Scalable and Anonymous Computation Offloading Solution in Blockchain

Shokufeh Norouzi[1], Yoosef Ghobadi[2], Zeinab Movahedi[3 *]

[1]PhD Student, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.
[2]MSc Graduated, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.
[3]Associate Professor, Faculty of Computer Engineering, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.
E-mails: shokufeh_norouzi@comp.iust.ac.ir, uoosef_ghobadi@comp.iust.ac.ir, zmovahedi@iust.ac.ir.
[*] Means corresponding author

Short Abstract
Today, with the implementation of the new generation of communication networks, we are witnessing a huge evolution in the development of the Internet of Things (IoT) and the emergence of new programs in this context. The limitation in the computing power and energy of the devices connected to this platform creates a challenge and lack of support for these devices to run programs with high computation load and low delay. Computation offloading in the cloud and edge network has been introduced as a suitable approach to deal with these limitations. Using the capacity of devices with appropriate power in the vicinity of IoT devices as an offloading destination prevents the exchange of a huge amount of data in the network core. The use of these devices requires maintaining the privacy and security of the offloaded workload so that the sensitive and confidential information of IoT users is not compromised during the computation offloading process. For this purpose, blockchain is used. Blockchain technology has unique features such as transparency, immutability and decentralization, securing and automating applications, which makes it a suitable option for securing the transfer and storage of data generated in the IoT platform. The use of blockchain in computation offloading faces limitations such as managing a large number of requests due to the expensive design of consensus methods. In addition, by analyzing the transactions and traffic, the influential groups can obtain the identity of the owners of the offloaded workloads and their sensitive content and violate the privacy. In order to solve these challenges, this article takes a step forward by presenting a scalable and anonymous computation offloading method in blockchain. The proposed approach changes the blockchain architecture using Merkel chain as a Directed Acyclic Graph and optimizes the consensus method to solve the challenges of scalability. As well, the proposed appraoch uses the zero-knowledge proof to improve privacy and anonymity.

Keywords
Computation offloading, blockchain, anonymity, scalability.

1- Short Introduction

In today's world, blockchain technology has garnered attention from academic and industrial communities following its remarkable successes in the realm of digital currencies. With the growing public interest in harnessing the potential of blockchain, various industries are strategically planning to capitalize on the distributed advantages of this technology, including transparency, high security, real-time information sharing, process automation, and asset management and tracking. This technology finds numerous applications and benefits across diverse domains such as finance and banking, insurance, supply chain, healthcare, cybersecurity, transportation, energy management, and infrastructure and is extensively utilized in practice.

2- Proposed Work and Methodology

The use of blockchain in computation offloading faces limitations such as managing a large number of requests due to the expensive design of consensus methods. In addition, by analyzing the transactions and traffic, the influential groups can obtain the identity of the owners of the offloaded workloads and their sensitive content and violate the privacy. In order to solve these challenges, this article takes a step forward by presenting a scalable and anonymous computation offloading method in blockchain. The proposed approach changes the blockchain architecture using Merkel chain as a Directed Acyclic Graph and optimizes the consensus method to solve the challenges of scalability. As well, the proposed appraoch uses the zero-knowledge proof to improve privacy and anonymity. The proposed approach is evaluated through the implementation of multiple scenarios. The evaluation platform consists of a server with a 10th generation Xeon processor, 32GB RAM, and a 1Gbps network card, partitioned based on Docker. Network nodes in the blockchain platform are developed using the Golang programming language. Each node securely connects to one or more other nodes through the GRPC protocol over TLS channels. Additionally, application programs connect to the nodes through REST APIs, generating transactions. After creation, each transaction is referred to the gossiping process. Upon receiving a transaction, neighboring nodes temporarily store it in their memory before gossiping, and after gossiping, if the transaction is valid, it is persisted in a directed acyclic graph-based No-SQL database. The smart contract in the system is also developed in Rust. Each evaluation is precisely executed 10 times, and all results are reported with a 95% confidence interval.

3- Conclusion

This paper discusses a scalable and anonymous computation offloading method based on blockchain technology. In this regard, the possibility of in-chain offloading is explored instead of using other technologies such as cloud computing and edge computing. Additionally, scalability in the blockchain is improved by modifying the consensus structure, transaction validation, as well as the storage and retrieval structure of information. Furthermore, zero-knowledge proofs are employed to enhance privacy and anonymity.
For future work, we plan to utilize Sharding and intelligent summarization approaches to accelerate transaction registration on the network. Moreover, we intend to combine the proposed approach with the InterPlanetary File System (IPFS) decentralized storage protocol to leverage transaction sharing in the network and handle a vast amount of offloaded computation in a modified node.

تخلیه بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی

شکوفه نوروزی
دانشجوی دکتری، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران ، ایران

یوسف قبادی
فارغ‌التحصیل کارشناسی ارشد، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران ، ایران

زینب موحدی
دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران ، ایران

چکیده
امروزه با پیاده‌سازی نسل جدید شبکه‌های ارتباطی شاهد تحولی عظیم در توسعه اینترنت اشیاء و ظهور برنامه‌های جدید در این بستر می‌باشیم. محدودیت در توان محاسباتی و انرژی دستگاه‌های متصل به این بستر موجب ایجاد چالش و عدم پشتیبانی این دستگاه‌ها از اجرای برنامه‌ها با بار محاسباتی بالا و نیازمند تاخیر کم می‌شود. تخلیه بار محاسباتی در ابر و لبه شبکه به عنوان یک رویکرد مناسب برای مقابله با این محدودیت‌ها معرفی شده است. استفاده از ظرفیت دستگاه‌های دارای توان مناسب در مجاورت ادوات اینترنت اشیاء به عنوان مقصد تخلیه از مبادله حجم عظیمی از داده‌ها در هسته شبکه جلوگیری می‌کند. بهره‌مندی از این دستگاه‌ها نیازمند حفظ حریم خصوصی و امنیت بار تخلیه‌شده می‌باشد تا اطلاعات حساس و محرمانه کاربران اینترنت اشیاء در طی فرآیند تخلیه‌بار با خدشه‌ای مواجه نگردد. به این منظور از زنجیره بلوکی استفاده می‌شود. فناوری زنجیره بلوکی ویژگی‌های منحصر به فردی از جمله شفافیت، تغییرناپذیری و تمرکززدایی، ایمن کردن و خودکارسازی کاربردها را دارا است که سبب می‌گردد گزینه مناسبی برای تامین امنیت انتقال و ذخیره‌سازی داده‌های تولیدشده در بستر اینترنت اشیاء باشد. استفاده از زنجیره بلوکی در حوزه تخلیه بار محاسباتی به علت طراحی پرهزینه‌ی روش‌های اجماع با محدودیت‌هایی همچون مدیریت تعداد زیاد درخواست‌ها روبه‌رو است. به‌علاوه، گروه‌های با نفوذ می‌توانند با تحلیل تراکنش‌ها و ترافیک، هویت صاحبان بارهای محاسباتی تخلیه‌شده و محتوای حساس آن‌ها را به دست آورند و حریم خصوصی را با خدشه مواجه کنند. به منظور رفع این چالش‌ها، این مقاله با ارائه یک روش تخلیه‌بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی، با تغییرات در معماری زنجیره بلوک با استفاده از گراف جهت‌دار بدون دور، زنجیره مرکل و بهینه‌سازی روش اجماع برای رفع چالش‌های مقیاس‌پذیری گام برداشته و با استفاده از اثبات دانش صفر حفظ حریم خصوصی و بی‌نام مانی را بهبود می‌دهد.

کلمات کلیدی
تخلیه بار محاسباتی، زنجیره بلوکی، بی‌نام‌مانی، مقیاس‌پذیری.

