Computational Intelligence in Electrical Engineering
Vol. 15, No. 04, 2025
pp. 67- 82
Research Paper

Enhancing Security and Privacy in Ride-Sharing Services through a Smart Contract-Based Approach and Reputation-Based Consensus

Milad Ramani [1], Mohammad Dakhilalian *[1], Parvin Rastegari[2] , Behzad Nazari [1]

[1] Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
[2] Electrical and Computer Engineering Group, Golpayegan College of Engineering, Isfahan University of Technology, Golpayegan, Iran

Abstract:
The Internet of Vehicles (IoV) has been developed to improve driving quality and enhance pedestrian safety. One of the services IoV provides is ride-sharing, which allows drivers to share the empty seats in their vehicles with passengers traveling in the same direction. This service leads to reduced fuel consumption, lower air pollution, and decreased traffic congestion, while also being economically beneficial for both vehicle owners and passengers. However, ride-sharing services face significant security threats such as man-in-the-middle attacks, Sybil attacks, and message forgery. This paper aims to enhance the security of ride-sharing services by utilizing blockchain technology and its associated features, including smart contracts and a consensus algorithm based on proof of service and reputation. The main objective of this paper is to maximize the decentralization of network management to avoid creating a centralized management unit that could become a bottleneck. In summary, the goal is to improve safety and efficiency, reduce security risks, and ensure that all parties fulfill their commitments.

Keywords: Internet of Vehicles, Blockchain, Ride-sharing, Proof of Service and Reputation Consensus, Smart Contract.

https://doi.org/10.22108/ISEE.2024.143148.1711

مقاله پژوهشی

ارتقای امنیت و حریم خصوصی در خدمات اشتراک‌گذاری سفر با رویکردی مبتنی بر قرارداد هوشمند و اجماع مبتنی بر شهرت

میلاد رحمانی[۱]، محمد دخیل علیان[۲*]، پروین رستگاری[۳]، بهزاد نظری[۴]

۱- دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران
ml.rahmani1369@gmail.com

۲- دانشیار، دانشکدهٔ مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران
mdalian@iut.ac.ir

۳- استادیار، گروه مهندسی برق و کامپیوتر، دانشکدهٔ فنی مهندسی گلپایگان، دانشگاه صنعتی اصفهان، گلپایگان، ایران
p.rastegari@iut.ac.ir

۴- استادیار، دانشکدهٔ مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران
nazari@iut.ac.ir

چکیده: اینترنت وسایل نقلیه (IoV) با هدف بهبود کیفیت رانندگی و افزایش ایمنی عابران پیاده توسعه یافته است. یکی از خدمات IoV اشتراک‌گذاری سفر است که به رانندگان اجازه می‌دهد صندلی‌های خالی خودروهای خود را با مسافران هم‌مسیر به اشتراک بگذارند. این خدمت به کاهش مصرف سوخت، آلودگی هوا و ازدحام ترافیک منجر می‌شود و برای صاحبان خودرو و مسافران از نظر اقتصادی سودمند است؛ با این حال، در این خدمت تهدیدهای امنیتی همچون حملات مرد میانی، حملات سیبیل و جعل پیام‌ها خطراتی جدی به همراه دارند. در این مقاله، تلاش شده است تا امنیت اشتراک‌گذاری سفر با استفاده از فناوری زنجیره‌بلوکی و ویژگی‌های مرتبط با آن، از جمله قراردادهای هوشمند و الگوریتم اجماع بر اساس اثبات خدمت و شهرت، ارتقا یابد. هدف اصلی این مقاله تمرکززدایی از مدیریت شبکه به حداکثر میزان ممکن است تا از ایجاد یک واحد مدیریت مرکزی به عنوان گلوگاه جلوگیری شود و به طور خلاصه، هدف افزایش ایمنی و کارایی، کاهش ریسک‌های امنیتی و تضمین اجرای تعهدات توسط همهٔ طرفین است.

واژه‌های کلیدی: اشتراک‌گذاری سفر، اثبات خدمت و اجماع شهرت، اینترنت وسایل نقلیه، زنجیره‌بلوکی، قرارداد هوشمند.

۱- مقدمه

اینترنت وسایل نقلیه (IoV)[۱] به شبکه‌ای از خودروهای متصل اشاره دارد که قادر به برقراری ارتباط با یکدیگر و با دستگاه‌های دیگر مانند چراغ‌های راهنمایی، حسگرها و واحدهای کنار جاده (RSU)[۲] هستند [۲]. IoV پتانسیلی جالب توجه برای بهبود ایمنی جاده، مدیریت ترافیک، حفاظت از محیط‌زیست و ارتقای راحتی کاربران دارد. یکی از خدمات IoV که در سال‌های اخیر بسیار محبوب شده است، اشتراک‌گذاری سفر[۳] است [۳]. در این خدمت، رانندگان می‌توانند صندلی‌های خالی خود را با مسافران هم‌مسیر به اشتراک بگذارند. این مدل مزایای بسیاری برای هر دو طرف دارد؛ به طوری که رانندگان می‌توانند هزینهٔ

[۱] تاریخ ارسال مقاله: ۱۴۰۳/۰۸/۰۵
تاریخ پذیرش مقاله: ۱۴۰۳/۰۸/۲۸
نام نویسندهٔ مسئول: محمد دخیل علیان
نشانی نویسندهٔ مسئول: ایران، اصفهان، دانشگاه صنعتی اصفهان، دانشکدهٔ برق و کامپیوتر

سوخت خود را کاهش دهند، درآمد اضافی کسب کنند و در حل مسائل اجتماعی و زیست‌محیطی سهیم باشند. در مقابل، مسافران نیز از مزایایی همچون کرایهٔ کمتر، سفرهای سریع‌تر و راحتی بیشتر بهره‌مند می‌شوند. به علاوه، این خدمت می‌تواند به کاهش ازدحام ترافیک، آلودگی هوا، انتشار گازهای گلخانه‌ای و تصادفات جاده‌ای از طریق کاهش تعداد خودروهای موجود در جاده کمک کند [۴]؛ با وجود این مزایا، اشتراک‌گذاری سفر با چالش‌هایی جالب توجه در زمینهٔ امنیت و حفظ حریم خصوصی روبه‌رو است. این خدمت معمولاً به یک واحد مدیریت مرکزی (CMU)[۴] متکی است تا ارتباطات میان شرکت‌کنندگان در شبکه را هماهنگ کند. CMU وظایفی مانند ایجاد حساب‌های کاربری، تطبیق رانندگان و مسافران، تأیید هویت‌ها، پردازش پرداخت‌ها و رسیدگی به اختلافات را به عهده دارد؛ اما این واحد مرکزی به عنوان نقطه ضعف واحد و هدفی برای حملات مختلف نیز عمل می‌کند. مهاجمان مخرب می‌توانند با نفوذ به CMU به اطلاعات حساس کاربران دسترسی پیدا کنند یا عملکرد شبکه را دستکاری کنند که این امر ممکن است پیامدهای جدی برای امنیت، اعتماد و رضایت کاربران داشته باشد [۵].

برای برطرف کردن این چالش‌ها، فناوری زنجیره‌بلوکی[۵] می‌تواند به منظور تمرکززدایی مدیریت این خدمت استفاده شود [۶]. زنجیره‌بلوکی یک دفتر کل توزیع‌شده است که تراکنش‌ها را به شیوه‌ای امن، شفاف و غیرقابل تغییر ثبت می‌کند. تمرکززدایی و تغییرناپذیری آن، این فناوری را برای کاربردهای گوناگون مناسب ساخته است [۷]؛ از جمله در پزشکی قانونی [۸]، سیستم‌های بهداشتی [۹]، سیستم‌های رأی‌گیری [۱۰]، بیمه‌های سلامت [۱۱]، سیستم‌های احراز هویت [۱۲] و به ویژه اینترنت اشیا و اینترنت وسایل نقلیه [۱۳].

در مطالعات پیشین، زنجیره‌بلوکی به عنوان یک عنصر اساسی در حوزه‌های مختلف شناخته شده است. برای مثال، در [۸]، از ماهیت غیرمتمرکز و تغییرناپذیر زنجیره‌بلوکی برای تضمین ذخیره‌سازی غیرقابل دستکاری داده‌ها، اشتراک‌گذاری امن و ردیابی قابل اعتماد رویدادها و تراکنش‌ها در اکوسیستم وسایل نقلیهٔ متصل استفاده شده است. این چارچوب از قراردادهای هوشمند، تکنیک‌های رمزنگاری و سرچشمهٔ داده برای افزایش یکپارچگی و اعتبار شواهد قانونی بهره می‌برد.

در پژوهشی دیگر [۱۲]، طرحی پیشنهاد شده است که با استفاده از ویژگی‌های غیرمتمرکز و مقاوم در برابر دستکاری زنجیره‌بلوکی، چالش‌های احراز هویت را برطرف می‌کند. این طرح با بهره‌گیری از روش‌های رمزنگاری و قراردادهای هوشمند، احراز هویت امن و ناشناس را برای وسایل نقلیه در شبکه‌های VANET[۶] ارائه می‌دهد و هم‌زمان حریم خصوصی آن‌ها را حفظ می‌کند. وسایل نقلیه می‌توانند از یک مرجع معتبر گواهی دریافت کنند و در حین احراز هویت، بدون افشای هویت واقعی خود، اعتبار و صلاحیتشان را اثبات کنند.

