دانشگاه آزاد اسلامی

واحد اسلامشهر

دانشکده فنی و مهندسی، گروه کامپیوتر

پایان‌نامه برای دریافت درجهٔ کارشناسی ارشد « M.Sc. »

گرایش: نرم افزار

عنوان:

ارائه یک شبکه مبتنی بر بلاکچین برای کاهش هزینه سفر در سرویس اشتراک گذاری سفر

استاد راهنما:

دکتر محمد حسین شفیع آبادی

استاد مشاور:

دکتر فاطمه صف آرا

نگارش:

مهران مظهر

زمستان ۱۴۰۱

بسم الله الرحمن الرحيم

منشور اخلاقی پژوهش

با یاری از خداوند سبحان و اعتقاد به این که عالم محضر خداست و همواره ناظر بر اعمال انسان و به منظور پاس داشت مقام بلند دانش و پژوهش و نظر به اهمیت جایگاه دانشگاه در اعتلای فرهنگ و تمدن بشری، ما دانشجویان و اعضا هیأت علمی واحدهای دانشگاه آزاد اسلامی متعهد می گردیم اصول زیر را در انجام فعالیت های پژوهشی مد نظر قرار داده و از آن تخطی نکنیم:

۱. اصل حقیقت جویی: تلاش در راستای پی جویی حقیقت و وفاداری به آن و دوری از هرگونه پنهان سازی حقیقت.
۲. اصل رعایت حقوق: التزام به رعایت کامل حقوق پژوهشگران و پژوهیدگان (انسان، حیوان و نبات) و سایر صاحبان حق.
۳. اصل مالکیت مادی و معنوی: تعهد به رعایت کامل حقوق مادی و معنوی دانشگاه و کلیه همکاران پژوهش.
٤. اصل منافع ملی: تعهد به رعایت مصالح ملی و در نظر داشتن پیشبرد و توسعه کشور در کلیه مراحل پژوهش.
٥. اصل رعایت انصاف و امانت: تعهد به اجتناب از هرگونه جانب داری غیرعلمی و حفاظت از اموال، تجهیزات و منابع در اختیار.
٦. اصل رازداری: تعهد به صیانت از اسرار و اطلاعات محرمانه افراد، سازمان‌ها و کشور و کلیه افراد و نهادهای مرتبط با تحقیق.
۷. اصل احترام: تعهد به رعایت حریم ها و حرمت ها در انجام تحقیقات و رعایت جانب نقد و خودداری از هرگونه حرمت شکنی.
۸. اصل ترویج:تعهد به رواج دانش و اشاعه نتایج تحقیقات و انتقال آن به همکاران علمی و دانشجویان به غیر از مواردی که منع قانونی دارد.
۹. اصل برائت: التزام به برائت جویی از هرگونه رفتار غیر حرفه ای و اعلام موضع نسبت به کسانی که حوزه علم و پژوهش را به شائبه های غیرعلمی می آلایند.

تعهدنامه اصالت پایان‌نامه / رساله دانشجویان تحصیلات تکمیلی (ارشد و دکتری)

دانشگاه آزاد اسلامی واحد اسلامشهر

اینجانب مهران مظهر دانش‌آموخته مقطع کارشناسی ارشد ☑ / دکتری □ در رشته مهندسی کامپیوتر گرایش نرم افزار که در تاریخ از پایان‌نامه / رساله خود تحت عنوان ارائه یک شبکه مبتنی بر بلاکچین برای کاهش هزینه سفر در سرویس اشتراک گذاری سفر با کسب نمره و درجه دفاع نموده‌ام. بدین وسیله متعهد می‌شوم:

۱) این پایان‌نامه / رساله حاصل تحقیق و پژوهش انجام شده توسط اینجانب بوده و در مواردی که از دستاوردهای علمی و پژوهشی دیگران (اعم از پایان‌نامه، کتاب، مقاله و ...) استفاده نموده‌ام، مطابق ضوابط و رویه موجود، نام منبع مورد استفاده و سایر مشخصات آن را در فهرست مربوطه ذکر و درج کرده‌ام.

۲) این پایان‌نامه / رساله قبلاً برای دریافت هیچ مدرک تحصیلی (هم‌سطح، پایین‌تر یا بالاتر) در سایر دانشگاه‌ها و مؤسسات آموزش‌عالی ارائه نشده است.

۳) چنانچه بعد از فراغت از تحصیل، قصد استفاده و هرگونه بهره‌برداری اعم از چاپ کتاب، ثبت اختراع و ... از این پایان‌نامه داشته باشم، از حوزه معاونت پژوهشی واحد مجوزهای مربوطه را اخذ نمایم.

٤) چنانچه در هر مقطع زمانی خلاف موارد فوق ثابت شود، عواقب ناشی از آن را می‌پذیرم و واحد دانشگاهی مجاز است با اینجانب مطابق ضوابط و مقررات رفتار نموده و در صورت ابطال مدرک تحصیلی‌ام هیچ گونه ادعایی نخواهم داشت.

نام و نام خانوادگی

تاریخ و امضا

اسلامی آزاد دانشگاه

واحد اسلامشهر

دانشکده فنی و مهندسی، گروه کامپیوتر

پایان‌نامه برای دریافت درجهٔ کارشناسی ارشد « M.Sc. »

گرایش: نرم افزار

عنوان:

ارائه یک شبکه مبتنی بر بلاکچین برای کاهش هزینه سفر در سرویس اشتراک گذاری سفر

استاد راهنما:

دکتر محمد حسین شفیع آبادی

استاد مشاور:

دکتر فاطمه صف آرا

نگارش:

مهران مظهر

زمستان ۱۴۰۱

سپاسگزاری

سپاس خدای را عز وجل
که طاعتش موجب قربت است
و به شکر اندرش مزید نعمت

لازم می‌دانم، مراتب تشکر و قدردانی خود را از استاد راهنمای بسیار عزیزم ، دکتر محمد حسین شفیع آبادی، ابراز دارم. بدون شک اگر راهنمایی‌ها، نقد سازنده و بخصوص دلسوزی ایشان در طول این تحقیق کنارم نبود، انجام آن میسر نمی‌افتاد. در پایان از تمامی‌کسانی که مرا در اجرای این پایان نامه یاری کردند، بی نهایت سپاسگزاری می‌نمایم.

تقدیم و تشکر

به پاس محبت بی دریغی که فروکش نمی‌کند و انسانیتی که در نبرد روزگار از پای در نمی‌آید و به پاس عاطفه ی سرشار و قلب بزرگی که فریادرسمان همواره بوده است ، این پایان نامه را به پدر، مادر فداکارم تقدیم می‌کنم.

فهرست مطالب

عنوان **صفحه**

چکیده **۱**

فصل ۱ کلیات تحقیق **۲**

۱-۱ مقدمه ۲

۱-۲ بیان مسئله تحقیق ۲

۱-۳ اهمیت و ضرورت تحقیق ۳

۱-٤ اهداف ٤

۱-۵ فرضیه ها ٤

۱-٦ ساختار پایان نامه ۵

فصل ۲ مروری بر ادبیات تحقیق و پیشینه پژوهش **٦**

۲-۱ مقدمه ٦

۲-۲ انواع سیستم های متمرکز، غیرمتمرکز و توزیع شده ٦

۲-۳ انواع پایگاه داده متمرکز، غیر متمرکز و توزیع شده ۷

۲-٤ دفتر کل توزیع شده ۸

۲-۵ بلاکچین ۹

۲-۵-۱ تاریخچه پیدایش بلاکچین ۹

۲-۵-۲ ویژگی های اصلی بلاکچین و دستاورد های آن ۱۰

۲-۵-۳ طبقه بندی شبکه های بلاکچین ۱۱

۲-۵-٤ معماری بلاکچین ۱۳

۲-۵-۵ بلوک ۱٤

۲-۵-٦ تراکنش ۱۵

۲-۵-۷ مکانیزم اجماع در شبکه بلاکچین ۱٦

۲-۵-۷-۱ اثبات کار ۱۷

۲-۵-۷-۲ اثبات سهام ۱۸

۲-۵-۸ برنامه های توزیع شده ۱۹

۲-٦ رمزنگاری ۱۹

۲-٦-۱ امضای دیجیتال ۲۱
۲-٦-۱-۱ ساخت امضای دیجیتال ۲۱
۲-٦-۱-۲ تایید امضای دیجیتال ۲۲
۲-٦-۲ توابع هش (درهم ساز) ۲۲
۲-۷ اشتراک گذاری سفر ۲۲
۲-۸ پیشینه تحقیق ۲۳
۲-۹ خلاصه فصل ۲۵
فصل ۳ روش اجرای تحقیق ۲٦
۳-۱ مقدمه ۲٦
۳-۲ تشریح روش پیشنهادی ۲٦
۳-۲-۱ ثبت نام راننده / مسافر ۲۸
۳-۲-۲ تایید هویت ۲۹
۳-۲-۲-۱ تولید پارامتر های اشتراکی برای امضای دیجیتال ۲۹
۳-۲-۲-۲ ساخت امضای دیجیتال ۳۰
۳-۲-۲-۳ الگوریتم بررسی معتبر بودن امضای دیجیتال ۳۰
۳-۳ درخواست سفر توسط مسافر ۳۱
۳-٤ ثبت درخواست پیشنهاد انجام سفر توسط راننده ۳۲
۳-۵ تایید کردن یکی از پیشنهاد ها توسط مسافر ۳۳
۳-٦ مکانیزم پاداش/جریمه برای اثبات رسیدن به مبدا ۳٤
۳-٦-۱ معایب رویکرد ارائه شده در پژوهشB-Ride ۳٦
۳-٦-۲ تشریح مراحل پیشنهادی جهت از بین بردن وابستگی به اثبات کننده ی مکان ۳٦
۳-٦-۲-۱ ارسال اثبات رسیدن به مبدا توسط مسافر یا راننده ۳۸
۳-٦-۲-۲ ثبت شکایت توسط مسافر یا راننده ۳۹
۳-۷ پرداخت کرایه توسط مسافر در حین سفر ٤۰
۳-۸ خلاصه فصل ٤۱
فصل ٤ تجزیه و تحلیل یافته ها ٤۲
٤-۱ مقدمه ٤۲
٤-۲ ابزار شبیه سازی ٤۲

٤-٣ مشخصات سیستم پیاده سازی ٤٣
٤-٤ مجموعه داده ها ٤٤
٤-٥ معیار های ارزیابی ٤٥
٤-٥-١ معیار هزینه تراکنش و هزینه اجرا..... ٤٥
٤-٥-٢ معیار تعداد تراکنش در ثانیه (TPS)..... ٤٦
٤-٥-٣ معیار وابستگی به اثبات کننده مکان ٤٧
٤-٥-٤ معیار شفافیت ٤٧
٤-٥-٥ معیار غیرمتمرکز سازی..... ٤٧
٤-٥-٦ پرداخت منصفانه ٤٧
٤-٦ ارزیابی نتایج پیشنهادی ٤٨
٤-٦-١ مقایسه هزینه تراکنش و اجرا..... ٤٨
٤-٦-٢ هزینه وابستگی به به اثبات کننده مکان ٥٠
٤-٧ جمع بندی..... ٥٠
فصل ٥ نتیجه گیری و پیشنهادات..... ٥١
٥-١ مقدمه..... ٥١
٥-٢ مروری بر یافته های تحقیق ٥١
٥-٣ نتیجه گیری ٥٢
٥-٤ پیشنهادات آینده ٥٣
فهرست منابع فارسی ٥٤
فهرست منابع غیر فارسی..... ٥٥
Abstract **..... ٥٨**

فهرست جدول ها

عنوان **صفحه**

جدول ۲-۱ مقایسه ای از شبکه های بلاکچین عمومی، کنسرسیوم و خصوصی ۱۲
جدول ۲-۲ تفاوت های بین برنامه های کاربردی وب متمرکزو برنامه های توزیع شده بلاکچین..... ۱۹
جدول ۲-۳ مقایسه از پیشینه های تحقیق در زمینه ارائه سرویس اشتراک گذاری مبتنی بر بلاکچین ۲۵
جدول ٤-۱ : مشخصات سیستم جهت شبیه سازی و ارزیابی نتایج ٤۳
جدول ٤-۲ : ویژگی های مجموعه داده ها در سرویس اشتراک گذاری سفر ٤٤
جدول٤-۳: مقایسه ای از هزینه های صرف شده در سرویس های اشتراک گذاری سفر.....٤۸
جدول ٤-٤: مقایسه ای از مکانیزم های ارائه شده MATCHMAKING سرویس های اشتراک گذاری سفر ۵۰

فهرست شکل ها

عنوان **صفحه**

شکل۲-۱ انواع شکبه های متمرکز، غیرمتمرکز و توزیع شده ۷
شکل ۲-۲ سه پیاده سازی مختلف از فناوری دفتر کل توزیع شده..... ۸
شکل ۲-۳ ایده های مختلفی که به اختراع بیت کوین و بلاک چین کمک کردند ۱۰
شکل۲-٤ نمونه از قرارگیری بلوک های یک شبکه بلاکچین..... ۱۳
شکل۲-۵ مثالی از یک بلوک در شبکه بلاکچین ۱۵
شکل۲-٦ مثالی از تراکنش ها در شبکه بلاکچین..... ۱٦
شکل ۲-۷ انواع رمزنگاری بر اساس الگوریتم..... ۲۰
شکل ۲-۸ ساخت یک امضای دیجیتال..... ۲۱
شکل۲-۹ تایید یک امضای دیجیتال..... ۲۲
شکل ۳-۱ : فلوچارت سرویس اشتراک گذاری سفر مبتنی بر بلاکچین..... ۲۷
شکل ۳-۲: فلوچارت پاداش/ جریمه برای اثبات رسیدن به مبدا ۳۷
شکل ٤-۱: نمودار هزینه صرف شده برای راننده در تعداد سفر..... ٤۹

فهرست الگوریتم ها

عنوان **صفحه**

الگوریتم ۳-۱: الگوریتم ثبت نام راننده/ مسافر ۲۸
الگوریتم ۳-۲: الگوریتم تولید پارامتر های اشتراکی برای امضای دیجیتال ۲۹
الگوریتم ۳-۳: الگوریتم امضای ساخت امضای دیجیتال ۳۰
الگوریتم ۳-٤: الگوریتم بررسی معتبر بودن امضای دیجیتال..... ۳۱
الگوریتم ۳-۵: الگوریتم درخواست سفر توسط مسافر ۳۱
الگوریتم ۳-٦: الگوریتم ثبت درخواست پیشنهاد انجام سفر توسط راننده ۳۲
الگوریتم ۳-۷: الگوریتم تایید پیشنهاد توسط مسافر..... ۳۳
الگوریتم ۳-۸ الگوریتم ارسال اثبات رسیدن به مبدا..... ۳۸
الگوریتم ۳-۹: الگوریتم ثبت شکایت ۳۹
الگوریتم ۳-۱۰: الگوریتم پرداخت کرایه توسط مسافر در حین سفر ٤۰

چکیده

سرویس اشتراک گذاری سفر امکانی است رانندگان وسایل نقلیه و مسافرانی که مایل به انجام سفر هستند از طریق یک شبکه دستگاه های تلفن همراه به هم متصل میکند. امروزه سرویس های اشتراک گذاری سفر به دلیل مزایایی که نسبت به مدل های سنتی دارند از جمله کاهش هزینه های سفر، کاهش اتلاف زمان و همچنین کاهش ترافیک و آلودگی های زیست محیطی، انقلابی در صنعت حمل و نقل ایجاد کرده اند. اگرچه این مزایا باعث ایجاد بهبود هایی در صنعت حمل نقل شده است ولی ارائه دهندگان این سرویس ها با مرکزیت و انحصاری که ایجاد کرده اند باعث ایجاد مشکلاتی از جمله، عدم شفافیت، نقص حریم خصوصی وسو استفاده از داده های کاربران و همچنین به دلیل وجود یک مرکزیت واحد امکان از کار افتادن و آلودگی این سیستم ها وجود دارد.همچنین به دلیل هزینه های بالا نگه داری این شرکت ها و کارمزد هایی که از سفر ها برداشت می کنند هزینه های سفر در این روش به طرز چشمگیری افزایش یافته است.

در این پایان نامه با استفاده از مزایایی که شبکه های مبتنی بر بلاکچین دارند سرویسی مبتنی بر بلاکچین ارائه شده است که بدون وجود مرکزیت و یک سازمان واحد قادر خواهد بود رانندگان و مسافران را به هم متصل کند. در روش ارائه شده با کمک گیری از مزایایی که شبکه های بلاکچین ایجاد کرده اند سرویسی ارائه شده است که سعی در حفظ حریم خصوصی افراد و در عین حال کاهش هزینه های مربوطه برای مسافران و رانندگان شده است.

کلید واژه ها: سرویس اشتراک گذاری سفر – هزینه سفر- بلاکچین- شبکه های مبتنی بر بلاکچین

فصل ۱ کلیات تحقیق

۱-۱ مقدمه

در این فصل ابتدا به بررسی مسئله اصلی تحقیق فعلی پرداخته و پس از اهمیت تحقیق، اهداف اصلی تحقیق و فرضیه ها را بیان خواهیم نمود. در انتها نیز ساختار اصلی پایان نامه ذکر می‌گردد.

۱-۲ بیان مسئله تحقیق

سرویس اشتراک گذاری سفر سرویسی است که مسافران و رانندگان (سفیران) می توانند با کمک وب سایت ها و برنامه های تلفن های همراه به هم متصل شوند و سفر های درون شهری یا بین شهری خود را انجام دهند. از جمله مزایایی که این سرویس ها نسبت به مدل های سنتی دارند می توان به کاهش کرایه ها، کاهش اتلاف زمان سفر، کاهش ترافیک شهری بخصوص در شهرهای بزرگ و پرجمعیت که در آن افراد زمان زیادی صرف رفت و آمد میکنند اشاره کرد. همچنین سیستم‌های اشتراک‌گذاری سفر می‌توانند با کاهش مسافتی که وسایل نقلیه نیمه خالی رانده می‌شوند، به رفع ازدحام ترافیک کمک کنند که همین عامل باعث کاهش آلودگی هوا و نیز مصرف سوخت خواهد شد (Schrank et al., 2015). امروزه استفاده از سرویس های اشتراک گذاری سفر در بسیاری از کشور ها رواج یافته است. در این زمینه شرکت های بسیاری از جمله اسنپ و تپسی در ایران و اوبر و لیفت در سطح بین المللی فعالیت میکنند. طبق پیشبینی ها تا سال ۲۰۳۰ درآمد شرکت ها در این بازار به ارزش تقریبی ۲۸۵ میلیارد دلار خواهد رسید(Shivers et al., 2021). همچنین در ایران طبق آخرین آمار موجود از شرکت اسنپ در سال ۱۳۹۹ بیش از ٤ میلیارد کیلومتر سفر فقط با استفاده از سرویس این شرکت انجام شده است (snap, 2021).

علارغم بهبود ها و میزیت هایی که با ارائه سرویس اشتراک سفر توسط این شرکت ها فراهم شده است این سرویس ها دارای مشکلات و چالش های زیر میباشند:

- ✓ قیمت گذاری:

شرکت های ارائه دهنده سرویس اشتراک سفر به مسافران امکانی را می دهند که هزینه کرایه و خدمات مورد نظر خود را پرداخت کنند. همین امر موجب ایجاد وابستگی بین این شرکت ها و مسافران و

رانندگان می شود. حدودا ۱۰ الی ۲۰ درصد از کل هزینه سفر را به عنوان کارمزد به این شرکت ها تعلق میگیرد(Huckle et al., 2016).

- ✓ عدم شفافیت:

مرکزیت این خدمات توسط شرکت های ارائه دهنده سرویس اشتراک گذاری سفر باعث می شود که این شرکت ها بتوانند قیمت گذاری هر سفر را بر اساس نرخ های ناعادلانه تعیین کنند و گاها موجب اعتراض راننده ها و مسافران شوند.

- ✓ امنیت:

قرارگیری تمام اطلاعات سفر ها در سرور های مرکزی یک شرکت این خطر را پی دارد که با هر نقص امنیتی این سرور ها ممکن است مورد هجوم هکر ها قرار بگیرند. همچنین این امکان وجود دارد که با هر مشکل نرم افزار یا سخت افزاری سیستم به طور کامل از دسترس خارج شود. به عنوان مثال شرکت اوبر شاهد نشت اطلاعاتی ۵۷ میلیون راننده و مسافر خود بوده است. همچنین در اوریل ۲۰۱۵، به دلیل نقص سخت افزاری سرویس اوبر به طور کامل قطع شد و مسافران و رانندگان دچار مشکلاتی شدند(Baza et al., 2019).

- ✓ حریم خصوصی افراد:

قرار گرفتن این اطلاعات در پایگاه های داده این شرکت ها امکان سو استفاده کردن از این داده ها و نقص حریم خصوصی افراد خواهد شد. در سرویس های اشتراک گذاری سفر حریم خصوصی یعنی تمامی اطلاعات مبدا و مقصد هر سفر در هنگام استفاده از این سرویس ها می باشد. بدیهی است این سو استفاده از این اطلاعات حریم خصوصی افراد را نقص خواهد کرد.

هدف از این تحقیق ارائه یک شبکه مبتنی بر بلاکچین برای به روشی که بدون بدون وجود مرکزیت یک سازمان مسافران و رانندگان به هم متصل کند. با استفاده از فناوری بلاکچین این سیستم قادر خواهد بود توسط جامعه غیر متمرکزی از کاربران اداره شود بنابراین قیمت گذاری بر مبنای عرضه و تقاضا کاربران خواهد بود. همچنین رانندگان امکان تعیین قیمت را خواهند داشت که باعث شفافیت در قیمت گذاری خواهد شد. با توجه به این که نود های این شبکه مبتنی بر بلاکچین قابلیت اجرا در چندین سرور را خواهند داشت خطر از کار افتادن سیستم کاهش چشمگیری خواهد داشت. در این شبکه با استفاده از امکانات رمزگزاری برچسب اسم افراد از اطلاعاتی مثل مبدا و مقصد حریم خصوصی افراد را بهتر مدیریت کنیم(Nakamoto, 2008) .