نام نویسنده مسئول: دکتر زینب موحدی
ایمیل نویسنده مسئول: zmovahedi@iust.ac.ir

تاریخ ارسال مقاله: ۱۴۰۲/۱۰/۰۴
تاریخ(های) اصلاح مقاله: ۱۴۰۳/۰۴/۱۹
تاریخ پذیرش مقاله: ۱۴۰۳/۰۶/۱۷

۱- مقدمه

یکی از ماموریت‌های نسل جدید شبکه‌های ارتباطی ارائه اتصالات گسترده به منظور پشتیبانی تطابق‌پذیر با توسعه روزافزون اینترنت اشیاء[1] می‌باشد. اینترنت اشیاء به خصوص اینترنت اشیاء صنعتی به صورت فراگیر و با رشد زیادی در حال استفاده می‌باشد. بصورتیکه پیش‌بینی شده است تا سال ۲۰۲۵ تعداد دستگاه‌های متصل به اینترنت به مرز ۷۵ میلیارد برسد [۲]. برنامه‌های جدید در بستر اینترنت اشیاء همچون واقعیت افزوده، بازی‌های تعاملی و پردازش زبان طبیعی برای اجرا در دستگاه‌های متصل به این بستر به توان محاسباتی بالا و تاخیر کم نیاز دارند. یکی از چالش‌های اساسی در اینترنت اشیاء محدودیت توان محاسباتی و انرژی دستگاه‌های متصل بوده که موجب می‌شود این دستگاه‌ها قادر به اجرای برنامه‌ها با بار محاسباتی سنگین و نیازمند تاخیر کم نباشند. روش‌های تخلیه‌بار محاسباتی در ابر و لبه شبکه به عنوان راهکاری کارآمد برای مقابله با چالش‌های اینترنت اشیاء پیشنهاد شده است [۳، ۱۹].

با فراگیری و رشد بستر اینترنت اشیاء، حجم عظیمی از داده‌ها برای پردازش در خدمت‌گزاران ابری و لبه در شبکه مبادله می‌شوند. این درحالی است که می‌توان از قدرت پردازشی دستگاه‌های بیکار دارای توان و انرژی مناسب واقع در لبه شبکه استفاده بهینه کرد. بهره‌برداری از ظرفیت دستگاه‌های موجود در لبه شبکه برای تخلیه‌بار محاسباتی نیازمند حفظ حریم خصوصی و امنیت پردازش‌های تخلیه‌شده می‌باشد تا اطلاعات حساس و محرمانه کاربردهای حساسی چون صنایع در طی فرآیند تخلیه‌بار افشا نشود.

غالب کارهای موجود در حوزه تخلیه‌بار محاسباتی در لبه شبکه مبتنی بر یک موجودیت متمرکز برای مدیریت و تصمیم‌گیری تخلیه‌بار عمل می‌کنند. این درحالی است که وجود موجودیت متمرکز و غیرشفاف باعث مشکلاتی از

[1] Internet of Things (IoT)

جمله نقض حریم خصوصی و تنها نقطه شکست شده و همچنین به علت محدودیت منابع پردازشی در آن موجودیت، مقیاس‌پذیری با چالش مواجه می‌شود. برای مقابله با مشکلات ذکر شده در بالا می‌توان از فناوری زنجیره بلوکی بهره برد.

دنیای امروز فناوری زنجیره بلوکی[۲] پس از موفقیت‌های چشمگیر ارزهای دیجیتال مورد توجه مجامع علمی و صنعتی قرار گرفته است. با افزایش اقبال عمومی نسبت به استفاده از توان بالقوه زنجیره بلوکی، صنایع مختلف در حال برنامه‌ریزی برای استفاده از مزایای این فناوری توزیع‌شده از جمله شفافیت، امنیت بالا، اشتراک‌گذاری اطلاعات به صورت لحظه‌ای، خودکارسازی فرآیندها و مدیریت و ردیابی دارایی می‌باشند. این فناوری در امور مالی و بانکداری، بیمه، زنجیره تامین، سلامت، امنیت سایبری، حمل و نقل، مدیریت انرژی و زیرساخت، کاربردها و مزایای فراوانی داشته و مورد استفاده قرار می‌گیرد [۱].

زنجیره بلوکی با توان بالقوه خود در انواع کاربردها با تمرکززدایی از فرآیندهای تصمیم‌گیری باعث افزایش مقیاس‌پذیری، امنیت و حفظ حریم خصوصی می‌شود [۲۰]. با این حال، این فناوری به علت طراحی پرهزینه روش‌های اجماع و ذخیره و بازیابی اطلاعات با محدودیت‌هایی همچون مدیریت تعداد روبه‌رشد درخواست‌ها در یک سیستم توزیع‌شده مواجه است که در این مقاله از آن به عنوان چالش مقیاس‌پذیری یاد می‌کنیم. همچنین، گروه‌های با نفوذ و برخوردار از توان لازم همچون دولت‌ها می‌توانند با تحلیل تراکنش‌ها و ترافیک شبکه، هویت صاحبان تراکنش‌ها و محتوای حساس آن‌ها را به دست آورند و حریم خصوصی را با خدشه مواجه کنند [۴].

در این مقاله برآنیم که با ارائه یک روش تخلیه‌بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی، در جهت رفع چالش‌های یادشده گام برداریم. بر این اساس، با ایجاد تغییر در معماری زنجیره بلوک همچون استفاده از گراف جهت‌دار بدون دور[۳] (DAG)، زنجیره مرکل و همچنین استفاده از روش‌های اجماع میان بخشی از گره‌های شبکه بجای همه گره‌های آن در جهت رفع چالش‌های مقیاس‌پذیری تلاش می‌کنیم. همچنین، با استفاده از اثبات دانش صفر[۴] (ZKP) حفظ حریم خصوصی و بی‌نام مانی را مورد بهبود قرار می‌دهیم.

ادامه این مقاله، به شرح زیر ساختاربندی شده است. در بخش دوم به بررسی کارهای انجام‌شده در زمینه تخلیه بار محاسباتی در فناوری زنجیره بلوکی می‌پردازیم. در بخش سوم روش پیشنهادی تخلیه بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی را ارائه خواهیم کرد. در بخش چهارم نتایج ارزیابی رویکرد پیشنهادی در محیط عملیاتی را به نمایش در می‌آوریم. در نهایت نیز نتیجه‌گیری و پیشنهاداتی برای کارهای آتی را مطرح می‌کنیم.

۲- مروری بر کارهای گذشته

در این بخش، ابتدا رویکردهای موجود در زنجیره بلوکی برای افزایش مقیاس‌پذیری را بررسی کرده و سپس به بررسی کارهای مرتبط در حوزه تخلیه‌بار محاسباتی در فناوری زنجیره بلوکی می‌پردازیم.

رویکردهای موجود برای افزایش مقیاس‌پذیری به چهار دسته درون‌زنجیره‌ای[۵]، برون‌زنجیره‌ای[۶]، زنجیره جانبی[۷] و میان‌زنجیره‌ای[۸] تقسیم می‌شوند. معیارهایی که مقیاس‌پذیر بودن یک رویکرد مبتنی بر زنجیره بلوکی می‌سنجد گذردهی، هزینه تایید تراکنش و گنجایش بلوک است. گذردهی به معنی تعداد تراکنش‌ها تقسیم بر بازه زمانی میان ثبت یک تراکنش تا تایید آن بوده و هرچه این بازه زمانی کوچکتر باشد گذردهی بیشتر است. هزینه تایید تراکنش نیز کارمزدی است که گره‌های میانی برای تایید یک تراکنش دریافت می‌کنند. گنجایش بلوک نیز تعداد تراکنش‌هایی که در یک بلوک قرار می‌گیرند را مشخص می‌کند.

رویکردهای درون-زنجیره‌ای با کار بر روی عناصر درون زنجیره بلوک سعی در بهبود مقیاس‌پذیری دارند. در [۵]، یک زنجیره بلوکی سبک به نام LightChain برای اینترنت اشیاء صنعتی معرفی شده است که برای افزایش مقیاس‌پذیری از رویکرد درون-زنجیره‌ای استفاده کرده و مبتنی بر یک روش اجماع جدید با میزان همکاری کاربران بوده است. این اجماع از نظر مفهومی مشابه Proof of Stack (POS) است با این تفاوت که در آن به جای سرمایه مالی، میزان مشارکت کاربر در نگهداری از بلوک‌های زنجیره به عنوان معیار انتخاب به عنوان تاییدکننده تراکنش مبنا قرار داده می‌شود. همچنین، در [۶] برای افزایش مقیاس‌پذیری از تقسیم معنایی دفترکل توزیع‌شده به چندین پایگاه‌داده کوچکتر برای افزایش مقیاس‌پذیری استفاده شده است. به این منظور، دفترکل با توجه به نوع تراکنش میان گره‌ها تقسیم شده و هر گره مسئول تایید گروه خاصی از تراکنش‌ها خواهد بود و به این ترتیب گذردهی و سرعت تایید تراکنش در شبکه افزایش یافته و اندازه بلوک کاهش می‌یابد. این در حالی است که امنیت هر گروه به میزان قابل توجهی کاهش پیدا می‌کند زیرا گره‌های بدخواه با مجاب کردن تعداد کمتری گره می‌توانند دست به تبانی بزنند.