در نهایت، معماری مطرح‌شده در [۱۳] از ویژگی‌های ذاتی زنجیره‌بلوکی مانند تمرکززدایی، شفافیت و تغییرناپذیری برای ایجاد سیستم مدیریت دسترسی مقیاس‌پذیر و امن برای دستگاه‌های IoT استفاده کرده است. در این معماری، یک دفتر کل توزیع‌شده برای ثبت سیاست‌های کنترل دسترسی و اطلاعات احراز هویت دستگاه‌های IoT به کار گرفته می‌شود. همچنین، قراردادهای هوشمند برای اعمال قوانین کنترل دسترسی استفاده می‌شوند و مدیریت دسترسی به صورت خودکار و قابل اعتماد انجام می‌شود. این معماری از کنترل دسترسی دقیق و به‌روزرسانی پویای سیاست‌ها پشتیبانی می‌کند و در مدیریت دستگاه‌های IoT و تعاملات آن‌ها انعطاف‌پذیری زیادی را فراهم می‌آورد.

همان‌طور که در مثال‌های بالا نشان داده شد، زنجیره‌بلوکی با بهره‌گیری از ویژگی‌های ذاتی خود مانند تغییرناپذیری، شفافیت، مقاومت در برابر دستکاری و استفاده از قراردادهای هوشمند، به حل چالش‌های مختلف در شبکه‌ها کمک می‌کند. این چالش‌ها شامل دستکاری شبکه توسط گره‌های مخرب و حفظ حریم خصوصی و ناشناس بودن هستند. شبکهٔ اینترنت وسایل نقلیه، به ویژه سیستم‌های اشتراک‌گذاری سفر، با مسائل امنیتی منحصربه‌فردی در محیط عملیاتی خود مواجه هستند؛ از این رو، استفاده از شبکه‌های مبتنی بر زنجیره‌بلوکی می‌تواند امنیت و حریم

خصوصی را در این سیستم‌ها بهبود دهد که این موضوع در بخش‌های بعدی این مقاله بیشتر بررسی خواهد شد.

در ادامه و در بخش ۲، مفاهیم و پیش‌نیازهای مورد نیاز معرفی می‌شوند. در بخش ۳، پژوهش‌های مرتبط مرور می‌شوند و دربارهٔ مزایا و معایب آن‌ها بحث می‌شود. بخش ٤ مدل پیشنهادی را با جزئیات توصیف می‌کند و اجزای مختلف آن را توضیح می‌دهد. در بخش ۵، نتایج شبیه‌سازی و تحلیل‌های مربوط ارائه می‌شود تا اثربخشی مدل پیشنهادی نشان داده شود و در نهایت، در بخش ٦ نتیجه‌گیری مقاله ارائه می‌شود.

۲- پیش‌نیازها

در این بخش، مفاهیم و فناوری‌های اساسی مرتبط با موضوع پژوهش، از جمله زنجیره‌بلوکی، الگوریتم‌های اجماع، قراردادهای هوشمند و اشتراک‌گذاری سفر معرفی و کاربردها، زیرساخت‌های فنی و اهمیت آن‌ها در چارچوب اینترنت وسایل نقلیه توضیح داده می‌شوند.

۲-۱ زنجیره‌بلوکی

زنجیره‌بلوکی یک دفتر کل توزیع‌شده و غیرمتمرکز است که امکان انجام تراکنش‌های امن و شفاف را بدون نیاز به یک مرجع یا واسطهٔ مرکزی فراهم می‌آورد. این فناوری سیستم‌های تراکنش سنتی را با ایجاد ثبت مقاوم در برابر دستکاری و قابل راستی‌آزمایی برای تراکنش‌ها و داده‌ها متحول کرده است. زنجیره‌بلوکی شامل زنجیره‌ای از بلاک‌هاست که داده‌هایی مانند تراکنش‌ها، قراردادها و سوابق را ذخیره می‌کند [۱٤]. هر بلاک شامل چکیدهٔ رمزنگاری‌شدهٔ بلاک قبلی، برچسب زمانی[۷] و یک شناسهٔ منحصربه‌فرد است که یک توالی قوی و غیرقابل تغییر از اطلاعات را برقرار می‌کند [۱۵]. این ارتباطات بین بلاک‌ها یکپارچگی داده‌ها و تغییرناپذیری آن‌ها را تضمین می‌کند. هر گونه تلاش برای تغییر یا حذف یک بلاک کل زنجیره را نامعتبر می‌کند و توسط شبکه رد می‌شود. شبکه‌های زنجیره‌بلوکی براساس مدل‌های دسترسی و حکمرانی به انواعی مختلف تقسیم می‌شوند [۷]:

– زنجیره‌بلوکی عمومی: محیطی باز و بدون مجوز را فراهم می‌کند که هر کسی می‌تواند در آن شرکت کند، تراکنش‌ها را اعتبارسنجی کند و به شبکه کمک کند.

– زنجیره‌بلوکی خصوصی: دسترسی را به شرکت‌کنندگانی مشخص محدود می‌کند و از این طریق، حریم خصوصی و محرمانگی شبکه را تضمین می‌کند.

– زنجیره‌بلوکی کنسرسیوم: تحت نظارت گروهی از سازمان‌ها فعالیت می‌کند.

– زنجیره‌بلوکی ترکیبی (هیبرید): ترکیبی از انواع دیگر است و ویژگی‌های چند نوع زنجیره‌بلوکی را در خود دارد [۱٦].

۲-۲ الگوریتم‌های اجماع

اجماع یک عنصر حیاتی در فناوری زنجیره‌بلوکی است که تضمین می‌کند همهٔ گره‌های شبکه دربارهٔ وضعیت فعلی دفتر کل توزیع‌شده به توافق می‌رسند. اجماع از دوبار خرج کردن ، کلاهبرداری و حملات مخرب به شبکه جلوگیری می‌کند [۱۷]. الگوریتم‌های اجماع مختلفی برای دست‌یابی به این هدف پیشنهاد شده‌اند. برخی از الگوریتم‌های رایج عبارت‌اند از:

– اثبات کار (PoW)[۸]: در این روش، گره‌ها برای حل معماهای پیچیده ریاضی رقابت می‌کنند.

– اثبات سهام (PoS)[۹]: در این روش، تأثیر گره‌ها بر شبکه بر اساس میزان سهمی است که در شبکه دارند. این روش جایگزینی کم‌مصرف‌تر نسبت به PoW است.

– تحمل خطای بیزانسی (PBFT)[۱۰]: الگوریتمی که در سیستم‌های توزیع‌شده، از جمله شبکه‌های زنجیره‌بلوکی، کاربرد دارد [۱۸]. این الگوریتم از یک فرآیند رأی‌گیری برای دست‌یابی به اجماع استفاده می‌کند. PBFT در برابر خطاهای بیزانسی مقاوم است و تأثیر گره‌های مخرب یا معیوب را کاهش می‌دهد.

– نسخه‌های پیشرفتهٔ PBFT که عملکرد و کاربردپذیری این الگوریتم را در محیط‌های عملیاتی بهبود داده‌اند [۱۹].

۲-۳ قراردادهای هوشمند

قرارداد هوشمند برنامه‌ای است که روی سکوی زنجیره‌بلوکی اجرا می‌شود و شرایط و ضوابط توافق‌شده بین طرفین را اعمال می‌کند. این قراردادها می‌توانند وظایفی مانند انتقال وجوه، تأیید هویت، صدور توکن یا فعال‌سازی رویدادها را انجام دهند [۲۰]. هدف اصلی قراردادهای هوشمند حذف نیاز به واسطه‌های مورد اعتماد در تراکنش‌هاست. شفافیت و تغییرناپذیری زنجیره‌بلوکی این امکان را فراهم می‌آورد که همهٔ افراد بتوانند اجرای قرارداد را نظارت و اعتبارسنجی کنند [۲۰].

ماهیت خودکار قراردادهای هوشمند کارایی فرآیندهای تراکنشی را افزایش و احتمال خطای انسانی را کاهش می‌دهد. قراردادهای هوشمند به دو دسته تقسیم می‌شوند:

– قراردادهای هوشمند قطعی: برای ورودی‌های یکسان، خروجی یکسانی تولید می‌کنند.

– قراردادهای هوشمند غیرقطعی: ممکن است بر اساس شرایط خاص یا عوامل خارجی، نتایجی متفاوت ارائه دهند.

۲-٤ اشتراک‌گذاری سفر

اشتراک‌گذاری سفر یکی از خدمات IoV است که به رانندگان اجازه می‌دهد صندلی‌های خالی وسایل نقلیهٔ خود را با مسافرانی که مقصدی مشابه دارند به اشتراک بگذارند. این خدمت مزایای بسیاری برای هر دو طرف دارد [٤]. نحوهٔ عملکرد آن به این صورت است که رانندگان و مسافران مبدأ، مقصد و زمان حرکت خود را در یک سکوی برخط اعلام می‌کنند. سپس، ارائه‌دهندهٔ خدمت با استفاده از الگوریتم‌ها یا مداخلهٔ دستی، رانندگان و مسافران را با مسیرهای مشابه تطبیق می‌دهد [۲۱]. رانندگان در طول مسیر مسافران را سوار و در مقصد مدنظر پیاده می‌کنند. در پایان سفر، ارائه‌دهندهٔ خدمت کمیسیونی از هر دو طرف دریافت می‌کند. اشتراک‌گذاری سفر علاوه بر مزایای فردی، مزایای اجتماعی نیز به همراه دارد، از جمله:

– کاهش ازدحام ترافیک از طریق کاهش تعداد خودروها در جاده.