۱-۳ اهمیت و ضرورت تحقیق

مباحث مربوط به اشتراک گذاری سفر امروزه مورد توجه محققین و پژوهشگران مختلف قرار گرفته است.سرویس اشتراک گذاری سفر مورد کاربرد برای رانندگان تاکسی، افرادی که نیاز به خدمات حمل

نقل درون شهری و برون شهری دارند و افرادی که می توانند از طریق اشتراک گذاری سفر در مسیری که هر روزه رفت و آمد میکنند درآمدزایی داشته باشند. با توجه به رشد روز افزون استفاده از سرویس های اشتراکی سفر نیاز به ارائه روشی برای سرویسی است که مشکلات مربوط به انحصار و قابل کنترل بودن این سرویس ها فقط توسط شرکت های ارائه دهنده را برطرف کند (Zhang et al., 2019).

یکی از آیتم ها و متغیرهای مهم پیرامون شبکه های مبتنی بر بلاکچین سرعت شبکه می باشد. سرعت شبکه بیانگر میزان تعداد تراکنش هایی که یک شبکه مبتنی بر بلاکچین در زمان مشخصی قادر به ثبت می باشد(Du et al., 2017). همچنین از دیگر آیتم ها و متغیر های مهم پیرامون شبکه های مبتنی بر بلاکچین هزینه ثبت تراکنش ها در شبکه می باشد. یکی از چالش ها و مشکلات اصلی بررسی شده در این پژوهش هزینه تراکنش ها می باشد. در سرویس های اشتراک گذاری سفر هزینه استفاده از این شبکه برای سرویس اشتراک گذاری سفر بالا می باشد و همین امر موجب افزایش هزینه سفر خواهد شد. یکی دیگر چالش ها و مشکلات اصلی بررسی شده در این پژوهش ارائه شبکه ای است که سرعت آن برای اجرای سرویس اشتراک گذاری سفر در بهینه شده است.

بلاک چین های قدیمی با هدف خاصی از برنامه ها طراحی نشده اند. در نتیجه این بلاکچین ها توسعه دهنده را مجبور می کند که در چارچوب قوانین کلی که ایجاد شده است کار کنند . در مورد سرویس اشتراک گذاری سفر محدودیت هزینه تراکنش و سرعت تراکنش و همچنین قابلیت بروز رسانی برای ارائه این سرویس وجود دارد. بنابراین بررسی و بهبود هزینه ها سرویس اشتراک گذاری سفر از اهمیت و ضرورت بالایی برخوردار می باشد.

با توجه به اهمیت و ضرورت ارائه یک راه حل مفید و مطلوب در جهت ارائه یک سرویس اشتراک گذاری سفر مبتنی بر بلاکچین اقدام به بهبود سرعت و هزینه تراکنش ها در شبکه مبتنی بر بلاکچین می نماید.

۱-٤ اهداف

برخی از مهمترین اهداف اصلی در این پژوهش عبارتند از:

۱- یک شبکه مبتنی بر بلاکچین برای کاهش هزینه سفر در سرویس اشتراک گذاری سفر

۲- کاهش هزینه های تراکنش ها در شبکه های بلاکچین برای سرویس اشتراک گذاری سفر

۳- افزایش سرعت تراکنش های اجرایی بر روی شبکه بلاکچین برای استفاده در سرویس اشتراک گذاری سفر

۱-۵ فرضیه ها

برخی از مهمترین سوالات و فرضیات مطرح در این پژوهش عبارتند از:

برخی از مهمترین فرضیات این تحقیق عبارتند از:

۱. با یک شبکه مبتنی بر بلاکچین می توان هزینه سفر در سرویس اشتراک گذاری سفر را کاهش داد.
۲. هزینه های تراکنش ها در شبکه های بلاکچین برای سرویس اشتراک گذاری سفر را می توان کاهش داد.
۳. سرعت تراکنش های اجرایی بر روی شبکه بلاکچین برای استفاده در سرویس اشتراک گذاری سفر را می توان افزایش داد.

۱-٦ ساختار پایان نامه

در ادامه فصل‌ها به بحث و پژوهش در رابطه با موارد ذیل خواهیم پرداخت :

- ✓ در فصل دوم برخی از مهمترین پژوهش‌های انجام شده در زمینه‌های مرتبط به موضوع تحقیق مورد بررسی قرار می‌گیرد. همچنین در این فصل به معرفی مروری کلی بر نظریه و مفاهیم اولیه تحقیق، جزئیات مربوط به الگوریتم‌ها، متغیرها و مجهولات پژوهش و سایر موارد لازم جهت آگاهی بیشتر پرداخته خواهد شد.
- ✓ در فصل سوم تشریح کامل روش پیشنهادی با ارائه جزئیات بیشتر هر قسمت همراه با تشریح کامل فلوچارت روش مطرح شده و همچنین الگوریتم پیشنهادی نیز توصیف می‌گردد. بطور کلی در این فصل ابتدا فلوچارت و معماری طرح پیشنهادی مورد بررسی قرار گرفته و مطابق با این طرح مراحل اجرا و شبیه سازی روش مطرح شده تشریح می‌گردد و در انتهای فصل الگوریتم پیشنهادی مطرح می‌گردد.
- ✓ فصل چهارم مبنع داده استفاده شده به صورت کامل شرح داده شده، مراحل شبیه سازی روش پیشنهادی با نرم افزار مربوطه در فصل چهارم به صورت کامل مورد بررسی قرار گرفته و در نهایت مقایسه و ارزیابی با سایر روشها مورد تشریح می‌گردد. همچنین ابزار شبیه سازی، پارامترها شبیه ساز ، نتیجه شبیه سازی ، توضیح نمودارها و مقایسه ذکر خواهد شد.
- ✓ در فصل پنجم نیز یافته‌های تحقیق، نتیجه گیری نهایی و پیشنهادات آتی مطابق با فرضیات ارائه شده در پژوهش و اهداف محقق مورد بررسی قرار خواهد گرفت.

فصل ۲ مروری بر ادبیات تحقیق و پیشینه پژوهش

۲-۱ مقدمه

در این فصل برخی از مهمترین پژوهش‌های انجام شده در زمینه‌های مرتبط به شبکه های مبتنی بر بلاکچین و سرویس های اشتراک گذاری سفر مورد بررسی قرار می‌گیرد. همچنین در این فصل به معرفی مروری کلی بر ادبیات تحقیق، جزئیات مربوط به پیاده سازی ها، متغیرها و مجهولات پژوهش و سایر موارد لازم جهت آگاهی بیشتر پرداخته خواهد شد.

۲-۲ انواع سیستم های متمرکز، غیرمتمرکز و توزیع شده

زمانی که بحث از بلاکچین می شود همیشه اصطلاحات سیستم های توزیع شده و غیر متمرکز همراه آن می آید ولی اغلب این تفاوت ها آشکار نیست و باعث سردرگرمی می شود. می توان این سیستم ها از دو منظر سطوح کنترل و محل قرارگیری مورد بررسی قرار داد.

در ابتدا به تفاوت بین سیستم های متمرکز و غیرمتمرکز خواهیم پرداخت. به طور کلی سیستم های متمرکز و سیستم های غیر متمرکز به سطوح کنترل اشاره دارند. در سیستم های متمرکز تصمیم گیری و کنترل یک سیستم توسط یک موجودیت (به عنوان مثال یک شخص، ارگان) گرفته می شود. در سیستم های غیرمتمرکز یک موجودیت واحد برای اعمال کنترل وجود ندارد و در عوض کنترل بین چندین موجودیت مستقل به اشتراک گذاشته شده است.

سیستم های توزیع شده به محل قرارگیری سیستم اشاره دارد (Poenitzsch J, 2018).سیستم های توزیع شده یک سیستمی است که در دو یا چند گره با هم در یک مدل هماهنگ شده همکاری می کنند . این همکاری منجر به یک نتیجه مشترک می شود که در نهایت باعث می شود کاربران نهایی آن را به عنوان یک سیستم واحد ببینید.

یک گره را می توان یک موجودیت مستقل در سیستم توزیع شده می باشدکه منابع سخت افزاری و نرم افزاری خود را دارد. همه گره ها قادر به ارتباط با یکدیگر و ارسال و دریافت پیغام از هم می باشند. همچنین در سیستم های توزیع شده هر گره ممکن است عملکرد مخربی داشته باشد که برای عملکرد شبکه مخرب باشد. در نتیجه چالش اصلی در سیستم های توزیع شده هماهنگی بین گره ها و همچنین

تحمل خطا است به طوری که اگر گره یا گره هایی رفتار مخربی داشته باشند سیستم باید بدون نقص به کار خود ادامه دهد (Bashir, 2017).

درک سیستم های توزیع شده کمک بسیاری به درک بلاکچین خواهد کرد به این دلیل که بلاکچین ها به شکل زیر ساختی می توانند به عنوان نوعی از سیستم های توزیع شده باشند.

شکل۲-۱ انواع شکبه های متمرکز، غیرمتمرکز و توزیع شده

۲-۳ انواع پایگاه داده متمرکز، غیر متمرکز و توزیع شده

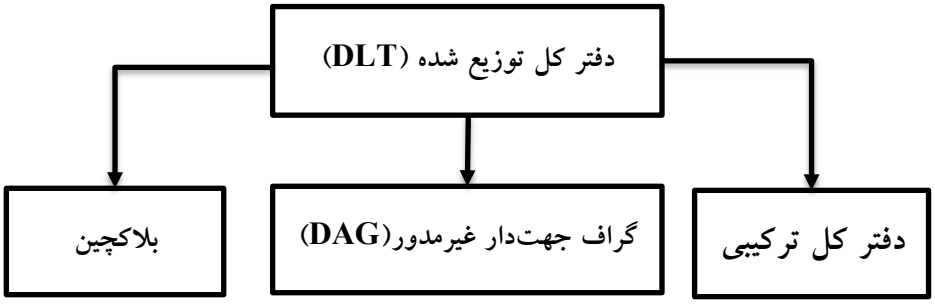
ذخیره سازی و مدیریت اطلاعات بخش جدایی ناپذیری از بسیاری از نرم افزار ها می باشد.به همین دلیل پایگاه داده ها از اهمیت فراوانی برخوردار می باشند. عمدتا اطلاعات در پایگاه داده رابطه ای با جداول و وابستگی ها ذخیره می شوند. سازماندهی اطلاعات در پایگاه داده ها با چهار عملیات خواندن، نوشتن، به روز رسانی و حذف انجام می شود که به اختصار CRUID گفته می شود.

برای سازماندهی اطلاعات می توان از سه نوع پایگاه داده استفاده کرد: پایگاه داده متمرکز، غیر متمرکز و توزیع شده. در پایگاه داده های متمرکز تمام اطلاعات در یک محل ذخیره سازی نگه داری می شود که همین امر موجب اشکلاتی از جمله از دسترس خارج شدن و کارایی می شود. در پایگاه داده های غیرمتمرکز یک دستگاه ذخیره سازی واحد وجود ندارد بلکه مجموعه ای از دستگاه های ذخیره سازی وجود دارند که اطلاعات در یک ساختار سلسله مراتبی در آن ها سازماندهی می شوند.پایگاه داده های توزیع شده برای افزایش دسترسی و حل مشکلات کارایی پیاده سازی شده اند. در پایگاه داده های توزیع شده تکرار داده ها در دستگاه های مختلف ذخیره می شوند که همین امر باعث می شود اگر یکی از دستگاه های ذخیره سازی از کار بیوفتد یا برای مدتی نمی توان دسترسی به پایگاه داده داشت. دیگر

دستگاه های ذخیره سازی به کار خود ادامه می دهند. در این نوع از پایگاه داده ها معمولا از یک ساختار سلسله مراتبی پیروی نمی کنند بلکه مجموعه ای از دستگاه های متصل به هم را تشکیل می دهند.
پایگاه داده توزیع شده نوعی از پایگاه داده می باشد که درآن داده ها در چندین دستگاه ذخیره سازی (گره) با حقوق برابر تکرار می شوند (Sunyaev, 2020).

۲-٤ دفتر کل توزیع شده[1]

دفترکل توزیع شده یک نوع خاصی از پایگاه داده توزیع شده می باشد. اساسا فناوری دفتر کل توزیع شده پایگاه داده ای است که بر روی چندین دستگاه فیزیکی که معمولا در مکان های مختلفی قرار دارند می باشد. هر یک از این دستگاه ها معمولا به عنوان گره شناخته می شوند (Liu et al., 2020).
دفتر کل فقط اجازه اضافه کردن داده را می دهد در نتیجه حذف و به روز رسانی داده های اضافه شده غیر ممکن خواهد بود. در یک دفتر کل توزیع شده گره هایی با اهداف مخرب در نظر گرفته می شود و طراحی این نوع سیستم ها به این بستگی دارد که چطور در برابر این رفتار ها مقاومت کرده و از بروز اشکال در سیستم جلوگیری کند. در نتیجه در این فناوری این امکان را به گره های خوش خیم می دهد که از طریق یک مکانیسم اجماع مشترک، بر روی یک وضعیت تغییر ناپذیر به توافق برسند.
فناوری های دفتر کل توزیع شده را می توان براساس شیوه اجرا به به سه دسته مختلف تقسیم بندی کرد.(شکل ۲-۲)



شکل ۲-۲ سه پیاده سازی مختلف از فناوری دفتر کل توزیع شده

بنابراین هدف یک سیستمDLT تولید مجموعه ای از سوابق معتبری که از طریق یک فرایند اجماع بین گره ها تایید و اجرا می شوند.تمام این فرایند از در غیاب یک مرجع مرکزی انجام می شود. کاربران و استفاده کنندگان از این سیستم تراکنش هایی را ایجاد و پخش می کنند. این تراکنش ها توسط تولید

[1] Distributed Ledger Technology

کنندگان رکورد ها جمع آوری می شود و با توجه به دستور العمل هایی موجود در معاملات که اکنون تایید شده انده به طور خودکار توسط همه گره ها اجرا می شوند (Rauchs et al., 2018).

۲-۵ بلاکچین

در این قسمت به تشریح اصول بلاکچین و زیر ساخت های زیر اصلی آن ها خواهیم پرداخت. مباحث مطرح شده در این بخش مبانی اصول اولیه برای رویکرد ارائه شده در فصول بعدی خواهد بود.

۲-۵-۱ تاریخچه پیدایش بلاکچین

بسیاری از افراد فکر می کنند ایده بلاکچین توسط بیت کوین ارائه شده است در صورتی که اینطور نبوده است. ایده اصلی بلاکچین در اواخر دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ ظهور کرد.در سال ۱۹۸۹ لزلی لمپورت پرتکل پاکسوس را توسعه داد و در سال ۱۹۹۰ مقاله خود را با عنوان پارلمان پاره وقت ارسال کرد .بلاخره مقاله در شماره ۱۹۹۸ به چاپ رسید(Lamport, 1998).در این مقاله یک مدل اجماع برای رسیدن به توافق بین رایانه ها، با این شرایط که ممکن رایانه ها یا خود شبکه غیر قابل اعتماد باشند، توصیف می شود.همچنین در سال ۱۹۹۱، یک زنجیره اطلاعات امضا شده به عنوان یک دفتر کل الکترونیکی برای امضای دیجیتالی اسناد استفاده شد، به گونه ای به راحتی نشان می داد هیچ یک از استاد امضا شده در این مجموعه تغییری نکرده است (Arvind Narayanan et al., 2016).

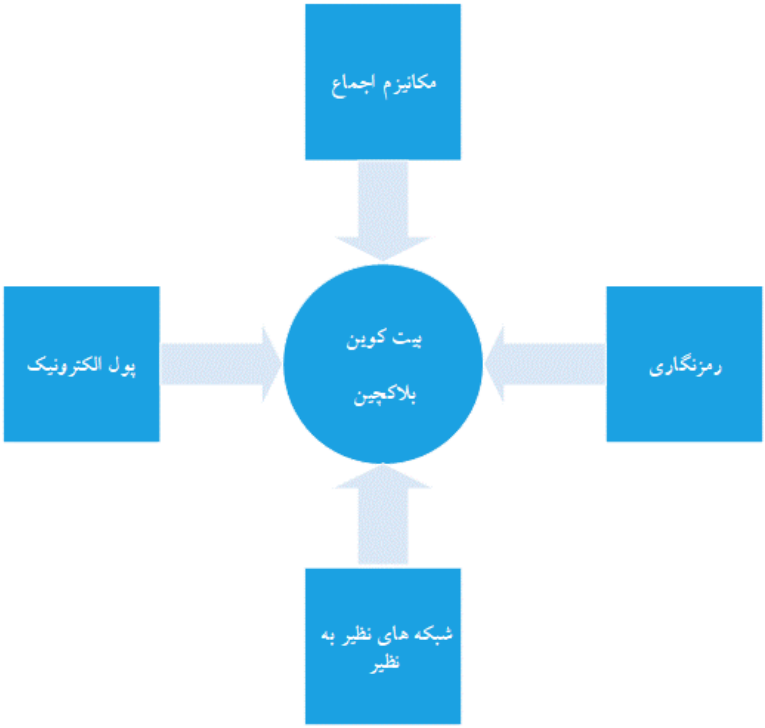
یک مفهوم متفاوت اما مرتبط به نان هش کش توسط ادام بک در سال ۱۹۹۷ به عنوان یک سیستم مبتنی بر اثبات کار برای کنترل هرزنامه های ایمیل معرفی شد. ایده بسیار ساده است: اگر کاربری قانونی بخواهد ایمیل بفرستد باید مقدار معقولی از منابع محاسباتی را قبل از ارسال ایمیل صرف کند(Back, 1997) .

ایده مشابه دیگر توسط نیک سازبو به نام بیت گلد در سال ۲۰۰۵ ارائه شده یک راه حل برای حل پازل های محاسباتی برای تولید ارز دیجیتال معرفی کرد، اما مشکل اصلی این رویکرد همچنان بر یک مرجع قابل اعتماد متمرکز متکی بود (Szabo N, 2005).

با الهام از این ایده ها و منابع در سال ۲۰۰۸ یک ارز دیجیتال با نام بیت کوین در مقاله ای با عنوان بیتکوین: سیستم نقدی الکترونیکی نظیر به نظیر (Nakamoto, 2008) با نام مستعار ساتوشی ناکاموتا ارائه شد.پس از آن در سال ۲۰۰۹ اولین پیاده سازی عملی یک ارز دیجیتال(بیت کوین) معرفی شد. برای اولین بار مشکل اجماع توزیع شده در یک شبکه بی اعتماد حل شد.در بیت کوین از رمزنگاری کلید عمومی با هش برای ارائه روشی امن، کنترل شده و غیرمتمرکز برای نگه داری ارز دیجیتال استفاده شده است. نوآوری کلیدی که در بیت کوین استفاده شده، ایده یک لیست منظم از بلوک ها که از تراکنش ها تشکیل شده اند و از نظر امنیت توسط مکانیزم مبتنی بر اثبات کار تامین شده است (Bashir, 2017).

با بررسی به تحقیقات پیش از بیت کوین و تاریخچه آن ها، می توان دریافت که چگونه این ایده ها و مفاهیم پول های الکترونیک و سیستم های توزیع شده برای اختراع بیتکوین و بلاکچین کمک کرده است.

این را می توان با کمک نمودار زیر مشاهده کرد.



شکل ۲-۳ ایده های مختلفی که به اختراع بیت کوین و بلاک چین کمک کردند

۲-۵-۲ ویژگی های اصلی بلاکچین و دستاورد های آن

از زمان تولد اولین بلاکچین یعنی بیتکوین، فعالیت های بالقوه بلاکچین به سه دسته تقسیم می شود: بلاکچین۱، ۲ و بلاکچین ۳. بلاکچین ۱ یک را ما به عنوان ارز های دیجیتالی و توسعه رمز ارز هایی مرتبط با پول نقد، انتقال ارز، حواله و سیستم های پرداخت دیجیتال می شناسیم.علاوه بر بیتکوین انواع دیگری از ارزه های دیجیتال وجود دارد که در مجموع ارزشی بیش از ۹۰۰ میلیارد دلار است (*Global Cryptocurrency Market*, 2022) . بلاکچین ۲ را با عنوان قراردادهای هوشمند و معاملاتی که گسترده تر از معاملات نقدی هستند می شناسیم . بلاکچین ۳ چیزی فراتر از ارزها و بازار های مالی می باشد و در حوزه هایی مانند سلامت، علم و هنر کاربرد دارد.

از آنجایی در مکانیزم بیتکوین کاربران شناسه های مستعار دارند و قابل شناسایی نیستند، مکانیزم هایی برای ایجاد اعتماد ضروری بود. قبل از استفاده از فناوری بلاکچین، این اعتماد معمولا از طریق واسطه های مورد اعتماد هر دو طرف ارائه می شد (Swan M, 2015).

در ادامه به بررسی چندین مورد از ویژگی های اصلی که بلاکچین ارائه می دهد خواهیم پرداخت (Yaga et al., 2019):

- **تمرکز زدایی**: در سیستم های متمرکز مرسوم، هرتراکنش باید از طریق یک سازمان مرکزی(به عنوان مثال، بانک مرکزی) اعتبار سنجی شود که به ناچار منجر به هزینه و احتمال خطا و سو استفاده در سرور های مرکزی می شود.تراکنش ها در شبکه بلاکچین می تواند بین هر دو طرف معامله بدون احراز هویت یک سازمان مرکزی انجام شود که بدین ترتیب هزینه های توسعه و نگه داری توسط این سازمان و خطر سو استفاده از این مرکزیت به طرز چشمگیری کاهش خواهد یافت.
- **پایداری**: از آنجایی که هر یک از تراکنش هایی که در سراسر شبکه بلاکچین پخش می شوند و نیاز به تایید و ثبت در بلوک های توزیع شده در کل شبکه دارند، دستکاری آن ها تقریبا غیر ممکن است.علاوه بر این هر بلوک پخش شده در شبکه نیاز باید توسط گره های دیگر اعتبار سنجی شود و تراکنش ها بررسی شوند، بنابراین هر گونه جعل به راحتی قابل تشخیص خواهد بود.
- **نا شناس بودن:** هر کاربر می تواند با یک آدرس تولید شده با شبکه بلاکچین تعامل داشته باشد. علاوه بر این، یک کابر برای جلوگیری از شناسایی شدن آدرس های زیادی را ایجاد کند. در واقع در بلاکچین هیچ مرکزیتی برای این که اطلاعات کاربران ذخیره کند وجود ندارد.
- **قابلیت اعتبار سنجی**: از آنجایی که هر یک از تراکنش های شبکه بلاکچین با یک مهر زمانی تایید و ثبت می شود، کاربران شبکه می توانند به راحتی تراکنش های قبلی را از طریق ارتباط با یک گره از شبکه تایید و ردیابی کنند. قابلیت ردیابی و شفافیت تراکنش های ذخیره شده در
- شبکه بلاکچین به طرز چشمگیری به نسبت سیستم های مرکزی حال حاظر افزایش یافته است.