رویکردهای برون‌زنجیره‌ای از پردازش تراکنش خارج از زنجیره اصلی برای افزایش مقیاس‌پذیری استفاده می‌کنند [۷، ۸]. در کار [۹]، با استفاده از یک رویکرد برون‌زنجیره‌ای به جای انجام همه تراکنش‌ها در شبکه زنجیره بلوکی، از یک ماشین موقت میان افرادی که تعداد تراکنش بالایی با یکدیگر دارند استفاده می‌شود. بدین ترتیب، پس از مدت مشخصی دارایی ابتدایی و دارایی پس از اتمام تراکنش‌های مشترک میان افراد در دفترکل توزیع‌شده ثبت می‌شود. این دسته از رویکردها محدود به تبادلات مالی خواهند بود.

در [۱۰، ۱۱]، از یک رویکرد مبتنی بر زنجیره‌ی جانبی برای افزایش مقیاس‌پذیری استفاده می‌شود، بطوریکه در کنار زنجیره اصلی یک انشعاب از یک ارز دیجیتال نیز مورد استفاده قرار می‌گیرد. به این منظور، از آنجایی که Bitcoin بالاترین ارزش و ثبات را در میان ارزهای دیجیتال در اختیار دارد، برای نگه‌داری طولانی مدت و محافظت از سرمایه استفاده گردیده است. در مقابل، برای کاربردهای روزمره و خریدهای خرد، یک انشعاب از سرمایه Bitcoin به یک ارز دیجیتال چابک با عنوان Bitcoin-cash تبدیل شده و در زمان و هزینه صرفه‌جویی می‌شود. همچنین اندازه بلوک در آن به نسبت Bitcoin افزایش یافته است.

در [۱۲]، از یک رویکرد میان‌زنجیره‌ای با هدف اتصال شبکه‌های مختلف زنجیره بلوکی متعدد به یکدیگر استفاده شده است که زیرساختی برای پیاده‌سازی دسته زنجیره جانبی خواهد بود. بدین ترتیب یک ارز دیجیتال توزیع‌شده و متشکل از چند ارز دیگر با عنوان Unitary Interchain ایجاد می‌شود تا تمامی کاربران بتوانند دارایی‌های خود را به این ارز دیجیتال میانی تبدیل کنند. بر این اساس، برای افزایش مقیاس‌پذیری هر نوع از دستگاه‌های شبکه از ادوات اینترنت اشیاء گرفته تا تلفن‌های همراه می‌توانند با توجه به منابع در دسترس خود با استفاده از ارز میانی از LightChain یا FlopCoin استفاده نمایند. از معایب این رویکردها شرایط پیچیده جهت اجرا می‌باشد.

با بررسی کارهای ارائه شده برای افزایش مقیاس‌پذیری در زنجیره بلوکی، رویکرد مورد استفاده در این مقاله درون-زنجیره‌ای خواهد بود. در ادامه، کارهای موجود در حوزه تخلیه‌بار محاسباتی در فناوری زنجیره بلوکی مورد بررسی قرار

[2] Blockchain
[3] Directed Acyclic Graph (DAG)
[4] Zero Knowledge Proof
[5] On-Chain
[6] Off-Chain
[7] Side-Chain
[8] Inter-Chain

خواهند گرفت.

در [۱۳]، پردازش‌های تخلیه‌شده به صورت برون‌زنجیره‌ای اعتبارسنجی می‌شوند و هدف اصلی این کار افزایش بهره‌وری تخلیه‌بار بوده و به مقیاس‌پذیری و بی‌نام مانی توجهی ندارد. در واقع در این کار فرآیند تخلیه ایمن است اما بستر زنجیره بلوکی در آن مقیاس‌پذیر و ایمن نیست.

در [۱۴]، رویکرد تخلیه‌بار در بستر زنجیره بلوکی از ساز و کار مبتنی بر شهرت برای تعیین میزان قابلیت اطمینان به نتیجه پردازش تخلیه شده در گره‌های شبکه استفاده می‌کند. امکان تقلب برای یک گره خوش‌نام در این رویکرد فراهم خواهد بود.

در [۱۶]، از زنجیره بلوک برای احراز هویت غیرمتمرکز برای افزایش امنیت ادوات اینترنت اشیاء در تخلیه‌بار استفاده شده و روش اجماع در آن اثبات مبتنی بر هویت می‌باشد. در ابتدای کار چند گره به عنوان گره‌های مورد اطمینان در نظر گرفته شده و به مرور ضریب اطمینان هر گره با عملیات احراز هویت موفق در شبکه بالا خواهد رفت.

در [۱۶]، از خدمت‌گزاران لبه برای تخلیه‌بار مبتنی بر رویکرد پردازشی تابع به عنوان خدمت[9] (FaaS) در بستر زنجیره بلوکی استفاده شده است. در این کار هیچ ساز و کاری برای حفظ حریم خصوصی در کاربران ارائه نشده است.

با بررسی کارهای مرتبط تخلیه بار محاسباتی در بستر زنجیره بلوکی و با محوریت افزایش مقیاس‌پذیری و بهبود حریم خصوصی مشخص می‌شود که غالب کارها از رویکردهای شهرت و انگیزه‌دهی برای افزایش مقیاس‌پذیری استفاده می‌کنند و امکان بروز تقلب، خطا و کاهش امنیت در زنجیره بلوکی در آن‌ها چالش برانگیز است. همچنین، در کارهای مرتبط از ظرفیت دستگاه‌های بیکار در لبه شبکه استفاده نشده است. بر همین اساس، در بخش بعدی به ارائه یک روش تخلیه‌بار مقیاس‌پذیر و بی‌نام در زنجیره بلوکی می‌پردازیم که ضمن استفاده از دستگاه‌های دارای توان مناسب در لبه شبکه به عنوان مقصد تخلیه، با عدم امکان ارتباط دادن هر تراکنش به صاحب آن از بی‌نام مانی پشتیبانی کرده و حریم خصوصی را بهبود دهد و همچنین، با ایجاد اصلاحات در ذخیره و بازیابی اطلاعات و فرآیند اجماع، زنجیره بلوکی را نیز مقیاس‌پذیر کند.

۳- روش پیشنهادی تخلیه بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی

همانطور که پیش‌تر ذکر گردید، هدف این مقاله بهبود مقیاس‌پذیری و بی‌نام مانی تخلیه بار محاسباتی می‌باشد. مقیاس پذیری به قابلیت پاسخگویی سیستم با وجود تعداد رو به رشد درخوست‌ها و بی‌نام مانی به عدم افشای هویت صاحبان تراکنش‌ها و محتوای تخلیه‌شده آن‌ها اطلاق می‌گردد. همانطور که در بخش پیشین اشاره شد کارهای انجام‌شده در زمینه تخلیه بار محاسباتی در فناوری زنجیره بلوکی غالبا از روش‌های انگیزه‌دهی و شهرت برای افزایش مقیاس‌پذیری استفاده می‌کردند و امکان بروز خطا یا تقلب و کاهش امنیت در آن‌ها مطرح بود. همچنین، هیچ یک از کارهای مرتبط ساز و کاری برای افزایش بی‌نام مانی و بهبود حریم خصوصی ارائه نمی‌دهد. برای حل این چالش‌ها، در این بخش به ارائه یک روش تخلیه بار محاسباتی مقیاس‌پذیر و بی‌نام در فناوری زنجیره بلوکی می‌پردازیم. در این روش برای افزایش مقیاس‌پذیری از ساختمان داده DAG برای ذخیره و بازیابی اطلاعات استفاده شده و چکیده‌ای از آن در قالب درخت مرکل مورد ذخیره محلی در هر گره قرار می‌گیرد. همچنین، فرآیند اجماع نیز با اصلاحاتی برای افزایش مقیاس‌پذیری مواجه است. به علاوه، با استفاده از بی‌نام مانی و ارائه آن با اثبات دانش صفر، حریم خصوصی بهبود داده خواهد شد. در ادامه به تفصیل به معرفی رویکرد پیشنهادی پرداخته، معماری و اجزای سیستم را شرح می‌دهیم.