– افزایش ایمنی جاده از طریق کاهش تصادفات.

– صرفه‌جویی مالی از طریق تقسیم هزینه‌های سفر.

این خدمت شامل مدل‌هایی مختلف از جمله کارپولینگ، اشتراک‌گذاری سفر همتا به همتا (P2P)[۱۱] و خدمات درخواستی است. خدمات اشتراک‌گذاری سفر به طرزی جالب توجه در سراسر جهان محبوب شده‌اند و بخشی جالب توجه از بازار حمل‌ونقل را به خود اختصاص داده‌اند. انعطاف‌پذیری، مقرون‌به‌صرفه بودن و راحتی این خدمات باعث شده است تا به یکی از گزینه‌های اصلی جابه‌جایی در مناطق شهری تبدیل شوند و به کاهش مالکیت خودروهای شخصی کمک کنند.

– کارپولینگ: در این مدل، افرادی که همدیگر را می‌شناسند، از یک خودرو برای سفر یا رفت‌وآمد مشترک استفاده می‌کنند و معمولاً طبق برنامه‌ای از پیش تعیین‌شده و با تقسیم هزینه‌ها سفر می‌کنند.

– خدمات درخواست خودرو: در این خدمات، شرکت‌هایی مانند اوبر[۱۲] و لیفت[۱۳] از طریق یک برنامهٔ کاردی موبایلی، مسافران را به رانندگان نزدیک متصل می‌کنند [۲۲].

در حالی که کارپولینگ به افرادی محدود می‌شود که همدیگر را می‌شناسند، خدمات درخواست خودرو و همتا به همتا به مسافران اجازه می‌دهند تا حتی با افراد غریبه برای سفرهای درخواستی یا طولانی‌مدت همراه شوند؛ با وجود این مزایا، اشتراک‌گذاری سفر با چالش‌هایی در زمینهٔ امنیت و حریم خصوصی مواجه است. این چالش‌ها شامل سرقت هویت، کلاهبرداری کاربران مخرب، دستکاری یا حذف داده‌ها، افشای اطلاعات حساس کاربران توسط هکرها و رقابت ناعادلانه هستند؛ از این رو، نیاز به راه‌حل‌هایی برای غلبه بر این چالش‌ها وجود دارد. در بخش بعدی، مدل پیشنهادی ما برای تضمین امنیت و حفظ حریم خصوصی در خدمات اشتراک‌گذاری سفر ارائه خواهد شد.

۳- پیشینهٔ پژوهش

در این بخش، مروری مختصر بر پژوهش‌های پیشین ارائه می‌شود تا به درک دستاوردها و شناسایی نقاط ضعف موجود کمک کند. در سال‌های اخیر، پژوهش‌هایی متعدد با هدف طراحی سیستم‌های اشتراک‌گذاری سفر (RSS)[۱٤] مبتنی بر فناوری زنجیره‌بلوکی انجام شده‌اند.

در [۲۳]، نویسندگان الگوریتم اجماع اثبات رانندگی (PoD)[۱۵] را معرفی کرده‌اند که با تصادفی‌سازی انتخاب ماینرهای صادق، راندمان استخراج بلاک‌ها را برای کاربردهای VANET مبتنی بر زنجیره‌بلوکی بهبود می‌بخشد. این اجماع به حل مشکلات کارایی، عدالت و مقیاس‌پذیری پروتکل‌های اجماع موجود مانند PoS،PoW و PBFT کمک می‌کند. همچنین، آن‌ها تکنیکی مبتنی بر امتیاز استاندارد خدمت (Sc) برای فیلتر کردن و حذف گره‌های مخرب پیشنهاد داده‌اند که انتخاب منصفانه و کارآمد ماینرها در شبکه‌های VANET را امکان‌پذیر می‌کند و باعث می‌شود PBFT در شبکه‌های عمومی بزرگ خودروها سازگارتر شود.

در [۲۴]، نویسندگان BlockV را معرفی کرده‌اند که راه‌حلی مبتنی بر زنجیره‌بلوکی برای تضمین عدالت در اشتراک‌گذاری سفر است. این سیستم با ثبت رویدادهای مربوط به سفر در یک دفتر کل زنجیره‌بلوکی، برای همهٔ شرکت‌کنندگان در شبکهٔ همتا به همتا امکان دسترسی به این اطلاعات را فراهم می‌کند، شفافیت را ارتقا می‌دهد و یک سیستم شهرت عادلانه را حفظ می‌کند. این راه‌حل مشکلات ناشی از مدل‌های متمرکز اعتماد را مدنظر قرار می‌دهد که در آن‌ها کاربران باید به ارائه‌دهندگان خدمت اعتماد کنند؛ موضوعی که ممکن است به فعالیت‌های مخرب و بی‌عدالتی منجر شود.

در [۲۵]، CoRide به عنوان یک سرویس اشتراک‌گذاری سفر مشارکتی مبتنی بر زنجیره‌بلوکی معرفی شده است که حفظ حریم خصوصی را در اولویت قرار می‌دهد. این سرویس با چالش‌های امنیتی و حفظ حریم خصوصی که از همکاری بین ارائه‌دهندگان خدمات مختلف ناشی می‌شود، مقابله می‌کند. در این مقاله، چهار جنبهٔ کلیدی بررسی شده‌اند: احراز هویت ناشناس کاربران، استفاده از زنجیره‌بلوکی کنسرسیوم برای ثبت سفرهای مشارکتی، احراز هویت مکان و تطبیق رانندگان، و بهره‌گیری از Zerocash برای پرداخت‌های ناشناس و جلوگیری از حملات دوبار خرج کردن.

در [۲۶]، پژوهشی در زمینهٔ اشتراک‌گذاری سفر برای وسایل نقلیهٔ خودران (AVs)[۱۶] ارائه شده است. AVها مزایایی همچون راحتی و ایمنی بیشتر را برای کاربران ارائه می‌دهند؛ اما چالش‌هایی جدید از جمله هماهنگی، اعتماد و مسئولیت‌پذیری را نیز ایجاد می‌کنند. در این مقاله، یک معماری غیرمتمرکز اشتراک‌گذاری سفر بر بستر Hyperledger Fabric پیاده‌سازی شده است که محدودیت‌های سیستم‌های اشتراک‌گذاری سفر متمرکز را برطرف می‌کند. یکی از ویژگی‌های کلیدی این سیستم امکان مشارکت مالکان خودروهای خودران در یک ناوگان اشتراکی در زمان‌های بیکاری است. استفاده از زنجیره‌بلوکی به دلیل تغییرناپذیری و تحمل خطا در این معماری مورد توجه قرار گرفته است.

در [۲۷]، نویسندگان از زنجیره‌بلوکی خصوصی برای ارتقای امنیت در خدمات اشتراک‌گذاری سفر استفاده کرده‌اند. این پژوهش نگرانی‌های مرتبط با ماهیت متمرکز سکوهای سنتی اشتراک‌گذاری سفر را بررسی کرده است که در آن‌ها مرجع مرکزی می‌تواند گزارش‌ها و اطلاعات کاربران را دستکاری یا حذف کند. برای کاهش این مشکلات اخلاقی، راه‌حلی مبتنی بر Hyperledger پیشنهاد شده است که اطمینان می‌دهد پس از ثبت گزارش توسط کاربران، سازمان قادر به تغییر یا حذف آن نخواهد بود و این امر شفافیت و پاسخ‌گویی را ارتقا می‌دهد.

در [۲۸]، B-Ride به عنوان یک سیستم غیرمتمرکز اشتراک‌گذاری سفر مبتنی بر زنجیره‌بلوکی عمومی معرفی شده است. B-Ride وابستگی به یک مرجع مورد اعتماد را حذف می‌کند و به رانندگان و مسافران اجازه می‌دهد تا بر جزئیات سفر خود کنترل داشته باشند. چالش اصلی این سیستم سوءاستفاده از ناشناس بودن توسط کاربران مخرب است. برای حل این مشکل، B-Ride از پروتکل سپرده‌گذاری زمان‌دار با استفاده از قراردادهای هوشمند و اثبات عضویت در مجموعهٔ ناشناس استفاده کرده است. این پروتکل رانندگان و مسافران را ملزم می‌کند تا برای تعهد به سفر، سپرده‌ای را ارائه دهند. همچنین، راننده باید حضور به‌موقع در مکان سوار شدن را به بلاک‌چین اثبات کند. برای حفظ حریم خصوصی، از اثبات عضویت در مجموعهٔ ناشناس برای مخفی‌سازی مکان دقیق سوار شدن استفاده شده است. پرداخت عادلانه نیز بر اساس مکانیسم پرداخت

به‌ازای مسافت طی‌شده انجام می‌شود. B-Ride همچنین یک مدل شهرت ارائه می‌دهد که رفتارهای گذشتهٔ رانندگان را ارزیابی و به مسافران کمک می‌کند تا تصمیم‌هایی بهتر بر اساس تاریخچهٔ سیستم اتخاذ کنند.

