فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال پنجم، شماره ۶۰، بهار ۱۴۰۰- جلد نهم، ص ۱۱۸-۹۹

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

بررسی بهبود امنیتی تجارت های آنلاین با استفاده از فناوری بلاکچین

مهشید سلطان سلیمی [۱]

تاریخ دریافت: ۱۴۰۰/۰۲/۲۵ تاریخ چاپ: ۱۴۰۰/۰۳/۰۶

چکیده

گسترش اینترنت، راه‌های جدیدی را برای چگونگی دریافت خدمات و نحوه‌ی اجرای عملیات شرکت‌ها ارائه کرده است. این روزها، ارتباط اینترنتی و خدمات مرتبط که توسط اینترنت فراهم می‌شوند، برای اکثریت مردم ضروری هستند. یکی از آن خدمات یا صنایع، تجارت الکترونیک است. در سال‌های اخیر، کاربردهای تجارت الکترونیک، توجه بسیاری از کاربران و تجار را به خود جلب کرده است تا کسب و کار روزانه‌ی خود را به صورت آنلاین انجام دهند که شامل پرداخت صورت‌حساب، بانکداری آنلاین، خرید بلیط و خرید کالا و غیره است. امنیت تراکنش‌های تجارت الکترونیکی یک نگرانی عمده برای وب سایت‌های تجارت الکترونیک همراه با مشتریان خود است. در تجارت الکترونیک، فناوری امنیت، به یک مسئله‌ی محدود کننده‌ی توسعه‌ی سریع و تعمیم تجارت الکترونیک تبدیل شده است. راهکارهای موجود پروتکل‌های بلاکچین بر بهبود اعتبار تراکنش‌ها اثر دارد، اما بسیاری از آنها، محدودیت‌هایی، از جمله توان عملیاتی پایین‌تر و نهفتگی اجماع بالاتر دارند و این مشکلات، استفاده‌ی گسترده از فناوری بلاکچین را دشوار می‌سازد. این مقاله یک چارچوب قابل‌اعتماد (ETTF) را با استفاده از پروتکل بلاکچین در تجارت الکترونیک برای دستیابی به یک سبک تجارت معتبر بالاتر ارائه می‌کند. ETTF شامل یک پروتکل بلاکچین همتا (PBP) بر مبنای ساختار بلاکچین همتا می‌باشد تا از ذخیره‌ی تراکنش‌های بزرگ و تراکنش‌های فوری پشتیبانی کند. در PBP، میزان توان عملیاتی تقریباً به صورت خطی با محاسبه افزایش می‌یابد: هرچه قدرت محاسباتی بیشتری در دسترس باشد، بلوک‌های بیشتری به ازای واحد زمان انتخاب می‌شوند. علاوه بر این، برای اطمینان از امنیت بالاتر تراکنش‌ها، یک الگوریتم اجماع قوی (ECA) را در تجارت الکترونیک معرفی می‌کنیم. ETTF نیز کارآمد است، چرا که تعداد پیام‌هایی که نیاز دارد، در اندازه‌ی شبکه، تقریباً خطی است. در مقایسه با بلاکچین برگرفته از بیت کوین، ETTF عملکرد بهتری را در توان عملیاتی، نهفتگی و ظرفیت در تجارت الکترونیک نشان می‌دهد.

واژگان کلیدی

بلاکچین، مکانیسم اجماع، فوری، قابل‌اعتماد، بلاکچین، تجارت الکترونیک، امنیت سایبری، DoS، ECC

[۱] دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، دانشکده علوم انسانی، دانشگاه پیام نور، تهران، ایران.
(mahshid.ssalimi@gmail.com)

