با سفارش اصلی اش در هنگام دریافت سازگار است،را تضمین می‌کند.

۴.۳بازرسی عمیق بسته

بازرسی عمیق بسته مهم است برای اطمینان از جریان داده که تحت حفاظت همه جانبه قرار می گیرد.AtomOSامنیت اتصال را براي هر لایه در مدلOSI(جدول ۲ را ببینید)فراهم می کند که اتصال Deeperبا مجموعه ی کاملی از عملکردهای امنیتی شبکه ایجاد می کند.امروزه،تمرکز امنیت شبکه از پروتکل لایه پایین به بالاترین لایه تغییر کرده است.علاوه بر محافظت های مختلف برای لایه های شبکه AtomOS 1-3همچنین عملکرد فایروال پیشرفته زیر را برای لایه های 7-4اجرا می کند.

مشخصات برنامه،تشخیص جریان داده مخرب	۷.لایه کاربرد
رمز گذاری و رمزگشایی داده برای جلوگیری از حملات تکراری	۶.لایه نمایش
بررسی پروتکل لایه ی نشت مانندHTTP/SIP	۵.لایه نشت
بررسی وضعیت سختگیرانه برای جلوگیری از حملات سیلی	۴.لایه انتقال
محافظت از حملات تکه تکه شدن وIPجعلی	۳.لایه شبکه
محافظت ازARP جعلی	۲.لایه پیوند داده
حفظ اتصال هنگام قطع برق	۱.لایه فیزیکی

[59] pipeline

جدول۲-عمق لایه ی محافظتی OSI

بررسی وضعیت TCPسخت‌گیرانه برای جلوگیری از نقاب زنی[60] TCPممکن و ربوده شدن:برای هر اتصالTCP ،AtomOSوضعیت خود را در میز جلسه ذخیره می کند و تنها بسته هایی که موکدا ماشین حالتstate machine و TCPرا برآورده می کند،ارسال خواهند شد.به طور همزمان، فایروال آزمایشگاه هایNSS معتبر مواردی را در صنعت بررسی می کنند که در حین اجرا برای اطمینان از مهار انواع مختلف و شناخته شده ی فرار ازTCP اشاره کرده بود.

مشخصات برنامه و کنترل جریان:AtomOSموتور شناسایی مشخصات برنامه که قابل اعتماد ،کار آمد و توسعه پذیر است را با هم ادغام می کند.این ترکیب شبکه معمولی را شناسایی و کنترل جریان یا مسیریابی هوشمند را به منظور بهینه سازی تجربه ی کاربر برای برنامه های کلیدی انجام می دهد. همچنین، این یک خدمات تونل روان بدون مصرف بیش از حد منابع محلی را تضمین می‌کند.

فیلترAtomOS:URLمی تواند به طور خودکار وب سایت های مخرب (از جمله بارگیری بدافزارها،وب های فیشینگ و غیره)برای ایجاد یک محیط امن اینترنتی فیلتر می نماید.کاربران می توانند همچنین کنترل والدین را برای درجه بندی محتوای اینترنت و تنظیم سطوح دسترسی مناسب برای هریک از اعضای خانواده را فعال کنند.

آدرس شبکه و ترجمه پورت(NAPT):به طور پیش فرض،AtomOSاز آدرس شبکه و ترجمه ی پورت برای جریانات داخلی اجتناب می کند تا باعث دسترسی به اینترنت بدون پیکر بندي با کابل زنده شود.با این حال،در برخی شرایط ،AtomOSمی تواند از حالت متقارنNAPT برای پنهان سازی بیشتر ساختار شبکه ی داخلی در صورت لزوم بهره ببرد.

5.شبکه سازی

علاوه بر ویژگی های بازرسی عمیق شبکه که در بخش ۴.۳ توضیح داده شد، Deeperهمچنین به طور مستقل پروتکل سه گانه، تونل سازی تطبیقی،مسیریابی هوشمند وIP چند گانه و کنترل تراکم لایه تونلی را طراحی کرده است. این فناوری‌ها، بازرسی بسته را عمیق تر و تجربه ی کاربری بهتر را فراهم می نماید.

5.1 پروتکل سه گانه

هدف فناوری تونل زنی Deeper(توسط پروتکل سه گانه اجرا می شود)دور زدن سانسور شبکه است.به دلایل مختلف، دولت‌هاي خاص در سراسر جهان در حال حاضر بیشتر بارها بازرسی عمیق را اداره می کنند و ترافیک شبکه کاربری را فیلترینگ می نمایند(۲۰).سانسور شبکه متکی است به فایروال ها یا دستگاه های تجزیه و تحلیل ترافیک آفلاین که در مرز شبکه های اصلی مستقر شده است. بنابراین، به منظور معرفی ویژگی های میانبری پروتکل سه گانه، اجازه دهید تا ما عملکرد فایروال ها را مرور کنیم. در حال حاضر، حالات فایروال ها از پورت براساس لیست کنترل دسترسی به محتوای پیشرفته براساس شناسایی برنامه تکامل داشته است.حالت پیشرفته می تواند به روش های زیر اجرا شود.چهار رویکرد اول

[60] Masquerading

متعلق به روش شناسایی منفعل و آخرین مورد فعال است. بعضی از فایروال ها می توانند از چندین روش برای شناسایی برنامه های استریم(جریان)[61] داده های کاربر استفاده کنند. به علاوه، بعضی رویکردهای هوش مصنوعی همچون قضیه بیز [62](۴۶)یا درخت تصمیم [63](۴۴)می توان برای اجرای شناسایی برنامه استفاده کرد.

1.فیلترینگ پورت اصلی

فیلترینگ پورت اصلی به روش شناسایی برنامه بر اساس پورت مقصد اشاره دارد. مرجع واگذاری اعداد در اینترنت[64] (IANA)(18)نهادی است که پورت های شبکه و برنامه های شبکه مربوط به آن را اختصاص می‌دهد. در حال حاضر، تقریباً همه پورت های ۰ تا ۱۰۲۴ اختصاص داده شده است(۲۸).فایروال ها قادرند یک ایده ی اساسی از برنامه‌های کاربران را به سادگی بر اساس پورت های شبکه به دست آورند. به عنوان مثال، پورت مقصد معمولاً از طریق پروتکل NFSکه ۲۰۴۹ است، استفاده می‌کند. حتی بدون الگوی محتوای واضح، هنوز فایروال ها قادرند برنامه را بر اساس پورت مقصد مشخص کنند.

2.شناسایی محتوا

شناسایی محتوا به روش شناسایی برنامه که مبتنی بر محتوای جریان داده هاست، اشاره دارد. از آنجایی که برنامه های شبکه باید پروتکل شبکه از پیش تعریف شده را دنبال کنند، جریان داده ها تمایل دارند که یک الگوی محتوای متمایز داشته باشند .به عنوان مثال، دستورات معمولاً توسط HTTP(GET/POST)استفاده می شود. همیشه به عنوان اولین بسته بعد ازدستیابی به TCP ,ظاهر می شود. همچنین ،اولین خط داده همیشه با HTTP/X.X(نسخه ی HTTPمورد استفاده) به پایان می‌رسد. فایروال ها قادرند برنامه‌هایHTTP که در یک پورت مقصد خاص بر اساس این طراحی، رخ می دهند را شناسایی کنند. به طور مشابه، تمامی پروتکل‌های استاندارد دارای الگوی محتوای قابل شناسایی هستند .برای بعضی از پروتکل های غیر استاندارد، الگوی محتوا ممکن است به خاطر ارتقاء نسخه پروتکل تغییر کند و بنابراین، فایروال ها باید دائماً دیتابیس(پایگاههای داده)[65] الگوی محتوای خود را ارتقا دهند و همچنین با این تغییرات تطبیق دهند.