در این مقاله، مدلی را برای غلبه بر این محدودیت‌ها و کاستی‌ها ارائه می‌دهیم. مدل پیشنهادی با بهره‌گیری از زنجیره‌بلوکی و قراردادهای هوشمند، عملکردهایی مانند تطبیق رانندگان و مسافران بر اساس ترجیحات آن‌ها بدون افشای اطلاعات شخصی، اجرای خودکار تراکنش‌ها، ایجاد بلاک‌های مقاوم در برابر دستکاری برای ذخیرهٔ سوابق و ارائهٔ امتیازات شهرت برای سنجش اعتمادپذیری کاربران را انجام می‌دهد. در بخش‌های بعدی، مدل پیشنهادی خود را شرح می‌دهیم و مزایای امنیتی و کارایی آن را در مقایسه با مدل‌های موجود ارزیابی خواهیم کرد.

٤- مدل پیشنهادی

در این بخش، مدل پیشنهادی خود را که با هدف دست‌یابی به تمرکززدایی، حفظ حریم خصوصی و ایجاد مشوق‌هایی برای رفتار صادقانه در سیستم اشتراک‌گذاری سفر طراحی شده است، توصیف می‌کنیم [۱].

٤-١ فرضیات

در بدترین سناریو، دست‌کم دوسوم از عناصر شبکه به صورت صحیح و بدون قصد مخرب یا سوءاستفاده فعالیت می‌کنند و وظایف خود را به‌درستی انجام می‌دهند.

٤-٢ اجزای شبکه

در مدل پیشنهادی، اجزای زیر دخیل هستند:

– مرجع ثبت‌نام (RA)[۱۷]: این نهاد مسئول ثبت کاربران جدید، شامل مسافران یا رانندگان، است. هر کاربر باید اطلاعات عمومی مانند کد شناسایی خود را ارائه دهد. کاربر جدید می‌تواند زوج کلید خود را تولید کند و کلید خصوصی را نزد خود نگه دارد و کلید عمومی را به RA ارسال کند. پس از تکمیل ثبت‌نام، اطلاعات کاربر روی بلاک‌چین اول ثبت و از حافظهٔ RA حذف می‌شود. با عدم ذخیره اطلاعات روی RA، امنیت و عملکرد شبکه بهبود می‌یابد.

– واحد انتخاب گروه برنده (WGSU)[۱۸]: این واحد گروهی از خودروها را برای استخراج بلاک بعدی در بلاک‌چین دوم انتخاب می‌کند.

– بلاک‌چین اول (BC1): یک دفتر کل توزیع‌شده است که اطلاعات کاربران (مانند کد ملی یا شمارهٔ پلاک) را به صورت چکیدهٔ سازشده ذخیره می‌کند. این اطلاعات در RSUهایی با شمارهٔ شناسایی فرد (ID) ذخیره می‌شوند.

– بلاک‌چین دوم (BC2): دفتر کل توزیع‌شده‌ای است که اطلاعات سفر را در قالب قراردادهای هوشمند ذخیره می‌کند. این اطلاعات توسط RSUهای دارای شمارهٔ زوج نگهداری می‌شود که هر دو بلاک‌چین خصوصی هستند.

– واحد کنار جاده (RSU): این واحد در کنار جاده (مانند چراغ‌های راهنمایی یا علائم ترافیکی) قرار دارد و دارای قابلیت پردازش، ذخیره‌سازی و ارتباطات است. در سیستم پیشنهادی، RSU وظایفی مختلف از جمله نگهداری BC1 و BC2، تأیید اعتبار خودروها، کمک به WGSU برای انتخاب ماینرها،تسهیل ارتباطات میان وسایل نقلیه و ارائهٔ اثبات‌های دانش صفر برای تأیید حضور خودروها در مبدأ را انجام می‌دهد.

– خودرو: علاوه بر ارائهٔ خدمت حمل‌ونقل، به عنوان ماینر در الگوریتم اجماع BC2 مشارکت می‌کند.

– مسافر: کاربری است که درخواست سفر از یک خودرو دارد.

٤-٣ درخواست‌های سرویس

چارچوب پیشنهادی شامل دو نوع درخواست سرویس با امنیت زیاد و معمولی است.

٤-٣-١ درخواست سرویس با امنیت زیاد

مراحل درخواست سرویس با امنیت زیاد به شرح زیر هستند:

– ایجاد کلید موقت: مسافر یک جفت کلید موقت برای سفر تولید می‌کند.

– ایجاد درخواست: مسافر مبدأ (o) و مقصد (d) خود را با استفاده از کلید خصوصی موقت رمزنگاری و همراه با کلید عمومی موقت ارسال می‌کند:

$$R_{eq.} = \varepsilon(o,d)||\rho \quad (۱)$$

که در آن، ε بیانگر رمزنگاری با کلید خصوصی موقت و ρ نشان‌دهندهٔ کلید عمومی موقت مسافر است.

– ارسال پیشنهاد توسط راننده: رانندگان پیشنهاد خود شامل زمان رسیدن به مبدأ (To)، زمان رسیدن به مقصد (Td) و هزینهٔ سفر (C) را ابتدا با کلید خصوصی خود و سپس با کلید عمومی موقت مسافر رمزنگاری می‌کنند:

$$Offer = \psi\big(\varepsilon(T_0, T_d, c)\big) \quad (۲)$$

که در آن، ε و ψ به‌ترتیب بیانگر رمزنگاری با کلید خصوصی راننده و کلید عمومی موقت مسافر هستند.

– انتخاب پیشنهاد بهینه: مسافر پیشنهادها را با توجه به شهرت[19] راننده، زمان سفر $(Tt = To + Td)$ وهزینه (C) مقایسه و پیشنهاد بهینه را انتخاب می‌کند:

$$Choose = max\,(Repute) \cap min\,(Tt) \cap min\,(C) \quad (۳)$$

– ایجاد قرارداد هوشمند: مسافر هزینهٔ سفر را در قرارداد هوشمند سپرده‌گذاری و مکان و کلید عمومی را با عدد تصادفی چکیده ساز می‌کند و در قرارداد قرار می‌دهد. سپس، قرارداد را به مخزن تراکنش ارسال می‌کند تا در بلاک‌چین ثبت شود.

– تأیید و رمزنگاری قرارداد: مسافر قرارداد را به صورت زیر رمزنگاری و به راننده ارسال می‌کند:

$$Accept \cdot = E(\varepsilon(Skey(SC)||Rnd)) \quad (٤)$$

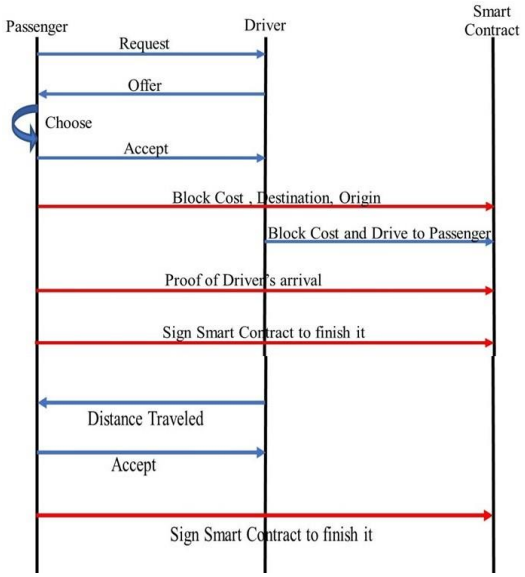
در رابطهٔ بالا، Rnd بیانگر عدد تصادفی، SC مبین قرارداد هوشمند[20]، $Skey$ نشانگر رمزنگاری با کلید خصوصی اصلی مسافر و ε و E به‌ترتیب معادل رمزنگاری با کلید خصوصی موقت مسافر و رمزنگاری با کلید عمومی راننده است.

– سپرده‌گذاری راننده: راننده مبلغی برابر هزینهٔ سفر را به عنوان ضمانت در قرارداد هوشمند سپرده‌گذاری می‌کند و به محل مبدأ می‌رود.

– تأیید حضور در مبدأ: مسافر حضور راننده در مبدأ را تأیید می‌کند. در صورت عدم تأیید، راننده می‌تواند با استفاده از عدد تصادفی و قرارداد هوشمند، حضور خود را اثبات کند. در این صورت، اعتبار مسافر کاهش می‌یابد و کل مبلغ به راننده پرداخت می‌شود.

– پرداخت چندمرحله‌ای: برای اطمینان از رضایت طرفین، پرداخت به صورت چندامضایی و مرحله به مرحله انجام می‌شود. راننده پس از طی هر مرحله از مسیر، مسافت طی‌شده را به مسافر ارسال و مسافر تراکنش را تأیید می‌کند. در پایان سفر، راننده تراکنش نهایی را امضا و مبلغ را به حساب خود واریز می‌کند.

این مکانیسم کلاهبرداری و تقلب را کاهش می‌دهد و از حملات انکار سرویس (DoS)[21] جلوگیری می‌کند. همچنین، استفاده از پرداخت چندمرحله‌ای رضایت هر دو طرف را تضمین می‌کند و امنیت سفر را افزایش می‌دهد. مراحل این سرویس در شکل (۱) قابل مشاهده هستند.