۳-۱- معماری سیستم

سیستم پیشنهادی، یک سیستم باز و مبتنی بر مشارکت عادلانه و سودمند گره‌های شبکه بوده و از دو لایه زیرساخت و کاربرد تشکیل می‌شود.

لایه زیرساخت، یک زنجیره بلوکی به صورت همپوشان (Overlay) روی بستر اینترنت با تعدادی زیادی گره ناهمگن از نظر قدرت پردازشی، سکوی اجرایی و نحوه دسترسی به اینترنت، می‌باشد. این لایه از دو فرآیند اصلی شایعه پراکنی (Gossiping) برای حفظ ثبات و بروزرسانی گره‌های شبکه و پرس‌وجو (Querying) برای هرس گراف جهت‌دار بدون دور تشکیل می‌شود.

لایه کاربرد یک لایه انتزاعی بوده و متشکل از چندین قرارداد هوشمند است که هر یک نقش یک برنامه کاربردی توزیع‌شده را ایفا می‌نمایند. فرآیند تخلیه‌بار نیز خود یک قرارداد هوشمند بوده و هویتی مستقل و قابل ارجاع دارد که تمامی گره‌ها با رجوع به آن امکان سنجش صحت فرآیندهای انجام‌شده را خواهند داشت. هر قرارداد هوشمند همچون تمام برنامه‌های کاربردی از چندین زیر برنامه و تابع تشکیل شده و هر گره هر یک از این توابع را در قالب یک تراکنش اجرا می‌کند.

همچنین، از آنجایی که سیستم پیشنهادی باز و ناهمگن است، وجود گره‌های بدخواه با هدف تقلب برای کسب سود بیشتر و همچنین نقض حریم خصوصی، حتمی می‌باشد. در مدل سیستم پیشنهادی فرض بر این است که گره‌های بدخواه دارای منابع قدرتمند هستند که می‌توانند روی ترافیک ورودی و خروجی هر گره در شبکه و تراکنش‌های انجام‌شده در شبکه به صورت مداوم نظارت کنند و در صورت وجود هر گونه ارتباط میان تراکنش‌های سیستم و هویت اصلی گره‌های شبکه، این ارتباط را کشف کرده و به هویت واقعی کاربران شبکه پی ببرند. همچنین، می‌توانند در حداکثر $\frac{1}{k}$ از کل تراکنش‌های در جریان در ترافیک شبکه حذف موردی انجام داده، مقصد را تغییر دهند، در ارسال و دریافت آن‌ها تاخیر ایجاد کنند و یا ترتیب ارسال آن‌ها را عوض کنند.

۳-۲- اجزای سیستم

DAG ساختمان داده مورد استفاده برای ذخیره و بازیابی تراکنش‌های سیستم پیشنهادی در این مقاله بوده و با توجه به عملی نبودن نگهداری از کل آن در حافظه موقت سیستم به علت حجم بالا، چکیده‌ای از آن در قالب درخت مرکل به عنوان وضعیت جاری گره شبکه نگه‌داری می‌شود. همچنین، هویت هر گره از شبکه متناظر با کلید عمومی او بوده و هر گره می‌تواند بی‌نهایت کلید عمومی با قابلیت استفاده در یک کاربرد خاص داشته باشد.

هر عملی در زنجیره بلوک تحت یک تراکنش که می‌تواند شامل یک یا چند رکورد (record) باشد، انجام شده و هر گره پس از دریافت تراکنش جدید و بررسی صحت آن، درخت مرکل خود را به صورت محلی بروزرسانی می‌کند. هر رکورد با حداکثر عمر طول یک تراکنش نیز شامل یک عمل تجزیه ناپذیر (Atomic) بوده و مسئولیت بروزرسانی وضعیت محلی سیستم را برعهده دارد. رکورد پس از انجام تراکنش و اعمال آن در سیستم از بین می‌رود و با از بین رفتن آن شماره سریال آن نمایش داده می‌شود.

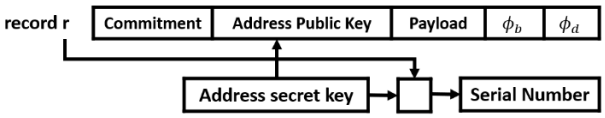
هر رکورد در سیستم با r نمایش داده شده و تنها دو رویداد تولد و مرگ را تجربه می‌کنند. بنابراین هر رکورد می‌تواند ساخته و مصرف شود و از اجزای زیر تعریف شده است:

- Commitment: چکیده‌ای از کل رکورد که در فرآیند تایید صحت یک تراکنش کاربرد دارد.
- APK: آدرس کلید عمومی که دارنده تراکنش را مشخص می‌کند.

[9] Function as a Service

- Data Payload: داده محرمانه مربوط به عملی که رکورد باید انجام دهد را شامل می‌شود. (ورودی داده یک کد تخلیه‌شده)
- ϕ_a و ϕ_b توابع احتمال دودویی غیرقطعی برای کنترل دو رویداد تولد و مرگ رکورد هستند و بررسی می‌کنند رکورد از مسیر صحیحی تولید شده و به شکل صحیحی مصرف شود.

هر گره از شبکه که قصد مصرف یک رکورد را دارد بایستی کلید خصوصی یک تراکنش را داشته باشد تا با رمزگشایی رکوردهای تراکنش شماره سریال-های رکوردها را در شبکه اعلام کند. بدین ترتیب، کسانی که صاحب رکورد نیستند و درواقع کلید خصوصی که رکوردهای تراکنش با آن رمز شده را ندارند نمی‌توانند مانع استفاده صاحب تراکنش از آن شوند و شماره سریال را آشکار کنند. شکل ۱ ساختار یک رکورد را نمایش می‌دهد.



شکل ۱- ساختار یک رکورد

هر تراکنش نیز که از یک یا چند رکورد تشکیل می‌شود به صورت Tx= (id, depth, parents, tag, serials, commits, ptoof, public mem, Encrypted Tail) نمایش داده می‌شود که از اجزای زیر متشکل است:

- شناسه یکتا: گره سازنده تراکنش بایستی درهم‌ساز تراکنش‌های والد آن و اثبات آن را حساب کند.
- عمق: عمق هر تراکنش برابر با حداکثر فاصله والدین تراکنش تا Genesis به علاوه ۱ است.
- والدین: هر تراکنش بجز Genesis و تراکنش‌های سطح اول باید برای مشروعیت خود حداقل ۲ تراکنش قبل از خودش را تایید کند.
- Tag: تابعی از قرارداد هوشمند است که این تراکنش اجرا می‌کند.
- سریال: مجموعه شماره سریال‌های رکوردهایی است که این تراکنش مصرف می‌کند.
- Commits: مجموعه Commitmentهای رکوردهای جدیدی است که تراکنش جدید می‌سازد.
- **π**: اثبات بدون دانش در مورد صحت انجام تراکنش است و با وجود آن نیازی به باز اجرای یک پردازش برای تایید صحت اجرای آن نیست.
- Public mem: متغیرهایی از تراکنش که باید به صورت عمومی برای همه گره‌های شبکه قابل مشاهده باشد در این ساختمان داده قرار می‌گیرد.
- Encrypted Tail: محتوای محرمانه یک تراکنش شامل بخش‌های محرمانه رکوردها به صورت رمزشده در این ساختمان داده قرار می‌گیرد.

از آنجایی شماره سریال هیچ دو رکوردی یکسان نیست با استفاده از اثبات دانش صفر و رمزنگاری داده حساس هر تراکنش، راهی برای تفکیک تراکنش‌ها از یکدیگر برای گره‌های بدخواه وجود ندارد و هرچه استفاده از این سیستم بیشتر شود، ضریب بی‌نام مانی سیستم افزایش می‌یابد.

۳-۳- فرآیند شایعه‌پراکنی و اثبات دانش صفر

در گره‌های شبکه برای برقراری فرآیند انتها به انتها، از الگوریتم ایمنی به نام Secure/Kademlia استفاده می‌کنند که در برابر حملاتی همچون Sybil مقاومت بالایی ارائه می‌دهد. بر این اساس، به هر گره در شبکه یک آدرس ۱۲۸ بیتی دودویی منتسب می‌شود. فاصله میان هر دو گره حداقل ۱ بیت و حداکثر ۱۲۷ بیت می‌باشد. در نتیجه هر گره می‌تواند تمامی گره‌های دیگر را در فاصله ۱ تا ۱۲۷ دسته‌بندی نماید و گره‌ها با فاصله حداکثر ۱ نسبت به هم، همسایه در نظر گرفته می‌شوند. در جریان فرآیند شایعه پراکنی، هر گره با دریافت خبر جدید از جمله اضافه شدن یک گره جدید به سیستم یا دریافت یک تراکنش جدید بایستی به تمام همسایه‌های خود اطلاع‌رسانی کند.