۱. مقدمه

ظهور تجارت الکترونیکی تا حد زیادی، سبک زندگی مردم را تغییر داده است و تقریباً برای همه اجتناب‌ناپذیر است. با این حال، در حالی که تجارت الکترونیکی برای ما راحتی را به ارمغان آورده است، مشکلات بسیاری را هم در بر دارد که باید حل شوند. اول از همه، مسئله‌ای که ما باید نگران آن باشیم، امنیت است که شامل مقدار زیادی مطالب، مانند امنیت اطلاعات است. امنیت یک مسئله‌ی حیاتی است که به اعتماد عموم مردم در تجارت الکترونیک و حتی افت و خیز تجارت الکترونیک مربوط می‌شود. دوم، آزاد بودن تراکنش‌ها نیز باید با دقت در نظر گرفته شود. از آنجا که پلتفرم تجارت الکترونیک، یک سیستم متمرکز است، خدمات ارائه شده بسیار متمرکز می‌باشد که پلتفرم را قادر می‌سازد که تقریباً تمام اطلاعات و اعتبار را داشته باشد که یک امتیاز انحصاری مطلق را شکل می‌دهد. وجود اختلاف بین مشتری و پلتفرم، برای مشتری زیان‌آور است که در برخی موارد، حتی ممکن است داده‌ها را حذف یا دستکاری کند. حتی به شکل جدی‌تر، وقتی پلتفرم شکست بخورد یا از سوی مجرمان مورد حمله قرار گیرد، نتیجه فجیع خواهد بود (مانند اطلاعات افشا شده، از دست‌رفته و دستکاری شده) که به طور ویژه در زمینه‌ی تجارت الکترونیک غیرقابل جبران می‌باشد. با این حال، در حقیقت، چنین حوادث امنیتی دور و بر ما غیرمعمول نیستند. با توجه به این مشکلات، اگر فناوری غیرمتمرکز بلاکچین اتخاذ شود، مشکلات به خوبی قابل‌حل خواهند بود (Xie et al., ۲۰۱۸).

بلاکچین، یک سیستم پایگاه داده‌ی توزیع شده‌ی باز است. علاوه بر اطلاعات خصوصی مربوط به طرفین درگیر در تراکنش، داده‌های روی بلاکچین در کل، آشکار می‌باشند. غیرمتمرکزسازی بر اساس پروتکل بلاکچین به دست آمده از بیت کوین، به هر گره شرکت‌کننده در یک سیستم اجازه می‌دهد تا دقیقاً همان حقوق و تعهدات گره‌های دیگر را به دست آورد. به دلیل مکانیسم اجماع، تمام گره‌ها، همزمان‌سازی اطلاعات تراکنش را مجدداً تکمیل می‌کنند و دوباره طبق آن، به طوری که داده‌ها بر روی تمام گره‌ها در شبکه‌ی بلاکچین کاملاً منطبق شوند، پس از آن، تمام گره‌ها با داده‌های هر تراکنش ۱۰ دقیقه‌ای همزمان خواهند شد، به طوری که هر مورد حفظ شده در هر همتا به طور کامل سازگار است. هر بلوک شامل یک مقدار هش از بلوک قبلی است که برای ردیابی و اتصال به بلوک قبل به کار می‌رود. از آنجا که الگوریتم هش دارای ویژگی‌های برگشت‌ناپذیری و عدم مناقشه است و بلوک‌ها را به ترتیب به هم متصل می‌کند، دستکاری داده‌ها را بسیار دشوار می‌کند. به علاوه، زمانی که اطلاعات تأیید می‌شوند و به بلاکچین اضافه می‌گردند، برای همیشه ذخیره خواهند شد. اصلاح پایگاه داده روی یک گره واحد، نامعتبر است، مگر اینکه بیش از ۵۱٪ گره‌ها در سیستم، در همان زمان قابل کنترل باشند، بنابراین، بلاکچین دارای سطح بالایی از پایداری و قابلیت اطمینان است. این ویژگی‌ها [۳]، تراکنش‌های قابل‌اعتماد را بدون یک مکانیسم مدیریت متمرکز ممکن می‌سازند حتی اگر شرکت کنندگان غیرقابل اعتماد در شبکه وجود داشته باشند و صرف هزینه‌ی مضاعف را دشوار سازند (Xie et al., ۲۰۱۸).

اگر چه فناوری بلاکچین برگرفته از بیت کوین، مزایای برجسته‌ی بسیاری دارد که هنوز برخی از آنها رضایت‌بخش نیستند و باید بهبود یابند، مانند اندازه‌ی بلوک، در بلاکچین برگرفته از بیت کوین که در حال حاضر محدود به ۱ مگابایت است، در نتیجه فقط ۱ تا ۳/۵ تراکنش در هر ثانیه برای بیت کوین، انجام می‌شود. در تجارت الکترونیک، نه تنها مقدار زیادی تراکنش باید به طور همزمان مدیریت شود، بلکه هر تراکنش نیز باید به سرعت پردازش گردد. بدیهی است که اگر تجارت الکترونیک، بلاکچین برگرفته از بیت کوین را برای حل این مشکلات اتخاذ کند، برآورده کردن تقاضاهای تجارت الکترونیکی ممکن نیست؛ بنابراین، ما یک چارچوب تجاری مورد اعتماد مبتنی بر بلاکچین را در تجارت

الکترونیک (ETTF) ارائه می‌کنیم که می‌تواند داده‌های نامحدود را حفظ کند و از تراکنش های فوری پشتیبانی نماید و می‌تواند راهکار خوبی برای مشکلات فوق باشد. هدف ما ساخت یک محیط تجارت الکترونیک کارآمدتر، امن‌تر، عمومی‌تر، قابل‌اعتمادتر و مستقل است (Xie et al., ۲۰۱۸).