3.شناسایی طول بسته[66]

شناسایی طول بسته به روش شناسایی برنامه بر اساس ترتیب طول بسته یا توزیع طول بسته در جریان داده ها اشاره دارد. این رویکرد بسیار خوب عمل می کند به ویژه وقتی که هیچ الگوی محتوای واضحی برای جریان داده ها در دسترس نباشد .طول بسته بین مشتری و سرور که به طور کلی چندین الگو را در مرحله ی مذاکره پروتکل شبکه دنبال می‌کند ،طی می‌کند. یک پروتکل شبکه در طی مرحله ی مذاکره

---

[61] Stream
[62] Bayes's Theorem
[63] Decision tree
[64] Internet assigned numbers Authority
[65] Database
[66] Packet length

مشخص می‌کند که مشتری باید یک بسته TCPرا با طول بار ۶۰ بایتی به عنوان یک درخواست ارسال کند و سرور باید بسته ۴۰ بایتی به عنوان پاسخی که بسته ی دیگر ۲۰-۳۰بایتی را دنبال می‌کند، ارسال کند. در این مورد، پروتکل شبکه دارای الگوی واضحی از نظر طول بسته است که می تواند به راحتی توسط یک فایروال شناسایی شود .به منظور فرار از شناسایی طول بسته، برنامه هایی برای به هم زدن یا رمزگذاری بسته‌های داده برای پنهان کردن الگوی طول بسته نیاز است.

4.شناسایی فاصله بسته

شناسایی فاصله(مدت) بسته به رویکرد شناسایی برنامه بر اساس بسته های نگهدارنده ی دوره‌ای مشخص شده در پروتکل شبکه، اشاره دارد .در پروتکل تونل زنی ،سرور و مشتری نیاز است که به صورت دوره‌ای بسته های نگهدارنده را به منظور نظارت بر دسترسی تونل، ارسال کنند. بسته های نگهدارنده (زنده بمان)[67] به طور کلی در یک فاصله معین و اندازه آنها نسبتاً کوچک است،ارسال می شوند. پروتکل های تونل زنی غیر استاندارد هنوز این الگو را حفظ می کنند. در نتیجه، فایروال های مورد استفاده برای سانسور شبکه می‌توانند برنامه‌های تونل زنی که بر اساس این الگو هستند را شناسایی و متوقف کنند.

5.شناسایی تشخیص فعال

شناسایی تشخیص فعال به این معناست که فایروال به عنوان یک واسطه عمل می‌کند تا محتوای بسته داده را بین مشتری و سرور تغییر دهد و برنامه‌ها را با توجه به محتوای بسته داده که از سرور برگردانده شده ،شناسایی کند .به عنوان مثال، کانال کنترلIRC معمولاً توسط بد افزار ها (۴۲)استفاده می شوند. با اینکه آنها با پروتکل IRCاستاندارد(یک پروتکل چت شبکه ای مشخص شده توسط IETF)مطابقت داشته اند، آنها جهش ساده که معمولاً در دستورات IRCمورد استفاده هستند را پشتیبانی نمی کنند .بر اساس این الگو، فایروال ها می توانند درخواست ها را به طور فعال ارسال کنند و پاسخ سرور برای تشخیص اینکه آیا برنامه های شبکه نرم افزار چت معمولی است یا بدافزار، تجزیه و تحلیل می کند. این رویکرد، فایروال ها را قادر می سازد تا بر محتوای جریان داده ها نظارت کند و همچنین به طور فعال بسته‌های داده را برای شناسایی برنامه تغییر داده یا ارسال کند. هدف گذاری تمامی رویکردهای شناسایی بالا، پروتکل سه‌گانه دو حالت تونل را ترکیب می‌کند تا از هرگونه تلاش شناسایی فایروال جلوگیری کند؛روش پروتکل مبهم سازی[68]و روش پروتکل استتارسازی از آنجایی که فایروال ها قادر به شناسایی هرگونه الگوی ترافیک در روش پروتکل مبهم سازی نیستند، سانسور اینترنت امکان پذیر نمی باشد .هرچند، برای سیستم ها با لیست سفید، همه برنامه های کاربردی ناشناس به خوبی مسدود می‌شوند. در این مورد، پروتکل سه گانه به طور خودکار به روش پروتکل استتار سازی برای دور زدن سانسور اینترنت تغییر خواهد کرد.

1.روش پروتکل مبهم سازی

-پورت تصادفی

در مورد پورت جلسه داده به صورت تصادفی بحث می شود

[67] Keep alive
[68] Obfuscation protocol

-رمزگذاری محتوا
همه‌ی محتوای بسته ها رمزگذاری می شوند
اطمینان حاصل کنید که ویژگی های محتوا نمی توانند در عبارات باقاعده و منظم [69]
بیان کرد.
-مبهم سازی طول بسته
همه ی طول بسته ها تصادفی هستند
-بسته های داده نگهدارنده دوره ای نیستند
-بسته داده،بسته ی نگهدارنده را سرقت می کند(piggy back).
-هیچ بسته ی داده نگهدارنده ی مجزا (جداگانه)وجود ندارد.
-جلوگیری از تشخیص فعال
سرورها از پاسخگویی به هر بسته ای که از مشخصات پروتکل را دنبال نمی کند،خودداري می کند.
۲.روش پروتکل استتار سازی:دو روش استتارسازی موجود است:
-پروتکل HTTP
پروتکل تونل زنی کاملاً در بدنه ی پیام "HTTP GET"و"HTTP POST"محصور شده است. درخواست" دریافت پاسخ "[70]برای میزان سرعت اتصال مودم برای دریافت داده[71] استفاده می‌شود و بدنه ی پیام POSTبرای میزان سرعت مودم برای ارسال داده[72] استفاده می‌شود .از آن جایی که پورت توسط مشتری و سرور مذاکره می‌شود پیش از این ،هیچ الگوی نام رشته[73] خاصی در فیلد HTTPموجود نیست.
-پروتکلTLS

در این روش، تابع بلیت جلسه[74] TLS ۱,۲استفاده می شود ترافیک تونل شبیه یک اتصال HTTPاستاندارد با استفاده از بلیت جلسه مذاکره شونده است. از آنجایی که هیچ فاز(مرحله)مذاکره ای وجود ندارد ،فایروال نمی‌تواند به عنوان یک واسطه رمزگشایی یا رمزنگاری کند. Atom OSهمچنین از رمزنگاری و مکانیسم ضد شناسایی مشابه روش پروتکل مبهم سازی که در بالا توضیح داده شد، استفاده خواهد کرد. یکی دیگر از مشکلات رایج در شبکه هایP2P، پیمایش(36)NAT است.NAT(برگردان نشانی شبکه) عملکرد مشترک دستگاه‌های شبکه در یک محیط شبکه IPv4است. دستگاه‌های شبکه ای معمولاً باIP آدرس های خصوصی درLAN تنظیم می شوند.هرچند، به منظور انتقال بسته ها خارج از اینترنت آدرس IPمقصد و آدرس IPمنبع بسته باید به آدرس IPعمومی ترجمه شوند(برگردانده شوند). برای رفع این تناقض، دستگاه شبکه‌ای که به عنوان گیت وی عمل می‌کند، می‌تواند ازNAT برای تبدیل آدرس