۲-۵-۳ طبقه بندی شبکه های بلاکچین

شبکه های بلاکچین را می توان از چند نظر که در زیر توضیح داده شده است به سه دسته ی شبکه عمومی، شبکه خصوصی و کنسرسیوم طبقه بندی کرد (Wang et al., 2017):

أ. **تعیین اجماع:** همه گره ها ی شبکه های بلاکچین می توانند در فرایند اجماع در بلاکچین های از نوع عمومی مثل بیتکوین شرکت کنند، ولی در بلاکچین های از نوع کنسرسیوم تنها چند مجموعه از قبل انتخاب شده از گره ها مسئول تایید یک بلوک هستند.همچنین در بلاکچین های خصوصی یک مقام مرکزی، نمایندگانی را که می توانند بلوک ها تایید کنند، تعیین میکند.

ب. **مجوز خواندن:** بلاکچین های عمومی اجازه خواندن اطلاعات در دفتر کل را به همه کاربران می دهند در صورتی که در بلاکچین هایی از نوع خصوصی یا کنسرسیوم دسترسی به اطلاعات دفتر کل محدود شده می باشد. بنابراین یک سازمان یا کنسرسیوم می تواند تصمیم بگیرد که چه بخش یا بخش هایی از اطلاعات دفتر کل در اختیار کاربران قرار بگیرد.

ج. **تغییرناپذیری:** در شبکه بلاکچین عمومی غیرمتمرکز که تراکنش ها در دفتر کل توزیع شده ذخیره می شوند و توسط همه همتایان تایید می شوند، که تغییر در این دسته از شبکه ها تقریبا غیر ممکن است. در مقابل در بلاکچین های از نوع خصوصی و کنسرسیوم سازمان مرکزی کنترل کننده می توانند با تمایل خود این اطلاعات تغییر یا دستکاری کنند.

د. **کارایی:** در بلاکچین عمومی، هر گره با تمایل خود می تواند به شبکه بپیوندد یا از آن خارج شود که این امکان شبکه بلاگچین را مقیاس پذیر می کند.با این حال این امکان باعث افزایش پیچیدگی برای فرآیند استخراج می شود. همچنین دسترسی گره ها ی جدید به شبکه، ممکن است منجر به توان عملیاتی محدود و تاخیر بیشتر شود. در شبکه های بلاکچین خصوصی و کنسرسیوم با مکانیزم های اجماع انتخابی عملکرد و کارایی می تواند به راحتی افزایش پیدا کند (Alharby & van Moorsel, 2017).

ه. **مرکزیت:** تفاوت قابل توجه که بین سه نوع شبکه عمومی، خصوصی و کنسرسیوم وجود دارد این است که عموما بلاکچین عمومی غیر متمرکز است در حالی که بلاکچین های کنسرسیوم و خصوصی توسط یک مرکزیت کنترل می شوند..

و. **مشارکت اجماع:** در بلاکچین های عمومی همه افراز می توانند به روند اجماع بلاکچین شرکت کنند. بر خلاف بلاکچین عمومی، هر دو بلاکچین کنسرسیوم و خصوصی نیاز به داشتن یک سطح دسترسی از شبکه یا مسئولان شبکه نیاز است.

به این ترتیب به این دلیل که بلاکچین های عمومی به روی همه باز است و دسترسی و مشاهده عملکرد شبکه برای همه امکان پذیر است جوامع موجود در ان هم فعال ترند و این نوع شبکه ها طرفداران بیشتری دارند و روز به روز شاهد پیشرفت بیشتری در آن ها می باشیم. در مورد بلاکچین کنسرسیوم، می توان آن را برای بسیاری از برنامه های تجاری اعمال کردو در حال حاظر هایپر لیجر در حال توسعه چارچوب هایی در این زمینه می باشد (Uddin, 2021).

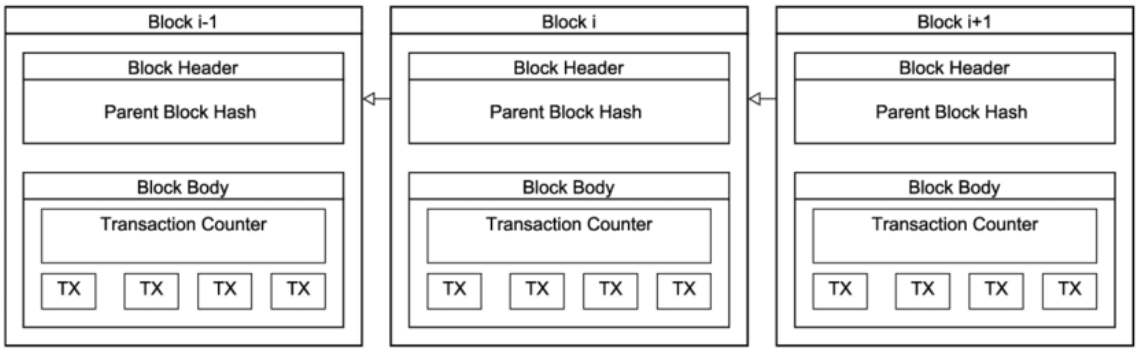
جدول ۲-۱ مقایسه ای از شبکه های بلاکچین عمومی، کنسرسیوم و خصوصی

ویژگی	شبکه عمومی	شبکه کنسرسیوم	شبکه خصوصی
تعیین اجماع	همه استخراج کنندگان	گره های انتخاب شده	گره های انتخاب شده
مجوز خواندن	عمومی	عمومی/ محدود شده	عمومی/ محدود شده
تغییر ناپذیری	تقریبا غیر ممکن	امکان دستکاری	امکان دستکاری
کارایی	کم	زیاد	زیاد
مرکزیت	خیر	قسمتی از آن	بله
مشارکت در اجماع	بدون نیاز به دسترسی	نیاز به دسترسی	نیاز به دسترسی

۲-۵-٤ معماری بلاکچین

بلاکچین یک دفتر کل که به صورت توزیع شده نگه داری می شود و از طریق مکانیزم های رمزنگاری ایمن، تغییر ناپذیر و فقط از طریق یک مکانیزم اجماع یا توافق بین گره ها می تواند به روز رسانی شود (Bashir, 2017).

بلاکچین یک زنجیره از بلوک هاست که فهرست کاملی از سوابق تراکنش های یک دفتر کل قراردادی را در خود نگه داری می کند(Lee D, 2015) . شکل ۲-٤ نمونه ای از یک بلاکچین را نشان می دهد.هر بلوک از طریق یک مرجع به بلوک قبلی(بلوک والد) اشاره می کند. این مرجع از طریق یک مقدار هش شده از بلوک والد است. در بعضی از بلاکچین ها مانند پیاده سازی شبکه اتریوم بلاک های هم جوار هم در محسابه مقدار هش در نظر گرفته می شود(Buterin, 2014) .



شکل۲-٤ نمونه از قرارگیری بلوک های یک شبکه بلاکچین

برخی از تعاریف فنی مختلف از بلاکچین به شرح زیر می باشد:

- بلاکچین یک مکانیزم اجماع غیر متمرکز است. در بلاکچین همه گره ها در نهایت در مورد وضعیت اخر و کلی بلاکچین به توافق می رسند.
- بلاکچین یک دفتر کل مشترک توزیع شده است. بلاکچین را می توان یک دفتر کل مشترک تراکنش ها در نظر گرفت که در آن تراکنش ها در بلوک ها گروه بندی و اجرا می شوند.در حال حاظر مدل واقعی آن پایگاه داده هایی هستند که به صورت خصوصی هر سازمان نگه داری میکنند .
- بلاکچین یک ساختار داده است. اساساً یک لیست پیوندی است که از نشانگر های هش به جای نشانگر های معمول استفاده می کند. از نشانگر ها برای اشاره به بلوک قبل استفاده می شود. (Bashir, 2017)

۲-۵-۵ بلوک

کاربران شبکه بلاکچین تراکنش ها از طریق یک نرم افزار(برنامه های دسکتاپ، برنامه های کاربردی تلفن همراه، کیف پول دیجیتال و ...) به شبکه بلاکچین ارسال می کنند. روش کارکرد این است که این تراکنش ها از طریق این نرم افزار ها به یک یا چند گره درون شبکه بلاکچین ارسال می شود.همچنین ممکن است این گره ها تراکنش ها را به سایر گره های شبکه نیز ارسال کنند.پس از این مرحله تراکنش ها به خودی خود در بلاکچین قرار نمی گیرد. برای بیشتر پیاده سازی های بلاکچین، تراکنش ها ابتدا در یک صف منتظر می مانند تا توسط یک گره نویسنده بلوک به بلاکچین اضافه شوند.

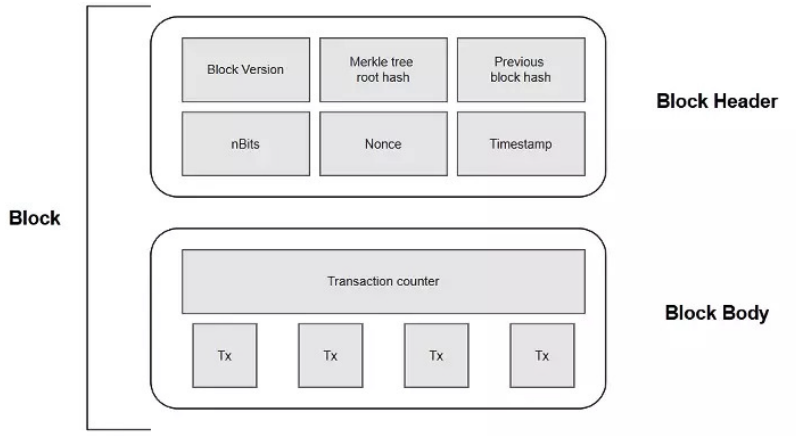
زمانی که یک گره نویسنده یک بلوک به تولید و منتشر می کند، تراکنش ها به شبکه بلاکچین اضافه می شوند. داده های بلوک باید شامل لیستی از تراکنش های معتبری باشد که بلاکچین ارسال شده است.اعتبار و صحبت این تراکنش ها با توجه به رمزنگاری های آن تضمین می شود. در ادامه به بررسی بیشتری از شیوه رمزنگاری و امضای دیجیتال خواهیم پرداخت. سپس از تولید و انتشار بلوک توسط گره نویسنده گره سایر بلوک ها می توانند اعتبار و صحت بلوک را بررسی و در صورتی که اعتبار سنجی به درستی انجام شده است این بلوک را بپذیرند (Yaga et al., 2019).

اولین بلوک از کل شبکه بلاگچین را بلوک پیدایش نام دارد که بلوک والدی ندارد. یک بلوک شامل یک لازم به ذکر است که بلاکچین های مختلف بسته به نیاز خود فیلد های خود را تعریف می کنند با این حال بسیاری از پیاده سازی های بلاکچین از مواردی که در زیر آورده شده است استفاده می کنند:

یک بلوک از هدر و بدنه تشکیل شده است که هدر شامل موارد زیر می باشد:

- بلوک ورژن: نشان دهنده این است که کدام مجموعه از اعتبار سنجی ها در این بلاک صدق می کند.
- نشانگر بلوک والد: شامل مقدار ۲۵٦ بیتی هش که به بلاک والد اشاره می کند.
- هش ریشه درخت مرکل: شامل هش تمام تراکنش های موجو در بلوک می باشد.
- مهر زمانی: شامل مقدار زمان فعلی به ثانیه از زمان جهانی از ۱ ژانویه سال ۱۹۷۰ میلادی
- nBits : شامل مقدار آستانه هدف یک هش بلوک معتبر می باشد.
- نانس: یک فیلد ٤ بایتی که از ۰ شروع می شود و برای هر محاسبه هش افزایش می یاد.

بدنه بلوک از یک شمارنده تراکنش و تراکنش ها تشکیل شده است. حداکثر تعداد تراکنش هایی که یک بلوک می تواند داشته باشد به اندازه بلوک و اندازه هر تراکنش بستگی دارد. بلاکچین از یک مکانیزم رمزنگاری نامتقارن برای تایید اعتبار تراکنش ها استفاده می کند (Zheng et al., 2017).

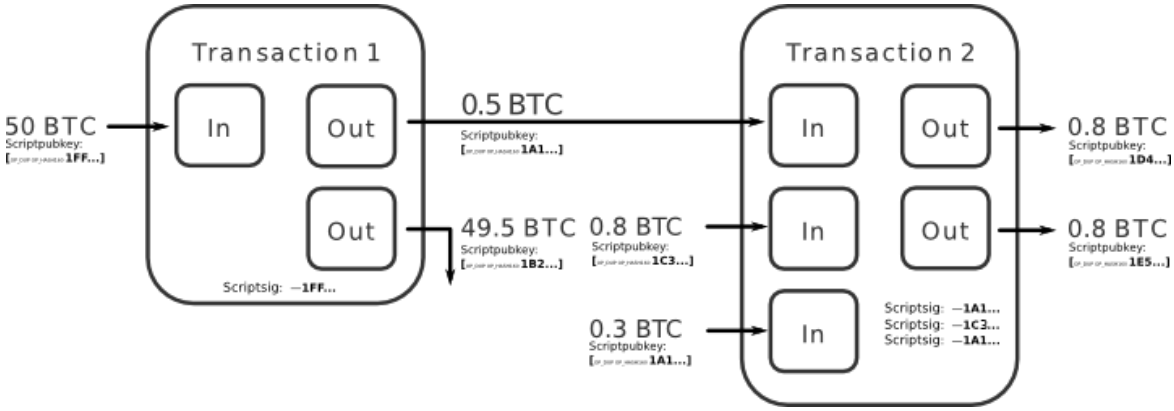


شکل۲-۵ مثالی از یک بلوک در شبکه بلاکچین

۲-۵-٦ تراکنش

تراکنش ها در بلاکچین در واقع داده هایی که به بلوک های زنجیره بلوکی شما راه پیدا می کنند را تعیین می کنند (Substrate, 2022). تراکنش بیانگر تعامل بین طریفین در یک معامله می باشد.در رمز ارز ها تراکنش ها نشان دهنده انتقال ارز بین کاربران شبکه بلاکچین است.در سناریو های تجاری تراکنش ها راهی برای ثبت فعالیت هایی باشد که روی دارایی های دیجیتال یا فیزیکی می افتد.شکل ۲-۵ تراکنش در ارز های دیجیتال را نشان می دهد.هر بلوک در یک شبکه بلاگچین می تواند هیچ یا چند تراکنش در خود جای دهد. برای برخی از پیاده سازی هایی که از شبکه بلاکچین شده است، تولید بلوک های ثابت جدید (حتی با هیچ تراکنشی) برای حفظ ثبات و امنیت شبکه ضروری می باشد.

داده هایی که یک تراکنش را ایجاد می کنند می تواند برای هر شبکه از بلاکچین بسته به نیاز های آن شبکه متفاوت باشند، اما مکانیزم تراکنش تا حد زیادی یکسان است. یک کاربر شبکه بلاکچین اطلاعاتی را به شبکه بلاکچین در زمان ثبت بلاکچین ارسال می کند . این اطلاعات ممکن است شامل آدرس فرستنده، کلید عمومی، امضای دیجیتال، ورودی و خروجی تراکنش باشد.



شکل۲-٦ مثالی از تراکنش ها در شبکه بلاکچین

یک تراکنش در شبکه بلاکچین رمز ارز به طور معمول به اطلاعات زیر نیاز دارد(می تواند حاوی اطلاعات بیشتری باشد):

- **ورودی ها** : ورودی ها معمولا فهرستی از دارایی های دیجیتالی می باشند که باید منتقل شوند.یک تراکنش به منبع دیجیتالی یا تراکنشی که در آن به فرستنده دارایی داده شده است اشاره می کند.(در مورد دارایی های جدید به رویداد مبدا اشاره می کند). ازآنجایی که ورودی تراکنش ها اشاره به رویداد یا دارایی های گذشته دارد در نتیجه می توان این نتیجه را گرفت که دارایی در بلاکچین قابل تغییر نیستند. در مورد شبکه های بلاکچین رمز ارز ها این دارایی، یک دارایی می تواند به چندین دارایی کوچکتر(بار ارزش کمتر) یا چندین دارایی کوچک به یک دارایی بزرگتر تبدیل شود.تقسیم کردن یا ادغام کردن دارایی ها در خروجی تراکنش ها مشخص خواهد شد.فرستنده همچنین باید ثابت کند دارایی ها اشاره شده تحت مالکیت خود است که معمولا از طریق امضای دیجیتالی یک تراکنش از طریق یک کلید خصوصی این اثبات به شبکه بلاکچین اعلام می شود.
- **خروجی ها:** خروجی ها معمولا حساب هایی هستند که دارایی های دیجیتال ومقدار آن را دریافت خواهند کرد. در واقع هر خروجی تعدادی دارایی دیجیتالی است که به مالکان جدید انتقال می یابند. همچنین خروجی ها ممکن است دارای شروطی برای مالکان جدید در زمانی که می خواهند دارایی انقال یافته را خرج کنند وجود داشته باشد.

هدف اصلی یک شبکله بلاکچین فراهم کردن یک مکانیزم ذخیره سازی امن و انعطاف پذیر برای تراکنش ها است (Gupta & Sadoghi, 2021).

۲-۵-۷ مکانیزم اجماع در شبکه بلاکچین

در برنامه ها و کاربرد هایی که بلاکچین دارد، باید دو مشکل را حل کنیم: مشکل دو بار هزینه کردن و مشکل ژنرال های بیزانسی. مشکل دوبار هزینه کردن یعنی استفاده مجدد از یک ارز در دو تراکنش به صورت همزمان.در ارز های سنتی به دلیل اینکه ارز سنتی یک موجودیت است در هنگام استفاده از آن ها دچار این مشکل نمی شویم.همچنین می توانیم مشکل هزینه دوبار هزینه کردن در تراکنش های اینترنتی را با ایجاد مرکزیت سازمان های مورد اعتماد حل کنیم.در بلاکچین این مشکل با تایید تراکنش ها توسط گره های سیستم های توزیع شده حل می شود (Du et al., 2017).

مشکل ژنرال های بیزانسی یک مشکل در سیستم های توزیع شده می باشد. داده ها را می توان بین گره های مختلف از طریق ارتباطات همتا به همتا تحویل داد. با این حال، برخی از گره ها ممکن است به طور مخرب مورد حمله قرار گیرند که منجر به تغییر محتوای ارتباطی می شود. گره های معمولی(گره هایی که الوده نشده اند یا رفتار مخربی ندارند) باید اطلاعات دستکاری شده را متمایز کنند و نتایج یکسانی را با سایر گره های عادی به دست آورند.برای رسیدن به این اصل نیاز به طراحی الگوریتم اجماعی بین گره ها نیاز است. در ادامه به بررسی چندین الگوریتم برای رسیدن به اجماع خواهیم پرداخت.

۲-۵-۷-۱ اثبات کار[1]

الگوریتم اجماع مورد استفاده در بیت کوین الگوریتم اثبات کار است. ایده اصلی آن تخصیص پاداش به گره های بر اساس قدرت محسباتی هش بین گره ها است.بر اساس اطلاعات قبلی از بلوک قبلی، گره های مختلف راه حل خاص یک مسئله ریاضی را محاسبه می کنند. حل این مسئله ریاضی سخت است. اولین گره های که بتواند این مسئله را حل کند می تواند بلوک بعدی را ایجاد کند و به عنوان پاداش مقدار مشخصی از بیت کوین دریافت می کند. ساتوشی ناکاموتو از هشکش برای طراحی این مسئله ریاضی در بیت کوین استفاده کرد (Back, 1997).

مراحل محسابه در شرح زیر می باشد:

۱. تعیین سختی شبکه: پس از تولید هر ۲۰۱٦ بلوک، الگوریتم استخراج بیت کویت به صورت پویا مقدار دشواری را با توجه به نرخ هش کل شبکه تنظیم می کند
۲. جمع آوری تراکنش ها: جمع آوری تمام تراکنش های معلق در شبکه پس از تولید آخرین بلوک.پر کردن شماره بلوک، مقدار هش ۲٥٦ بیتی بلوک قبلی، هش فعلی و شماره تصادفی در بلوک.
۳. محسابه هش: با تغییر پارامتر تصادفی و محاسبه هش و بررسی این مقدار که ایا کمتر یا مساوی با مقدار هش اعلامی شبکه می باشد یا خیر . اگر بله بلوک می تواند پخش شود و توسط سایر گره ها تایید شود.
۴. راه اندازی مجدد: اگر گره نتواند مقدار هش را در زمان مشخص تعیین کند، مرحله دو را تکرار می کند. اگر هر بتواند از مرحله یک مجددا راه انازی می شود.

الگوریتم اجماع یک بار کاری را به عنوان محافظ در نظر می گیرد. بلوک جدید ایجاد شده به بلاکچین پیوند داده می شود. طول زنجیره متناسب با حجم کار است. همچنین همه گره ها به طولانی ترین زنجیره اعتماد دارند. در الگوریتم اجماع اگر کسی بخواهد در بلاکچین دستکاری کند باید بیش از ۵۰ درصد

[1] Proof of work

قدرت هش کل شبکه را کنترل کند تا مطمئن باشد که می تواند اولین کسی باشد که اخرین بلاک را تولید می کند و بر طولانی بودن زنجیره تسلط پیدا کند. هزینه و عواقب دستکاری کردن بلاکچین می تواند از سود آن بیشتر باشد که همین عامل به طور موثر ایمنی بلاکچین را تضمین کند.