شکل (۱): نحوهٔ درخواست سرویس اشتراکی با امنیت زیاد

٤-۳-۲ درخواست سرویس معمولی

این نوع درخواست برای مسافرانی مناسب است که نیازی به امنیت زیاد در سفر خود ندارند و هزینهٔ کمتر را به حفظ حریم خصوصی ترجیح می‌دهند. فرآیند این روش مشابه روش امنیت زیاد است؛ با این تفاوت که در اینجا مسافر کلید موقت تولید نمی‌کند و مبدأ، مقصد و کلید عمومی خود را بدون رمزنگاری مستقیماً در قرارداد هوشمند قرار می‌دهد. این دو رویکرد انعطاف‌پذیری بیشتری برای مسافران فراهم می‌کنند؛ به طوری که مسافران می‌توانند بسته به نیاز خود، امنیت بیشتر یا هزینهٔ کمتر را انتخاب کنند [۱].

٤-٤ مدیریت شهرت

مدیریت شهرت یکی از مؤلفه‌های اساسی روش پیشنهادی است. شهرت هر وسیلهٔ نقلیه نشان‌دهندهٔ عملکرد و قابلیت اطمینان آن در انجام وظایف محوله است. اگر راننده مسافر را به‌موقع به مقصد برساند، شهرت وسیلهٔ نقلیه مطابق سیاست‌های شبکه افزایش می‌یابد. در مقابل، اگر راننده در رساندن مسافر به‌موقع موفق نباشد، شهرت وسیلهٔ نقلیه کاهش خواهد یافت. شهرت بیشتر شانس انتخاب راننده توسط مسافران را افزایش می‌دهد؛ زیرا نشان‌دهندهٔ قابل‌اعتماد بودن راننده است. افزون بر این، شهرت بیشتر احتمال انتخاب راننده برای استخراج یک بلوک در بلاک‌چین و دریافت پاداش آن را نیز افزایش می‌دهد که در بخش بعدی توضیح داده خواهد شد.

٤-٥ استخراج بلوک

همان‌طور که پیش‌تر اشاره شد، وسایل نقلیه در شبکهٔ ما به عنوان ماینر عمل می‌کنند؛ با این حال، به‌جای استفاده از روش‌های اثبات کار (PoW) یا اثبات سهام (PoS) که دارای معایبی هستند، ما روشی جدید را پیشنهاد می‌دهیم که شامل فیلتر چندمرحله‌ای گره‌های ماینر است. این روش پیشنهادی را اثبات خدمت و شهرت یا PoSR[۲۲] می‌نامیم.

٤-٥-۱ اثبات خدمت

وسایل نقلیه به طور دوره‌ای درآمد خود را در بازهٔ زمانی مشخصی محاسبه می‌کنند و این مقدار را به سامانهٔ مرکزی ارسال می‌کنند. سامانهٔ مرکزی میانگین درآمد گزارش‌شده توسط تمامی وسایل نقلیه را محاسبه و آن را به عنوان مقدار خدمت متوسط (AS)[۲۳] معرفی می‌کند. در مرحلهٔ بعد، وسایل نقلیه‌ای که درآمد گزارش‌شدهٔ آن‌ها در محدوده‌ای مشخص از مقدار خدمت متوسط قرار دارد، به مرحلهٔ بعدی انتخاب می‌شوند و در این مرحله، بر اساس شهرت خود با یکدیگر رقابت می‌کنند.

دلیل حذف وسایل نقلیه با درآمد بیشتر این است که در صورت انتخاب مداوم وسایل نقلیه با درآمد بیشتر، یک وسیلهٔ مخرب می‌تواند با گزارش درآمد جعلی زیاد همواره در گروه برنده باشد؛ اما با استفاده از روش پیشنهادی ما، هیچ وسیله‌ای نمی‌تواند از مقدار دقیق خدمت متوسط مطلع شود و درآمد گزارش‌شدهٔ خود را مطابق آن تنظیم کند. الگوریتم (۱) این فرآیند را نشان می‌دهد.

```
Algorithm 1: Selecting Average Service Winners
Input: n Driver
Output: Avg Service Winner
    1- Sum = 0
    2- for i in 0 to n-1:
        a. sum = sum + i (value)
    3- Avg = sum / n
    4- Up Avg   = Avg + 10% Avg
    5- Down Avg = Avg - 10% Avg
    6- for i in 0 to n-1:
        a. if i(value) < Up Avg:
            i. if i(value) > Down Avg:
                1. add i to Avg Service Winner
```

٤-٥-۲ اثبات شهرت

در این مرحله، واحد انتخاب گروه برنده (WGSU) به صورت تصادفی m واحد RSU با شناسه‌های فرد را انتخاب و آدرس خودروهایی را که در مرحلهٔ قبل برنده شده‌اند، به آن‌ها ارسال می‌کند و امتیاز شهرت این خودروها را درخواست می‌کند.

RSUها که هر کدام امتیاز شهرت هر وسیلهٔ نقلیه را به طور جداگانه ثبت کرده‌اند، امتیازهای درخواست‌شده را به WGSU ارسال می‌کنند. اگر دوسوم از پاسخ‌ها یکسان باشند، WGSU صحت امتیازهای شهرت ارسال‌شده را تأیید می‌کند و به مرحلهٔ بعدی می‌رود.

در مرحلهٔ نهایی، WGSU مجموع امتیازهای شهرت تمام خودروهای برنده را محاسبه و مجموع کل را ثبت

می‌کند. سپس، خودروها را به صورت تصادفی انتخاب و امتیازهای شهرت آن‌ها را ثبت می‌کند. این فرآیند تا زمانی ادامه می‌یابد که مجموع امتیازات خودروهای انتخاب‌شده به ۲۵ درصد از کل امتیاز شهرت برسد.

در نهایت، WGSU برندگان نهایی را برای ساخت بلاک به کل شبکه اعلام می‌کند (۲۵ درصد می‌تواند بر اساس سیاست‌های شبکه تغییر یابد). الگوریتم (۲) این فرآیند را به طور خلاصه نمایش می‌دهد.

Algorithm 2: Selecting Final Winners
Input: n Reputation
Output: Final Winners for Consensus list
1- for i in 0 to n-1:
   a. sum = sum + i (Reputation)
2- quarter = sum * 25%
3- Total Reputation = 0
4- While Total Reputation < quarter:
   a. Choose a random number between 0 to n-1
   b. Total Reputation = Total Reputation + Random number (value)
   c. Add Random number to Final Winners for Consensus list
   d. Remove the driver at the Random number index from list
   e. n = n-1

۳-۵-٤ استخراج بلوک توسط گروه برنده

پس از تعیین گروه برنده، وسیلهٔ نقلیه‌ای که بیشترین امتیاز شهرت را دارد به عنوان رهبر انتخاب می‌شود و سایر وسایل به عنوان گره‌های اعتبارسنج شناخته می‌شوند. این الگوریتم وسایل نقلیه را ترغیب می‌کند تا برای کسب امتیاز شهرت بیشتر تلاش کنند. رهبر بلوک را ایجاد و آن را به گره‌های اعتبارسنج ارسال می‌کند تا اعتبار تراکنش‌های موجود در بلوک را تأیید کنند. اگر دوسوم از گره‌های اعتبارسنج تراکنش را تأیید کنند، رهبر بلوک را همراه با امضای گره‌های اعتبارسنج به واحدهای RSU ارسال می‌کند تا به زنجیره اضافه شود. اگر تعداد گره‌های موجود در گروه برنده n باشد، تعداد پیام‌های ارسالی به صورت زیر محاسبه می‌شود:

– رهبر بلوک را ماین و به $n-1$ گره دیگر ارسال می‌کند. این مرحله شامل $n-1$ پیام ارسالی است.

– پس از تأیید تراکنش‌ها، هر گره اعتبارسنج نظر خود را به n-2 گره دیگر ارسال می‌کند. این مرحله شامل $(n-1)(n-2)$ پیام ارسالی است.

– نظر اکثریت توسط *n-1* گره به رهبر ارسال می‌شود که برابر $n-1$ پیام است.

بنابراین، تعداد کل پیام‌های ارسالی برابر است با n^2-n که از رابطهٔ زیر به دست می‌آید:

$$n-1+(n-1)(n-2)+(n-1)=n^2-n \quad (۵)$$

در نتیجه، سعی شد تا تعداد وسایل نقلیه در فرآیند اجماع قبل از استخراج بلوک‌های جدید کاهش یابد تا کارایی شبکه بهتر شود.

۵. ارزیابی

در ادامه، ارزیابی روش پیشنهادی را از جنبه‌های مختلف بررسی خواهیم کرد.

۱-۵ تحلیل امنیتی

چارچوب پیشنهادی ما برای اشتراک‌گذاری سفر ممکن است با انواعی مختلف از حملات امنیتی مواجه شود. تعدادی زیاد از گره‌های شبکه پتانسیل مخرب بودن یا آلوده شدن توسط گره‌های بدخواه را دارند. در این بخش، جنبه‌های امنیتی طرح پیشنهادی خود را تحلیل می‌کنیم.