هر گره با دریافت تراکنش جدید، پس از بررسی شروطی مربوط انتخاب والدین، شرط ارضای پاسخ بدون دانش را بررسی می‌کند.

پاسخ بدون دانش در راستای افزایش حریم خصوصی به معنای بی‌نام نگاه داشتن تراکنش‌ها از نظر هویت صاحبان تراکنش و محتوی حساس آن‌ها است. به علت ماهیت شفاف فناوری زنجیره بلوکی در ارائه جزئیات معاملات در دفترکل توزیع‌شده، یک مهاجم قوی مانند دولت‌ها و گروه‌های خاص می‌توانند با تحلیل ترافیک ورودی و خروجی گره‌های شبکه، هویت او را کشف کنند. در یک مجموعه بی‌نام به اندازه کافی داده برای تشخیص یک گره موردنظر از سایر گره‌ها توسط گره بدخواه وجود نداشته و عملا دسته‌بندی ممکن نخواهد بود زیرا همه گره‌ها حداکثر در یک زیرمجموعه قرار خواهند گرفت. در رویکردهای پیشین از شبه بی‌نامی برای ارائه حریم خصوصی استفاده می‌شد که در آن‌ها از یک مشخصه شبه بی‌نام یا مستعار از یک گره همچون کلید عمومی به عنوان مشخصه اصلی آن گره و هویت او استفاده می‌شد.

رمزنگاری کامل داده‌ها در زنجیره بلوکی مانع از افشای اطلاعات حساس شده اما برای سایر گره‌های شبکه تایید صحت تراکنش رخ داده را غیرممکن می‌سازد. با استفاده از اثبات دانش صفر و زیرمجموعه آن یعنی اثبات دانش صفر غیرمحاوره‌ای (ZK-Snarks) در کنار رمزنگاری داده‌ها بدون در اختیار قرار دادن اصل یک گزاره می‌توان صحت ادعای درست یا نادرست بودن آن گزاره را اثبات نمود. بنابراین در این مقاله از ZKP به عنوان ابزار اصلی حفظ حریم خصوصی در زنجیره بلوکی استفاده می‌شود. بر این اساس، دو موجودیت اثبات‌کننده و تاییدکننده تعریف می‌گردد. هر دو موجودیت تابع دودویی S و دانش عمومی x را دانسته و هدف این است که اثبات‌کننده به تاییدکننده صحیح بودن خروجی S(x) را بدون آشکار کردن چرایی این صحیح بودن و یا هرگونه اطلاعات اضافه‌ای ثابت کند. برای این منظور، اثبات‌کننده شاهدی برای درستی ادعا در اختیار دارد که با نشان دادن آن به تاییدکننده، او را از صحت گزاره مورد نظر مطمعن می‌سازد. اثبات‌کننده و تاییدکننده به اندازه‌ای با یکدیگر پیام مبادله می‌کنند تا تاییدکننده در مورد صحت دانش مورد تایید راضی شود. این فرآیند به اندازه‌ای تکرار خواهد شد که احتمال اندک این موضوع که اثبات‌کننده دانش را نداند و جواب صحیح دهد به صفر میل کند.

۴-۳- فرآیند پرس‌وجو و اجماع

فرآیند پرس‌وجو شامل هرس و اجماع به موازات فرآیند شایعه‌پراکنی در شبکه اجرا می‌شود و مسئول مرتب‌سازی و اعمال تراکنش‌ها به صورت محلی در هر گره شبکه می‌باشد.

اجماع پس از گذشت مدت زمانی مشخص، تراکنش‌ها را به صورت دسته‌ای پردازش می‌کند. این فرآیند تراکنش‌ها را به چندین نوبت اجماع افراز می‌کند. با توجه به این که در فرآیند شایعه‌پراکنی شبکه به ۱۲۸ بخش کوچک تبدیل شده، هر بخش شامل یک گره و همسایه‌های آن با روش Byzantine Fault Tolerance (BFT) دودویی به اجماع می‌رسد. با این کار نیاز به تشکیل کمیته یا اجماع مبتنی بر رهبر از بین می‌رود. پس رسیدن به اجماع برای هرس و حفظ ترکیب تراکنش‌ها یک جستجو اول سطح (BFS) روی گراف جهت‌دار بدون دور تراکنش‌ها در هر گره اعمال می‌شود. تراکنش‌هایی که در این جستجو ملاقات نشوند زائد بوده و دور ریخته می‌شوند. همچنین گره‌ها بر اساس رفتار خود در فرآیند اجماع BFT دسته‌بندی شده و به سه دسته خوش‌رفتار، مشکوک و بدرفتار تقسیم می‌شوند. هر گره دارای دو مقدار Stack+ و Stack- است که پس از هر دور اجماع مورد بروزرسانی قرار می‌گیرد. هرگاه گره در یک دور

اجماع نظر موافق با اکثریت از خود ارائه دهد مقدار Stack+ او یک واحد افزایش یافته و در غیر این صورت مقدار Stack- او یک واحد افزایش می‌یابد. گره مقدار Stack- غیر مساوی با صفر مشکوک شناخته شده و گره با سه مقدار منفی گره بدرفتار است.

۵-۳- فرآیند تخلیه بار محاسباتی

در در مطابق آنچه در بخش قبل مورد بررسی قرار گرفت همه رویکردهای تخلیه بار موجود از خدمت‌گزاران لبه برای تخلیه بهره می‌گرفت و عملا فناوری زنجیره بلوکی در آن‌ها به علت کندی و گذردهی پایین، توان اجرای توابع تخلیه‌شده با ویژگی‌های مورد نیاز سرعت محاسبه، گذردهی و امنیت بالا را نداشت. در این مقاله ابتدا قطعه‌بندی و تصمیم‌گیری برای تخلیه قطعه مناسب برای هر گره اجرا می‌شود. در ادامه، گره مناسب برای تخلیه انتخاب شده و قطعه اجرا و نتیجه پردازش آن به گره مبداء بازگشت داده می‌شود. انتخاب گره مناسب برای تخلیه، پردازش و بازگشت نتیجه در ارتباط مستقیم با فناوری زنجیره بلوکی بوده و در قالب قرارداد هوشمند در شبکه پیاده‌سازی می‌شود. اجرای مراحل فوق نیازمند تضمین موارد زیر می‌باشد:

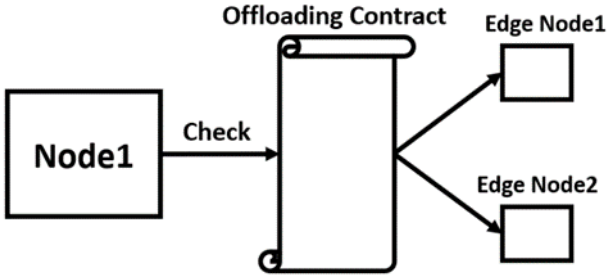
- گره متقاضی تخلیه باید در ازای هزینه خود برای تخلیه، جواب درست دریافت کند.
- هزینه پردازش بار محاسباتی تخلیه‌شده باید عادلانه باشد و گره مقصد در صورت انجام درست پردازش حتما آن را دریافت کند.
- با توجه به هزینه‌بر بودن فرآیند تخلیه، در صورت بروز عمل بدخواهانه توسط گره متقاضی و گره مقصد، ساز و کار تنبیهی مناسبی برای بازدارندگی از اعمال بدخواهانه در نظر گرفته شود.

فرآیند تخلیه بار از دو مرحله اصلی برگزاری مناقصه معکوس برای یافتن گره مقصد برای تخلیه و مرحله انتقال هزینه و دریافت نتیجه تشکیل می‌شود. این دو مرحله به فاصله $\Delta_{exec}= \left|T_{EndAuction} - T_{StartMoneyTransfer}\right|$ از یکدیگر انجام می‌شوند که حد بالایی برای زمان پردازش بار محاسباتی تخلیه‌شده در گره مقصد را مشخص کرده و به شناسایی گره‌های بدرفتار کمک می‌کند.