۲-۵-۷-۲ اثبات سهام[1]

در اولین پروژه بیت کوین ذکر شده است ولی به دلیل برخی از مسائل دیگر از آن استفاده نشده است. از اولین استفاده ها در پی پی کوین بوده است (King & Nadal, 2012) .در الگوریتم اثبات سهام مفهوم سن سکه وجود دارد. سن سکه روشی برای نمایش مدت زمانی است که یک سکه در اختیار فرد بوده است تا آن را در معملات اولویت بندی کنیم. ارزش آن بر اساس مقدار آن ضرب در مدت زمانی که بعد از آن ساخته شده است.هرچه یک گره ارز ها را طولانی تر نگه دارد، حقوق بیشتری در شبکه خواهد داشت.دارندگان سکه نیز با توجه به سن سکه پاداش مشخصی دریافت خواهند کرد. الگورتیم اثبات سهام دارنگان ارز ها را تشویق می کند تا مدت زمان بیشتری از ارز ها نگه داری کنند. با مفهوم سن سکه، بلاکچین دیگر به طور کامل به اثبات کار متکی نیست. این به طور موثر مشکل اتلاف منابع را در اثبات کار را حل می کند. همچنین امنیت بلاکچین با استفاده از اثبات سهام بهبود می یابد. در این روش مهاجمان باید تعداد زیادی از سکه را جمع کنند و به اندازه کافی برای حمله به بلاکچین نگه دارند. این سختی حمله را تا حد زیادی افزایش می دهد (Du et al., 2017).

مکانیسم اثبات کار بیت کوین نوعی فرآیند انتخاب تصادفی را تسهیل می کند که بر اساس آن یکی از استخراج کنندگان را برای صدور بلاک بعدی انتخاب می کند. علاوه بر این، مشروط بر این که همه استخراج کنندگان از پروتکل پیروی کنند، این انتخاب به صورت تصادفی متناسب با قدرت محاسباتی هر استخراج کننده انجام می شود. در واقع به جای اینکه استخراج کنندگان منابع محاسباتی را برای شرکت در فرایند انتخاب گره سرمایه گذاری کنند، در عوض روندی را پیروی می کنند که به طور تصادفی یکی از آن ها متناسب با سهامی که هر کدام در بلاکچین دارند، انتخاب می کنند (Kiayias et al., 2017).

از آنجایی که انتخاب بر اساس موجودی حساب کاملا نا عادلانه است زیرا ثروتمندترین افراد در شبکه از تسلط بیشتری برخوردار خواهند بود. درنتیجه راه حل هایی برای حل این مسئله ارائه شده است که چه کسی بلوک بعدی را بسازد. به طور خاص بلک کوین(Vasin P, 2014) از تصادفی سازی برای تعیین سازنده بلوک بعدی استفاده می کند.پی پی کوین از انتخاب بر اساس سن سکه استفاده می کند که در آن سکه های قدیمی تر و بزرگ تر از احتمال بیشتری برای استخراج بلوک بعدی برخوردار هستند.

[1] Proof of stake

۲-۵-۸ برنامه های توزیع شده[1]

برنامه های توزیع شده بر روی یک شبکه بلاکچین میزبانی می شوند.از این برنامه ها در حوزه های مختلفی از جمله بیمه، انرژی، امورمالی، سلامت، حمل و نقل و بسیاری موارد دیگر استفاده می شود.ویژگی های برنامه های توزیع شده به صورت زیر مشخص می شود:

- منبع باز(سورس باز): کدهای برنامه های توزیع شده منبع باز هستندو بازرسی کردن از این کدها عمومی می باشد.
- عدم وجود مرکزیت: به دلیل ماهیت غیر متمرکز آن، هیچ نقطه مرکزی برای خرابی وجود ندارد.
- اجماع: برای فعال کردن شفافیت، اجماع بین گره ها اجتناب ناپذیر است.
- پشتیبانی از یک ارز: رمز ارز داخلی عامل اصلی است که اکوسیستم هر برنامه غیر متمرکز را اجرا می کند.

تفاوت های کلیدی بین برنامه های کاربردی وب متمرکز و برنامه های توزیع شده بلاکچین در جدول ۲-۲ نشان داده شده است.

جدول ۲-۲ تفاوت های بین برنامه های کاربردی وب متمرکزو برنامه های توزیع شده بلاکچین

برنامه های تحت وب متمرکز	برنامه های توزیع شده بلاکچین
از معماری سرور و کلاینت پشتیبانی می کندد	کاربران از طریق رابط کاربری شبکه ارتباط برقرار می کنند
پایگاه داده غیر شفاف توسط ارائه دهنده سرویس	پایگاه داده ای که هر کس یک نسخه از آن را در شبکه بلاکچین دارد
نیاز به دسترسی توسط یک مرکزیت واحد	هیچ مرکزیت واحدی وجود ندارد
امن، تغییرناپذیرو مستقل	برای امنیت و حریم خصوصی نگرانی های وجود دارد

۲-٦ رمزنگاری

در این دوران که اینترنت ارتباط بین ده ها میلیون نفر را فراهم می کند و به طور فزاینده ای به عنوان ابزاری برای تجارت استفاده می شود، امنیت به یک موضوع بسیار مهم تبدیل شده است.جنبه های امنیتی و کاربردی بسیاری وجود دارد، از تجارت امن و پرداخت ها گرفته تا ارتباطات خصوصی و محافظت از رموز های عبور. یکی از جنبه های ایمن برای رمز نگاری برای ارتباطات ایمن ضروری است. در تبادل

[1] DApp

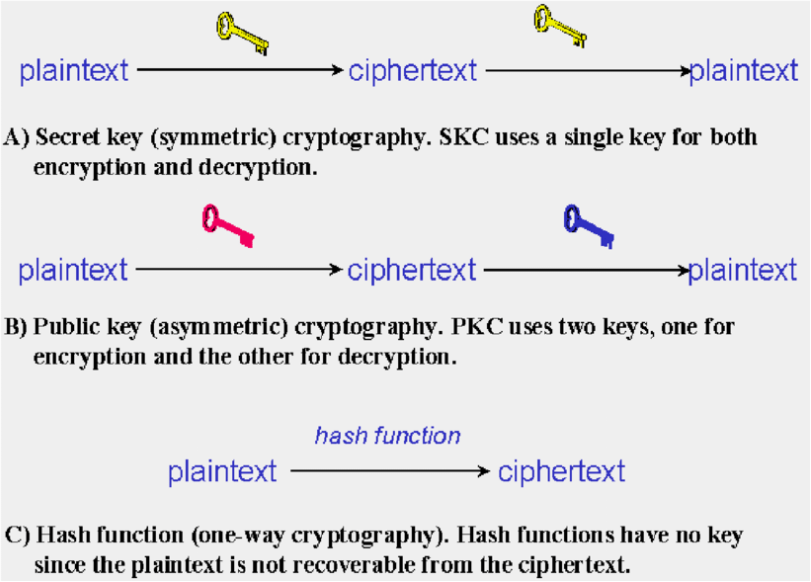
اطلاعات از راه دور، رمزنگاری هنگام برقراری ارتباط از طریق هر رسانه غیر قابل اعتماد، که تقریبا شامل هر شبکه، به ویژه اینترنت می شود، ضروری است.

درارتباطات بین برنامه های با یکدیگر، برخی الزامات امنیتی خاصی وجود دارد از جمله:

- احراز هویت: فرایند احراز هویت. (احراز هویت بر اساس میزبان در اینترنت بر اساس نام یا آدرس عملکرد خوبی ندارد)
- حریم خصوصی/ محرمانگی : اطمینان از اینکه هیچ کس نمی تواند پیام را به جز گیرنده مد نظر بخواند.
- صداقت: به گیرنده این اطمینان را می دهد که پیام دریافتی از پیام اصلی ارسالی تغییری نکرده است.
- عدم انکار: مکانیزمی برای اثبات اینکه فرستنده واقعا این پیام را ارسال کرده است.

بنابراین رمزنگاری نه تنها از داده ها برابر سرقت یا تغییر اطلاعات محافظت می کند، بلکه می تواند برای احراز هویت کاربر نیز استفاده شود (Zheng et al., 2017). سه نوع الگورتیمی که در رمزنگاری در آن استفاده می شود:

- رمزنگاری کلید مخفی: از یک کلید واحد برای رمزگذاری و رمزنگاری استفاده می کند.
- رمزنگاری کلید عمومی: از یک کلید برای رمزگذاری و یک کلید برای رمز کشایی استفاده می کند.
- توابع هش: از یک تبدیل ریاضی برای رمزگذاری غیر قابل برگشت اطلاعات استفاده می کند.



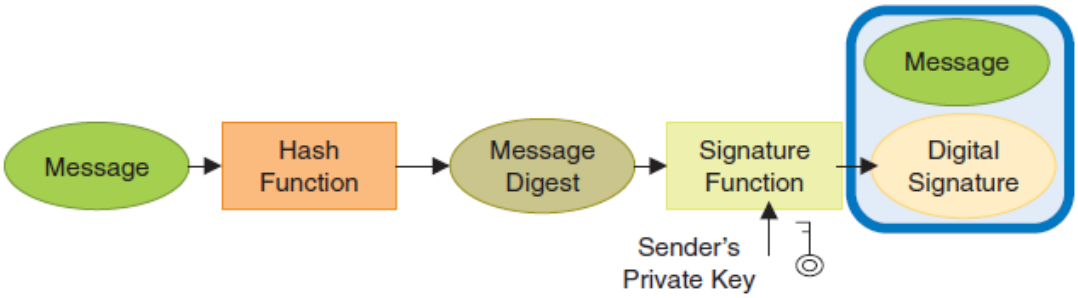
شکل ۲-۷ انواع رمزنگاری بر اساس الگوریتم

۲-٦-۱ امضای دیجیتال[1]

امضای دیجیتال، نسخه الکترونیکی امضاهای دست نویس برای اسناد دیجیتالی می باشد: امضای کاربر در پیام m رشته ای است که به m، به کلید عمومی و کلید مخفی کاربر و احتمالا به داده های انتخابی تصادفی بستگی دارد. این امضا (یک رشته) به گونه ای می باشد که همه می توانند اعتبار امضا را با استفاده از کلید عمومی بررسی کنند.در واقع می خواهیم از جعل امضای دیجیتال بدون دانستن کلید خصوصی جلوگیری کنیم (Gupta & Sadoghi, 2021) .

امضای دیجیتال معمولا از دو بخش تشکیل شده شده است: یک الگوریتم امضا و یک الگوریتم تایید. الگوریتم امضا برای تولید یک امضای دیجیتال بر روی پیام تنظیم می شود، امضا معمولا توسط کلید امضا کنترل می شود.الگوریتم امضا یا کلید امضا معمولا توسط امضا کننده مخفی نگه داشته می شود.الگوریتم تایید به منظور تایید امضای دیجیتال استفاده می شود و پیام را می توان مطابق با امضا تایید کرد.الگوریتم تایید و کلید تایید معمولا عمومی هستند، بنابراین شخصی که نیاز به تایید امضا دارد به راحتی می تواند آن را تایید کند (Adeeb et al., 2019).

۲-٦-۱-۱ ساخت امضای دیجیتال

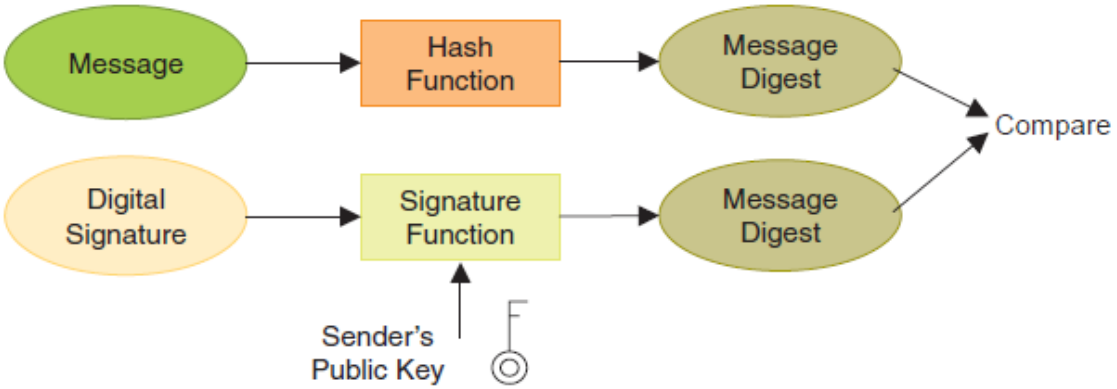


شکل ۲-۸ ساخت یک امضای دیجیتال

شکل ۲-٦ یک طرح عمومی ساده برای ایجاد امضای دیجیتال را نشان می دهد.یک تابع هش به پیام اصلی اعمال می شود که یک خلاصه پیام با اندازه ثابت را ارائه می دهد(در قسمت های بعدی در مورد تابع هش یا درهم ساز توضیح داده خواهد شد).تابع ساخت امضای دیجیتال با استفاده از کلید خصوصی و این پیام خلاصه برای تولید امضای دیجیتال استفاده می کند.شکل بسیار ساده ای از امضای دیجیتال با رمزنگاری خلاصه پیام با استفاده از کلید خصوصی به دست می آید.اکنون می توان پیام و امضای دیجیتال را برای گیرنده ارسال کرد.پیام رمزگذاری نشده است و هر کسی می تواند آن را بخواند. با این حال، امضا اصالت فرستنده را تضمین می کند(چیزی شبیه به یک بخشنامه ارسال شده توسط یک مرجع برای خواندن بسیاری از افراد، با امضای تایید صحت پیام).

[1] Digital signature

۲-٦-۱-۲ تایید امضای دیجیتال



شکل۲-۹ تایید یک امضای دیجیتال

شکل ٦-٤ روش تایید یک امضای دیجیتال را نشان می دهد. در گیرنده تابع معکوس به امضای دیجیتال اعمال می شود.تا خلاصه پیام اصلی را بازیابی کند. پیام بازیابی شده همان تابع هش است که پیام اصلی در معرض آن قرار گرفته است (Subramanya & Yi, 2006).

۲-٦-۲ توابع هش (درهم ساز)

تابع هش یک تابع محاسباتی است که رشته های محاسباتی با طول دلخواه را به رشته های باینری که گاها طول ثابتی، تبدیل می کند.ایده ایده اصلی این است که یک مقدار هش به عنوان نماینده فشرده یک رشته ورودی عمل می کند. برای استفاده در رمزنگاری یک تابع هش به گونه ای انتخاب می شود که از نظر محاسباتی امکان اینکه برای دو ورودی متفاوت یک مقدار هش پیدا کنیم وجود نداشته باشد.

رایج ترین کاربرد رمزنگاری با توابع هش با امضای دیجیتال و برای یکپارچگی داده ها است. یکی دیگر ار روش های استفاده از توابع هش برای یکپارچگی داده ها به این شرح می باشد. مقدار هش مربوط به یک ورودی خاص در یک مقطع زمانی محاسبه می شود. در یک مقطع زمانی بعدی برای تایید اینکه داده های ورودی تغییر نکرده اند، مقدار هش با استفاده از ورودی مجددا محاسبه می شود و با مقدار هش قبلی مقایسه می شود. اگر برابر باشند یکپارچگی داده ها حفظ شده است (Menezes, 2021).

۲-۷ اشتراک گذاری سفر

در مطالعات نشان داده شده است که در سراسر جهان تعداد وسیله نقلیه به ازای هر نفر در چند سال اخیر به سرعت افزایش یافته است که منجر به حرکت کند وسایل نقلیه به دلیل ظرفیت محدود جاده ها شده است. بنابراین، برای جلوگیری از ترافیک وسایل نقلیه در جاده ها، هدف اصلی تشویق استفاده از ظرفیت کامل وسایل نقلیه است. از راه های دیگر، تشویق مالک وسیله نقلیه تا از وسیله نقلیه خود به

عنوان بخشی از سیستم حمل و نقل عمومی استفاده کند و افراد دیگری با توجه به ظرفیت ازاد وسیله نقلیه خود حمل کند.این منجر به کاهش نسبت وسیله نقلیه به فرد و دستیابی به شرایط تراکم روان می شود.افرادی که از خودروی شخصی استفاده می کنند، تنها در صورتی که روش ها را ساده، قابل توضیح و مقرون به صرفه و منصفانه بندانند، به روش های اشتراک گذاری سفر روی می آورند (Ruj, 2019) .
حمل و نقل یکی از جنبه های مهم هر جامعه است. اخیرا، سرویس دهندگان اشتراک گذاری سفر که عمدتا مبتنی مدل کسب و کار بر اساس تقاضا هستند (J. WALKER SMITH, 2016) که به مصرف کنندگان این امکان را می دهند که یک خودرو با چند ضربه بر روی یک تلفن همراه رزرو کنند. با پرداخت به طور خودکار از حساب های کاربران، این روش راحت تر از استفاده از یک تاکسی سنتی شده است (Posen, 2015).

اشتراک گذاری وسیله نقلیه راهی مهم برای کاهش تراکم ترافیک و هزینه های سفر برای مسافران در سراسر جهان است. اشتراک گذاری سفر همچنین سازگار با محیط زیست است، چرا که تولید کربن را کاهش می دهد.در بسیاری از کشور ها برای تشویق اشتراک گذاری سفر، از خطوط وسیله نقلیه پرشمار استفاده می کنند، که خطوط ترافیکی است که محدود به وسایل نقلیه با بیش از یک مسافر است (U.S. Department of transportation, n.d.).

امروزه استفاده از سرویس های اشتراک گذاری سفر در بسیاری از کشور ها رواج یافته است. در این زمینه شرکت های بسیاری از جمله اسنپ و تپسی در ایران و اوبر[1] و لیفت [2]در سطح بین المللی فعالیت میکنند. طبق پیشبینی ها تا سال ۲۰۳۰ درآمد شرکت ها در این بازار به ارزش تقریبی ۲۸۵ میلیارد دلار خواهد رسید .(Shivers et al., 2021)

۲-۸ پیشینه تحقیق

در این بخش به ارائه سوابق تحقیق و پژوهش های صورت گرفته در زمینه سرویس اشتراک گذاری سفر مبتنی بر بلاکچین پرداخته می شود. در بخش اول، سوابق از سال های اخیر در زمینه تحقیق فعلی ارائه می گردد.

پرادیپ شارما و همکارانش[3] در سال ۲۰۱۷، یک معماری شبکه خودرویی مبتنی بر بلاکچین توزیع شده در شهر هوشمند ارائه دادند. آن ها در تحقیق خود یک معماری شبکه وسایل نقلیه توزیع شده ارائه دادند. آن ها بررسی کردند که چگونه شبکه وسایل نقلیه با پارادایم ها تکامل می یابند. دپارتمان وسایل نقلیه هر بار که ثبت نام خودرو صادر می شود، جزئیات را به مرجع ابطال ارسال می کنند. سپس مرجع ابطال،

---

[1] Uber

[2] Lyft

[3] Sharma, P.K., Moon, S.Y. and Park, J.H.

بلاک چین توزیع شده را از تمام اطلاعات مربوط به گره های خودروی معمولی و ماینر مطلع می کند (Sharma et al., 2017).

آنه فام و همکارانش [1]در سال ۲۰۱۷، یک سرویس حمل و نقل با حفظ حریم خصوصی و در عین حال پاسخگو ارائه دادند.آن ها در تحقیق خود یک سیستم حفظ حریم خصوصی، SHE را بهینه کردند تا نیازهای پهنای باند و سربار پردازش با استفاده از بسته‌بندی متن رمزی و پردازش تبدیل شده کاهش یابد (Pham et al., 2017).

نیکولای ولادیمیر بوزدوگ و همکارانش [2]در سال ۲۰۱۸، یک سرویس تطبیق همتا به همتای مسافران برای سهیم شدن کارآمد ارائه دادند. راه حل آن ها یک معماری است که در آن مشتریان از یک پایگاه داده مرکزی برای یافتن مسافران موجود استفاده نمی کنند، بلکه از یک روش همتا به همتا استفاده می کنند، یعنی گروه های اشتراک گذاری سواری را به صورت آنلاین تشکیل می دهند. در این برنامه، یک گره تصمیم می گیرد و یک فعالیت را اجرا می کند. به دنبال گره ای می گردد که مسیرهای آن کاملاً مطابقت دارند(Bozdog et al., 2018).

پانچالیکا پال و سوشمیتا روج [3]در سال ۲۰۱۹، یک سرویس اشتراک گذاری سفر همتا با بلاک چین ارائه دادند. آن ها در تحقیق خود از یک سیستم رتبه بندی داخلی استفاده کردند. برای اطمینان از عادلانه بودن سواری، همه چیز در مورد سواری به طور دائم در دفتر ثبت می شود و دسترسی به همه افراد در شبکه همتا به همتا را تضمین می کند. با نقشه برداری مشخص از هر حساب، از سرقت هویت جلوگیری می کند و هنگامی که شکایتی ثبت می شود، مقامات می توانند با بررسی دفتر کل آن را تأیید کنند . (Pal & Ruj, 2019)

محمد باز و همکارانش در سال ۲۰۱۹، یک سرویس اشتراک گذاری سواری با حفظ حریم خصوصی، اعتماد و پرداخت عادلانه در یک شبکه بلاک چین عمومی ارائه دادند. آن ها در تحقیق خود یک مدل رتبه بندی را معرفی می کنند که رانندگان را بر اساس رفتار قبلی رتبه بندی می شوند و به مسافران اجازه می دهد بر اساس مجموعه تعاملات رانندگان انتخاب کنند. تایید با استفاده از اثبات دانش صفر برای محافظت از مسافر انجام می شود(Baza et al., 2019).

سلام خنجی و سامیر عساف در سال ۲۰۱۹، جهت افزایش کارایی اشتراک‌گذاری سواری از طریق بلاکچین یک روشی ارائه دادند. آن ها با اجرای تمرکززدایی در جایی که کاهش انتشار کربن را تسهیل می کند، تعهدات اجتماعی بین افراد را ترویج دادند. روش آن ها از دو ساختار تشکیل شده است:

[1] Anh Pham, Italo Dacosta, Guillaume Endignoux, and Juan Ramon Troncoso Pastoriza, EPFL; Kevin Huguenin
[2] Nicolae Vladimir Bozdog, Marc X. Makkes, Aart van Halteren, Henri Bal
[3] Panchalika Pal, Sushmita Ruj

دستورات متمرکزی که درGoogle Cloud App Engine و GRT های غیرمتمرکز. نتیجه پژوهش آن ها موجب منجر به این امر می گردد که مشاغل، کالج ها و سازمان های دولتی ردپای کربن سالانه خود را کاهش دهند (Khanji & Assaf, 2019) .