با توسعه‌ی فناوری اینترنت، فضای شبکه به عنوان مبنایی برای بقا و توسعه در جامعه‌ی مدرن تبدیل شده است [۸، ۳]. با این حال، از آن‌جا که اینترنت امن نیست، همه نوع مشکلات امنیتی برای اطلاعات وجود دارد. حملات شبکه‌ای متعددی مانند پنهان‌سازی (فریب دادن)، استراق سمع، دسترسی غیرقانونی، دستبرد و تغییر، انکار، جعل، انکار خدمت، تنظیم در پشتی، گسترش ویروس‌ها و غیره وجود دارند (Gao, ۲۰۱۹). بلاکچین یک ساختار داده‌ی جدید با غیرمتمرکزسازی و عدم نیاز به اعتماد است. این شرکت، تحت مالکیت تمام گره‌ها در شبکه، مدیریت و نظارت می‌شود و کنترل طرف منفرد را نمی‌پذیرد. فناوری هسته‌ی واحد ارز دیجیتال رمزنگاری شده‌ی جدید مانند بیت کوین است. اگرچه ارز دیجیتال رمزنگاری شده در اقتصاد و جامعه‌شناسی بحث‌برانگیز است، نوآوری فنی، توجه هر چه بیشتر و بیشتر را به خود جلب کرده است. این مورد توسط بیل گیتس، اریک اشمیت مورد ارزیابی قرار گرفت (Gao, ۲۰۱۹). IBM هم دارای فناوری بلاکچین است که در عصر اینترنت اشیا، TCP / IP می‌باشد. این مورد به فناوری کلیدی برای حل مشکلات اصلی امنیت اطلاعات، ذخیره‌سازی داده‌ها و پردازش تعاملی در اینترنت اشیا تبدیل خواهد شد (Gao, ۲۰۱۹).

معمولاً، صحت اطلاعات به اعتماد مرکز سیستم یا موجودیت شخص ثالث، مانند گره اصلی، پایگاه اطلاعاتی مرکزی، رئیس سیستم، مدیر پایگاه داده و غیره بستگی دارد. زمانی که مرکز سیستم دیگر قابل اعتماد نیست، صحت این داده‌ها از بین می‌رود و یافتن آنها دشوار است، بنابراین، رمزگذاری داده‌های پلتفرم تجارت الکترونیکی ضروری است. هیچ گونه تمرکزی از گره‌ها، سرورها و پایگاه‌های داده در داده‌های پلتفرم تجارت الکترونیکی رمزنگاری شده وجود ندارد (Gao, ۲۰۱۹). عملیات و نگهداری این سیستم به کارکنان مدیریت وابسته نیست. گره‌های شبکه به شدت، اثرانگشت اطلاعات تراکنش‌ها را در زمان خاص مربوط به بلاک کردن حفظ می‌کنند و به سرعت، به کل شبکه پخش می‌شوند. از فناوری هش برای تشکیل یک زنجیره‌ی پیوند محکم بین بلوک‌ها استفاده می‌شود تا یک حساب عمومی بسیار امن ایجاد گردد که به آن بلاکچین می‌گویند. با استفاده از فناوری بلاکچین، حتی بالای ۵۰۰ سوپررایانه‌ی جهان، به طور مشترک حمله را آغاز خواهند کرد که این مسئله، امنیت کلی داده‌های پلتفرم تجارت الکترونیک را به چالش می‌کشد؛ بنابراین، فناوری بلاکچین، اثر خوبی بر رمزنگاری داده‌ها دارد، اما برای رمزنگاری داده‌های پلتفرم تجارت الکترونیک با فناوری بلاکچین، فرآیند رمزنگاری بسیار پیچیده است و داده‌های رمزنگاری شده در معرض تحریف یا حتی از دست رفتن قرار می‌گیرند که کاربرد فناوری بلاکچین را در رمزنگاری داده‌ها برای پلتفرم تجارت الکترونیک تحت تأثیر قرار می‌دهد (Gao, ۲۰۱۹).