در مناقصه معکوس[10] برای یافتن گره مقصد تخلیه، پس از انتخاب قطعه مناسب برای جهت تخلیه، پیچیدگی زمانی اجرای قطعه تخمین زده شده و تابع ثبت مناقصه جدید در قرارداد هوشمند تخلیه بار صدا زده می‌شود. در این تابع حداکثر زمان قابل قبول برای پردازش بار محاسباتی تخلیه‌شده و کلید عمومی یکبار مصرف گره متقاضی نیز مشخص شده است.

گره‌های لبه شبکه با پتانسیل انتخاب به عنوان گره مقصد با دریافت تقاضای تخلیه و بررسی پیچیدگی قطعه و حداکثر زمان قابل قبول برای اجرای آن، در صورت وجود منابع لازم برای پردازش بار، پاسخ خود شامل هزینه که گره متقاضی باید بپردازد، بیشینه زمانی که برای پردازش بار تضمین می‌کند و کلید عمومی تصادفی و یکبار مصرف خود به عنوان شناسه را ارسال می‌کند.

گره متقاضی، گره با بهترین هزینه پیشنهادی را به عنوان گره برنده مناقصه برگزیده و آن را به اطلاع گره منتخب می‌رساند. آشکار بودن قیمت‌های پیشنهادی گره‌های شرکت کننده در مناقصه باعث افزایش انگیزه منابع بیکار جهت ارائه قیمت کم برای برنده شدن در مناقصه می‌شود. لازم به ذکر است هویت اصلی گره متقاضی و منتخب مقصد از یکدیگر و کل شبکه حفظ می‌شود. شکل ۲ برگزاری این مناقصه را نمایش می‌دهد.



شکل ۲- برگزاری مناقصه معکوس برای یافتن گره مناسب برای تخلیه

در مرحله انتقال هزینه و دریافت نتیجه، هم گره متقاضی و هم گره مقصد بایستی برای تضمین این که هدف آن‌ها اشغال منابع شبکه و حملاتی همچون منع دسترسی نیست، هزینه‌ای معادل هزینه انجام تراکنش را در قرارداد هوشمند وثیقه قرار دهند. همچنین، گره متقاضی یک جفت کلید عمومی تصادفی جدید جهت انتقال ناشناس نتیجه تخلیه بار ایجاد می‌کند. گره مقصد پس از دریافت بار محاسباتی تخلیه‌شده به همراه ورودی ارسالی آن، تراکنش را رمزگشایی کرده و پیچیدگی بار محاسباتی را تخمین زده و با تخمین اولیه ارائه شده در درخواست متقاضی مقایسه می‌کند. در صورت عدم تطابق و تخمین پیچیدگی بالاتر توسط مقصد به نسبت پیچیدگی اعلامی توسط متقاضی، اجرای الگوریتم متوقف شده و کلید خصوصی که با آن تراکنش رمزگشایی شده را در غالب تراکنش جدید برای اعتراض به ارضا نشدن قیود مسئله در شبکه ارسال می‌کند. با اثبات تقلب توسط متقاضی، هزینه وثیقه متقاضی به مقصد داده می‌شود. در صورتی که مقصد بدون دلیل کلید خصوصی را در شبکه فاش کرده باشد هزینه وثیقه‌ی او در قرارداد هوشمند در اختیار گره متقاضی قرار می‌گیرد.

در صورت عدم رخداد این مشکلات، گره مقصد بار محاسباتی را پردازش کرده و یک تراکنش حاوی نتیجه رمزشده به همراه اثبات دانش صفر برای تایید صحت نتیجه را منتشر می‌کند و مهر زمانی به این نتیجه نیز اضافه خواهد شد. پس از دریافت نتیجه در اولین نوبت فرآیند اجماع، صحت نتیجه دریافتی و همچنین رعایت بازه زمانی مجاز برای ارسال نتیجه در گره متقاضی بررسی خواهد شد و در صورت ارضا گره مقصد علاوه بر بازپس‌گیری هزینه وثیقه خود، خزینه اجرای تراکنش را نیز دریافت می‌کند.

۴- ارزیابی روش پیشنهادی

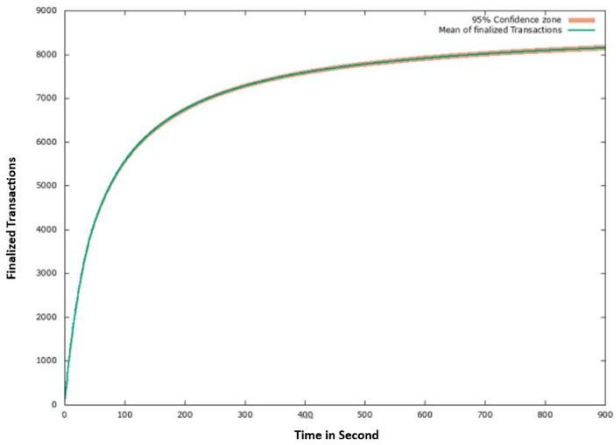
در این بخش، برای ارزیابی رویکرد پیشنهادی سناریوهای متعددی پیاده‌سازی و بررسی می‌شود. بستر ارزیابی یک سرور با هسته Xeon نسل ۱۰، RAM 32GB و کارت شبکه 1GBps می‌باشد که مبتنی بر Docker تقسیم‌بندی شده است. گره‌های شبکه در بستر زنجیره بلوک با زبان برنامه نویسی Golang توسعه داده شده‌اند. هر گره با پروتکل GRPC در کانال TLS ایمن به یک یا چند گره دیگر متصل می‌شود. همچنین از طریق REST API اتصال برنامه‌های کاربردی به گره‌ها ایجاد شده و تراکنش‌ها پدید می‌آید. هر تراکنش پس از ایجاد برای فرآیند شایعه‌پراکنی ارجاع داده می‌شود. گره‌های مجاور پس از دریافت تراکنش و قبل از هرس، آن را در حافظه موقت خود نگاه می‌دارند و پس از هرس در صورت صحیح بودن، تراکنش مذکور از بین نرفته و در یک پایگاه‌داده No-SQL مبتنی بر گراف جهت‌دار بدون دور ذخیره می‌شوند. قرارداد هوشمند در سیستم نیز مبتنی بر زبان Rust توسعه یافته است. هر ارزیابی دقیقا ۱۰ بار اجرا شده و تمامی نتایج حاصله با ضریب اطمینان ۹۵٪ درج شده است.

[10] Reverse Auction

۴-۱- بررسی تاثیر تاخیر بر تعداد تراکنش‌های نهایی

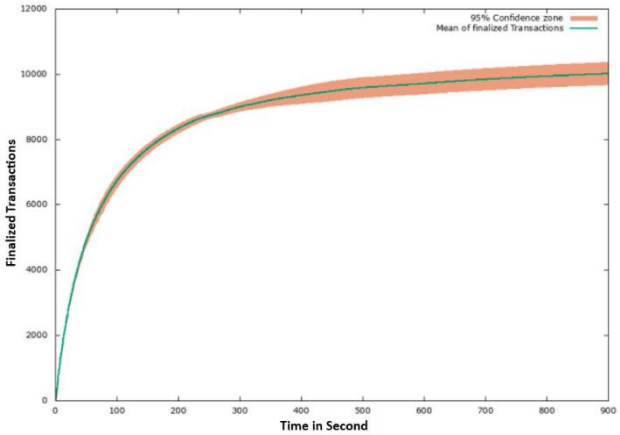
در ابتدا برای تعیین حداکثر تعداد تراکنش ممکن در لحظه، شبکه‌ای با ۳ گره، یعنی حداقل گره‌های مورد نیاز برای رسیدن به اجماع، با منابع حداقلی ۱ هسته پردازنده و ۲ گیگابایت RAM با شرایط شبکه‌ای ایده‌آل شامل تاخیر، احتمال خرابی و گم‌شدن تراکنش‌های اندک به مدت ۹۰۰ ثانیه مورد بررسی قرار می‌گیرد.