[69] Regex
[70] Get response
[71] Downstream
[72] Upstream
[73] String
[74] Session's ticket

IPv4خصوصی به آدرس IPعمومی گیت وی استفاده کند .هنگامی که بسته‌های داده ازLAN به سمت اینترنت حرکت داده می شوند. این رویکرد نه تنها مسئله ی محدودیت آدرس های IPv4را حل می‌کند بلکه همچنین الزامات سازمان ها برای پنهان سازی ساختار شبکه ی داخلی و جداسازی شبکه های خارجی را برآورده میسازد. در عمل، اتصال Deeperممکن است در پشت ارائه‌دهندگان خدمات دستگاه NATقرار بگیرد و یک آدرس IPخصوصی را به آن اختصاص دهد .هر چند که باعث می شود اتصالDeeper قادر نباشد درخواست‌های اتصال از اینترنت را دریافت کند. ما از تکنیک های زیر برای حل این مشکل استفاده میکنیم:

- اگر طرف گیرنده اتصال دارای آدرس IPخصوصی باشد و فرستنده آدرسIP عمومی داشته باشد، گیرنده، درخواست های اتصال را معکوس وارد می کند. اگر هر دو طرف آدرسهای IPخصوصی استفاده کنند، شناسایی نوع NATبیشتر مورد نیاز برای تشخیص راه مناسب جهت وارد نمودن درخواست اتصال است.

AtomOSپروتکلی شبیه پروتکلSTUN(RFC3489) (۴۵)را اجرا می‌کند .دستگاه شبکه ای قادر به شناسایی نوع NATو انتشار آن همراه با سایر اطلاعات راجع به نود که در مرحله اولیه ثبت شبکه طی می‌شوند، هستند. بالاخره هر دو دستگاه های شبکه با استفاده ازNAT متقارن(متناسب) یا پورت محدود شده به Cone NATمی توانند هنگام راه اندازی اتصال اجتناب شود. برای سایر انواع (NAT(cone NAT,Restricted cone NATو یا راه‌اندازی اتصال باید راه‌حلی را ارائه دهد.

۵.۲فناوری تونل زنی تطبیقی

اتصالDeeper از یک فناوری تونل زنی کارآمد، انعطاف‌پذیر و تطبیقی به جای نوع استاندارد IPSECاستفاده می‌کند. در مرحله ی طراحی و اجرای فناوری تونل زنی تطبیقی، ما به طور گسترده از صنایع مختلف مورد تایید فناوری های شتاب دهنده WANرا به امانت گرفته ایم. با توجه به تأخیر زیاد ،نرخ از دست دادن بسته ها و مسائل بی نظم اینترنت چندملیتی، ما این فناوری ها را در لایه تونل داده بهبود بخشیدیم تا به طور مؤثر استفاده از پهنای باند را حداکثر می‌کند و به طور قابل توجهی تجربه آنلاین کاربر را بهبود می‌بخشد.

۱.فشرده سازی داده های تطبیقی و ادغام آن

با فناوری تونل زنی تطبیقی, اتصال Deeperتعیین می کند که آیا بسته ها در جریان داده قابل فشرده سازی هستند و اینکه تصمیم می گیرند آیا فشرده سازی را انجام دهند یا خیر. به عنوان مثال، رایج ترین پروتکلHTTP عمدتاً از کاراکترهای لاتین تشکیل شده است که می‌تواند تقریبا ۷۰ درصد پهنای باند ذخیره شده را فشرده کنند و در نتیجه تا حد زیادی کارایی انتقال را بهبود می‌بخشد. در همین حال ،با توجه به این واقعیت که MP4و سایر فرمت ها که معمولاً در ترافیک صوتی و تصویری استفاده می‌شوند(یا پروتکل های شبکه مانند HTTPS/SFTPکه در رمزگذاری TLSوSSLمورد استفاده قرار می‌گیرند) قبلاً محدوده نظری آنتروپی اطلاعات(۴۸)[75] نزدیک شده است، فشرده سازی بیشتر فقط باعث افزایش مصرف CPUبدون صرفه جویی در پهنای باند می‌شود که منجر به پردازش و فشرده سازی و به نوبه ی خود کاهش سرعت انتقال می گردد .بنابراین، تونل زنی تطبیقی نیاز به شناسایی و پردازش بر اساس محتوا

[75] Information entropy

برای هم کاراییCPU و هم پهنای باند است. از طریق فناوری تونل زنی تطبیقی ،اتصالDeeper همچنین می‌تواند کارایی انتقال را از طریق ترکیب بسته‌های داده کوچک، بهبود ببخشد. بسیاری از پروتکل های شبکه دارای میزان زیادی بسته های کنترلی با اطلاعات کم یا بدون داده در پی لود [76]هستند. به عنوان مثال یک جریان انتقال ۳۰ کیلو بایتیHTTP را در نظر می‌گیریم، حتی اگر پشته پروتکل مشتری برای هر دو بستهTCPوACK بهینه کند، ۴۰ درصد بسته ها هنوز کمتر از ۱۰۰ بایت هستند. چنین حجم زیادی از بسته‌ها شامل مقدار بسیار کمی از داده ها که باعث تأخیر [77]قابل ملاحظه‌ای در کارایی انتقال می شوند . فناوری تونل زنی تطبیقی برای کارایی انتقال بهینه می تواند بسته‌های داده را از چندین جریان داده بدون تأثیرپذیری از تأخیراتصالTCP(شکل ۱۳ را ببینید) ترکیب یا فشرده و انتقال پیدا کند.

۲.برنامه های کاربردی براساس کنترل ترافیک

عملکرد برنامه های کاربردی بر اساس کنترل ترافیک بر طبق نوع برنامه جریان داده است تا از برنامه‌های کاربردی حساس به تأخیر و یا حجم که از سطح QoSبالاتری برخوردار هستند، اطمینان حاصل کند. پهنای باند در شبکه خانگی، اغلب محدود هستند هنگامی که از چندین برنامه به طور همزمان استفاده می شود، تقاضا برای پهنای باند اغلب بسیار بیشتر از آنچه در دسترس است، می شود.

شکل ۱۳:ادغام بسته‌های خودکار، طرح واره(شماتیک)[78]انتقال فشرده

خطاب به این مسئله ی اختصاصی، تونل زنی تطبیقی می‌تواند به طور خودکار نوع برنامه را با توجه به جریان داده ی کاربر تعیین کند و سطحQoS مربوطه را اعطا کند .به عنوان مثال، مرور وب یا بارگیری ایمیل ها باید به عنوان حساس به تاخیر طبقه‌بندی شوند، در حالی که برنامه های کاربردی همچون بارگیری فایل ها اینطور نیستند . تونل زنی تطبیقی ابتدا به طور خودکار پهنای باند واقعی تونل شبکه و الزامات پهنای باند آن را تخمین می زند .اگر تقاضا بیش از عرضه شود، تونل زنی تطبیقی استفاده از پهنای باند را بر اساس سطحQoS برنامه‌های کاربردی، کنترل خواهد کرد. برنامه‌های سطح پایین به طور موقت در صف بسته های محمود محدود بافر خواهند شد. اگر صف بسته کامل باشد، بسته‌های سرریز[79] دور انداخته خواهند شد. اگرچه کاربرد برنامه های عمومی ممکن است به خاطر افزایش تاخیر و از دست دادن بست تحت تاثیر قرار گیرند، تجربه کلی کاربر به طور قابل توجهی بهبود می یابد.