همان طور که خدمات ارائه شده توسط برنامه‌های کاربردی تجارت الکترونیک ساده و مقرون به صرفه هستند، بسیاری از مشتریان، به طور منظم در حال استفاده از کامپیوترهای شخصی خود برای خرید روزانه می‌باشند. گفته می‌شود تجارت الکترونیک، شهودی می‌باشد، مدیریت آن، آسان و دارای میزان تهدید کمتر است. روند رو به افزایشی برای ایجاد تجارت الکترونیکی «هوشمندانه» وجود دارد و این برای افزودن بیشتر و اتوماسیون (خودکارسازی) فعالیت‌های تجارت الکترونیک رخ می‌دهد. با تجارت الکترونیک، کاربران وب‌سایت‌ها که به دنبال محصولات مختلف اینترنتی می‌گردند، اقلامی را سفارش می‌دهند و پراخت خود را به صورت آنلاین یا آفلاین انجام می‌دهند. استفاده از کسب و کار آنلاین، امکان

پردازش تعداد زیاد سفارشات را با نیروی انسانی کم فراهم می‌کند و در نتیجه، قابلیت کسب و کارهای کوچک برای رقابت شرکت‌های بزرگ گسترش می‌یابد (Shaikh & Iliev, ۲۰۱۸).

رشد سریع اینترنت در چند سال گذشته، افزایش در انواع حملاتی مانند افزایش دسترسی غیر مجاز، سرقت منابع، افشای اطلاعات، دستکاری اطلاعات و غیره را تسهیل کرده است. در بین طیف وسیعی از این حملات، یکی از مضرترین و قدرتمندترین حملات، حمله‌ی انکار خدمات (DoS) است. حمله‌ی DoS که به روش توزیع شده توسط یک مکانیسم به نام Botnet از طریق شبکه‌ای از کامپیوترهای تحت کنترل انجام می‌شود، به عنوان حمله‌ی انکار خدمات (DDoS) به آن اشاره شده است. در یک محیط محاسبه‌ی توده‌ای، حملات DoS، تهدید امنیتی اولیه به عنوان منابعی هستند که اغلب توسط کاربران به اشتراک گذاشته می‌شوند. هدف اولیه از چنین حملاتی، مصرف انواع مختلفی از منابع نظیر فضای پردازش واحد پردازش مرکزی (CPU)، حافظه، یا پهنای باند شبکه است به طوری که کاربران نهایی / کاربران قانونی به این منابع دسترسی نخواهند داشت. این امر می‌تواند با شکستن ارتباطات شبکه و یا انکار خدمات به کاربر قانونی انجام شود. به طور کلی، حملات DDoS منابعی را که در خدمات شبکه مورد استفاده قرار می‌گیرند، مسدود می‌کنند. حملات DoS در حال تبدیل شدن به عامل اختلال در تمام سایت‌هایی هستند که مرتبط با اینترنت می‌باشند. اجرای بعضی از انواع این حملات آسان است و استقرار موارد دیگر کار دشواری است. حمله‌ی DDoS اساساً یک مشکل بارگذاری بیش از حد منابع است. با فشار چند کلید، مهاجم می‌تواند حملات DDoS را بر روی دستگاه هدف راه‌اندازی کند. تمام راهکارهای امنیتی موجود کارآمد نیستند، بنابراین یک مکانیسم قوی مورد نیاز است که بتواند خدمات محرمانگی و یکپارچگی را همراه با محافظت در برابر حمله‌ی DoS به همراه داشته باشد (Shaikh & Iliev, ۲۰۱۸).