با توجه به شکل ۳، رشد تعداد تراکنش‌های نهایی‌شده در طول زمان برای یک شبکه ایده‌آل به صورت لگاریتم طبیعی است. از ثانیه ۰ تا ۲۰۰ رشد تعداد تراکنش‌های نهایی در سیستم با شیب زیادی افزایش می‌یابد و از ثانیه ۸۰۰ به بعد شیب تقریبا به ۰ می‌گراید که نشان از اشباع منابع سیستم دارد. بازه اطمینان کوچک در شکل نشان از تخمین دقیق از وضعیت سیستم در هر ثانیه دارد.



شکل ۳- بررسی تعداد تراکنش‌های نهایی‌شده در طول زمان در شرایط ایده‌آل شبکه

در شکل ۴، به منظور ارزیابی عملکرد رویکرد پیشنهادی در شرایط واقعی که شبکه دارای خطا و تاخیر است، نتایج با اعمال ۲ میلی ثانیه تاخیر روی ۱ گره یعنی ۳۰ درصد از گره‌ها مورد بررسی قرار می‌گیرد. مطابق نتایج بدست آمده، اعمال تاخیر روی یکی از ۳ گره سبب افزایش تعداد تراکنش‌های نهایی در سیستم شده و با توجه به ساز و کار مناقصه برای انتخاب بهترین هزینه برای اعمال تراکنش تخلیه‌بار، گره‌ای که دارای تاخیر است از مناقصه خارج و تنها یک کاندید برای عمل تخلیه باقی می‌ماند.

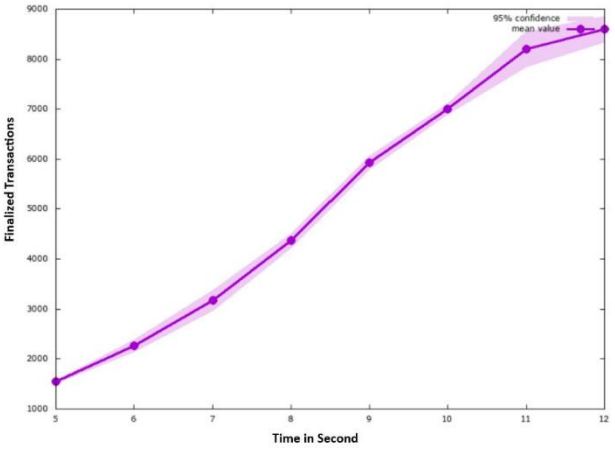


شکل ۴- بررسی تعداد تراکنش‌های نهایی‌شده در طول زمان با اعمال تاخیر روی ۳۰٪ از گره‌های شبکه

۴-۲- بررسی تاثیر منابع سیستم بر تعداد تراکنش‌های نهایی‌شده

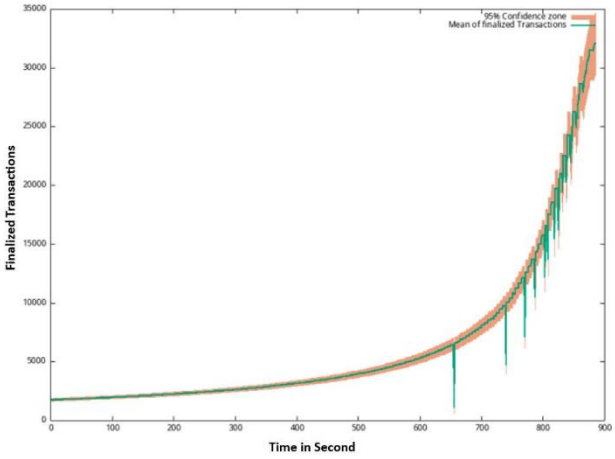
به منظور بررسی تاثیر میزان منابع سیستم بر گذردهی و بهره‌وری، در این سناریو هر گره در ابتدا محدود به یک هسته پردازشی بوده و نتیجه افزایش تعداد هسته‌های پردازشی بر تعداد تراکنش‌های نهایی شده در سیستم پس از گذشت ۳۰ دقیقه از اجرای سناریو مورد بررسی قرار می‌گیرد. این سناریو برای ۷ شبکه مختلف متشکل از ۵، ۷، ۸، ۹، ۱۰، ۱۱ و ۱۲ گره با مجموع قدرت پردازشی متعدد ارزیابی شده است.

مطابق شکل ۵، قدرت پردازشی با افزایش تعداد هسته‌های پردازشی افزایش یافته و در نتیجه تعداد تراکنش نهایی شده افزایش می‌یابد. علت این امر اینست که با افزایش منابع موجود در سیستم، امکان انجام تراکنش‌های بیشتر تخلیه‌بار فراهم شده و گره‌های شبکه می‌توانند تعداد تراکنش بیشتری را ثبت و نهایی کنند که در نتیجه گذردهی شبکه افزایش می‌یابد.



شکل ۵- بررسی تاثیر افزایش قدرت‌پردازشی گره‌های شبکه بر تعداد تراکنش‌های نهایی شده

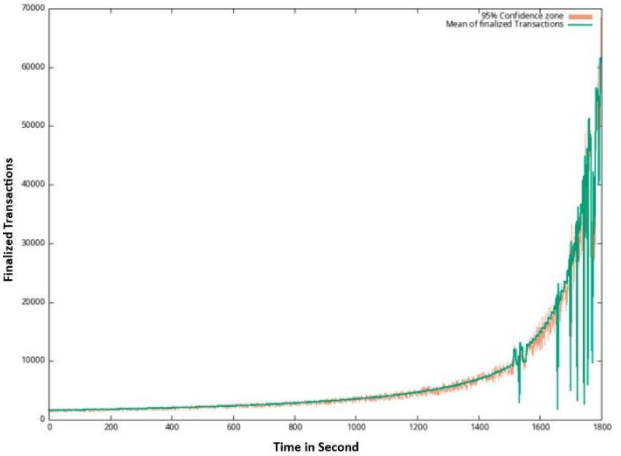
در شکل ۶، تاثیر افزایش قدرت پردازشی گره‌ها از طریق اضافه کردن تعداد هسته‌های پردازنده در دسترس بعضی از گره‌های شبکه مورد بررسی قرار گرفته است. در این سناریو ۴ گره با مجموع قدرت پردازشی ۶ هسته وجود دارد. مطابق شکل ۶ برخلاف حالت همگن، تعداد تراکنش‌های نهایی‌شده شبکه به نسبت زمان تا رسیدن به حداکثر قدرت گذردهی، بصورت نمایی رشد می‌کنند و همچنین در برخی از قسمت‌های نمودار افت گذردهی مشاهده شده است که اعوجاج نمودار نیز در اثر همین افت گذردهی ایجاد شده است. با بررسی دقیق‌تر در می‌یابیم که ناهمگن بودن گره‌ها از نظر قدرت پردازشی در برخی مواقع شامل تعداد تراکنش نهایی‌شده بالاتر سبب بوجود آمدن حالت ازدحام در شبکه می‌شود و بطور مقطعی گذردهی شبکه کاهش پیدا می‌کند، با اینحال شاهد هستیم که شبکه بسرعت به‌حالت طبیعی باز می‌گردد.



شکل ۶- بررسی تاثیر ناهمگنی گره‌ها برتعداد تراکنش‌های نهایی‌شده (سناریو اول)

در شکل ۷، سناریو بررسی تاثیر ناهمگن بودن گره‌ها از نظر قدرت پردازشی در شبکه‌ای متشکل از ۶ گره و مجموع قدرت پردازشی ۱۲ هسته مورد بررسی قرار گرفته است. گره اول ۴ هسته، گره دوم ۲ هسته و مابقی هر یک ۱ هسته دارا می‌باشند.