۵۰۳فناوری مسیریابی هوشمندانه

مسیریابی هوشمند به پیکربندی خودکار مسیریابی شبکه بر اساس ویژگی‌های جریان داده و اینکه آیا باید از طریق تونل انتقال یابند ،اشاره می کند ما دو روش را پیشنهاد می کنیم یک روش فازت از حریم خصوصی و روش دور زدن شبکه

مسیریابی هوشمند به پیکربندی خودکار مسیریابی شبکه بر اساس ویژگی‌های جریان داده و اینکه آیا باید از طریق تونل انتقال یابند ،اشاره می کند. ما دو روش را پیشنهاد می کنیم، یک روش حفاظت از حریم خصوصی و روش دور زدن شبکه

[76] Pay load
[77] Lag
[78] Schematic
[79] Overflow packets

روش پیش فرض،روش دور زدن شبکه است
شکل۱۴:مسیریابی هوشمندانه
-روش حفاظت از حریم خصوصی: در این روش، همه جریانات داده مربوط به مرور آنلاین ردیابی است که از طریق تونل وابسته به سطح ناشناس تنظیم شده توسط کاربر، پردازش می‌شوند.
روش دور زدن شبکه: در این روش، همه جریانات آنلاین داده در تونل پردازش خواهند شد بسته به اینکه آیا پایگاه داده نمایش داده میشود یا نه ،و گرنه در منطقه محلی مسدودمیشوند. مسیریابی هوشمند مزایای زیر را برای کاربران فراهم می‌کنند:
۱.پس انداز پولی
تونل های شبکه از طریق دو اتصال Deeperیا بیشتر ایجاد می شوند .هنگامی که یک اتصال Deeperسعی می کند با یکی دیگر جهت ایجاد یک تونل، پرداخت ارز رمزنگاری شده(با توجه به پهنای باند و حجم ترافیک محاسبه می شود) ارتباط برقرار کند از طریق پلتفرم به شبکه امن مشترک نیازمند می شود .بدیهی است، خدمات تونل زنی نمی تواند به صورت رایگان ارائه شود .مسیریابی هوشمند به طور خودکار تعیین می‌کند که آیا از طریق تونل با توجه به ویژگی های جریان داده انتقال می‌یابد یا نه. این روش نه تنها میزان استفاده از تونل را کاهش می دهد بلکه از تاخیر ناشی از تونل زنی جلوگیری می کند و تجربه ی آنلاین بهتر را بدون وارد آمدن هزینه‌های اضافی، ایجاد می کند.
۲.خدمات (سرویس)گمنامی [80]
سرویس گمنامی به منظور پنهان کردن آدرسIP کاربر برای فرار از ردیابی اشاره دارد. از زمانی که تونل شبکه رمزگذاری سرتاسر است ،جریان داده منتقل شده از طریق این هیچ اثری بر جای نخواهد گذاشت. ما سطح ها را با توجه به دسترسی کاربر به شی قابل‌مشاهده تنظیم خواهیم کرد و بر اساس تنظیمات کاربر، تصمیم بگیریم که آیا کپسول سازی[81] را بر روی جریان داده ی مربوطه انجام دهیم یا خیر. جریان‌های داده کاربر بسیار قابل مشاهده مانند بازدید از صفحه وب در بالاترین سطح سرویس گمنامی هستند. برای این سطح از جریان داده ی کاربر کپسول سازی الزامی است.
جریان های داده کاربر که کمتر در دسترس عموم اند مانند بارگیریP2P متعلق به دومین سطح عالی از سرویس گمنامی است. برای این سطح، کپسول سازی یک تنظیم اختیاری جهت کاهش هزینه‌های کاربر است. نه تنها این ،کاربران می توانند یک روش مسیریابی چند هاپی[82] را برای سرویس گمنامی دقیق تر انتخاب کنند.
در محیط مسیریابی چند هاپی، تونل شبکه توسط چندین اتصالDeeper به جای آن دو مورد معمول، ایجاد خواهد شد. مزیت این که اتصال Deeperبه عنوان یک نود میانی است، این است که نمی‌تواند به محتوا دسترسی پیدا کند زیرا جریان داده ی کاربر را نمی تواند رمزگشایی کند. آخرین نود اتصال Deeperمی تواند جریان داده کاربر را رمزگشایی کند اما نمی تواند منبع آن را

[80] Anonymity
[81] Encapsulation
[82] Multi-hop routing

بداند. بنابراین، هر چه نودهای اتصالDeeper در مسیر بیشتر باشد ،ردیابی فعالیت های کاربران، مشکل تر است.

۵.۴فناوری IPچند گانه

AtomOSاولینOS بدون پیکربندی در جهان است که می‌تواند مسیریابی هوشمند و کپسول سازی تونل را در روش سیم مجازی[83] اجرا کند. همه دستگاه‌های شبکه ای در حال حاضر موجود در بازار که عملکرد تونل را ایجاد می‌کنند،در حالت مسیریابی کار می‌کنند .یعنی کاربر نیاز به فناوری شبکه خاص و همچنین دانش کار در مورد برنامه ریزی آدرسIP و پیکربندی پروتکل تونل به منظور ایجاد صحیح تونل می باشد.

همچنین این به میزان معینی دانش مسیریابی جهت ارسال ترافیک ضروری به تونل برای کپسول سازی و جداسازی از کپسول[84] به طور مناسب مورد نیاز است. AtomOSاین را کاملاً تغییر می دهد که چگونه کاربران اتصال Deeper به دانش حرفه ای نیازی ندارند. بعد از اینکه کاربر دستگاه AtomOSرا به آپلینک[85] روتر خانگی متصل می‌کند ,AtomOSوارد فاز (مرحله) یادگیری(آموزش) می‌شود. این تحت تأثیر ترافیک ارسال قرار نمی‌گیرد و به طور خودکار جهت اتصال آن را با توجه به قوانین آماری آدرس‌های IPکه در دو پورت به نظر می‌رسد، تعیین می کند. در حالی که صدها میلیون نود در اینترنت وجود دارد، تعداد آدرس های IPمحلی نسبتاً کوچک و ثابت هستند. پس از اینکه به طور مختصر ترافیک را تجزیه و تحلیل کردیم، می‌توانیم پورت آپلینک و داون لینک[86] را تشخیص دهیم.AtomOS برای یادگیری آپلینک IP/MACآدرس و سرورDNS و سایر اطلاعات برای مذاکره و کپسول سازی تونل در آینده پیش خواهد رفت. ما معتقدیم که گیت وی خانگی هوشمند خود محصولی با فرکانس عملیاتی کاربر بسیار پایین است .نیازی نیست کاربران بیشتر اوقات از وجودشان آگاه باشند و پیکربندی کمی برای تغییر عملکرد ها لازم است. به ویژه با ترکیب فناوری مسیریابی هوشمند منحصر به فردمان ،حریم خصوصی کاربر و الزامات انتقال شبکه را با کمترین هزینه و هیچگونه دانش منحنی برآورده می‌شود.