بیشتر پروتکل‌های بلاکچین می‌توانند امنیت بالاتر تراکنش‌ها را با ارسال تمام تراکنش‌ها به همتایان دیگر خود در مصرف منابع محاسباتی تضمین کنند. ایده‌ی اصلی در ETTF، ساخت یک پروتکل بلاکچین همتا است که تمام همتایان را به کمیته‌های مختلف تقسیم می‌کند. برخلاف سایر بلاکچین‌ها، PBP دلیل کافی برای مکانیسم اثبات کار مورد استفاده در بیت کوین را ندارد. برخی از پروتکل‌های بلاکچین از یک مجموعه‌ی همتای اعتبار سنجی برای اعتبار بخشیدن به قانونی بودن تراکنش‌ها استفاده می‌کنند، اما تمام بلاکچین‌ها، الگوریتم انتخاب همتای اعتبار سنجی را در نظر می‌گیرند که می‌تواند به شکل پویا، عضویت هر دوره را تغییر دهد. PBP یک پروتکل مشارکتی بدون هدر دادن منابع محاسباتی است؛ زیرا PBP، هزینه‌های ارتباطات را افزایش می‌دهد. برای کاهش هزینه‌های ارتباطات، ما یک الگوریتم انتشار جدید را در تجارت الکترونیک (EPA) توسعه می‌دهیم. EPA یک مجموعه‌ی همتای اعتبار سنجی را به عنوان نماینده‌ی تمام همتایان معرفی می‌کند تا قانونی بودن بلوک تأیید گردد. همان طور که PBP نمی‌تواند به آزادی دست یابد و یک همتا هنوز هم می‌تواند اطلاعات را دستکاری کند، بنابراین، ما یک الگوریتم اجماع جهانی جدید (ECA) را توسعه می‌دهیم که در تمام همتایان قابل اجرا است. ECA مکانیسم اثبات کار را برای نوشتن مقدار هش یک بلوک به سمت یک بلوک جهانی در هر دوره به کار می‌برد (Xie et al., ۲۰۱۸).

با ساخت یک بلاکچین سه لایه، ما یک چارچوب تجاری مورد اعتماد (ETTF) را بر اساس بلاکچین ارائه می‌کنیم که عملکرد بهتری در تجارت الکترونیک دارد. دو سهم برای تحقیق ما وجود دارد، از یک سو، ETTF می‌تواند اعتبار بالاتری از تراکنش، حمایت از تراکنش فوری و حفظ اطلاعات نامحدود را تضمین کند. از طرف دیگر، تحت همان

مفروضات اعتماد مانند بیت کوین، ETTF می‌تواند با تقسیم کردن شبکه به چندین کمیته‌ی فرعی، به توان عملیاتی بالاتر و نهفتگی کمتر نسبت به بیت کوین دست یابد (Xie et al., ۲۰۱۸).

۲. بیان مسئله

داده‌های یک سازمان نه تنها اطلاعات شرکت را شامل می‌شود بلکه اطلاعات کارکنان و اطلاعات مربوط به مشتری را نیز شامل می‌شوند که باید در تمام مدت از آنها محافظت شود؛ بنابراین، سازمان‌ها همواره تلاش می‌کنند تا حفظ حریم خصوصی شرکت و مشتریان را تضمین کنند. رخنه و شکاف در یک شرکت تجارت الکترونیک ممکن است به صدمه وارد شدن به اعتبار و درآمد نام تجاری، خرابکاری آنلاین و یا درگیر شدن در سایر موارد جنایی با سو استفاده از داده‌ها منجر شود. فقدان رمزنگاری پایگاه داده و بخش امنیت ضعیف شبکه، خطر حملات سایبری را افزایش خواهد داد، بنابراین ابزارها و فناوری انتخابی برای شرکت باید بر روی حوزه‌هایی متمرکز شود که امنیت داده‌ها را افزایش دهند. چوئن (۲۰۲۰) یک برنامه‌ی کاربردی شخص ثالث را پیشنهاد داد تا به کاربران امکان فروش تجهیزات برای اعتبارات اولیه را بدهد (Xuan et al., ۲۰۲۰).

بنابراین، این تحقیق، فناوری بلاکچین را برای سیستم‌های پایگاه داده‌ای با ویژگی‌های منحصر به فرد خود توصیه کرده است که می‌تواند سطح امنیت داده‌های سازمان‌های تجارت الکترونیکی را افزایش داده و مانع از دسترسی غیر مجاز شود. بلاکچین، یک پلتفرم امن برای دسترسی مجاز به داده‌ها را در بلوک‌هایی ایجاد کرده است که به یکدیگر متصل هستند و امضاهای رمزنگاری منحصر به فردی بر روی هر یک از آنها دارند. سیستم غیر متمرکز بلاکچین، فرآیند اصلاح داده‌ها را سخت‌تر می‌کند، زیرا به یک نقطه‌ی کنترل مرکزی متکی است که برای بدست آوردن و اصلاح داده‌ها به روش‌های غیر مجاز توسط مهاجمان، آسان‌تر است. این فناوری می‌تواند یکپارچگی و محرمانه بودن داده‌ها را در سطحی بالاتر از یک سیستم پایگاه داده‌ی سنتی که از یک نقطه‌ی کنترل مرکزی استفاده می‌کند و می‌تواند مور حمله‌ی هکرها قرار گیرد، تضمین کند. از این رو، بلاکچین برای شرکت پلتفرم تجارت الکترونیک قابل‌اعتماد است، زیرا می‌تواند اعتماد و امنیت داده‌ها را در خدمات آنلاین افزایش دهد. تجارت الکترونیک می‌تواند در گسترش کانال، مدیریت زنجیره‌ی تأمین و فرآیند تراکنش تجارت الکترونیکی و افزایش عملکرد سازمان‌ها نقش داشته باشد (Xuan et al., ۲۰۲۰).