سومیا کودوا و همکارانش در سال ۲۰۲۰، یک سرویس عملی اشتراک گذاری سفر مبتنی بر بلاکچین شبکه اتریوم ارائه دادند. آن ها در پژوهش خود یک سرویس اشتراک گذاری سفر مبتنی بر قرارداد های هوشمند اتریوم ارائه دادند. به هر کاربر یک شناسه منحصربه‌فرد داده می‌شود که با استفاده از آن، با استفاده از مکانیسم ابهام، یک سفر در دفتر کل بلاک چین را جستجو می‌کند. داده ها بر اساس فناوری دفتر کل توزیع شده ذخیره می شوند و آن را غیرمتمرکز می کند. پروتکل اجماع سازگاری داده ها را تضمین می کند (Kudva et al., 2020).

در جدول ۲-۳ مقایسه ای از سوابق ارائه می گردد:

جدول ۲-۳ مقایسه از پیشینه های تحقیق در زمینه ارائه سرویس اشتراک گذاری مبتنی بر بلاکچین

نام	سال	نویسندگان	زیرساخت / شبکه مورد استفاده
Block-VN	۲۰۱۷	Sharma et al.,2017	Vehicular Network
Oride	۲۰۱۷	Pham et al.,2017	ارائه نشده است
RideMatcher	۲۰۱۸	Bozdog et al.,2018	fog infrastructure
Blockv	۲۰۱۹	Pal & Ruj,2019	Ethereum
B-ride	۲۰۱۹	Baza et al.,2019	Ethereum
Greenride	۲۰۱۹	Khanji & Assaf, 2019	private fork of Ethereum blockchain
Pebers	۲۰۲۰	Kudva et al.,2020	Ethereum

با توجه به بررسی کارهای پیشین از سوابق پیرامون موضوع تحقیق فعلی، مشاهده گردید که تحقیقات ارائه شده با چالش هایی مواجه می باشند. از این رو محقق در این پژوهش سعی بر این دارد که از رویکرد استفاده از شبکه ای مبتنی بر بلاکچین مختص سرویس اشتراک گذاری سفر جهت بهبود سرعت و هزینه تراکنش ها استفاده نماید.

۲-۹ خلاصه فصل

در این فصل به تشریح مبانی مورد نیاز برای ارائه راهکار فصل ۳ پرداختیم. این فصل به بررسی شبکه های بلاکچین و رویکرد آن ها که پیش نیاز اصلی مباحث مطرح شده در فصول بعدی می باشد.از جمله مواردی برای ارائه سرویس های بلاکچین نیاز می باشد از جمله امضای دیجیتال، تراکنش، بلوک و همچنین معماری کلی بلاکچین تشریح شد.

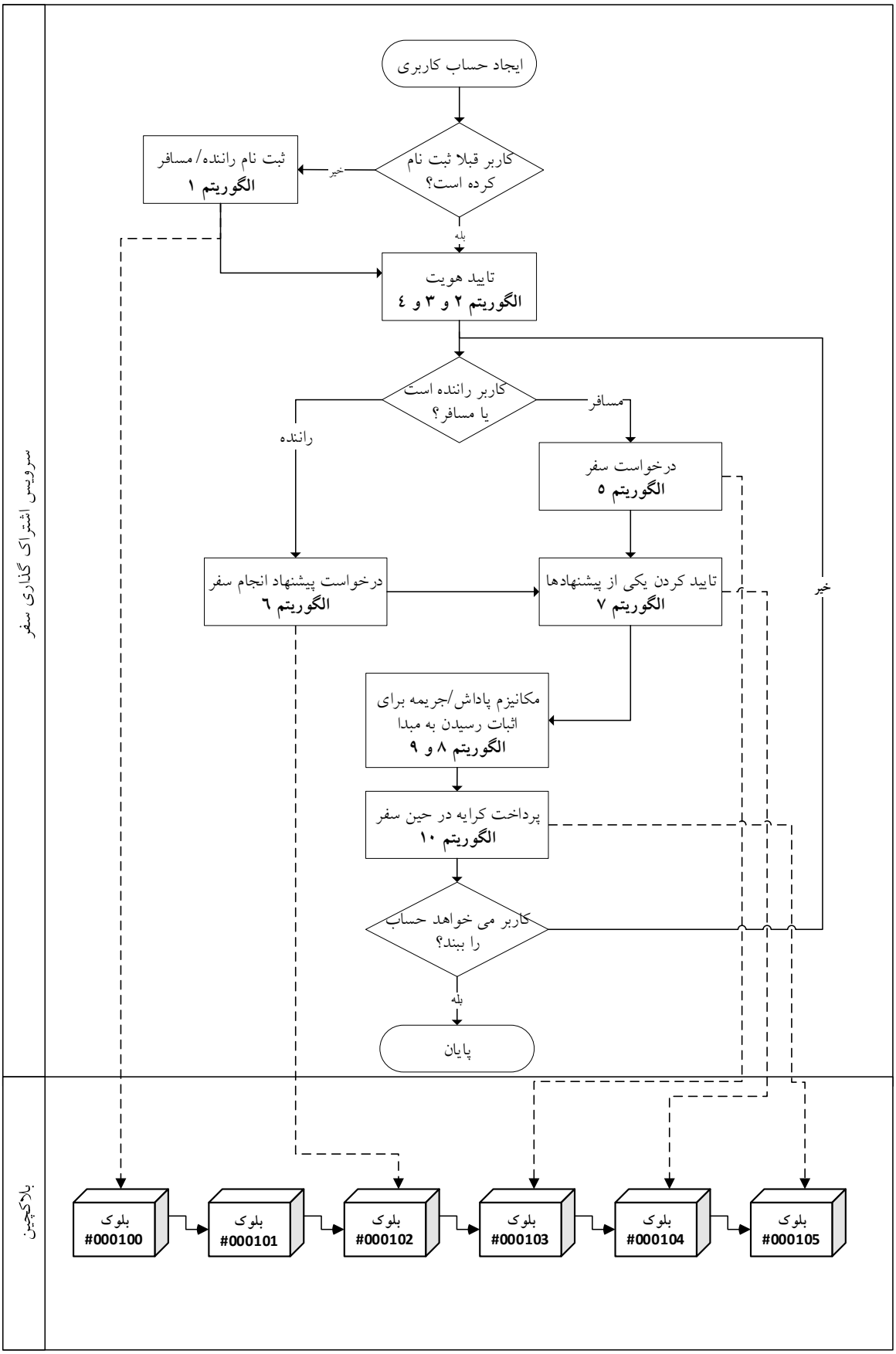
فصل ۳ روش اجرای تحقیق

۳-۱ مقدمه

پایه هر علمی، روش شناخت آن است و اعتبار و ارزش قوانین هر علمی مبتنی به روش شناختی است که در آن علم بکار می‌رود. روش تحقیق مجموعه ای از قواعد، ابزار و راه‌های معتبر و نظام یافته برای بررسی واقعیت‌ها، کشف مجهولات و دستیابی به راه حل مشکلات است؛ بطوریکه انتخاب متدلوژی یکی از مهمترین و فنی ترین مراحلی است که پژوهشگر باید با حساسیت ویژه ابزار مناسبی برای گردآوری داده‌ها طراحی کند و با انتخاب نمونه آماری و جمعیت شناختی مورد نیاز جمع آوری گردد.
در ادامه فلوچارت روش پیشنهادی سرویس اشتراک گذاری سفر مبتنی بر بلاکچین تشریح شده است.
در انتهای فصل به بررسی روش پیشنهادی مکانیزم پاداش/ جریمه برای سرویس اشتراک گذاری سفر خواهیم پرداخت.

۳-۲ تشریح روش پیشنهادی

در شکل ۳-۱ فلوچارت روش پیشنهادی برای سرویس اشتراک گذاری سفر مبتنی بر بلاکچین ارائه شده است. این فلوچارت، نحوه مشارکت کاربران به عنوان مسافر یا راننده را در سیستم را نمایش می دهد.
این فلوچارت از دو بخش تشکیل شده است. بخش فوقانی نشان دهنده رویکرد ارائه شده برای سرویس اشتراک گذاری سفر می باشد. در بخش زیرین نیز نحوه تعامل شبکه بلاکچین و سرویس اشتراک گذاری سفر نمایش داده شده است. خروجی هر الگوریتم یک تراکنش می باشد که در شبکه بلاکچین ذخیره می شوند. تمامی بلوک ها توسط گره های سازنده بلوک ساخته می شود که بر اساس الگوریتم اجماع شبکه بلاکچین این گره سازنده بلوک انتخاب می شود.



شکل ۳-۱ : فلوچارت سرویس اشتراک گذاری سفر مبتنی بر بلاکچین

همان طور که شکل ۳-۱ مشاهده می گردد در قست بالای فلوچارت، به ترتیب مراحلی که یک کاربر به عنوان راننده یا مسافر باید طی کند تا به سرویس مورد نظر خود برسد شرح داده شده است. در ادامه به تشریح هر یک از مراحل ذکر شده خواهیم پرداخت. همچنین در قسمت زیرین فلوچارت نیز وضعیت قرارگرفتن اطلاعات هر مرحله در شبکه بلاکچین نمایش داده شده است. هر یک از بلاک های شبکه بلاکچین در این سرویس شامل تعدادی تراکنش می باشد. در این سرویس کاربران برای اتصال به سرویس اشتراک گذاری سفر باید به یک گره بلاکچین اتصال شوند که بتوانند اطلاعات مورد نیاز خود را در هر مرحله را دریافت کنند. همچنین برای ارسال تراکنش به شبکه نیاز است که تراکنش ها ابتدا به یک گره بلاکچین ارسال شود. در این مرحله پس از اعتبار سنجی تراکنش ها در بلاک های بلاکچین قرار میگیرند. در ادامه به تشریح هر یک مراحل فلوچارت خواهیم پرداخت.

۳-۲-۱ ثبت نام راننده / مسافر[1]

برای استفاده از سرویس اشتراک گذاری سفر ابتدا کاربران باید در سیستم ثبت نام کنند تا علاوه بر نقش آن ها کلید های عمومی و خصوصی آن ها برای استفاده های بعدی ایجاد شود. در الگوریتم ۳-۱ ثبت نام کاربران به عنوان راننده یا مسافر در سرویس اشتراک گذاری سفر نشان داده شده است.

Algorithm 1: Driver/Passenger Registration

Input: *Role (Drvier,Passenger)*

Output: *Public Key , Private Key(secret key)*

1 ***Public Key*** ← *Generate a public key using the role that the user has chosen.*

2 ***Private Key*** ← *Private key generation with encryption algorithm.*

الگوریتم ۳-۱: الگوریتم ثبت نام راننده/ مسافر

همان طور که در الگوریتم ۳-۱ مشاهده می گردد، مسافر موجودیتی است که با ارسال درخواست به سیستم، خدمات اشتراک گذاری سفر را درخواست می کند. همچنین راننده نیز موجودیتی است که می خواهد درخواست سفر خود را با ارسال یک پیشنهاد به درخواست های مسافران به اشتراک بگذارد. فرایند سرویس اشتراک گذاری سفر با ایجاد حساب کاربری و ثبت نام شروع خواهد شد.هر کاربر(مسافر یا راننده) باید یک حسابرکاربری ایجاد کند تا بتواند توسط سیستم شناسایی شود. در صورتی که کاربران یک بار فرایند ثبت نام را انجام داده باشند می توانند با اطلاعات دریافتی خود به مرحله ورد(Login) بروند. هر کاربر در این مرحله باید نقش خود را به عنوان راننده یا مسافر تعیین کند. بنابراین کاربران کلید عمومی (شناسه هر کاربر در بلاکچین) و کلید خصوصی را به علاوه عنوان نقش خود (راننده یا مسافر) در این مرحله ایجاد می کنند.

[1] Driver/Passenger Registration

در خط ۱ و ۲ یک کلید عمومی با الگوریتم رمزنگاری که شامل نقش هرکاربر در آن می باشد ساخته می شود. نکته ای که در این مرحله حائز اهمیت می باشد این است که نقشی که به عنوان ورودی از کاربر دریافت می شود در کلید عمومی کاربر گنجانده می شود و در مراحل بعدی نقش هر کلید عمومی(کاربر) توسط شبکه بلاکچین و سازنده های بلوک ها قابل شناسایی می باشد.

۳-۲-۲ تایید هویت[1]

تایید هویت کاربران در شبکه بلاکچین توسط امضای دیجیتال که با استفاده از کلید خصوصی آن ها ساخته می شود، احراز می شود. همانطور که در فصل دوم امضای دیجیتال شرح داده شده گره های شبکه های بلاکچین با استفاده از اعتبار سنجی امضای دیجیتال می توانند صحت امضا و ارسال کننده آن را بررسی کنند. بنابراین تراکنش ها در شبکه بلاکچین از طریق امضاهای دیجیتال تایید می شوند.

الگورتیم های بالا نمایش دهنده روش ساخت پیغام و اعتبار سنجی و صحت تراکنش های ارسالی را نمایش می دهد. یک پیام m می تواند توسط کلید خصوصی امضا شود $m' = sign(m, k_{priv})$. همچنین تایید کننده می تواند با استفاده از کلید عمومی صحبت اعتبار بررسی کند . $verify(m', k_{pub})$ دو فاز جداگانه برای تولید کلید وجود دارد. یکی برای تولید پارامتر های الگوریتمی مشترک (الگوریتم۲) و همینطور فاز دوم (الگوریتم ۳ و ٤) برای استفاده کاربر و تولید امضای دیجیتال مورد استفاده قرار می گیرد.

۳-۲-۲-۱ تولید پارامتر های اشتراکی برای امضای دیجیتال

در الگوریتم ۳-۲ الگوریتم تولید پارامتر های اشتراکی برای امضای دیجیتال نمایش داده شده است.

Algorithm 2: Shared Parameter Generation

Input: *key length L, modulus length N,*

Output: *The algorithm parameters are (p, q, g).*

1 ***Choose an approved hash function H with output length |H| bits. If |H| is greater than the modulus length N , only the leftmost N bits of the hash output are used.***

2 ***Choose a key length L.***

3 ***Choose the modulus length N such that N < L and N ≤ |H|***

4 ***Choose an N bit prime q and L prime p such that p − 1 is a multiple of q.***

5 ***Choose an integer h randomly where 2 ≤ h ≤ p − 2.***

6 ***Compute g*** *= h mod p. If g is 1 try with different h.*

7 ***The algorithm parameters are (p, q, g).***

الگوریتم ۳-۲: الگوریتم تولید پارامتر های اشتراکی برای امضای دیجیتال

[1] Identity Verification

همان طور که در الگوریتم ۳-۲ مشاهده می گردد از این الگوریتم برای تولید پارامتر هایی استفاده می شود که در مراحل بعد تولید امضای دیجیتال استفاده می شود. در الگوریتم ۲ در خط ۱ یک تابع هش تایید شده H با طول خروجی |H| را انتخاب کنید بیت ها اگر |H| بزرگتر از طول مدول N است، فقط از سمت چپ ترین N بیت خروجی هش استفاده می شود. در خط ۲ طول کلید L را انتخاب می شود.در خط ۳ طول مدول N را طوری انتخاب می شود که $N < L$ و $N \leq |H|$. در خط ٤ نیز یک N بیت اول q و L اول p را طوری انتخاب می شود که $p - 1$ مضرب q باشد.در خط ٥ یک عدد صحیح h را به طور تصادفی انتخاب می شود که در آن $h \leq p - 2 \geq ۲$ باشد. در خط ٦ $g = h \bmod p$ محاسبه می شود که اگر g برابر ۱ است است با h دیگری امتحان می شود(تکرار این فرایند). در نهایت پارامترهای الگوریتم (p, q, g) هستند که در این مرحله انتخاب می شود.

۳-۲-۲-۲ ساخت امضای دیجیتال

در الگوریتم ۳-۳ الگوریتم ساخت امضای دیجیتال نشان داده شده است. با توجه به مجموعه پارامترهای مشترک که در الگوریتم ۲ شرح داده شد، در این مرحله جفت کلید را برای یک کاربر محاسبه می شود. همین رویه توسط همه کاربران برای تولید کلیدهای عمومی و خصوصی مربوطه مورد استفاده قرار می گیرد. x کلید خصوصی و y کلید عمومی است. کاربر باید فقط کلید عمومی را منتشر کند و کلید خصوصی را مخفی نگه دارد.

Algorithm 3: Signing Algorithm

***Input**: Message(m)*

***Output**:* The signature is (r, s)

1 ***Choose an integer k such that $1 \leq k \leq q - 1$.***

2 ***Compute $r = (g^k \bmod p) \bmod q$. If r is zero, start with different random k.***

3 ***Compute signature $= (k^{-1}(H(m) + xr)) \bmod q$. If s equals zero, start with different random k.***

الگوریتم ۳-۳: الگوریتم امضای ساخت امضای دیجیتال

همان طور که در الگوریتم ۳-۳ مشاهده می گردد در الگوریتم ۳ کاربر باید پیام m را امضا کند.در خط ۱ یک عدد صحیح k را طوری انتخاب می شود که $k \leq q - 1 \geq ۱$ باشد.در خط ۲ محاسبه $r = (g^k \bmod p) \bmod q$ انجام می شود. اگر r صفر است، با k تصادفی متفاوت شروع می شود. در خط ۳ محاسبه $s = (k^{-1}(H(m) + xr)) \bmod q$ انجام می شود که اگر s برابر با صفر باشد، با k تصادفی متفاوت شروع می شود. در نهایت امضای دیجیتال (r,s) تولید می شود.

۳-۲-۲-۳ الگوریتم بررسی معتبر بودن امضای دیجیتال

در الگوریتم ۳-٤ الگوریتم تایید معتبر بودن امضای دیجیتال نشان داده شده است.

Algorithm 4: Verication Algorithm

***Input**: Signature*

***Output**:* One can verify the signature is a valid signature for message m.

1 ***Verify that 0 < r, s < q.***

2 ***Compute w =*** s^{-1} *mod q.*

3 ***Compute*** $u_1 = H(m).w \bmod q$

4 ***Compute*** $u_2 = r.w \bmod q$

5 ***Compute*** $v = (g^{u_1} g^{u_2} \bmod p) \bmod q$

6 ***The signature is valid if and only if v equals r.***

الگوریتم ۳-٤: الگوریتم بررسی معتبر بودن امضای دیجیتال

همان طور که در الگوریتم ۳-٤ مشاهده می گردد، درالگوریتم ٤ می توان تأیید کرد که امضای (r, s) یک امضای معتبر برای پیام m است. در خط ۱ این الگوریتم $0 < r, s < q$ بررسی می شود. در خط ۲ $w = s^{-1} \bmod q$ محاسبه می شود. همچنین در خط ۳ می شود. $u_1 = H(m)\, w \bmod q$ محاسبه می شود. در خط ٤ $u_2 = r.w \bmod q$ محاسبه می شود و همینطور در خط ۵ هم $v = (g^{u_1} g^{u_2} \bmod p) \bmod q$ محاسبه می شود.در خط ۵ امضا در صورتی معتبر است که v برابر با r باشد.

۳-۳ درخواست سفر توسط مسافر[1]

در الگوریتم ۳-۵ الگوریتم درخواست سفر توسط مسافر نشان داده شده است. در این الگوریتم یک کاربر با نقش مسافر باید درخواست خود را در غالب یک تراکنش در شبکه بلاکچین ارسال کند.

Algorithm 5: Ride Request by passenger

***Input**: , Private Key Rider,Soruce location,Destination location ,Time of request , Fare, Expire Time in mintue*

***Output**: T*ransaction is submitted to blockchain or not

1 ***Message*** ← *create message with source location, destination location, time of request, Expire Time, fare is the offered fare*

2 ***Sign message***← *compute signed message with private key:* $m' = sign(message, private\ key)$

3 ***Submit transaction to blockchain network***

الگوریتم ۳-۵: الگوریتم درخواست سفر توسط مسافر

همانطور که در الگوریتم ۳-۵ مشاهده می گردد، در این مرحله مسافر با استفاده از اطلاعاتی مبدا، مقصد، زمان درخواست هزینه پیشنهادی سفر یک درخواست سفر را در شبکه بلاکچین با ثبت یک تراکنش ثبت می کند. در خط ۱ یک پیغام که شامل اطلاعات مبدا، مقصد، زمان درخواست و تاریخ معتبر بودن

[1] Ride Request

درخواست ساخته می شود . در خط ۲ این پیغام ساخته شده با استفاده از الگوریتم هایی که در مراحل قبلی توضیح داده شد امضای دیجیتالی می شود. اطلاعات موجود در این پیغام برای تمام شبکه قابل مشاهده است و امضای دیجیتال تضمین کننده ی این است که کاربر ارسال کننده پیام همانی می باشد که ادعا می کند. با تعیین مشخصه Expire in minute معتبر بودن درخواست سفر خود را به شبکه اعلام می کند که در مراحل بعد توسط رانندگان و گره های شبکه قابل مشاهده خواهد بود.

۳-٤ ثبت درخواست پیشنهاد انجام سفر توسط راننده[1]

در الگوریتم ۳-٦ الگوریتم ثبت درخواست پیشنهاد انجام سفر که توسط راننده ثبت می شود نشان داده شده است. در این مرحله کاربر با نقش راننده با استفاده از این الگوریتم قادر خواهد بود برای درخوست های موجود در شبکه پیشنهاد انجام سفر ثبت کند.

Algorithm 6: Ride Offer by driver

Input: *Selected Ride Request, Fare , Location*

Output: X ∈ {CONFIRM, ABORT }

```
IF time now is greater than Expire time of ride request
        X ← ABORT
END
If Selected Ride request does not exsist
        X ← ABORT
END
X ← CONFIRM
Message ← create message with Selected Ride Request, Fare , Location
Sign message ← compute signed message with private key
Submit transaction to blockchain network
```

الگوریتم ۳-٦: الگوریتم ثبت درخواست پیشنهاد انجام سفر توسط راننده

همان طور که در الگوریتم ۳-٦ مشاهده می گردد، در این مرحله راننده ها می توانند با جست و جو در اطلاعاتی که به صورت عمومی بر روی شبکه بلاکچین ذخیره شده است درخواست های مسافران را پیدا کنند. سپس بر اساس علاقه به صورت دلخواه می توانند درخواست انجام سفر را بر روی پیشنهادات مسافران ارسال کنند. این درخواست ممکن است بر اساس پارامتر های مثل فاصله مکانی به مسافر ، مقصد دلخواه (راننده ممکن درخواست هایی که به مقصد دلخواه خود نزدیک تر است را انتخاب کند)، هزینه سفر و غیره باشد.