۵.۵کنترل تراکم تونل

یکی از موارد کلیدی استفاده از شبکه یDeeper، ارائه شبکه ی گمنام به کاربران است که از حریم خصوصی آنها محافظت می کند و امکان دسترسی آزاد به محتوای اینترنت بدون سانسور یا مسدودی را می‌دهد .در سرویس گمنامی(که در شکل ۱۵ نشان داده شده است) کاربر داده را از طریق تونل امنAtomOS بین نودهایDeeper منتقل می کند ، بنابراین سرویس دسترسی به اینترنت نمی تواند داده خصوصی کاربر(مانند آدرسIP، مکان یابی) را ردیابی کند. به طور همزمان، زمانی که بسته‌های داده در تونلAtomOS موکدا رمز نگاری می‌شوند، فایروال های سانسورچی به طور موثر محو می‌شوند و قادر به شناسایی محتوای اینترنتی قابل دسترسی توسط کاربران نیستند.

شکل ۱۵:سرویس امن مشترک (SSS)

---

[83] Virtual wire mode

[84] Decapsulation

[85] Uplink

[86] Downlink

از طریق ترکیب امنیت شبکه ی منحصربه فردDeeper و فناوری های بلاک چین و SSSبه طور موثر امنیت و ثبات سرویس گمنامی شبکه ایDeeper را تضمین می‌کند .هرچند، کارایی انتقال داده در تونل AtomOSهمچنان یک مسئله باز باقی می‌ماند. دو چالش عمده برای انتقال داده باSSS وجود دارد:

۱.SSSدر درجه ی اول برای دسترسی به محتوای اینترنت در سایر کشورها یا مناطق در نظر گرفته شده است. انتقال داده از راه دور و تاخیر در انتقال زیاد سرعت بالای بی‌نظمی واز دست دادن بسته ها مشکلات مربوط به چنین دسترسی بین المللی به اینترنت است.

۲.اگرچه بسته ها در تونل AtomOSبه شدت رمزگذاری می شوند و بنابراین فایروال های سانسورچی نمی توانند آنها را شناسایی کنند و فایروال ها ممکن است سیاست حذف تصادفی بسته(به عنوان مثال حذف تصادفی بسته ۱ درصد) برای جریان داده های ناشناخته به منظور کم کردن تجربه ی کاربری اتخاذ می کنند. با توجه به چالش‌های فوق ،Deeperیک ارتباط اتصال گرا[87] و پروتکل انتقال قابل اعتماد در لایه ی تونل پیش می‌گیرد. این مسئله ی انتقال داده به طور موثر در SSSاز دیدگاه کنترل تراکم شبکه اصلی ترین مشکل برای حل است. مجموعه ی کاملی از راه حل های کنترل تراکم در شبکه یDeeperوTBBR(پهنای باند تنگنای تونلی و زمان انتشار رفت و برگشتی) نامیده می شود. این از دو بخش اصلی تشکیل شده است:

۱.استقرار الگوریتم کنترل تراکم جدید به نام BBRدر تونلAtomOS به گونه ای که در مورد نرخ از دست دادن زیاد بسته، تونل AtomOSمی‌تواند همچنان سرعت بالای انتقال و تاخیر کم انتقال را حفظ نماید .

۲.فعال کردن تشخیص سریع از دست دادن بسته و انتقال مجدد به منظور تطبیق بهتر با میزان از دست دادن بالای بسته درSSS است.

TBBRعمدتا در پیشرفت‌های در سمت فرستنده تمرکز می‌کند. سمت گیرند نیازی به هیچ تغییری ندارد. فرستند متکی به بازخورد [88]اضافی از گیرنده نیست. این یکی از مهمترین قواعد طراحی TBBRاست. این استقرار آسانترTBBR را فعال می کند طوری که هیچ تغییری از طرف گیرنده لازم نیست. مهمتر از همه ،در سناریوی سرعت از دست دادن بالای بسته و تأخیر زیاد SSSو بدون شک هیچ بازخورد اضافی از طرف گیرنده بار شبکه را افزایش می‌دهد و در چنین محیطی، هیچ بازخورد پایداری نمی‌تواند تضمین شود.

الگوریتم های کنترل تراکم سنتی(مانند TCP Reno(38),TCP Vegas(7),CUBIC(17))معمولاً بر اساس رویدادهای از دست دادن بسته است. از دست دادن بسته ها[89] به عنوان یک سیگنال ازدحام شبکه تلقی می شود. این نوع الگوریتم‌ها سرعت ارسال داده از طریق یک پنجره ارسال را کنترل می‌کنند. اندازه پنجره W(t)در زمان tتوسط AIMDکنترل می‌شود. الگوریتم (افزایش افزودنی /کاهش ضربی)

[87] Connection oriented
[88] Feedback
[89] Pocket loss

$$W(t+1) = \begin{cases} W(t) + a \\ W(t) * \beta \rightarrow \text{درغیراینصورت} \end{cases}$$

W(t)+a←اگر هیچ از بین رفتن بسته ای شناسایی نشود.

بدیهی است که الگوریتم AIMD تمایل به افزایش اندازه پنجره دارد(یعنی سرعت انتقال)تا زمانی که از بین رفتن بسته شناسایی شود .پس از شناسایی از بین رفتن بسته ،اندازه پنجره یک افت شدید را تجربه خواهد کرد. این منجر به دو مشکل اصلی میشود:

۱. درمان همه رویدادهای از بین رفتن بسته ها به عنوان سیگنال های تراکم شبکه ضد تولید[90] است.

در حقیقت ،از بین رفتن بسته نیز می تواند ناشی از خطاهای شبکه باشد. به علاوه، در زمان استفاده از SSS،فایروال های سانسورچی نیز ممکن است عمداً بسته ها را رها کنند. طبق الگوریتم AIMDو هنگام از بین رفتن بسته سرعت انتقال به شدت کاهش می‌یابد.

هنگامی که میزان از بین رفتن بسته به سطح خاصی برسد(به عنوان مثال از بین رفتن بسته یک درصد ناشی از فایروال های سانسورچی باشد) کل انتقال شبکه دچار مشکل می شود .از زمانی کهAIMD سرعت انتقال را افزایشی نگه می دارد تا این که از بین رفتن بسته شناسایی شود ،همچون یک مکانیسم که تمایل دارد همه ی بافر شبکه(مانند صف) اشغال کند .تعداد بسته های بزرگتری در صف انتظار باشند تاخیر صف زیادتر است. از زمانی که قیمت حافظه در سال‌های اخیر ارزان‌تر و ارزان‌تر می شود، بر این اساس فضای بافر شبکه در حال افزایش است که منجر به تاخیر فوق العاده در صف می شود. می توان دید که الگوریتم های سنتی کنترل تراکم نه سرعت انتقال بهینه و نه تأخیر در شبکه به طور مطلوب را به دست نمی آورند. Deeperیک نوع جدید الگوریتم کنترل تراکم به نام TBBRدر تونل AtomOS را مستقر می کند. TBBRبراساس الگوریتم BBR(۸) ترکیب شده با فناوری‌های تونل زنی توسعه یافته بود .BBR نخستین بار توسط گوگل معرفی شده بود و به طور وسیعی درWAN گوگل(شبکه گسترده) مستقر شده است .برخلاف الگوریتم های سنتی کنترل تراکم TBBR⁄BBR دیگر به رویدادهای از بین رفتن بسته به عنوان سیگنال های تراکم شبکه متکی نیستند ولی به ماهیت تراکم شبکه برمی‌گردند: طرف فرستنده داده را زودتر از ظرفیت شبکه بتواند رسیدگی کند، انتقال می دهد. به منظور اندازه گیری ظرفیت شبکه فعلی ، TBBR⁄BBRبه طور مداوم دو معیار اصلی را اندازه گیری می کنند به نامBtlBw(تنگنای پهنای باند)و RTprop (زمان انتشار رفت و برگشت) هستند. اگر مسیر شبکه یک لوله آب بود، تنگنای پهنای باندBtlBw حداقل قطر و زمان انتشار رفت و برگشت RTpropطول خواهد داشت. ظرفیت کل شبکه یعنیBDP(حاصلضرب پهنای باند تأخیر) دو محصول است :