۱-۱-۵ تحلیل امنیتی درخواست‌های خدمت

پیشنهاد مطرح‌شده الزامات زیر را برای امنیت و حفظ حریم خصوصی درخواست‌های خدمت در جنبه‌های مختلف برآورده می‌کند:

– تولید کلید موقت توسط مسافر: همان‌طور که اشاره شد، مسافر با استفاده از یک الگوریتم رمزنگاری، یک زوج کلید عمومی موقت تولید می‌کند. این اقدام شناسایی مسافر در طول سفر را عملاً غیرممکن می‌کند. در روش‌های دیگر، از هویت دائمی یا نام مستعار استفاده می‌شود که ممکن است توسط مهاجمان مخرب ردیابی یا افشا شود؛ در نتیجه، اگر مسافران از درخواست‌های با امنیت زیاد استفاده کنند، حریم خصوصی آن‌ها حفظ خواهد شد.

– استفاده از قرارداد هوشمند به‌جای CMU: پس از بررسی پیشنهادها، مسافر به‌جای ارتباط مستقیم با واحد مدیریت مرکزی از قرارداد هوشمند استفاده می‌کند. این روش در مقایسه با سرورهای متمرکز یا ارتباط همتا به همتا مزایای زیر را دارد:

– کاهش سربار ارتباطی و افزایش حریم خصوصی شرکت‌کنندگان شبکه: قرارداد هوشمند فقط به یک تراکنش برای شروع خدمت و یک تراکنش برای اتمام آن نیاز دارد. این قرارداد همچنین هویت و موقعیت جغرافیایی شرکت‌کنندگان را در شبکه پنهان نگه می‌دارد.

– این روش در برابر حملات افشا و محروم‌سازی از خدمت (DoS) که ممکن است CMU را هدف دهد، مقاوم است. تراکنش‌ها به‌جای CMU در دفترکل توزیع‌شده ثبت می‌شوند؛ بنابراین، CMU در برابر این حملات آسیب‌پذیر نخواهد بود؛ زیرا در این فرایند دخالت ندارد.

– دسترسی عمومی به قراردادهای هوشمند: از آنجا که قراردادهای هوشمند به صورت عمومی در دسترس هستند، احتمال سوءاستفاده از آن‌ها توسط افراد مخرب کاهش می‌یابد. این قرارداد قوانین و شرایط خدمت را تعریف و به طور خودکار اجرا می‌کند. همچنین، هر کسی می‌تواند به کد و روند اجرای آن دسترسی داشته باشد.

– اثبات حضور راننده با استفاده از اثبات دانایی صفر: راننده حضور خود در محل حرکت را با استفاده از تکنیک اثبات دانایی صفر ثابت می‌کند. این تکنیک به راننده اجازه می‌دهد تا بدون افشای اطلاعات حساس ثابت کند در محل تعیین‌شده حضور دارد. این کار حریم خصوصی مسافر را نیز حفظ می‌کند.

– امنیت پرداخت: اگر مسافر رفتاری مخرب داشته باشد و از ارسال مدارک مسافت طی‌شده خودداری کند، راننده می‌تواند سفر را خاتمه دهد و همچنان هزینهٔ مسافت‌های قبلی را دریافت کند. به طور مشابه، اگر راننده سفر را پایان دهد، مسافر نیز می‌تواند از ارسال مدارک باقی‌مانده خودداری و از پرداخت بیشتر جلوگیری کند.

۵-۱-۲ تحلیل امنیتی استخراج بلوک

در این بخش، جنبه‌های امنیتی استخراج بلوک در روش پیشنهادی ما را ارزیابی و آن را با سایر روش‌های موجود مقایسه می‌کنیم.

– عدم آگاهی گره‌ها از میانگین اثبات خدمت: هیچ وسیلهٔ نقلیه‌ای در شبکه از میانگین اثبات خدمت اطلاع ندارد و سیاست‌های تنبیهی برای وسایلی که اعداد تصادفی گزارش می‌کنند اعمال می‌شوند. هر وسیله مجبور است عملکرد واقعی خود را ارسال کند. همچنین، از آنجا که میانگین اثبات خدمت در شبکه منتشر نمی‌شود، گره‌های مخرب نمی‌توانند با شنود یا جست‌وجو در شبکه آن را تخمین بزنند. در روش‌های دیگر، از سرورهای متمرکز یا ارتباط P2P برای محاسبه و انتشار میانگین اثبات خدمت استفاده می‌شود که ممکن است در برابر حملات امنیتی آسیب‌پذیر باشند.

– انتخاب تصادفی واحد انتخاب‌کنندهٔ گروه برنده: واحدی که گروه برنده را انتخاب می‌کند به طور تصادفی انتخاب می‌شود که این امر دسترسی گره‌های مخرب به این واحد را دشوار می‌کند. علاوه بر این، این واحد به صورت فیزیکی نیز غیرقابل دسترس است.

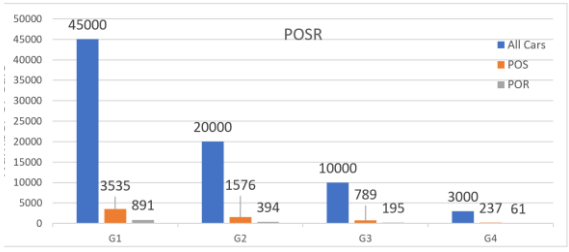
– الزام رهبر به استخراج بلوک صحیح: رهبر باید بلوکی صحیح استخراج کند؛ زیرا اگر بلوک شامل تراکنش‌های نادرست باشد، بیش از دوسوم گره‌های گروه برنده آن را تأیید نخواهند کرد و اجازهٔ انتشار آن را در شبکه نخواهند داد. این امر باعث کاهش شدید شهرت گره استخراج‌کننده می‌شود و انگیزه‌ای قوی برای رعایت قوانین ایجاد می‌کند.

۵-۲ تحلیل عملکرد

برای ارزیابی عملکرد روش پیشنهادی، از یک لپ‌تاپ با پردازندهٔ Core i7 نسل دهم، ۸ گیگابایت رم و حافظهٔ SSD و همچنین، از زبان برنامه‌نویسی Python و برنامه Postman برای شبیه‌سازی بخش‌های مختلف شبکه و برنامه‌نویسی بلاک‌چین استفاده شد.

۵-۲-۱ انتخاب گروه برنده

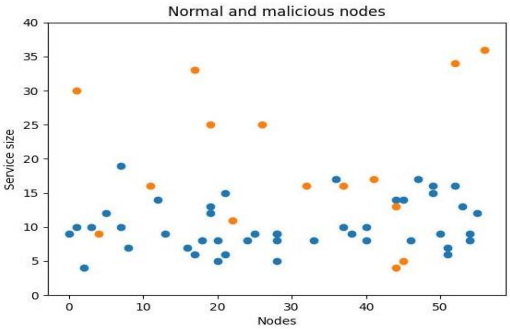
چالش اصلی در یک الگوریتم اجماع، سربار ارتباطی زیاد است که می‌تواند بر عملکرد شبکه تأثیر منفی بگذارد؛ بنابراین، لازم است تا حد ممکن تعداد گره‌ها کاهش یابد. شکل (۲) نشان می‌دهد چگونه معیارهای اثبات خدمت (POS) و اثبات شهرت (POR) که در روش پیشنهادی استفاده شده‌اند، تعداد وسایل نقلیه را کاهش می‌دهند.



شکل (۲): کاهش تعداد وسایل نقلیه از طریق POS و POR

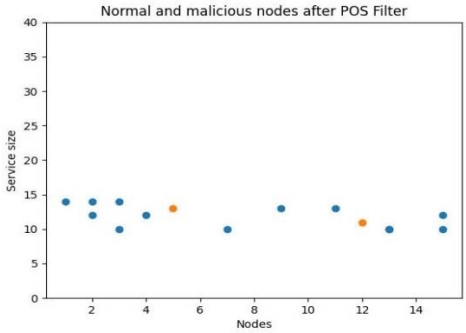
الگوریتم پیشنهادی گره‌های مخرب را از طریق سیستم شهرت شناسایی و حذف می‌کند. این سیستم بر اساس رفتار و عملکرد قبلی گره‌ها در شبکه، به هر گره یک امتیاز اختصاص می‌دهد.

در شکل (۳) نیز، تمامی گره‌های شبکه نشان داده شده‌اند؛ نقاط آبی نشان‌دهندهٔ گره‌های صادق و نقاط نارنجی نشان‌دهندهٔ گره‌های مخرب هستند.



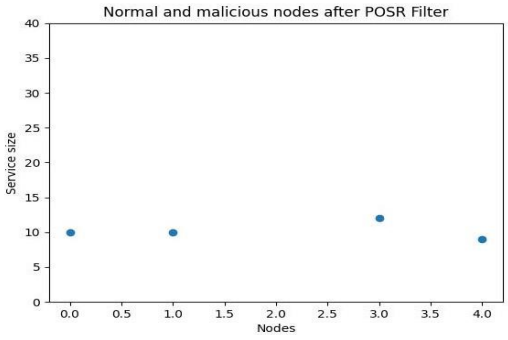
شکل (۳): تمام گره‌ها

در شکل (٤)، همان‌طور که مشاهده می‌شود، محدودهٔ خدمت متوسط به حدود ١٤ نزدیک است و بسیاری از وسایل نقلیه در اولین مرحله فیلتر شده‌اند.



شکل (٤): بعد از اولین فیلترینگ

همان‌طور که در شکل(۵) ملاحظه می‌شود، پس از فیلتر دوم، تعداد وسایل نقلیه به طرزی جالب توجه کاهش یافته است.