[1] Ride Offer

در خطوط ۱ تا ۳ شبکه با بررسی اینکه آیا درخواست انتخابی توسط راننده در بازه زمانی معتبر می باشد یا خیر از صحت تراکنش مطمئن می شود. در خطوط بین ٤ تا ٦ بررسی می شود که آیا درخواست سفر در گذشته در شبکه بلاکچین ثبت شده است یا خیر. در صورتی که این درخواست ثبت نشده بود درخواست رد می شود. سپس در خطوط بین ۷ تا ۹ در صورتی که این بازه معتبر باشد یک پیغام امضا شده دیجیتالی شامل اطلاعات درخواست انتخاب شده راننده، کرایه و محل سوار شده ساخته می شود و در خط ۱۰ این تراکنش به شبکه ارسال می شود.

۳-۵ تایید کردن یکی از پیشنهاد ها توسط مسافر[1]

در الگوریتم ۳-۷ الگوریتم تایید پیشنهاد که توسط مسافر تایید می شود نشان داده شده است. در این مرحله کاربران با نقش مسافر می توانند از بین پیشنهاد هایی که از سمت رانندگان دریافت کرده اند یکی را بسته به شرایط خود انتخاب کنند. ممکن است شرایط مطلوب برای هر کابر با کاربر دیگر متفاوت باشد که باعث می شود کاربران بر اساس نیاز خود این پشنهادات را بررسی و تایید کنند.

Algorithm 7: Ride Acceptance by passenger

```
    Input: Selected Ride Offer
    Output: x ∈ {CONFIRM, ABORT }
1   IF Ride Offer is not valid for this passenger //check by public key of passenger
2           x ← ABORT
3   END
4   Deposit Token Driver ← LOCK (Driver Publick key, token)
5   Deposit Token Passenger ← LOCK (Passenger Publick key, token)
6   IF Deposit Token Driver = NULL Or Deposit Token Passenger = NULL
7           x ← ABORT
8   END
9   X ← CONFIRM
10  Message ← create message with Selected Ride offer
11  Sign message ← compute signed message with private key
12  Submit transaction to blockchain network
```

الگوریتم ۳-۷: الگوریتم تایید پیشنهاد توسط مسافر

همان طور که در الگوریتم ۳-۷ مشاهده می گردد، در این مرحله مسافر بعد از این تعدادی پیشنهاد از سمت رانندگان دریافت کرده است یکی از پیشنهاد ها را تایید می کند. در این مرحله مسافر به راننده متصل می شود. تا زمان اتمام سفر تنها یک سفر قابلیت تایید شده شدن توسط مسافر را دارد (این مورد

[1] Ride Acceptance

توسط گره ها در شبکه بلاکچین بررسی می شود). توجه داشته باشید که روش انتخاب یک راننده ممکن از است برای هر مسافر متفاوت باشد. به عنوان مثال برخی ممکن است پیشنهادات با قیمت پایین را ترجیح دهند، برخی دیگر ممکن است زمان انتظار و فاصله مکانی را در اولویت انتخاب خود قرار دهند. با این حال تمام این انتخاب ها وابسته به مسافر خواهد بود و شفافیت در این سرویس پیشنهادی افزایش یافته است.

در خطوط بین ۱ تا ۳ ابتدا مسافر معتبر بودن درخواست را با توجه به کلید عمومی راننده ارسال کننده تراکنش بررسی می کند. در خطوط بین ٤ و ٥ سپرده ای از راننده و مسافر دریافت می شود. برای این کار ابتدا موجودی راننده و مسافر در خطوط ٦ تا ٨ بررسی می شود، در صورتی که موجودی برای سپرده گذاری کافی نباشد عملیات متوقف خواهد شد. در خطوط ۹ تا ۱۲ یک پیغام امضا شده دیجیتالی شامل درخواست تایید شده از سمت خود به شبکه ارسال می شود.

٣-٦ مکانیزم پاداش/جریمه برای اثبات رسیدن به مبدا

پرداخت کرایه از جمله مهمترین مشکل اصلی سرویس های اشتراک گذاری سفر می باشد. پرداخت کرایه سفر در سیستم های سنتی حال حاضر وابسته به یک سرویس دهنده مرکزی می باشد. بنابراین راننده در مورد تضمین پرداخت کرایه و مسافر هم در مورد تضمین رسیدن به مقصد به این سرویس دهنده ها اعتماد می کنند. در این سرویس ها عموما متولی مرکزی هزینه کرایه را نزد خود نگه می دارد و پس از اثبات رسیدن به مقصد توافق شده هزینه را به راننده پرداخت می کند. بنابراین این سرویس دهنده ها در قبال دادن این تضمین ها به کاربران، مقدار زیادی از مبلغ سفر(۱۰ الی ۲۰ درصد) را به عنوان کارمزد دریافت می کنند (Huckle et al., 2016)، که همین امر موجب افزایش سرسام آور هزینه سفر می شود. علاوه بر افزایش هزینه سفر برای راننده و مسافر، با این حال این روش اعمالی از سمت آن ها ممکن است عمل نکند چرا که طرفی که رفتار درستی داشته باید تلاش بیشتری را برای متقاعد کردن این سرویس دهنده ها انجام دهد، همچنین روشی که این شرکت ها برای این شرایط دارند به صورت شفاف برای کاربران قابل مشاهده نیست، علاوه بر این نیاز به اشتراک گذاری اطلاعات حساس به ارائه دهنده مرکزی خدمات همیشه نیاز می باشد.

بنابراین هدف از طراحی سیستم های غیر متمرکز مبتنی بر بلاکچین برای سرویس اشتراک گذاری سفر علاوه بر شفافیت عملکرد این سیستم ها، ایجاد بهبودی در هزینه های سفر است. با حل مسئله پرداخت کرایه در سیستمی غیر متمرکز مبتنی بر بلاکچین می توانیم هزینه های سفر در سرویس اشتراک گذاری سفر را به طرز چشم گیری کاهش دهیم. بنابراین پیدا کردن راه حلی برای پرداخت کرایه منصفانه در سیستمی که خودمختار و بدون هیچ مرکزیتی کار می کند را می توان مهمترین چالش برای این سرویس در نظر گرفت.

به طور کلی مهم ترین مشکلی که برای حل مسئله پرداخت کرایه در سیستم های مبتنی بر بلاکچین را می توان به این صورت خلاصه کرد: پرداخت منصفانه در محیط عمومی بلاکچین که تمامی تراکنش ها و اطلاعات آن ها برای عموم موجود می باشد، راهکاری ارائه داد که بدون اعتماد به راننده و مسافر بر اساس رفتار راننده و مسافر پرداخت کرایه را انجام به صورت منصفانه انجام دهد و از تقلب هر یک از طرفین در سیستم جلوگیری کند و در عین حال بتوان بهبودی در هزینه های سفر ارائه داد. هدف اصلی این پایان‌نامه بهبود رویکرد هایی است که برای حل این مسئله ارائه شده اند می باشد.

در ادامه به بررسی مطالعات پیشین و همچنین بهبود هایی که رویکرد ما در این پایان نامه ارائه داده است خواهیم پرداخت.

نویسندگان محمد باز، نورالدین لاسلا، محمد محمود و همکاران (Baza et al., 2019) سیستمی را مبتنی بر بلاکچین با تمرکز بر حریم خصوصی، اعتماد و پرداخت منصفانه پیشنهاد دادند. برای اطمینان از اعتماد بین مسافر و راننده انتخاب شده برای پرداخت منصفانه، یک پروتکل سپرده با زمان قفل شده برای سرویس اشتراک گذاری با استفاده از رویکرد مبتنی بر اثبات دانایی صفر[1] ارائه دادند. در اینجا یک سپرده اولیه توسط هر از طرفین برای پرداخت منصفانه به شبکه انجام می شود. رویکرد اصلی برای تعیین صحت ادعا و پاداش دادن و یا جریمه کردن بر اساس آن به شرح زیر عمل می کند.

۱. یک مسافر باید یک قرارداد هوشمند با سپرده اولیه به عنوان اثبات پذیرش پیشنهاد راننده ارسال کند.
۲. راننده انتخاب شده همچنین باید بودجه ای را به عنوان تعهد به پیشنهاد خود به قرارداد واریز کند.
۳. به محض ورود به محل توافق شده مبدا مسافر، راننده به عنوان (یک اثبات کننده) عمل می کند و یک مدرک برای اثبات رسیدن به محل مبدا به بلاکچین ارسال می کند.
۴. در نهایت، یک قرارداد هوشمند با بررسی اثبات رویکرد مبتنی بر اثبات دانایی صفر به عنوان یک (تأیید کننده) عمل می کند و سپس در صورت اثبات معتبر به راننده پاداش می دهد یا در صورت عدم اعتبار یا عدم ارسال قبل از زمان توافق شده، راننده را جریمه می کند.

همچنین روشی را برای اطمینان از پرداخت منصفانه به روشی بدون اعتماد بین مسافر و راننده پیشنهاد می کنند. راننده باید در یک بازه زمانی معین، مسافت سپری شده را برای مسافر بفرستد که آن را با امضای آن با استفاده از کلید خصوصی خود احراز هویت می کند. سپس، هنگامی که مسافر یک اثبات مسافت سپری شده (یعنی مسافت سپری شده و امضای راننده روی آن) ارائه می کند، قرارداد هوشمند

[1] zero-knowledge set membership proof

کرایه را به راننده منتقل می کند. به این ترتیب راننده هنگام رانندگی با پیمودن مسافتی دستمزد دریافت می کند. در همین حال، اگر مسافر ارسال این تراکنش ها به قرارداد هوشمند (شبکه بلاکچین) را متوقف کند، راننده می تواند بلافاصله سفر را متوقف کند. علاوه بر این، فقط مسافت های سپری شده در بلاکچین ذخیره می شود و هیچ اطلاعات حساس دیگری در اختیار عموم قرار نمی گیرد.

۳-٦-۱ معایب رویکرد ارائه شده در پژوهش B-Ride

در پژوهش ذکر شده و پژوهش های مشابه وابستگی سرویس به سیستم مرکزی دیگر از دلایل عدم امکان استفاده از این رویکرد ها برای ارائه سرویس اشتراک گذاری سفر شده است.

وابستگی به اثبات کننده ی مکان به محض ورود راننده به مبدا سفر توافق شده (مرحله سوم)، باید یک اثبات طریق یک اثبات کننده ی مکان به شبکه بلاکچین ارسال کند. عموما یک اثبات کننده مکان واحد های کنار جاده ای می باشد که قبلا برای فعال کردن شبکه های وسایل نقلیه مستقر شده اند.با توجه به این در بسیاری از نقاط کشور ها این واحدها وجود ندارند، وابستگی به این واحد های کنار جاده ای چالش بزرگی است و عملا باعث می شود در بسیاری از نقاط و کشور ها این سرویس غیر قابل استفاده باشد.

۳-٦-۲ تشریح مراحل پیشنهادی جهت از بین بردن وابستگی به اثبات کننده ی مکان

برای مقابله با این مشکل نیاز به رویکردی داریم که از تقلب هر یک از دو طرفین جلوگیری کنیم.همچنین رویکرد ارائه شده باید در مقابل رفتار بدافزار ها نیز مقاوم باشد (به این دلیل که در محیط عمومی بلاکچین هر کسی توان این را دارد که یک کاربر راننده یا مسافر ایجاد کند و در سیستم اختلال ایجاد کند) ابتدا برای بررسی بیشتر موضوع، تمام حالت هایی که ممکن است در این حالت رخ دهد را به شرح زیر لیست می کنیم :

۱. هیچ یک از طرفین به مبدا نرسند یا از ارسال اثبات رسیدن خودداری کنند.
۲. راننده به مبدا سفر برسد، مسافر به مبدا نرسد یا از ارسال اثبات رسیدن خودداری کند.
۳. مسافر به مبدا سفر برسد، راننده به مبدا نرسد یا از ارسال اثبات رسیدن خودداری کند.

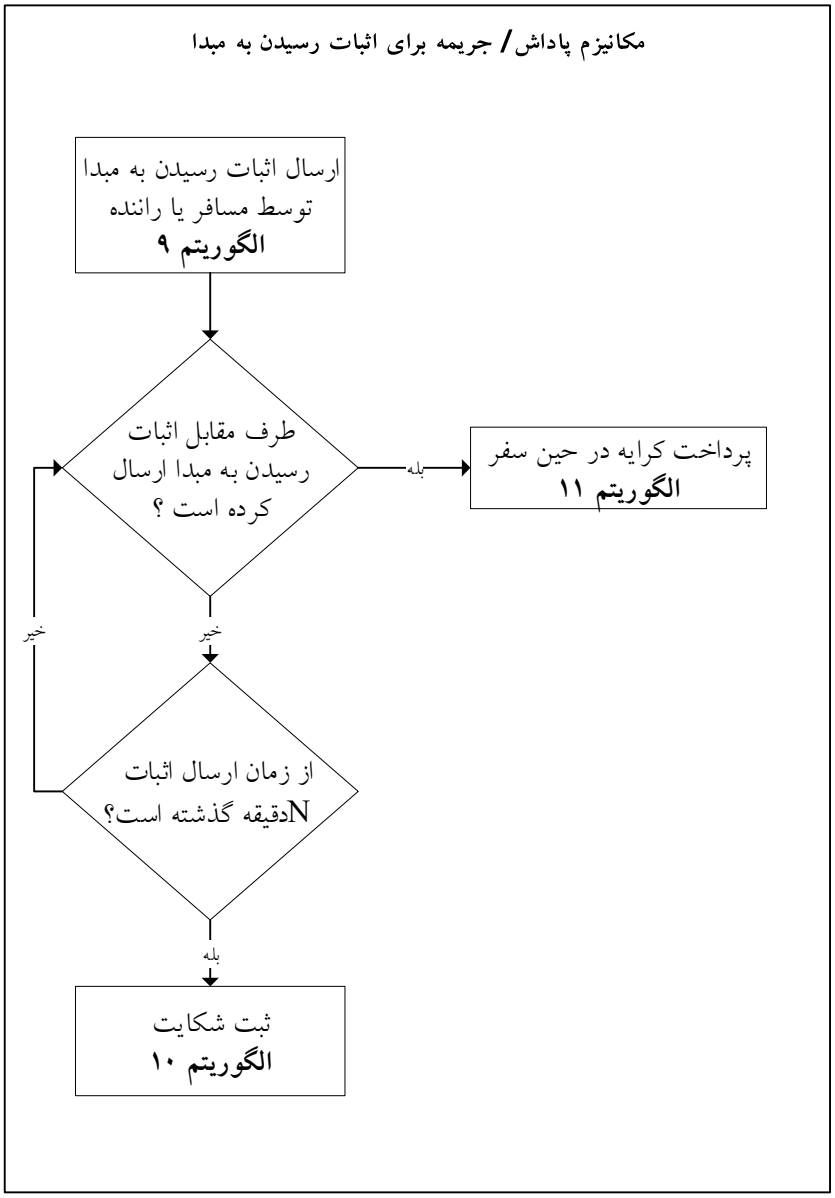
نکته : راننده و مسافر یک سپرده قبل از این مرحله در شبکه بلاکچین ثبت کرده اند (قفل کرده اند).

در حالت شماره ۱، تمام سپرده ی قفل شده مسافر و راننده در شبکه باقی می ماند.(در صورتی که در آینده یکی از کاربران راننده یا مسافر اثباتی برای رسیدن به مبدا ارسال کند حالت های شماره ۲ و ۳ پیش می آید که در ادامه توضیح خواهد داده شد.). ضمنا در این حالت هیچ کاربر مخرب یا بدافزاری نمی تواند در سیستم اختلال ایجاد کند چرا که شرکت در این فرایند نیاز به ثبت سپرده دارد.

حالت شماره ۲ و۳ زمانی پیش می آید که یکی از طرفین به مبدا نرسند و یا از ارسال اثبات رسیدن به مبدا به شبکه بلاکچین خودداری کنند(رفتار مخرب برای ایجاد اختلال در سیستم توسط کاربر مخرب)

و طرف مقابل اثبات رسیدن به مبدا ارسال کرده است. برای حل این مشکل در این حالت ها از یک مکانیزم به نام پاداش/ جریمه برای اثبات رسیدن به مبدا که در شکل ۳-۲ نشان داده شده است استفاده می کنیم.

پس از اینکه طرف اول اثبات رسیدن به مبدا (راننده یا مسافر) در شبکه ثبت شد طرف مقابل در مدت زمان توافق شده (که قبل از این مرحله در شبکه بلاکچین ثبت شده است) فرصت دارد تا اثبات رسیدن خود به مبدا رو ارسال کند و سفر شروع شود در غیر این صورت طرف اول ارسال کننده می تواند درخواست شکایت ثبت کند.



شکل ۳-۲: فلوچارت پاداش/ جریمه برای اثبات رسیدن به مبدا

همان طور در شکل ۲-۳ مشاهده می گردد، مکانیزم پاداش/جریمه برای رسیدن به مبدا از طریق ارسال اثبات رسیدن به مبدا شروع می شود. بنابراین این مکانیزم همیشه از طریق ارسال اولین اثبات به شبکه بلاکچین شروع می شود. سپس پس از بررسی اثبات رسیدن به مبدا طرف مقابل، در صورتی طرف مقابل نیز اثبات رسیدن به مبدا را به شبکه ارسال کرده باشد مکانیزم پاداش/ جریمه فرایند به بخش پرداخت کرایه در حین سفر که در بخش ۳-۸ توضیح داده شده است انتقال می یابد. در صورتی که طرف مقابل اثبات رسیدن به مبدا را ارسال نکرده باشد و همچنین از مدت زمان مشخصی گذشته باشد (زمان توافق شده) طرف مقابل می تواند با ارسال تراکنش ثبت شکایت مکانیزم جریمه برای طرف مقابله خود را فعال کند. در ادامه به تشریح هر یک از الگوریتم های این فلوچارت خواهیم پرداخت.

۳-٦-۲-۱ ارسال اثبات رسیدن به مبدا توسط مسافر یا راننده

در الگوریتم ۳-۸ الگوریتم ارسال اثبات رسیدن به مبدا نشان داده شده است که در این الگوریتم راننده و یا مسافر در زمان رسیدن به مبدا با ارسالی تراکنشی حضور خود در مبدا را به شبکه اطلاع می دهند.

Algorithm 8: Prove arrived to origin location

```
    Input: Selected Ride Offer
    Output: x ∈ {CONFIRM, ABORT}
1   IF Ride Offer is not valid for this passenger // check by public key of passenger
2           x ← ABORT
3   END
4   IF Has proof of origin been sent before?
5           x ← ABORT
6   END
7   X ← CONFIRM
8   Message ← create message with Selected Ride offer
9   Submit transaction to blockchain network
```

الگوریتم ۳-۸ الگوریتم ارسال اثبات رسیدن به مبدا

همان طور که در الگوریتم ۳-۸ مشاهده می گردد، در الگوریتم در خطوط بین ۱ تا ۳ راننده یا مسافر پس از رسیدن به مبدا سفر، اثبات رسیدن به مقصد را به شبکه بلاکچین ارسال می کند.سپس در خطوط بین ٤ تا ۷ بررسی می شود که آیا کاربر جاری قبلا یک تراکنش ارسال کرده است یا خیر، در صورتی که ثبت کرده باشد عملیات لغو خواهد شد.در خطوط ۷ تا ۹ تراکنش در شبکه بلاکچین با موفقیت ثبت می شود.

۳-٦-۲-۲ ثبت شکایت توسط مسافر یا راننده

در الگوریتم ۳-۹ الگوریتم ارسال ثبت شکایت با کاربری نقش راننده یا مسافر نشان داده شده است که در این الگوریتم بر اساس شرایط خاصی کاربران می توانند در شبکه بلاکچین از عدم حضور یا عدم ارسال اثبات طرف مقابل شکایتی را ثبت کنند.

Algorithm 9: Complain

```
    Input: Selected Ride Offer
    Output: x ∈ {CONFIRM, ABORT }
1   IF Has the other party sent proof of reaching the origin?
2           x ← ABORT
3   END
4   IF minutes have passed  < Agreed waiting minutes
5           x ← ABORT
6   END
7   X ← CONFIRM
9   Message ← The other party is fined.
10  Submit transaction to blockchain network
```

الگوریتم ۳-۹: الگوریتم ثبت شکایت

همان طور که در الگوریتم ۳-۹ مشاهده می گردد، در این الگوریتم برای ثبت شکایت توسط هر یک از طرفین نیاز است ابتدا بررسی شود که آیا طرف مقابل(راننده یا مسافر) اثبات رسیدن به مبدا را ارسال نکرده است. در صورتی که طرف مقابل این اثبات به شبکه بلاکچین ارسال کرده باشد شکایت رد می شود (خطوط بین ۱ تا ۳). سپس در مرحله بعد بررسی می شود که از زمان ارسال اثبات توسط کاربر فعلی بیشتر از مدت زمان توافق شده گذشته است یا خیر. در صورتی که بیشتر از این مدت زمان نگذشته باشد شکایت لغو می شود خطوط بین ٤ تا ٦. در ادامه در شکایت با موفیت ثبت می شود و طرف مقابل جریمه می شود و مبلغی به عنوان جریمه از حساب ان کسر می گردد.

مکانیزیم ارائه شده در این پایان‌نامه این تضمین را می دهد که هر دو طرفین سفر(راننده و مسافر) بدون وجود یک مرکزیت واحد رفتار درستی داشته باشند و در صورت تخلف طرفین جریمه می شوند. همچنین این رویکرد از حمله بدافزار ها و کاربران مخرب در سیستم جلوگیری می کند چرا که هر گونه رفتار مخرب در سیستم دچار جریمه خواهد شد و این مقرون به صرفه برای اختلال در سیستم نیست.

۳-۷ پرداخت کرایه توسط مسافر در حین سفر[1]

در الگوریتم ۳-۱۰ الگوریتم پرداخت کرایه که در حین سفر نشان داده شده است. این فرایند زمانی به کار می رود که در زمان طی مسیر در حین سفر نیاز به رویکردی داریم که بر بدون استفاده از اعتماد راهکاری امن برای پرداخت ارائه دهد.