$$\text{BDP} = \text{BtlBw} \times \text{RTprop}$$

BDPهمچنین می‌تواند به عنوان حداکثر میزان داده برجسته تفسیر شود که می‌تواند بدون ایجاد هیچ گونه تأخیر در صف(یعنی بدون اشغال هیچگونه فضای بافر) در شبکه انجام می شود. ایده اصلی TBBR⁄BBRاین است که وقتی میزان ورود داده به تنگنای شبکه برابر است با

[90] counterproductive

BtlBwو میزان داده‌های پرواز در شبکه معادل است با ظرفیت شبکه ی BDPکه شبکه در حالت بهینه حداکثر توان و حداقل تاخیر عمل می کند. TBBR/BBRسرعت انتقال را با اندازه گیریBtlBw و RTpropکنترل می‌کند. شایان ذکر است که ظرفیت کل شبکه به صورت پویا در حال تغییر است. بنابراین ،TBBR/BBRباید به طور مداوم BtlBwوRTpropرا اندازه‌گیری کنند تا سرعت انتقال به روز باشد .به علاوه ،BtlBwوRTprop به طور همزمان نمی‌توانند اندازه گیری شوند .به منظور اندازه گیری BtlBw،ابتدا باید بافر شبکه اشغال کرد تا حداکثر توان به دست آورد به منظور اندازه گیریRTprop، بافر شبکه تا حد امکان خالی باشد (یعنی بدون تاخیر در صف)تا حداقل تاخیر را به دست آورد. برای رسیدگی به این مشکلTBBR/BBR دو معیار را به طور متناوب اندازه‌گیری می‌کنند و با استفاده از مقادیر نمونه بر روی یک پنجره زمانی خاصw_R در زمانT، آنها را برآورد میکند.

$$BtlBw = \max(rt) \quad (3)$$

$$RTprop = \min(RTTt) \quad (۴)$$

جایی کهr_t سرعت انتقال داده در زمانt اندازه گیری شود وRTT_t زمان رفت و برگشت در زمان tاندازه گیری میشود.

TBBR/BBR دو ویژگی زیر را پردازش می کنند:

۱.در یک نرخ از بین رفتن بسته خاص، TBBR/BBR*هنوز* یک سرعت انتقال پایدار را که نزدیک به پهنای باند شبکه است، حفظ می‌کنند.

۲. در حالی که حداکثر توان آن را حفظ می‌کنند،TBBR/BBR تمایل به اشغال بافر شبکه ندارند و بنابراین تاخیر صف کاهش می‌یابد.

گوگلBBR را در گوگل دات کام[91] و سرورهای یوتیوب[92] خود مستقر کرده است .BBRبه طور موفقیت آمیزی تاخیر انتقال شبکه میانه ی یوتیوب را تا ۵۳ درصد کاهش داد. در کشورهای در حال توسعه این میزان بیش از ۸۰ درصد(۸) است. Deeperتجربه ی موفقBBR در برنامه‌های کاربردی SSSرا با استقرار*TBBR*، اولین تونل کنترل تراکم جهان در تونل*AtomOS* پیوند زده است. با*TBBR* ،ما متوجه می شویم که اتصال *Deeper*به طور موثر تاخیر در دسترسی به اینترنت بین المللی را کاهش می دهد در حال که هنوز سرعت انتقال شبکه را پایدار حفظ می‌کند هنگامی که فایروال ها عمداً باعث افت بسته ها می شوند.

شکل۱۶-توان شبکه در نرخ مختلف از بین رفتن بسته ها←شکل در متن اصلی موجود است

شکل۱۶توان شبکه در تونل*AtomOS* را با *TBBR* و آن تونل سنتی *IPSEC*بدون کنترل تراکم زیر نظر نرخ مختلف از بین رفتن بسته ها مقایسه می کند .راه اندازی آزمایشی یک جریان داده *BtlBw=100Mbps*و*RTTprop=100ms*است.

[91] Google.com
[92] You tube

- منحنی نمودار در بالا نشان دهنده ی سرعت انتقال ایده‌آل یعنی$BtlBw*(1_p)$ در جایی که pنرخ از بین رفتن بسته است. همانطور که در شکل می توان دید ،نرخ از بین رفتن بسته بسیار کوچک(۰,۰۱درصد) می تواند باعث شود توان$IPSEC$ به فقط ۳۰ درصد پهنای باند کاهش یابد. هرچه نرخ از بین رفتن بسته افزایش یابد، تنها ۵ درصد توان عملیاتی از پهنای باند باقیمانده را داراست در جایی که انتقال اغلب متوقف می‌شود .در مقابل، توان عملیاتی تونل $AtomOS$در میزان از دست دادن بسته ها حتی بیش از ۵ درصد، به توان عملیاتی ایده آل نزدیک می ماند. در از دست دادن ۱۵ درصد بسته‌ها ،تونل$AtomOS$ هنوز پهنای باند ۷۵ درصد را حفظ می‌کند .درSSS، فرض میکنیم فایروال های سانسورچی به طور تصادفی یک درصد ازبسته های ناشناخته را کم می کنند. توان عملیاتی تونل$AtomOS$ به صورت مجازی متأثر نخواهد بود و به توان عملیاتی ایده آل نزدیک خواهد ماند در حالی که $IPSEC$تنها ۵ درصد از پهنه باند باقی مانده را خواهد داشت.

شکل۱۷-تاخیر شبکه برای اندازه های مختلف بافر

شکل ۱۷ تاخیر شبکه تونل $AtomOS$و $IPSEC$در اندازه‌های مختلف بافر را مقایسه می کند. راه اندازی آزمایشی 8 جریان داده$BtlBw=128kbps$ و$RTT=40ms$ است. تونل سنتی$IPSEC$ تمایل به اشغال فضای کل بافر شبکه را دارد که این باعث تأخیر به صورت افزایش خطی با اندازه ی بافر می شود. حتی بدتر ،اگر تاخیر بیشتر از اتصال اولیه ی شبکه (SYN) زمان تعیین شده توسط سیستم عامل های مختلف شود ،این باعث قطع اتصال می شود. در مقابل تونل $AtomOS$ همیشه تاخیر با در نظر گرفتن حداقل اندازه بافر حفظ می‌نماید .در بالای BBR، تونل$AtomOS$ بهینه سازی های بیشتری برای تشخیص سریع از بین رفتن بسته ها و انتقال مجدد اجرا می کند.TCP قدیمی به طور عمده از بین رفتن بسته ها را به دو روش رسیدگی می‌کند:

۱.اگر تاییدیه (ACK)بسته در یک مدت زمان مشخص دریافت نشده باشد یعنی مهلت ارسال مجدد (RTO)اتمام یابد، بسته از دست رفت تلقی می‌شود و ارسال مجدد تریگر می‌شود.