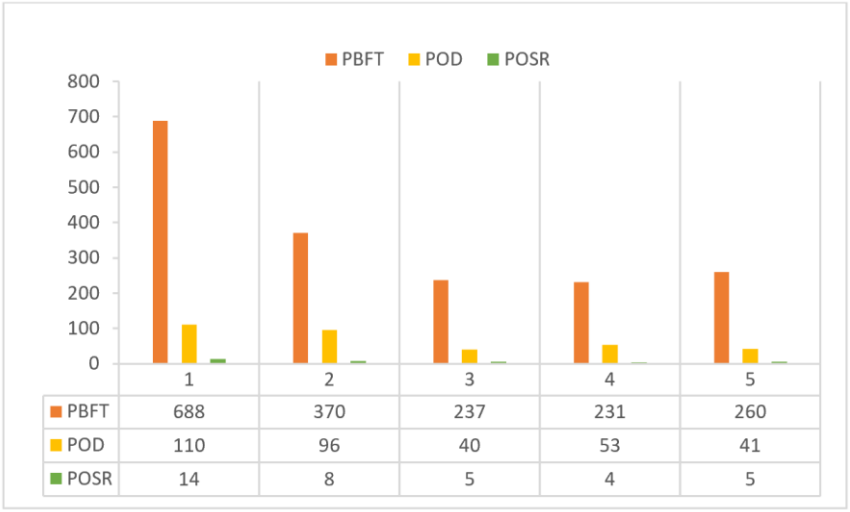


شکل (۵): بعد از فلیترینگ دوم

این نتایج نشان می‌دهد روش پیشنهادی ما با استفاده از فیلترینگ چندمرحله‌ای و به‌کارگیری معیارهای اثبات خدمت و شهرت، سربار شبکه را کاهش می‌دهد و بهره‌وری سیستم اجماع را بهبود می‌بخشد.

همان‌طور که در شکل (٦) نشان داده شده است، مقایسهٔ میان مدل پیشنهادی، مدل ارائه‌شده در [۲۳] و الگوریتم اجماع PBFT معمول نشان می‌دهد مدل پیشنهادی عملکردی بهتر در حذف وسایل نقلیه دارد. در الگوریتم پیشنهادی، در هر مرحله تعدادی زیاد از خودروها حذف می‌شوند و خودروهایی با بیشترین امتیاز در گردونهٔ رقابت باقی خواهند ماند که این خود شاخصی برای نشان دادن کیفیت سرویس‌دهی بیشتر شبکه است. از سوی دیگر، حذف گره‌ها در این مرحله سربار ارتباطی شبکه را به‌شدت کاهش خواهد داد. برای مثال، در مقایسهٔ اول، در صورتی که تعداد خودرو را ٦٨٨ در نظر بگیریم، با توجه به رابطهٔ (۵)، تعداد پیام های مبادله‌شده به منظور ساخت بلوک برابر ٤٧٢٦٥٦ خواهد شد؛ حال آنکه با الگوریتم پیشنهادی ارائه‌شده، فقط ١٤ خودرو به منظور ساخت بلوک باقی خواهند ماند که در این حالت، ساخت بلوک فقط با انتقال ۱۸۲ پیام ممکن خواهد بود که نشان از کاهش شدید پیام‌های مبادله‌شده دارد.

این امر به کاهش تعداد پیام‌های ارسالی در طول فرایند اجماع در شبکه منجر می‌شود.

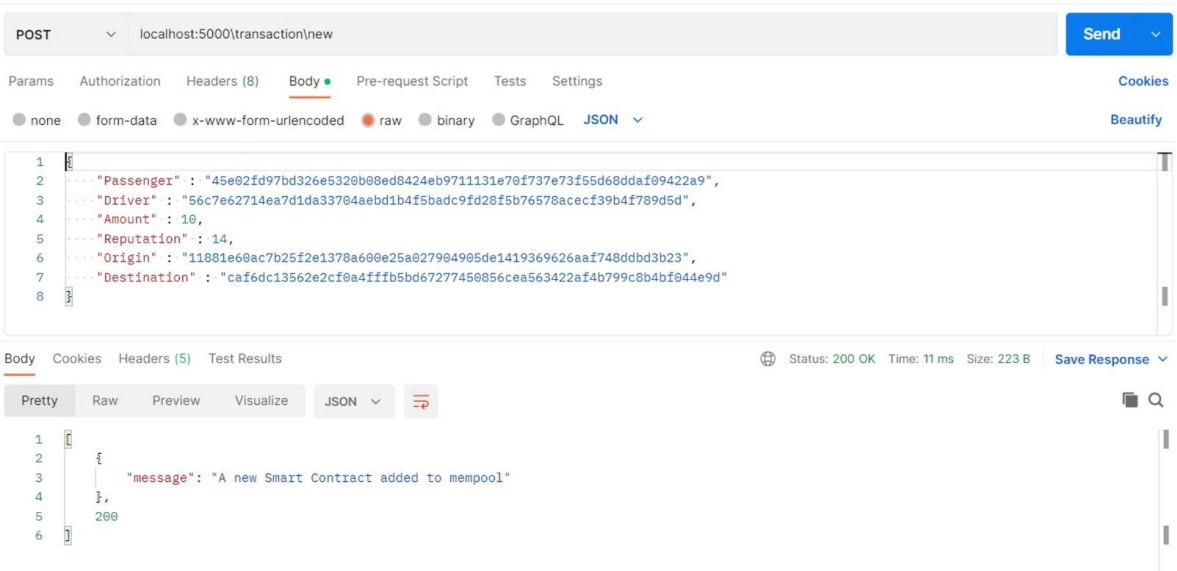


	1	2	3	4	5
PBFT	688	370	237	231	260
POD	110	96	40	53	41
POSR	14	8	5	4	5

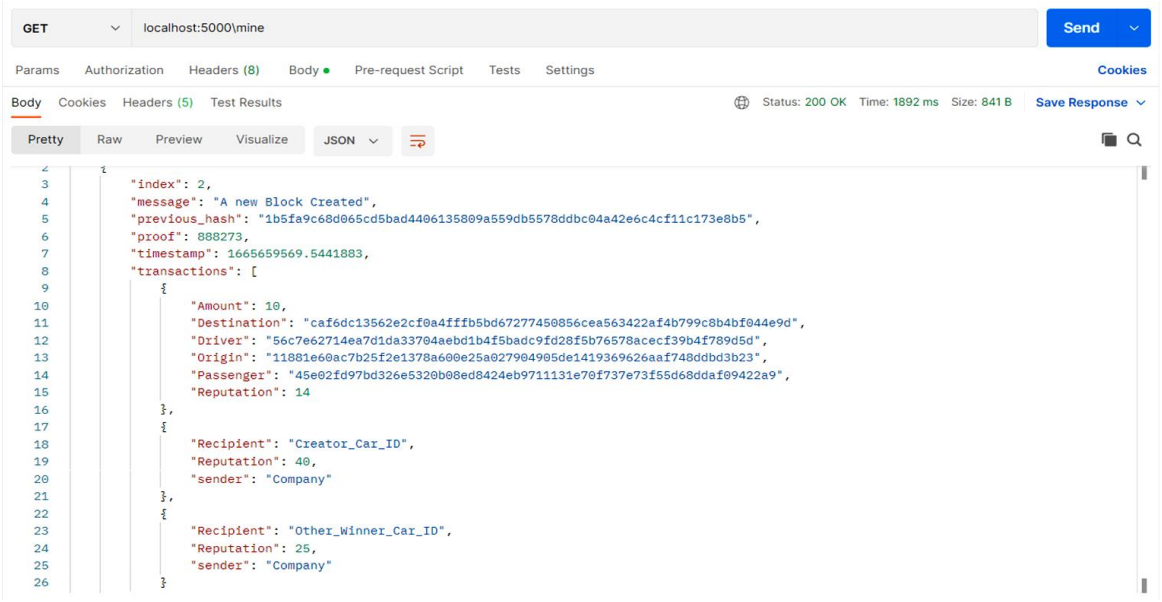
شکل (٦): مقایسهٔ بین مدل پیشنهادی ما (POSR) و مدل‌های پیشنهادی در[23] (PBFT و POD)

۲-۲-۵ ایجاد تراکنش، فراخوانی قرارداد هوشمند و استخراج بلوک

شکل (۷) نمونه‌ای از قرارداد هوشمند منتشرشده در شبکه را نشان می‌دهد. همان‌طور که در این شکل مشخص است، این قرارداد شامل اطلاعات مبدأ و مقصد، مبلغ پرداخت‌شده، هویت راننده و مسافر و شهرت تخصیص‌یافته به راننده است.



شکل (۷): نمونه‌ای از یک قرارداد هوشمند منتشرشده در شبکه



شکل (۸): استخراج یک بلوک توسط گره رهبر

وضعیت قرارداد نشان می‌دهد این قرارداد با موفقیت به استخر تراکنش‌ها اضافه شده و آماده است تا در بلوک اول شبکه گنجانده شود. افزون بر این، شکل (۸) نشان می‌دهد وسیلهٔ نقلیهٔ برنده با موفقیت یک بلوک استخراج کرده است. این فرآیند بیانگر آن است که تمامی شرایط و تراکنش‌های تعریف‌شده در قرارداد هوشمند به درستی تأیید شده‌اند و بلوک استخراج‌شده آمادهٔ اضافه شدن به زنجیرهٔ بلاک‌چین است. این فرآیند نشان‌دهندهٔ اتصال مؤثر قراردادهای هوشمند با فرآیند اجماع و استخراج است که به افزایش شفافیت، امنیت و اتوماسیون در شبکه منجر می‌شود.