Algorithm 10: Ride Payment

Input: *Driver Address, Distance from destination*

Output: x ∈ {CONFIRM}

1 ***WHILE*** *(The passenger has not reached the destination) //during the ride*

2 ***Distance*** ← *Compute distance between the current location and the destination*

3 ***Sign Distance*** ← *compute signed distance with private key*

4 ***Submit transaction to blockchain network***

5 **X** ← *CONFIRM*

6 ***END***

الگوریتم ۳-۱۰: الگوریتم پرداخت کرایه توسط مسافر در حین سفر

همان طور که در الگوریتم ۳-۱۰ مشاهده می گردد، برای حل این مشکل سرویس اشتراک گذاری سفر یک سپرده از راننده و مسافر دریافت می کند. اگر راننده با موفقیت سفر را به اتمام برساند و به محل توافق شده برسد تمام کرایه به او توسط سیستم پرداخت می شود. توجه داشته باشید که تمام این رویکرد در شبکه بلاکچین انجام خواهد شد. به طور خلاصه، بعد از انتخاب یک پیشنهاد توسط مسافر، راننده ای که این پیشنهاد را ارسال کرده است باید در زمان سفر مسافت طی شده را تا مقصد را اثبات کند. برای اثبات این موضوع از الگوریتم بالا استفاده می شود.

خطوط بین ۱ تا ٦ در این الگوریتم در تمام مدت سفر در بازه های زمانی اجرا می شوند. بنابراین این حلقه ای می باشد که در تمام طول سفر تا زمانی که مسافر به مقصد برسد اجرا می شود. بنابراین شرطی که باعث پایان یافتن این حلقه می شود این است که مسافر به مقصد برسد.در خط ۲ مسافت طی شده ای که از مکان حاظر تا مقصد باقی مانده است محاسبه می شود و به صورت یک عدد محاسبه می شود. سپس در خط ۳ و ٤ پیغامی شامل این مسافت وبا استفاده از کلید خصوصی مسافر (توسط مسافر) به شبکه ارسال می شود. شبکه پس از تایید مسافت طی شده مبلغی بر اساس همین پارامتر به راننده پرداخت

[1] Ride Payment

می کند. در این رویکرد در صورتی که مسافر از ارسال اثبات مسافت طی شده خودداری کند راننده می تواند از ادامه سفر جلوگیری کند و سفر را متوقف کند.

۳-۸ خلاصه فصل

در فصل سوم به تشریح کامل روش پیشنهادی سرویس اشتراک گذاری سفر مبتنی بر بلاکچین با ارائه جزئیات مربوط به هر قسمت همراه با تشریح کامل فلوچارت روش مطرح شده پرداخته شده است. همچنین فلوچارت روش پیشنهادی مکانیزم پاداش جریمه برای اثبات رسیدن به مقصد نیز پرداخته شده است. روش پیشنهاد شده باعث از بین بردن وابستگی این سرویس ها به یک اثبات کننده مکان شده است که این رویکرد باعث استفاده بهتر و بهینه تر از این سرویس می شود.

فصل ٤ تجزیه و تحلیل یافته ها

٤-١ مقدمه

در فصل ٤ ابتدا به بررسی ابزار های مورد نیاز برای شبیه سازی پرداخته می شود، سپس مشخصات سیستم مورد نیاز جهت پیاده سازی روش پیشنهادی را معرفی می شود. تشریح مجموعه داده ها[1] که برای شبیه سازی روش پیشنهادی مورد استفاده قرار گرفته است پرداخته می شود. سپس معیارهایی که برای ارزیابی روش پیشنهادی سرویس اشتراک گذاری سفر مبتنی بر بلاکچین ارائه می شود. همچنین در ادامه به جمع بندی تجزیه و تحلیل یافته ها خواهیم پرداخت.

در پژوهش B-Ride برای پیاده سازی سرویس اشتراک گذاری سفر مبتنی بر بلاکچین از شبکه اتریوم استفاده شده است (Baza et al., 2019). در این پژوهش برای اطمینان از صحت مکان گزارش شده مبدا توسط رانندگان از یک اثبات کننده مکان (LP[2]) استفاده می شود. در این روش، راننده به محض رسیدن به یک مکان خاص، باید مکان فعلی خود را از طریق یک اثبات کننده مکان به بلاکچین ارسال کند. در روش ما برای پیاده سازی سرویس اشتراک گذاری سفر مبتنی بر بلاکچین از یک الگوریتم تحت عنوان مکانیزم پاداش/ جریمه برای اثبات رسیدن به مبدا استفاده می کنیم که باعث حذف وابستگی به این واحد های سخت افزاری می شود. همین امر باعث بهبود سرویس اشتراک گذاری سفر می شود که منجر به استفاده بهینه تر از این سرویس خواهد شد، چرا که رویکرد اصلی شبکه های مبتنی بر بلاکچین ارائه سرویس هایی می باشد که بدون وابستگی به واحد های مرکزی عمل کنند.

٤-٢ ابزار شبیه سازی

روش پیشنهادی در این پژوهش با استفاده از ابزارهایی که در ادامه معرفی خواهد شد شبیه سازی شده است. زبان برنامه نویسی استفاده شده در این پژوهش #C می باشد. زبان برنامه نویسی #C برای بسیاری از انواع نرم افزار ها از جمله وب سایت ها، سیستم های مبتنی بر فضای ابری[3]، دستگاه های IOT4[4]،

[1] DataSet
[2] Location Prover
[3] Cloud-based systems
[4] Internet of Things

برنامه های موبایل، بازی ها و ابزار های خط فرمان[1] استفاده می شود.#C با پشتیبانی از کتابخانه ها و ابزار های که در مجموع Net. شناخته می شوند، یک پلتفرم چند سکویی [2] و متن باز[3] ارائه می دهد که زبان #C را قادر می سازد تا بر روی سیستم عامل های مختلف از جمله اندروید، IOS ، MacOS و لینوکس به مانند ویندوز اجرا شود (Ian Griffiths, 2022).

برای شبیه سازی اطلاعات موجود در شبکه بلاکچین از دیتابیس های Redis وSQL Server می شود. با توجه به این که اطلاعات موجود در دیتابیس SQL به صورت دائمی ذخیره می شود هر زمانی که نیاز به ذخیره اطلاعات بلوک ها و تراکنش ها می باشد از این دیتابیس استفاده می شود. برای زمانی که نیاز به دستیابی سریع به اطلاعات می باشد از دیتابیس Redis استفاده می شود به این دلیل که اطلاعات ذخیره شده در دیتابیس Redis در رم دخیره می شود و قابلبیت ذخیره سازی و خواندن اطلاعات سریع را به ما می دهد.

همچنین برای شبیه سازی از یک پروژه WebApi استفاده می شود که هر یک از مراحل و الگوریتم ها به صورت یک Http Method می باشد. IDE[4] استفاده شده در این پروژه ویژال استدیو ۲۰۲۲ [5]می باشد. کد منبع شبیه سازی انجام شده بر روی سورس کنترل گیت هاب[6] به آدرس زیر قابل دریافت خواهد بود.

https://github.com/MehranMazhar/node-clutch-gateway

٤-٣ مشخصات سیستم پیاده سازی

در جدول ٤-١ مشخصات مربوط به سیستمی که پیاده سازی روش پیشنهادی و ارزیابی نتایج در آن انجام شده نشان داده می شود.

جدول ٤-١ : مشخصات سیستم جهت شبیه سازی و ارزیابی نتایج

سخت افزار / نرم افزار	مشخصات
سیستم عامل	ویندوز 11 ، 64 بیتی
حافظه RAM	36 گیگابایت – 30 گیگ قابل استفاده
پردازنده	پردازنده اینتل – تعداد هسته‌ها 7 Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz (8 CPUs), ~4.2GHz
IDE	Visual Studio 2022
نوع پرژوه	Web API

[1] Command-line utilities
[2] Cross Platform
[3] Open Source
[4] Integrated development environment
[5] Visual Studio 2022
[6] GitHub

همان طور که در جدول ٤-١ مشاهده می گردد، سیستم عامل استفاده شده در این پژوهش ویندوز ١١، نوع سیستم عامل نیز سیستم عامل ٦٤ بیتی، حافظه رم استفاده شده ٣٢ گیگابایت، پردازنده اینتل Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz (8 CPUs), ~4.2GHz می باشد.

بنابراین با توجه به یک سیستم با مشخصات فوق شبیه سازی مربوطه انجام شده و نتایج ارزیابی شده است. لذا در همین بخش به صورت کامل نتایج بدست آمده تشریح می‌گردد.

٤-٤ مجموعه داده ها

مجموعه داده ها در سرویس اشتراک گذاری سفر متشکل از اطلاعات سفر می باشد. در جدول ٤-٢ ویژگی های مجموعه داده در سرویس اشتراک گذاری سفر نشان داده شده است.

جدول ٤-٢ : ویژگی های مجموعه داده ها در سرویس اشتراک گذاری سفر

ویژگی	نمونه داده	توضیحات
مبدا	٤٩.٧٧١٨ , ٣٥.٣٦٦٩	مختصات جغرافیایی مبدا
مقصد	٤٩.٨٢٠٩ ,٣٥.٣٩٧٠	مختصات جغرافیایی مقصد سفر
تاریخ درخواست سفر	٢٠٢٢-١١-٢٤	تاریخی که مسافر درخواست سفر ثبت کرده است.
کرایه پیشنهادی مسافر	٤٥٠٠٠	مبلغ پیشنهادی مسافر برای سفر
وضعیت راننده	{UA-A}	وضعیت UA: فعال وضعیت A: غیر فعال
محل راننده فعال	٤٩.٧٦٣٣ ,٣٥.٣٦٨١	محلی که راننده فعال درخواست سفر ارسال می کند.
پیشنهاد سفر	(F , L)	F: هزینه پیشنهادی L: محل مبدا
پیشنهاد سفر تایید شده	١٠٠٠١٢٥٤٤	شناسه پیشنهاد سفر تایید شده
اثبات رسیدن به مبدا	{CONFIRM, ABORT}	وضعیت ثبت ارسال رسیدن به مبدا
ثبت شکایت	{CONFIRM, ABORT}	وضعیت ثبت شکایت رسیدن به مبدا
مسافت طی شده در طول سفر	١٠٢٥٥	مسافت طی شده ازمبدا به مقصد بر اساس متر

همان طور که در جدل ٤-٢ مشاهده می گردد، در این جدول ویژگی های یک سفر شرح داده شده است. اطلاعات سفر از جمله مبدا، مقصد و ... در تراکنش های ثبت شده در بلاکچین ذخیره می شوند. هر یک از این اطلاعات پس از اعتبار سنجی و اجرا در یکی از الگوریتم ها توسط مسافر یا راننده در شبکه بلاکچین ذخیره می گردد.

٤-٥ معیار های ارزیابی

معیارهای ارزیابی تعیین کننده متغیر هایی می باشند که به علاوه بر کاهش هزینه سفر و سرعت به حفظ شفافیت و امنیت به کاربران کمک می کند. این معیار های ارزیابی برای سرویس های اشتراک گذاری سفر تشریح می گردد.

٤-٥-١ معیار هزینه تراکنش و هزینه اجرا

هنگامی که تراکنش ها در شبکه بلاکچین اجرا می شوند، وضعیت بلاکچین را تغییر داده و منابع بلاکچین را مصرف می کنند. از انجایی که منابع در دسترس برای یک بلاکچین محدود است، مدیریت نحوه مصرف منابع مهم است. منابع بلاکچین از نظر مانند ظرفیت ذخیره سازی و ظرفیت اجرا محدود است می همین عامل می تواند شبکه را در برابر حملات مخرب کاربر آسیب پذیر کند. یکی از روش های محافظت از شبکه هزینه ترکنش و هزینه اجرا می باشد.

در سرویس اشتراک گذاری سفر متمرکز [1]هزینه متغیری می باشد که بخشی از کرایه پرداختی مسافر به راننده به عنوان کارمزد دریافت می شود. این هزینه باعث افزایش هزینه سفر می شود چرا که این مقدار به عنوان کارمزد به ارائه کنندگان این سرویس ها پرداخت می شود. در سرویس اشتراک گذاری سفر مبتنی بر بلاکچین به این دلیل که تمام سیستم به صورت خودمختار و غیر متمرکز[2] کار می کند این هزینه شامل هزینه پرداختی کاربران به عنوان کارمزد شبکه در هنگام ثبت تراکنش ها می باشد. در شبکه های بلاکچین مبتنی بر اتریوم هزینه تراکنش ها با فرمول زیر محاسبه می شود.

$$Transaction\ Fee\ (Gwei) = Gas\ Price\ \times\ Gas\ Cost$$
$$1\ \text{ETH} = 1193\ \text{USD}$$
$$12\ (Gwei) \times\ 21000\ (Gas) =\ 252{,}000\ Gwei$$
$$252{,}000\ Gwei * 0.00000000128 =\ 0.00032256\ ETH$$
$$0.00032256\ ETH * 1193 =\ 0.38481408\ USD$$

همان طور که در رابطه بالا مشاهده می گردد، هزینه کارمزد تراکنش حاصل ضرب هزینه گس(Gas Price) در مقدار گس خرج شده (Gas Cost) در آن تراکنش می باشد. هزینه یک گس مقداری می باشد که ثبت کننده تراکنش برای تراکنش خود ثبت می کند. مقدار گس خرج شده نیز متغیری می باشد که میزان هزینه محاسباتی از منابع اجرا کننده EVM[3] را محاسبه می کند. در واقع با کمک این متغیر میزان منابع استفاده شده برای این تراکنش صرفه نظر از قیمت اتریوم محسابه می شود. گره های شبکه های بلاکچین همیشه بالاترین تراکنش هایی که هزینه گس بیشتری دارند را انتخاب می کنند به طور مثال

[1] Centralized
[2] Decentralized
[3] Ethereum Virtual Machine

ثبت تراکنش انتقال در شبکه بلاکچین معادل 21000 GWEI می باشد. بنابراین اگر هزینه گس در حال حاضر عدد ۱۱ باشد. هزینه تراکنش به صورت زیر محاسبه می گردد. در این رابطه قیمت اتریوم ۱۱۹۳ دلار در نظر گرفته شده است. بنابراین هزینه محاسبه شده برای تراکنش ۰.۳۸٤۸۱٤۰۸ دلار خواهد بود.

هزینه ها در شبکه بلاکچین اتریوم بر مبنای گس و به صورت زیر طبقه بندی می شود:

- هزینه تراکنش[1]: هزینه ارسال قرارداد هوشمند به شبکه بلاکچین می باشد که شامل هزینه پایه، سایز قرارداد هوشمند، هزینه فضای ذخیره شده اختصاصی به ازای بایت.
- هزینه اجرا[2]: برای اجرای کد در شبکه بلاکچین صرف می شود توسط ماشین مجازی اتریوم[3].
- هزینه ذخیره سازی[4]: هزینه ذخیره سازی داده ها در شبکه بلاکچین

٤-٥-٢ معیار تعداد تراکنش در ثانیه (TPS[5])

در شبکه های بلاکچین، هر تراکنش دارای هزینه (کارمزد) می باشد که به سازنده بلوک تعلق می گیرد. در سرویس اشتراک گذاری سفر، کارمزد تراکنش نقش مهمی دارد. رانندگانی که کارمزد تراکنش بالاتری دارند، شانس انتخاب تراکنش خود را افزایش می دهند. این به انتخاب رانندگانی کمک می کند که در مورد تمایل خود به انجام سفر صادقانه تر باشند. بنابراین از رفتار کاربران مخرب در سیستم جلوگیری می شود.

سرعت اجرای عملیات ها در سرویس اشتراک گذاری سفر مبتنی بر سرعت ثبت تراکنش ها توسط گره های شبکه بلاکچین می باشد. در زمانی که گره های شبکه بلاکچین تراکنش هایی را انتخاب می کنند که هزینه تراکنش بیشتری پرداخت می کنند.

$$Number\ of\ transactions\ per\ block = \frac{GasLimit}{Gas\ Cost}$$

$$TPS\ (transactions\ per\ second) = \frac{transactions\ per\ block}{Avrage\ block\ time\ in\ seconds}$$

$$Number\ of\ transactions\ per\ block = \frac{30000000}{21000}$$

$$TPS = \frac{1428.571428571429}{12} = 119$$

همانطور که در رابطه بالا مشاهده می گردد، سرعت ثبت تراکنش ها از طریق این رابطه محاسبه می گردد. GasLimit به حداکثر اندازه یک بلوک یا به حداکثر گس قابل ثبت در یک بلوک اشاره می کند که در

[1] Transaction Cost
[2] Execution cost
[3] Ethereum Virtual Machine
[4] Storage cost
[5] Transaction Per Second

زمان نوشته شدن این مطلب این مقدار در شبکه اتریوم ۳۰ میلیون گس می باشد. TPS واحد ثبت تراکنش در ثانیه می باشد. برای به دست آوردن این مقدار نیاز به محاسبه تعداد تراکنش ها در یک بلوک داریم.در مثال بالا حداقل میزان مورد نیاز برای تراکنش انتقال وجه در شبکه اتریوم ۲۱۰۰۰ می باشد. همچنین میانگین زمان ساخته شدن بلوک ۱۲ ثانیه می باشد. بنابراین تعداد تراکنش قابل ثبت در این شبکه ۱۱۹ تراکنش در ثانیه می باشد. انتخاب هزینه گس (Gas Cost) برای کاربران معمولا از طریق امار های موجود در اخرین تراکنش های ثبت شده بر روی شبکه بلاکچین انجام می شود.

٤-٥-٣ معیار وابستگی به اثبات کننده مکان

اثبات کننده مکان واحدهای کنار جاده که در نقاط ثابت و دارای ارتباطات رادیویی هستند. RSU [1]ها در امتداد جاده ها با حفظ فواصل معین قرار می گیرند. آنها برای کمک به پروتکل های ارتباطی خودرو طراحی شده اند.

وابستگی سرویس های اشتراک گذاری سفر به این واحد ها در زمان ورود رانند و مسافربه مبدا سفر می باشد. در این زمان واحد های کنار جاده ای می توانند اثبات رسیدن به مبدا هر یک از طرفین را برای شبکه بلاکچین محرز کنند، اما همین وابستگی به این واحد ها باعث ایجاد محدودیت هایی برای سرویس اشتراک گذاری سفر می شود. چرا که خطا یا رفتار مخرب یا قطعی این واحد ها کل شبکه بلاکچین تحت تاثیر قرار می دهد.

٤-٥-٤ معیار شفافیت

در سرویس اشتراک گذاری سفر بسیاری از کاربران از چگونگی عملکرد این سرویس ها بی اطلاع هستند. به عنوان مثال کاربران در مورد علت افزایش قیمت ها بی اطلاع هستند.بنابراین شفافیت عملکرد سیستم و روش قیمت گذاری در این سرویس ها وجود ندارد. در سرویس اشتراک گذاری سفر مبتنی بر بلاکچین اطلاعات قیمت گذاری در شبکه بلاکچین به صورت عمومی ثبت می شود بنابراین شفافیت در این سرویس ها ایجاد می شود.

٤-٥-٥ معیار غیرمتمرکز سازی

بخش مهمی از سرویس اشتراک گذاری سفر عملکرد مستقل و خودمختار این سرویس ها می باشد. این سرویس ها نباید بر اساس اعتماد به یک موجودیت عمل کنند چرا که هر موجودیت متمرکزی ممکن است عملکرد مخربی داشته باشد و تمام سرویس را دچار اختلال کنند. با استفاده از فناوری بلاکچین این سیستم قادر خواهد بود توسط جامعه غیر متمرکزی از کاربران اداره شود.

٤-٥-٦ پرداخت منصفانه

[1] Road Side Unit

پرداخت عادلانه بین مسافر و راننده متغیری در سرویس اشتراک گذاری سفر می باشد که باید برای هر دو طرف تامین شود. پرداخت باید با روشی بدون اعتماد به یکدیگر انجام شود تا از فعالیت کاربران مخرب در سیستم جلوگیری شود.

٤-٦ ارزیابی نتایج پیشنهادی

سرویس های اشتراک گذاری سفر را می توان در سه دسته سرویس های متمرکز، سرویس های همتا به همتا و سرویس های مبتنی بر بلاکچین مورد ارزیابی قرار داد که به ترتیب به ارزیابی این نتایج خواهیم پرداخت.سرویس های اشتراک گذاری فعلی به شدت به یک سرویس ثالث وابسته می باشد. این وابستگی مربوط به انجام تمام فرآیند ها از جمله رزرو و مدیریت پرداخت می باشد. استفاده کنندگان از این سرویس ها هیچ نقشی برای تعیین سیاست هایی که از طرف این شرکت های متمرکز ایجاد می شود ندارند. بنابراین مرجع متمرکز سیاست های قیمت گذاری و خدمات را تعیین می کنند که همین امر موجب مشکلاتی از جمله عدم شفافیت، خطای بیشتر، حریم خصوصی و امنیت را ایجاد می کند.

سرویس اشتراک گذاری ارائه شده در این پایان نامه مبتنی بر یک شبکه بلاکچین می باشد. استفاده از شبکه بلاکچین به عنوان هسته مرکزی این سرویس امکان ارائه راه حل هایی مبتنی بر بلاکچین که مشکلات سرویس های متمرکز و همتا به همتا را حل می کند را می دهد.

٤-٦-١ مقایسه هزینه تراکنش و اجرا

جدول ٤-٣ مقایسه ای از هزینه های صرف شده برای هزینه تراکنش، هزینه اجرا برای سرویس های اشتراک گذاری سفر را نشان می دهد.