۲.به جای اینکه برای اتمام مهلت زمان منتظر باشیم، اگر سه ACK تکراری از گیرنده دریافت شد، فرستنده نیز یک بسته را از دست رفته می‌پندارد و ارسال مجدد درگیر می‌شود.

این مکانیسم ارسال مجدد سریع نامیده می شود.

درTCP، هنگامی که گیرنده متوجه می‌شود که چندین بسته حذف شده اند ،های تکراری جهت یادآوری به فرستنده که هنوز چندین بسته در حال گم شده است، ارسال خواهد کرد .دو دلیل برای اینکه یک بسته ممکن است دست برود، وجود دارد: یا بسته گم می شود و یا بسته از نظم خارج می‌شود. یعنی بسته‌ها در اصل پس از دریافت یک بسته خاص ابتدا به طرف گیرنده برنامه ریزی شده اند .هنگامی که فرستنده یک ACKتکراری دریافت می کند، بلافاصله نمی تواند مشخص کند که کدام سناریو رخ داده است. بنابراین ضروری است برای سایرACK ها منتظر شود تا مشخص شود از دست رفتن بسته با احتمال زیاد اتفاق افتاده است. اگر از دست رفتن بسته خیلی زود مشخص شود، این منجر به انتقال مجدد غیرضروری خواهد شد که بار شبکه را افزایش می دهد؛ از طرف دیگر، اگراز دست رفتن بسته خیلی دیر مشخص شود، این باعث یک پاسخ کند به

رویداد از دست رفتن بسته خواهد داشت. امروزه ،یک مکانیسم انتقال مجدد سریع که معمولاً بر اساس سه *ACK*های تکراری مورد استفاده قرار می گیرد. برای ارسال حداقل ۴ بسته داده ها مورد نیاز است (یعنی اندازه پنجره ارسال کننده حداقل چهار است) تا سه *ACK*تکراری را مشاهده کنیم ؛در غیر این صورت ،فرستنده فقط می‌تواند به اتمام زمان *RTO*برای انتقال مجدد متکی باشد. بنابراین، مکانیسم انتقال مجدد سریع فعلی در تمامی موارد زیر ضعیف عمل می کند یا اصلاً کار نمی کند:

۱-مطالعات(۳) نشان داده شده است که ازمنظر لایه برنامه، یک اتصال *TCP*اغلب نیاز دارد تا مجموعا کمتر از ۴ بسته داده را ارسال کند .در این موارد، مکانیسم انتقال مجدد سریع فعلی هرگز تریگر نمیشود.

۲.پیکربندی شبکه ممکن است باعث شود پنجره ارسال به زیر ۴ کاهش یابد، که همچنین انتقال مجدد سریع را غیرفعال می‌کند .

۳.در روش*ACK* تجمعی ،گیرند ممکن است ارسال با تأخیر*ACK* را انتخاب کند تا چندین *ACK* را به منظور صرفه جویی در پهنای باند در یکی ادغام کند.

در این مورد، حتی بستر های داده بیشتری مورد نیاز است تا بتواند انتقال مجدد سریع را تریگر کند. یک مکانیسم انتقال مجدد سریع موثر از دست دادن بسته را شناسایی می کند و انتقال مجدد به موقع را تریگر می کند در حالیکه انتقال مجدد زیادی در حال کاهش است. *TBBR*الگوریتم آستانه انتقال مجدد سریع پویا را تصویب می‌کند. به طور خلاصه ،اگر بسته های داده بیشتری نتوانند ارسال شوند(یا به دلیل اندازه پنجره ارسال محدود است یا به خاطر لایه ی برنامه داده بیشتری برای ارسال ندارد) آستانه ی ارسال مجدد سریع به صورت پویا تنظیم می‌شود با توجه به تعداد بسته ها که هنوز تایید نشده اند؛ در غیر اینصورت از 3 آستانه استفاده می شود.

۱	فرض شود تعداد بسته های تایید نشده ی فعلی *k*باشد
۲	اگر بسته های بیشتری جهت ارسال وجود نداشته باشند سپس
۳	$\tau=max(min(k\_1,3),0)$
۴	و دیگر
۵	$\tau=3$

الگوریتم۱-الگوریتمی برای آستانه ی انتقال مجدد τسریع درTBBR
با توجه به RTOاتمام زمان ارسال مجدد ،TCPسنتی یک الگوریتم به نام عقب‌نشینی نمایی[93] (یعنی اگر یک مهلت زمان بسته تحتRTO فعلی به پایان برسد، بسته مجدداً انتقال می‌یابد وRTO دو برابر می شود)را تصویب می‌کند. در موارد شدید، اگر اتمام زمان بسته n دفعات متوالی اتفاق بیفتد، RTOاصلی دو مرتبه گسترده خواهد شد که سرعت انتقال را به طور زیادی متوقف می‌کند. TBBRاز منحنی رشد نرم ترRTO استفاده می کند که ۱,۵RTO بار مقدار قبلی

[93] Exponential backoff

در هر اتمام زمان تنظیم می کند. اگرچه طراحی کلی TBBRبر روی طرف فرستنده متمرکز است، ما هنوز می‌توانیم انتقال شبکه را به طور موثر از طرف گیرنده بهبود ببخشیم.دو روش اصلی وجود دارد:

۱-تاییدیه انتخابی ((SACK(32) در طرف گیرنده تصویب کنید. در مقابل تاییدیه تجمعی [94]که در آن گیرنده فقط کمترین توالی تعداد بسته ها که هنوز دریافت نکرده‌اند، را بازخورد می‌کند وSACK به گیرنده اجازه می‌دهد تا با صراحت به فرستنده اعلام کند که کدام بسته را دریافت شده است و کدام یک نشده است. فرستنده می تواند فقط آن بسته هایی که هنوز دریافت نشده اند را به صورت انتخابی مجددا ارسال کند .به علاوه، اگر چندین بسته داده‌ها در پنجره ی ارسال فعلی از دست بروند، تاییدیه تجمعی (cumulative acknowledgment) فقط فرستنده را مطلع می‌کند که یک بسته در یک زمان از دست رفته که منجر به ناکارآمدی می شود.SACK می تواند کلیه ی از دست رفتن بسته ها را یکباره بازخورد کند .تحقیقات نشان می دهد که در تاخیر زیاد و نرخ بالای از دست دادن شبکه ها، SACKمی تواند تعداد بسته های ارسال مجدد را تا حد زیادی کاهش دهد و انتقال را به طور موثری بهبود ببخشد .تایید تاخیر را به صورت پویا تنظیم کنید. همانطور که قبلاً ذکر شد ،گیرنده می تواند ACKهای ارسالی را به تأخیر بیندازد. در حالی که برای انجام آن بهتر است از پهنای باند استفاده کنیم و این همچنین تاییدیه ی بسته را به تأخیر می‌اندازد وانتقال مجدد سریع را به وقفه می اندازد .به خصوص در محیط با تاخیر زیاد و از دست دادن زیاد بسته‌ها، بسیار مهم است که گیرنده هر بسته ای را به موقع تایید نماید. بنابراین، در طرف گیرنده ،تأخیر تاییدیه می‌تواند به صورت پویا و با توجه به شرایط از دست رفتن بسته و تأخیر در شبکه ی فعلی تنظیم گردد.