جدول (۱) مقایسه‌ای میان مدل پیشنهادی و سایر مدل های موجود در ادبیات پژوهش ارائه می دهد. همان‌طور که ملاحظه می شود، مدل پیشنهادی از منظر حفظ حریم خصوصی، شفافیت، قابلیت گسترش پذیری و قابل تأیید بودن با روش‌های ارائهٔ قبلی مقایسه شده است. همان‌طور که در جدول مشاهده می شود، عمدهٔ این روش‌ها فاقد تمامی یا بیشتر ویژگی های یادشده هستند و مدل پیشنهادی طبق مطالب بیان‌شده در مقاله، تمامی ویژگی‌های یادشده را می‌تواند داشته باشد و در جنبه‌های مختلف بیان‌شده عملکردی بهتر نسبت به مدل‌های دیگر دارد و از کارایی کلی‌تری برخوردار است.

جدول (۱): مقایسهٔ روش پیشنهادی با مدل‌های موجود

Name	Architecture	Type	Smart Contract	Privacy	Transparency	Scalability	Verifiability
Existing RSSs	Centralized	-	-	-	-	-	-
Co- utile [29]	Decentralized	-	-	S*	-	-	-
B-Ride [28]	Blockchain	Public	U*	S	C*	-	-
Block V [24]	Blockchain	Private	N	S	S	-	-
Ride hailing [26]	Blockchain	Consortium	U	S	S	-	-
Ride-sharing Using IPFS [27]	Blockchain	Public	U	S	S	C	C
Our Proposal	Blockchain	Private	U	C	C	C	C

* N: Not Used, U: Used, S: Semi, C: Complete

٦. نتیجه‌گیری

در این مقاله، یک مدل شبکه‌ای برای سیستم اشتراک‌گذاری سفر پیشنهاد شد. هدف اصلی این پژوهش تمرکززدایی از واحد مدیریت مرکزی، از طریق توزیع وظایف آن بین اعضای گروه، بر اساس توانایی و کارایی هر عضو بود. هدف بعدی حفظ حریم خصوصی کاربران بود

که به دلیل ماهیت شفاف زنجیره‌بلوکی، در معرض سوءاستفاده قرار دارد. با استفاده از قراردادهای هوشمند، فرآیندهای مربوط به درخواست خودرو، انتخاب خودرو، رسیدن خودرو به مبدأ و حمل‌ونقل به مقصد به گونه‌ای طراحی شده‌اند که حقوق کاربران صادق در برابر مهاجمان مخرب حفظ شود و هم‌زمان حریم خصوصی آن‌ها نیز محافظت شود. علاوه بر این، با معرفی واحد شهرت و مدیریت آن، تلاش شد تا گره‌های شبکه را به رفتار صادقانه وادار کنیم. در نهایت، با استفاده از الگوریتم‌های اثبات خدمت و اثبات شهرت در فرآیند اجماع، مدل پیشنهادی از جنبه‌های مختلف بهبود یافت.

مراجع

[1] Rahmani, Milad. "Enhancing the Security of the Ride-Sharing System Using Smart Contracts and Proof-of-Service and Reputation Consensus." M.Sc. Thesis, Isfahan University of Technology, 2023.

[2] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, S. Qibo, "An Overview of Internet of Vehicles", China Communications, Vol. 11, No. 10, pp. 1-15, 2014.
http://dx.doi.org/10.1109/CC.2014.6969789

[3] N. D. Chan, S. A. Shaheen, "Ridesharing in North America: Past, Present, and Future", Transport Reviews, Vol. 32, No. 1, pp. 93-112, 2012.
https://doi.org/10.1080/01441647.2011.621557

[4] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects", IEEE Access, Vol. 4, pp. 5356-5373, 2016.
https://doi.org/10.1109/ACCESS.2016.2603219

[5] M. Arif, G. Wanga, M. Z. A. Bhuiyan, T. Wang, J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges", Vehicular Communications, Vol. 19, 2019.
https://doi.org/10.1016/j.vehcom.2019.100179

[6] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey", IEEE Internet of Things Journal, Vol. 8, No. 6, pp. 4157-4185, 2020.
https://doi.org/10.1109/JIOT.2020.3028368

[7] S. S. Sarmah, "Understanding Blockchain Technology", Computer Science and Engineering, Vol. 8, No. 2, pp. 23-29, 2018.

[8] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles", IEEE Communications Magazine, Vol. 56, No. 10, pp. 50-57, 2018.
https://doi.org/10.1109/MCOM.2018.1800137

[9] M. Mettler, "Blockchain technology in healthcare: The revolution starts here", in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 2016.
https://doi.org/10.1109/HealthCom.2016.7749510

[10] T. Moura, A. Gomes, "Blockchain Voting and its effects on Election Transparency and Voter Confidence", in Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 2017.
https://doi.org/10.1145/3085228.3085263

[11] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay, K.-Y. Lam, "A Blockchain Framework for Insurance Processes", in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 2018.
https://doi.org/10.1109/NTMS.2018.8328731

[12] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 27, No. 12, pp. 2792 - 2801, 2019.
https://doi.org/10.1109/TVLSI.2019.2929420

[13] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal, Vol. 5, No. 2, pp. 1184 - 1195, 2018.
https://doi.org/10.1109/JIOT.2018.2812239

[14] M. M. Khan, N. T. RoJa, F. A. Almalki, M. Aljohani, "Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract", Security and Communication Networks, Vol. 2022, 2022.
https://doi.org/10.1155/2022/2213336

[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Decentralized Business Review, 2008.

[16]Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", in IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017.
https://doi.org/10.1109/BigDataCongress.2017.8

5
[17] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks", IEEE Access, Vol. 7, pp. 22328-22370, 2019.
[18] W. L , C. Feng, L. Zhang, H. Xu, B. Cao, M. A. Imran, "A Scalable Multi-Layer PBFT Consensus for Blockchain", IEEE Transactions on Parallel and Distributed Systems, Vol. 32, No. 5, pp. 1146 - 1160, 2021.
https://doi.org/10.1109/TPDS.2020.3042392
[19] Y. Zhan, B. Wang, R. Lu, Y. Yu, "DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains", Information Sciences, Vol. 559, pp. 8-21, 2021.
https://doi.org/10.1016/j.ins.2020.12.077
[20] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, "An overview on smart contracts: Challenges, advances and platforms", Future Generation Computer Systems, Vol. 105, pp. 475-491, 2020.
https://doi.org/10.1016/j.future.2019.12.019
[21] M. Li, L. Zhu, X. Lin, "Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing", IEEE Internet of Things Journal, Vol. 6, No. 3, pp. 4573-4584, 2018.
https://doi.org/10.1109/JIOT.2018.2868076
[22] R. R. Clewlow, G. S. Mishra, "Disruptive Transportation: The Adoption, Utilization, and Impacts of Ride-Hailing in the United States", 2017.
[23] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, A. Zomaya, "Towards secure and practical consensus for blockchain based VANET", Information Sciences, pp. 170-187, 2021.
https://doi.org/10.1016/j.ins.2020.07.060
[24] P. Pal, S. Ruj, "BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service", in 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019.
https://doi.org/10.1109/Blockchain.2019.00070
[25] M. Li, L. Zhu, X. Lin, "CoRide: A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing", in Security and Privacy in Communication Networks, Orlando, 2019.
https://doi.org/10.1007/978-3-030-37231-6_24
[26] R. Shivers, M. A. Rahman, H. Shahriar, "Toward a secure and decentralized blockchain-based ride-hailing platform for autonomous vehicles", in 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021.
https://doi.org/10.48550/arXiv.1910.00715
[27] M. S. Hossan, M. L. Khatun, S. Rahman, S. Reno, M. Ahmed, "Securing Ride-Sharing Service Using IPFS and Hyperledger Based on Private Blockchain", in 2021 24th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2021.
https://doi.org/10.1109/ICCIT54785.2021.9689814
[28] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, M. Abdallah, "B-Ride: Ride Sharing With Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain", IEEE Transactions on Network Science and Engineering, Vol. 8, No. 2, pp. 1214 - 1229, 2019.
https://doi.org/10.1109/TNSE.2019.2959230
[29] D. Sánchez, S. Martínez, J. Domingo-Ferrer, "Co-utile P2P ridesharing via decentralization and reputation management", Transportation Research Part C: Emerging Technologies, Vol. 73, pp. 147-166, 2016.
https://doi.org/10.1016/j.trc.2016.10.017

[1] Internet of Vehicles
[2] Road Side Unit
[3] Ride-Sharing
[4] Central Management Unit
[5] Blockchain
[6] Vehicular Ad-Hoc NETwork
[7] Timestamp
[8] Proof-Of-Work
[9] Proof-Of-Stake
[10] Practical Byzantine Fault Tolerance

[11] Peer-to-Peer
[12] Uber
[13] Lyft
[14] Ride-Sharing Service
[15] Proof of Driving
[16] Autonomous Vehicles
[17] Registration Authority
[18] Winning Group Selection Unit
[19] Repute
[20] Smart Contract
[21] Denial-Of-Service
[22] Proof-of-Service-and-Reputation
[23] Average Service