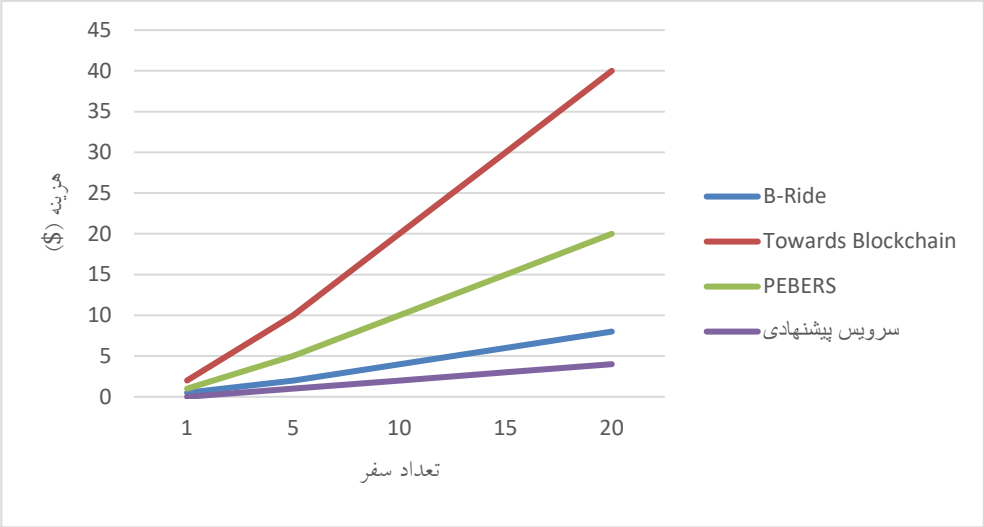
جدول٤-٣: مقایسه ای از هزینه های صرف شده در سرویس های اشتراک گذاری سفر

سرویس	شبکه	قرارداد(های) هوشمند	هزینه تراکنش	هزینه اجرا	مجموع
B-Ride	Ethereum	Bidding Contract Time-locked Deposit Payment	1,660,000 (Gwei)	1,100,000 (Gwei)	2,760,000 (Gwei)
Towards Blockchain	Ethereum	Deposit Contract Payment Contract	4,580,000 (Gwei)	3,250,000 (Gwei)	7,830,000 (Gwei)
Block-V	Ethereum	Block-v Contract	1,561,271 (Gwei)	171,122 (Gwei)	1,732,393 (Gwei)
PEBERS	Ethereum	CreateRide Authentication Registration	2,026,443 (Gwei)	1,165,931 (Gwei)	3,192,374 (Gwei)
سرویس پیشنهادی	Substrate Parachian	Node-Clutch Pallet	0	1,464,000 (Gwei)	1,464,000 (Gwei)

همان طور که در جدول ٤-٣ مشاهده می گردد، هزینه صرف شده در شبکه بلاکچین از مجموع هزینه تراکنش به علاوه هزینه اجرا تشکیل می شود. در شبکه بلاکچین اتریوم هزینه تراکنش شامل هزینه پایه ثابت، هزینه انتشار قرار هوشمند و هزینه فضای گرفته شده بر اساس بایت می باشد. همچنین هزینه اجرا مربوط به اجرای کد های سرویس اشتراک گذاری سفر که در شبکه اتریوم EVM نام دارد می شود.

در روش پیشنهادی ارائه شده در این پایان نامه هزینه تراکنش حذف شده است. در این سرویس شبکه سفارشی شده ای بلاکچین خاصی برای برای سرویس اشتراک گذاری سفر ارائه شده است. در این شبکه ارائه شده تمامی الگوریتم های مورد استفاده در این سرویس از پیش در شبکه تعیین شده شده است.بنابراین به ازای هر سفر نیازی به انتشار یک قرارداد هوشمند در شبکه بلاکچین نیست. این هزینه برای شبکه های بلاکچین عمومی مثل اتریوم که بر اساس قراردهای هوشمند کار می کنند.

در شکل ٤-١ نمودار میانگین هزینه صرف شده برای رویه های هزینه راننده را نشان می دهد.



شکل ٤-١: نمودار هزینه صرف شده برای راننده در تعداد سفر

همان طور که در نمودار ٤-١ مشاهده می گردد، هزینه صرف شده برای راننده نشان داده شده است. در شکل برای هزینه های صرف شده سرویس هایی با هسته شبکه اتریوم B-Ride,Toward Blockchain,PEBERS برای هزینه گس ٥ در نظر گرفته شده است. همچنین برای مقایسه بهتر قیمت ها بر اساس مبلغ اتریوم 217 دلار در تاریخ 02-12-2022 در نظر گرفته شده است.

٤-٦-٢ هزینه وابستگی به به اثبات کننده مکان

در روش ارائه شده در این پایان نامه وابستگی به اثبات کننده مکان توسط یک مکانیزم جایگزین شده است. در جدول ٤-٤ مقایسه ای از مکانیزم های ارائه شده برای سرویس اشتراک گذاری سفر نمایش داده شده است.

جدول ٤-٤: مقایسه ای از مکانیزم های ارائه شده Matchmaking سرویس های اشتراک گذاری سفر

سرویس	مکانیزم **Matchmaking**
B-Ride	Location Prover (Vanet)
PEBERS	Fog Node
سرویس پیشنهادی	مکانیزم پاداش/ جریمه

همان طور که در جدول ٤-٤ مشاهده می گردد، مکانیزم های ارائه شده در این پژوهش ها وابسته به واحد هایی می باشند که ارائه این سرویس ها در محیط هایی که این وابستگی ها را دارند دچار هزینه بیشتری می کنند. علاوه بر هزینه عملا این سرویس ها در محیط هایی کار می کنند که فقط این واحد ها وجود دارند. هر گونه خطا یا رفتار مخرب در عملکرد این واحدها باعث می شود سرویس اشتراک گذاری سفر دچار خطا شود.

٤-٧ جمع بندی

در این فصل به معرفی ابزار استفاده شده و مشخصات سیستم استفاده شده برای شبیه سازی روش ارائه شده در این پایان نامه را معرفی کردیم. مجموعه داده ها و مشخصات آن ها مورد بررسی قرار گرفت. همچنین به تشریح معیار های ارزیابی برای مقایسه سرویس های اشتراک گذاری سفر پرداختیم. با بررسی پژوهش های انجام شده در این زمینه به بررسی و مقایسه رویکرد ارائه شده در این پایان نامه و پرداخته شد.

فصل ۵ نتیجه گیری و پیشنهادات

۵-۱ مقدمه

در این فصل ابتدا به مروری بر پژوهش فعلی پرداخته، سپس یافته های پژوهش را بررسی نموده و در نهایت نتیجه گیری و پیشنهادات آتی که می توانند مورد مطالعه و ارزیابی قرار گیرند نیز ارائه می گردد.

۵-۲ مروری بر یافته های تحقیق

در این بخش به بررسی یافته های تحقیق فعلی پرداخته می شود:

- ✓ کاهش هزینه تراکنش: در سیستم های مبتنی بر بلاکچین با توجه عدم وجود سیستم های کنترل کننده مرکزی، هزینه تراکنش ها مهم ترین عاملی است که باعث پایداری سیستم می شود. این هزینه ها توسط کاربران استفاده کننده از سرویس ها پرداخت می شود. در سرویس اشتراک گذاری سفر متنی بر بلاکچین هزینه های تراکنش ها نسبت به پیاده سازی های مشابه کاهش یافته است. در نتیجه کاربران هزینه کمتری برای استفاده از سرویس اشتراک گذاری سفر پرداخت خواهند کرد. هزینه ها در تحقیق فعلی ۱۰ درصد نسبت به روش استفاده شده با قرار های هوشمند در شبکه اتریوم کاهش یافته است.
- ✓ وابستگی به سیستم های مرکزی اثبات کننده مکان: در این پژوهش با استفاده از مکانیزم پاداش/جریمه رویکردی ارائه شده است که سرویس های اشتراک گذاری سفر مبتنی بر بلاکچین، از وابستگی به اثبات کننده مکان بی نیاز می گردند. این واحد ها امکان اختلال، خطا در سیستم را افزایش می دهند. در نتیجه به دلیل هزینه های نصب و نگه داری بالا، این واحد ها باعث ایجاد عدم امکان استفاده از سرویس های اشتراک گذاری سفر در بسیاری از مناطق می شوند. حذف وابستگی به سیستم های مرکزی اثبات کننده مکان باعث کاهش مصرف ۱۵ درصدی انرژی و منابع مورد نیاز می شود.
- ✓ شبکه بلاکچین سفارشی شده: استفاده از شبکه های بلاکچین همه منظوره محدودیت هایی را برای توسعه دهندگان از جمله هزینه های بالا تراکنش ها تا فقدان قابلیت ارتقای شبکه به صورت خودکار، ایجاد می کند. در تحقیق صورت گرفته یک شبکه خوصوصی با مکانیزم اجماع پیشنهاد

شده است که باعث بهبود هزینه ها و عملکرد کلی شبکه بلاکچین برای سرویس اشتراک گذاری سفر شده است. از جمله بهبود های صورت گرفته در کاهش ۱۰ درصدی هزینه تراکنش ها و افزایش ۵ درصدی سرعت تراکنش نسبت به پیاده سازی به روش قرارهای هوشمند در شبکه همه منظوره اتریوم شده است.

با توجه به بهبود های حاصل شده از این موارد عملکرد سرویس اشتراک گذاری سفر مبتنی بر بلاکچین بهبود یافته است.

۵-۳ نتیجه گیری

در پژوهش فعلی، یک سرویس اشتراک گذاری سفر غیر متمرکز مبتنی بر یک شبکه بلاکچین ارائه شده است. سرویس های اشتراک گذاری مرکزی، از نظر روش قیمت گذاری، شفافیت، امنیت داده ها دچار چالش هایی می باشند. در پژوهش ارائه شده این چالش ها با سیستم های مبتنی بر بلاکچین برطرف کرد. رانندگان و مسافران از طریق یک شبکه واحد می توانند مستقیما به یکدیگر ارتباط بر قرار کرده و نیاز به هزینه های اضافی این سرویس دهندگان را کاهش دهند.

در روش ارائه شده با استفاده از پتانسیل شبکه های بلاکچین به دلیل این که هیچ واسطه ای وجود ندارد رانندگان فرصت های بیشتری برای کسب درآمد دارند. شبکه بلاکچین به استفاده کنندگان سرویس اشتراک گذاری سفر این قدرت را می دهد که بر اساس معیار های خود و بدون صرف کارمزد های سنگین، از این سرویس استفاده کنند. این سرویس علاوه بر مزیت های ذکر شده، این تضمین را می دهد که از رفتار مخرب کاربران در سرویس جلوگیری کند.

همچنین در پژوهش ارائه شده، با پیاده سازی یک شبکه بلاکچین سفارشی[1] هزینه تراکنش ها ۱۰ درصد کاهش یافته در نتیجه هزینه سفر کاهش داده شده است. در روش های قبلی، تمرکز اصلی روی همه جنبه ها به طور همزمان نبود. در روش های پیشنهادی سایر پژوهش ها تمرکز اصلی روی همه جنبه ها به طور همزمان نبوده است، از جمله نیاز به یک سیستم تایید فیزیکی برای اثبات حضور راننده در مبدا وجود داشته است که باعث ۱۵ درصدی استفاده از منابع شده است.

در روش های پیشنهادی هزینه های پیاده سازی و نگه داری این واحد های سخت افزاری و همچنین امکان بروز خطا و یا عملکرد مخرب در این سیستم ها امکان پیاده سازی این سرویس ها در بسیاری از محیط ها را دچار چالش می کند. در روش پیشنهادی ارائه شده در این پژوهش، با ارائه یک الگوریتم با نام الگوریتم پاداش/جریمه از وابستگی به این سیستم فیزکی جلوگیری شده است، که تمام چالش های ذکر شده را حل می کند. این مکانیزم وابستگی شبکه بلاکچین به یک سیستم مرکزی حذف می کند در نتیجه غیر متمرکز سازی سرویس اشتراک گذاری سفر بهبود یافته و تمکیل تر خواهد شد.

[1] Custom Blockchain

رویکرد اصلی استفاده از شبکه های بلاکچین در ارائه سرویس های مختلف از جمله رمز ارزها، سلامت، سرویس اشتراک گذاری سفر و ... ارائه مکانیزم هایی می باشد که از وابستگی به واحد های مرکزی جلوگیری کند و سرویس ها به طور غیر متمرکز قابل استفاده باشند که در این پژوهش با ارائه این الگوریتم سعی در رسیدن به این اصل مهم شده است.

۵-٤ پیشنهادات آینده

بر اساس مطالعه انجام شده در این پژوهش، نتایج زیر برای توسعه بیشتر پیشنهاد می شود، همچنین نکات زیر را می توان برای کار های بعدی در نظر گرفت:

۱. **سازگاری با سایر شبکه های بلاکچین**: پیشنهاد می گردد، با روش Parachain سازگاری شبکه بلاکچین و سرویس اشتراک گذاری سفر با سایر شبکه های بلاکچین را ایجاد کرد که موجب بهبود استفاده از سرویس اشتراک گذاری سفر خواهد شد.

۲. **اجماع در شبکه بلاکچین**: اجماع بلاکچین ابزاری است که گره های موجود در شبکه برای رسیدن به توافق در مورد وضعیت فعلی داده ها استفاده می کنند. پیشنهاد میگردد در شبکه بلاکچین سرویس اشتراک گذاری سفر، با استفاده از الگوریتم اجماع که در شبکه های خصوصی بلاکچین انجام می شود هزینه و عملکرد شبکه را بهبود داد.

۳. **تطبیق مسافر با راننده**: در پژوهش صورت گرفته تطبیق مسافر و راننده بر عهده نرم افزار های سوم شخص[1] می باشد. پیشنهاد می گردد با استفاده از پیاده سازی های Ride-Matching در شبکه بلاکچین این بخش از فرایند درون شبکه خاص بلاکچین سرویس های اشتراک گذاری سفر پیاده سازی شود.

۴. **پرداخت کرایه**: روش پیشنهادی برای پرداخت کرایه در تحقیق فعلی مبتنی بر مسافت طی شده از مبدا به مقصد می باشد. پیشنهاد می گردد، با استفاده از با ارائه الگوریتمی پرداخت آنی برای مسافر را ایجاد شود. این الگوریتم زمانی کاربرد دارد که راننده و مسافر به یکدیگر اعتماد دارند و پرداخت بدون اضافه شدن تراکنش های اضافی مبتنی بر مسافت طی شده انجام می شود. این الگوریتم می تواند به کاهش بیشتر هزینه های سفر کمک کند.

[1] Third Party Software

فهرست منابع فارسی

گزارش سالانه شرکت اسنپ سال ۱۳۹۹
https://snapp.ir/99-annual-report/assets/download/snap-annual-report-1399.pdf

فهرست منابع غیر فارسی

Adeeb, N., Abdu, A., Wang, Z., Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). *Research on the Application of Cryptography on the Blockchain*. 32077. https://doi.org/10.1088/1742-6596/1168/3/032077

Alharby, M., & van Moorsel, A. (2017). *Blockchain-based Smart Contracts: A Systematic Mapping Study*. 125–140. https://doi.org/10.5121/csit.2017.71011

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. https://www.google.com/books/edition/_/LchFDAAAQBAJ

Back, A. (1997). *Hashcash-A Denial of Service Counter-Measure*.

Bashir, I. (2017). *Mastering Blockchain Distributed ledgers, decentralization and smart contracts explained*. www.EBooksWorld.ir

Baza, M., Lasla, N., Mahmoud, M. M. E. A., Srivastava, G., & Abdallah, M. (2019). B-Ride: Ride Sharing with Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2019.2959230

Bozdog, N. V., Makkes, M. X., van Halteren, A., & Bal, H. (2018). RideMatcher: Peer-to-peer matching of passengers for efficient ridesharing. *Proceedings - 18th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2018*, 263–272. https://doi.org/10.1109/CCGRID.2018.00041

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform, White Paper.* https://nft2x.com/wp-content/uploads/2021/03/EthereumWP.pdf

Du, M., Ma, X., Zhang, Z., Wang, X., & Chen, Q. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*, *2017-January*, 2567–2572. https://doi.org/10.1109/SMC.2017.8123011

Global Cryptocurrency Market. (2022). https://coinmarketcap.com/charts/

Gupta, S., & Sadoghi, M. (2021). *Blockchain Transaction Processing*. https://doi.org/10.1007/978-3-319-77525-8_333

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, *98*, 461–466. https://doi.org/10.1016/J.PROCS.2016.09.074

Ian Griffiths. (2022). *Programming C# 10*. https://www.google.com/books/edition/Programming_C_10/0HJ_EAAAQBAJ?hl=en

J. WALKER SMITH. (2016). *The Uber-All Economy of the Future*.

Khanji, S., & Assaf, S. (2019). Boosting Ridesharing Efficiency Through Blockchain: GreenRide Application Case Study. *2019 10th International Conference on Information and Communication Systems, ICICS 2019*, 224–229. https://doi.org/10.1109/IACS.2019.8809108

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10401 LNCS*, 357–388. https://doi.org/10.1007/978-3-319-63688-7_12

King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*.

Kudva, S., Norderhaug, R., Badsha, S., Sengupta, S., & Kayes, A. S. M. (2020). PEBERS: Practical Ethereum Blockchain based Efficient Ride Hailing Service. *2020 IEEE*

International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020, 422–428. https://doi.org/10.1109/ICIOT48696.2020.9089473

Lamport, L. (1998). The part-time parliament. *ACM Transactions on Computer Systems (TOCS)*, *16*(2), 133–169. https://doi.org/10.1145/279227.279229

Lee D. (2015). *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments* (Lee D, Ed.). https://www.google.com/books/edition/_/RfWcBAAAQBAJ

Liu, X., Farahani, B., & Firouzi, F. (2020). Distributed Ledger Technology. *Intelligent Internet of Things*, 393–431. https://doi.org/10.1007/978-3-030-30367-9_8

Menezes, A. J. , van O. P. C. , & V. S. A. (2021). *Handbook of Applied Cryptography*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Pal, P., & Ruj, S. (2019). BlockV: A blockchain enabled peer-peer ride sharing service. *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, 463–468. https://doi.org/10.1109/BLOCKCHAIN.2019.00070

Pham, A., Dacosta, I., Endignoux, G., Ramon, J., Pastoriza, T., Huguenin, K., Hubaux, J.-P., Ramón Troncoso-Pastoriza, J., & Huguenin, K. (2017). {ORide}: A {Privacy-Preserving} yet Accountable {Ride-Hailing} Service. In *26th {{}USENIX{}} Security Symposium, {{}USENIX{}} Security 2017, Vancouver, BC, Canada, August 16-18, 2017.* http://ipads.se.sjtu.edu.cn/lib/exe/fetch.php?media=publications:vtz.pdf%0Ahttps://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/hua

Poenitzsch J. (2018). *What's the difference between Decentralized and Distributed?* https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4

Posen, H. A. (2015). Ridesharing in the Sharing Economy: Should Regulators Impose Uber Regulations on Uber. *Iowa Law Review*, *101*. https://heinonline.org/HOL/Page?handle=hein.journals/ilr101&id=415&div=&collection=

Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3230013

Ruj, S. (2019). *BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service Panchalika Pal*.

Schrank, D., Eisele, B., & Lomax, T. (2015). *2014 Urban Mobility Report : Powered by INRIX Traffic Data*.

Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. *Journal of Information Processing Systems*, *13*(1), 184–195. https://doi.org/10.3745/JIPS.03.0065

Shivers, R., Rahman, M. A., Faruk, M. J. H., Shahriar, H., Cuzzocrea, A., & Clincy, V. (2021). Ride-Hailing for Autonomous Vehicles: Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform. *Proceedings - 2021 IEEE International Conference on Big Data, Big Data 2021*, 5450–5459. https://doi.org/10.1109/BIGDATA52589.2021.9671379

Subramanya, S. R., & Yi, B. K. (2006). Digital signatures. *IEEE Potentials*, *25*(2), 5–8. https://doi.org/10.1109/MP.2006.1649003

Substrate. (2022). *Transactions and block basics*. https://docs.substrate.io/fundamentals/transaction-types/

Sunyaev, A. (2020). Distributed Ledger Technology. *Internet Computing*, 265–299. https://doi.org/10.1007/978-3-030-34957-8_9

Swan M. (2015). *Blockchain: Blueprint for a New Economy*. https://www.google.com/books/edition/Blockchain/RHJmBgAAQBAJ?hl=en

Szabo N. (2005). *Unenumerated: Bit gold*. http://unenumerated.blogspot.com/2005/12/bit-gold.html

Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, *597*, 120235. https://doi.org/10.1016/J.IJPHARM.2021.120235

U.S. Department of transportation. (n.d.). *U.S. Department of transportation, Federal Highway Administration*. Retrieved October 7, 2022, from https://ops.fhwa.dot.gov/freewaymgmt/faq.htm#faq1

Vasin P. (2014). *BlackCoin's Proof-of-Stake Protocol v2*. www.blackcoin.co

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Frontiers of Engineering Management*, *4*(1), 67–75. https://doi.org/10.15302/J-FEM-2017006

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain Technology Overview*. https://doi.org/10.6028/NIST.IR.8202

Zhang, X., Liu, J., Li, Y., Cui, Q., Tao, X., & Liu, R. P. (2019). Blockchain Based Secure Package Delivery via Ridesharing. *2019 11th International Conference on Wireless Communications and Signal Processing, WCSP 2019*. https://doi.org/10.1109/WCSP.2019.8927952

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85

Abstract

A ride sharing service is a possibility that connects vehicle drivers and passengers who wish to make a trip through a network of mobile devices. Today, ride sharing services have created a revolution in the transportation industry due to the advantages they have over traditional models, such as reducing travel costs, reducing time wastage, as well as reducing traffic and environmental pollution. Although these advantages have created improvements in the transportation industry, the providers of these services with the centrality and monopoly they have created have caused problems including lack of transparency, lack of privacy, and the use of user data, as well as due to the existence There is a single possibility of failure and contamination of these systems. Also, due to the high maintenance costs of these companies and the fees they collect from the trips, the travel costs have increased significantly in this way.

In this thesis, using the advantages of blockchain-based networks, a blockchain-based service is presented that will be able to connect drivers and passengers without centralization and a single organization. In the presented method, with the help of the benefits that blockchain networks have created, a service has been provided that tries to protect people's privacy and at the same time reduce related costs for passengers and drivers.

Keyword: Ride-sharing Service – Travel Cost – Blockchain – Blockchain based netwoks

Islamic Azad UNIVERSITY
ISLAM SHAHR Branch
Faculty of Technical Engineering – Department of Computer Engineering

« M.Sc.» Thesis

On Computer Software Engineering

Subject:

A blockchain-based network to reduce the travel cost in the Ride-Sharing service

Thesis Advisor:

Mohammadhossein Shafiabadi Ph.D

Consulting Advisor:

Fatemeh Safara Ph.D

By:

Mehran Mazhar

Winter 2022