۶.بلاکچین

دو لایه در زنجیره ی Deeper(شکل ۱۸)وجود دارد .لایه بالایی شامل صدها نود اعتبارسنج[95] شبیه هر بلاکچین دیگری است. لایه ی زیرین همچنین لایه ی Deeperنام دارد که شامل میلیون‌ها دستگاه Deeperاست. این دستگاه ها از طریق ارائه ی خدمات به شبکه ی Deeper ،به عنوان مثال ، اشتراک‌گذاری پهنای باند، اعتبار کسب می کنند.

شکل۱۸-ساختار۲لایه ای زنجیره ی Deeper

برخلاف پروتکل اجماع ناکاموتوی استاندارد، POCما(اثبات اعتبار) متکی به حل معمای محاسباتی مهم برای دادن رای به اجماع نیست و از این رو مصرف انرژی پایینی دارد. مکانیسم اجماع ما شبیه به اثبات سهام (proof of stake)است، اما قدرت رای دهی اعتبارسنج هم به توکن‌های سرمایه‌گذاری و هم به ارزش اعتباری واریز شده[96] بستگی دارد . از یک طرف، لایه ی بالایی با ارزش اعتباری دستگاه‌های Deeperایمن می شود. افراد بیشتری در خدمات Deeper درگیر شوند، امنیت شبکه بیشتر خواهد بود. از سوی دیگر، توزیع پاداش استخراج به

[95] validator

[96] Delegated credit scores

دستگاههای Deeper، افراد بیشتری را برای شرکت در خدمات Deeper تشویق خواهد کرد. این حلقه ی بسته باعث افزایش و ایمن‌سازی کل شبکه خواهد شد.

۶.۱مکانیسم اجماع

۶.۱.۱بررسی اجمالی

Deeperاز HotStuff(۵۵) برای چارچوب تکثیر ماشین حالت خود(SMR) استفاده می کند. HotStuffاولین پروتکل تحمل عیب بیزانسی[97] (BFT)است که هم پیچیدگی ارتباطات خطی(یعنی(O(n) و هم تاخیر شبکه ی پاسخگو را دارد.

شکل ۱۹-معماری خط لوله ایHotStuff

با انتزاع پارادایم [98]زنجیره ای از پروتکل‌های روش BFT،HotStuffمعماری خط لوله ای را که تا حد زیادی توان شبکه را بهبود می‌بخشد، معرفی کرده است . به جای رای صریح به یک پیشنهاد مراحل کامل (یعنی پیشنهاد، قبل از تعهد،تعهد و غیره) یک مرحله عمومی می شود و رای به پیشنهادی است که به بعضی والدین بر می گردد یک رای برای مرحله ی بعدی برای والدین در نظر گرفته می شود. به عنوان مثال ،رای به بلاک کردن، یک رای آماده برای خود بلوکه، یک برای قبل از تعهد برای والدین و یک رای تعهد برای پدربزرگ و مادربزرگش و یک رای تصمیم‌گیرنده برای سه نسل از اجداد در نظر گرفته می شود. بلوکه تنها زمانی که نسل سوم شان با موفقیت به آن رای دهد، اجرا می‌شود و از طریق تخمین تقریبی فرایند خط لوله‌ای در مقایسه با سایر پروتکل‌های اجماع BFT، توان را تا سه برابر افزایش می‌دهد. به علاوه ،HotStuffاز الگوی ارتباط ستاره ای(یعنی همه از طریق رهبر ارتباط برقرار کنند)و امضای آستانه(threshold signiture) بهره می برد تا از ارتباط خطی پیش از بلوکه اطمینان حاصل کند. رهبر[99] برای اعتبارسنج ها، بلوکه ارسال می‌کند و آنها امضای جزئی را تولید می‌کنند و رهبر به سادگی یک امضای آستانه را بازسازی می‌کند که به عنوان یک اثبات اعتبار بلوک عمل می‌کند .این اجازه می‌دهد تا اجماع برای تعداد زیادی از اعتبار سنج ها به طور همزمان مقیاس شود. درTendermint وPBFT ،تنها دو دور برای رسیدن به اجماع وجود دارد .با معرفی دور سوم همراه با کمک امضای آستانه، تغییر رهبر نیز از نظر پیچیدگی در مقایسه با پیچیدگی های درجه دومPBFT، خطی است. تاخیر شبکه ,تاخیر شبکه واقعی است به جای محدودیت‌های بالا که از طریق پروتکلی شبیهTendermint (تندرمنت) تعیین شده است .در کنار حملات سیبیل[100] معمولی به بلاکچین عمومی ،حریم خصوصی مربوط به شبکه اغلب می‌تواند ممنوعیت های هدفمند را برای اعتبار سنج ها و ارائه دهندگان خدمات از دولت‌ها را تجربه کند که منجر به خطاهای ناگهانی رهبر می‌شود .با تغییر رهبر خطیHotStuff این خطاها به طور قابل توجهی عملکرد شبکه را کاهش نخواهد داد.

۶.۱.۲کمیته ی انتخاب و زنده بمان[101]

---

[97] Byzantine fault tolerant

[98] Paradigm

[99] Leader

[100] Sybil attack

[101] Liveness

HotStuffدر شکل اصلی، زنده بمان و انتخاب رهبر را بخشی از اجماع خلاصه می‌کند. این عملکرد ها باید به طور جداگانه در هر نمونه ی خاص از HotStuff، بسته به توپولوژی[102] (همبندی) شبکه و پویایی اعتبارسنج، پیاده سازی شوند. به علاوه ،HotStuffکمیته ی چرخش(rotation committee) که باید همچنین به طور جداگانه اجراء شوند ،را در نظر نمی‌گیرد .درDeeper ،زنده بمان از طریق گواهینامه های اتمام زمان(timeout certificate) به دست می آید. هنگامی که اعتبارسنج برای پیشنهاد بلوک از رهبر دور جدید برای دوره ی اتمام زمان تعیین شده، منتظر می ماند و این نمی رسد، آنها یک پیام اتمام زمان تاحدی امضا شده به رهبر بعدی که از طریق برنامه زمانبندی نوبت گردشی[103] تعیین شده ،انتخاب می‌شود، ارسال کنند. رهبر جدید به محض دریافت امضای جزئی کافی،یک گواهینامه اتمام زمان تولید می کند که آنها با یک پیام دور جدید برای تمام اعتبارسنج ها آن را پخش می کنند. کمیته ی چرخش در شبکه های بدون مجوز برای نفوذ به مزایای پروتکل‌هایBFT اجرا می‌شود در حالیکه همچنین از استحکام در برابر آنچه که به اصطلاح حملات تطبیقی خصمانه[104] نام دارد، اطمینان دارد.

[102] Topology
[103] Round robin
[104] Adaptive adversary attack