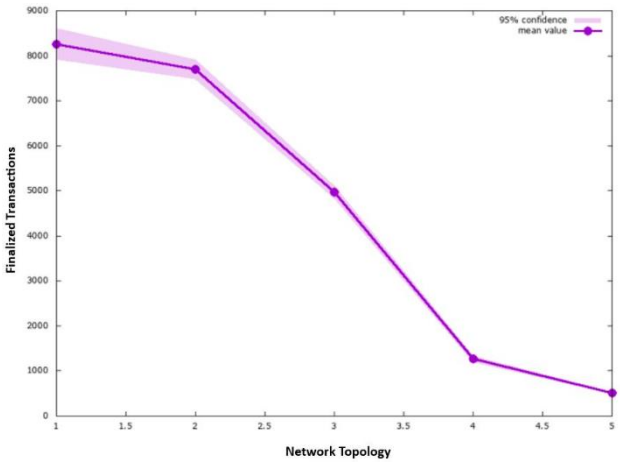
مطابق شکل ۷، با افزایش میزان ناهمگنی گره‌های تشکیل‌دهنده از نظر قدرت پردازشی، اعوجاج‌ها از زمان ۱۵۰۰ به بعد بیشتر شده است. با توجه به بررسی به عمل آمده سبب این اعوجاج تشدید حالت ازدحام شبکه بوده است. همچنین، دامنه تکرار افت مقطعی تراکنش‌های نهایی‌شده افزایش یافته است و میزان زمانی که شبکه نیاز دارد به حداکثر گذردهی دست یابد نیز افزایش یافته است. باید توجه داشت که میزان تراکنش ورودی در هر لحظه به شبکه به یک میزان است اما شبکه تا زمان گرم‌شدن نیاز به زمان دارد زیرا در لحظات اولیه امکان پاسخگویی به حجم عظیمی از درخواست‌ها را ندارد. همانند حالتی که شبکه به صورت همگن تحت بارکاری بوده، افزایش قدرت پردازشی گره‌های شبکه نیز سبب افزایش تعداد تراکنش‌های تاییدشده و گذردهی شبکه شده اما با افزایش ناهمگنی در شبکه میزان تاخیر و افت مقطعی تعداد تراکنش تاییدشده در لحظه بیشتر شده و شبکه به میزان زمان بیشتری برای رسیدن به حداکثر بهره‌وری نیازمند است.



شکل ۷- بررسی تاثیر ناهمگنی گره‌ها برتعداد تراکنش‌های نهایی‌شده (سناریو دوم)

۳-۴- بررسی تاثیر همبندی شبکه تعداد تراکنش‌های نهایی‌شده

همبندی شبکه از عوامل موثر بر میزان کارایی هر گره و در نتیجه کارایی کل شبکه است. از آنجایی که هر گره میزان محدودی از منابع در اختیار دارد، اگر یک گره مسئولیت بروزرسانی تعدادی از گره‌های دیگر در مورد تراکنش‌های جدید را دارا باشد به علت محدودیت یاد شده در منابع ممکن است شبکه را با کندی مواجه کند. ممکن است منابع گره تنها در مورد بروزرسانی سایر گره‌ها مصرف شده و گره فرصت مشارکت در فرآیند تخلیه‌بار را نداشته باشد. در این بررسی ۵ نوع همبندی متفاوت از جمله خطی و ستاره مورد ارزیابی قرار گرفته است و در محور عمودی در شکل ۸ هر همبندی با اعداد ۱ تا ۵ مشخص شده است. مطابق شکل ۸، هر چه همبندی از حالت خطی به ستاره‌ای نزدیک‌تر می‌شود (حرکت از توپولوژی ۱ به سمت ۵) تعداد تراکنش‌های نهایی‌شده کاهش می‌یابد. بنابراین، در محیط تست با تعداد محدودی گره توپولوژی خطی عملکرد بهتری از خود ارائه می‌دهد. البته بدیهی است که توپولوژی خطی در شبکه حالتی ایده‌آل است زیرا همه گره‌ها در شبکه آدرس اینترنتی معتبری نداشته و به کمک دیواره آتش به شبکه می‌پیوندند.



شکل ۸- بررسی تاثیر همبندی شبکه برتعداد تراکنش‌های نهایی‌شده

۵- نتیجه‌گیری

در این مقاله به ارائه یک روش تخلیه‌بار محاسباتی مقیاس‌پذیر و بی‌نام مبتنی بر فناوری زنجیره‌بلوکی پرداخته‌شد. در این راستا، امکان تخلیه بار درون-زنجیره‌ای به‌جای استفاده از فناوری‌های دیگر همچون رایانش ابری و لبه مورد بررسی قرار گرفت. همچنین، مقیاس‌پذیری در زنجیره‌بلوکی به‌کمک اصلاح ساختار اجماع و تایید تراکنش‌ها و همچنین ساختار ذخیره و بازیابی اطلاعات بهبود یافت. به‌علاوه، از اثبات دانش صفر برای بهبود حریم خصوصی و بی‌نام مانی استفاده گردید.

به عنوان کار آتی، در نظر داریم از رویکردهای Sharding و چکیده‌گیری هوشمند برای تسریع ثبت تراکنش‌ها در شبکه استفاده نماییم. همچنین، بنا داریم با تجمیع رویکرد ارائه شده با پروتکل ذخیره‌سازی غیرمتمرکز سیستم فایل (IPFS) ، از به اشتراک‌گذاری تراکنش‌ها در شبکه بهره جسته تا پردازش حجم عظیمی از بار محاسباتی تخلیه‌شده در یک گره مورد تعدیل قرار گیرد.

مراجع

[1] In J. Jayabalan, N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy", Journal of parallel and distributed computing, vol. 164, pp. 152-167, 2022.

[2] S. Reno, M. M. Haque, "Solving blockchain trilemma using off-chain storage protocol", IET information security, vol. 17, no. 4, pp. 681-702, 2023.

[3] Z. Yanjun, "Making smart manufacturings marter a survey on blockchain technology in Industry 4.0", Enterprise information systems, vol. 15, no. 10, pp. 1323-1353, 2021.

[4] Statista Research Department, "Internet of Things - Number of connected devices worldwide 2015-2025, " [Online}, Available: <https://www.statista.com/statistics/471264/iot-number-of–connected-devices-worldwide/>, Date Published: Nov 27, 2016, Last access on: 31 October 2021.

[5] N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey, " in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, 2018.

[6] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J.S. Song, K. Mankodiya, "Fusion of IoT, AI, Edge-Fog-Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine", IEEE internet of things journal, vol. 10, no. 5, p.1-1, 2023.

[7] Y. Hassanzadeh-Nazarabadi, A. Kupcu, O. Ozkasap, "LightChain: Scalable DHT-Based Blockchain," IEEE transactions on parallel and distributed systems, vol. 32, no. 10, pp. 2582-2593, 2021.

[8] M. Zamani, M. Movahedi, M. Raykova. "RapidChain: Scaling Blockchain via Full Sharding. " Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931–948, 2018.

[9] J. Jayabalan, N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy", Journal of parallel and distributed computing, vol. 164, pp. 152-167, 2022.

[10] S. Reno, M. M. Haque, "Solving blockchain trilemma using off-chain storage protocol", IET information security, vol. 17, no. 4, pp. 681-702, 2023.

[11] A. Miller, I. Bentov, R. Kumaresan, C. Cordi, P. McCorry, "Sprites and State Channels: Payment Networks that Go Faster than Lightning", arXiv preprint.

[12] Y. Kwon, H. Kim, J. Shin and Y. Kim, "Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash", 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 935-951, 2019.

[13] Bitcoin unlimited: The peer-to-peer electronic cash system for planet earth, 2020, [Online]. Available online: https://www.bitcoinunlimited.info.

[14] Q. Yang, H. Guo, V. Zhu, X. Fan, X. Cui, and X. Kong, "Smart Blockchain", First International Conference, SmartBlock 2018, Tokyo, Japan, Proceedings, pp. 179, 2018.

[15] B. Körbel, M. Sigwart, P. Frauenthaler, M. Sober, S. Schulte, "Blockchain-Based Result Verification for Computation Offloading", 19th International Conference, ICSOC 2021, pp. 99-115, 2021.

[16] "The golem project crowdfunding whitepaper, " White Paper, TheGolem Project, 2016. [Online]. Available: https://golem.network/doc/Golemwhitepaper.pdf

[17] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-5, 2019.

[18] S. Ghaemi, H. Khazaei, P. Musilek, "ChainFaaS: An Open Blockchain-Based Serverless Platform", IEEE Access, vol. 8, pp. 99, 2020.

[19] S.A. Mostafavi, E. Barkhordari, "A Mobility Aware Task Offloading Scheme Based On Ant Colony Optimization Algorithm In Software-Defined Fog Computing, " in Tabriz Journal of Electrical Engineering (TJEE), vol. 53, no. 4, pp. 245-256, 2023.

[20] R. Mehdikhan, H. Khaleghi Bizaki, S. G. H. Tabatabaei, " Blockchain Based Multi-Domain Resource Allocation of Network Slicing, " in Tabriz Journal of Electrical Engineering (TJEE), vol. 54, no. 1, pp. 73-85, 2024.