۳. فعالیتهای مرتبط

تعدادی از مکانیسم‌های امنیتی برای جلوگیری از حملات در سیستم تجارت الکترونیک استفاده شده‌اند. قربانی می‌تواند با استفاده از نوعی از ابزارهای امنیت سنتی مانند فهرست دسترسی، دیوار آتش یا سیستم تشخیص نفوذ در انتهای خود از حمله‌های گوناگون جلوگیری کند. با ظهور زمان بعد از راه‌اندازی حملات DoS، مهاجمان از مکانیسم‌های دفاعی آگاه شدند که برای جلوگیری و کاهش حملات DoS به کار گرفته شدند و هویت مهاجمان را ردیابی کردند.

مکانیسم‌های امنیتی موجود، شامل اصول اولیه، مدیریت کلیدی و کانال‌های امن، پروتکل‌های اصلی شبکه، خود مدیریتی و پروتکل‌های خود سازگار، حریم خصوصی و بی‌نام، حمایت مبتنی بر نرم‌افزار و آزمودن هستند. این مکانیسم‌های امنیتی، طبق مجموعه‌ای از الزامات امنیتی ابداع شدند (Shaikh & Iliev, ۲۰۱۸).

هوسانگ شان و همکاران، یک برنامه‌ی کاربردی حمله‌ی DDoS لایه‌ای را ارائه کردند که به شکل کوتاه DDoS متناوب (VSI – DdoS) شناخته شده است. یک مهاجم VSI – DDoS، وقتی طی مدت کوتاهی، DoS اجرا شد، یک درخواست ناگهانی را برای سیستم هدف می‌فرستد. هدف از این کار، ایجاد "DoS اشباع نشده« بود. حملات VSI

DDoS - برای کاهش کیفیت خدمات (QoS) مورد استفاده قرار می‌گیرند. گاهی کاربران قانونی از تأخیرات غیرقابل تحملی استفاده می‌کنند که در نهایت، هدف کسب و کار بلند مدت سیستم را مورد هدف قرار می‌دهد (Shaikh & Iliev, ۲۰۱۸).

دیوید بکت و همکاران، سیستم انتهای پشتی را با یک سنسور جدید در داخل ارائه کردند و با این روش، ویژگی‌های پایگاه داده‌ی اضافی نیز ایجاد شد. آگاهی بلادرنگ از بار کاری پایگاه داده‌ی واقعی در این روش، استفاده شده است که از تشخیص حملات DDoS فعال شده توسط کاربر ناشی می‌شود. منابع مصرف خارق العاده‌ی پایگاه داده، توسط این حملات مورد هدف قرار گرفتند. موتور طبقه‌بندی درخت تصمیم‌گیری در ماتریس منابع مورد استفاده قرار گرفت و تحلیل بلادرنگ با آنها انجام شد. در این روش، یک استراتژی برای تشخیص کاربرد حملات DDoS لایه‌ای طراحی شده است که اینجا، پرس و جوهای پایگاه داده‌ی بزرگ در منابع مورد هدف قرار داده شده‌اند. برای هر فرد، پرس و جوها پایش، ردیابی شدند و همچنین پروفایل استفاده از پایگاه داده نیز ایجاد شد. سهم این تکنیک، سنجش بود (Shaikh & Iliev, ۲۰۱۸).

چاکر عبدالعزیز کراچ و همکاران، یک طرح استقرار اعتماد ترکیبی را ارائه کردند که به عنوان چارچوب مبتنی بر اعتماد برای تحویل داده‌ی قابل‌اعتماد (TFDD) و VANETs برای دفاع از DoS شناخته شده‌اند. این روش، برای رویارویی با حملات DoS استفاده شده است و مورد اعتماد هم است و اتصالات قابل اعتماد میان رسانه‌ها را با توجه به سربار شبکه-ی کمینه تضمین می‌کند. ساختار مدولار، مبنای TFDD است که سه جزء به نام اجزای توزیع شده و مبتنی بر همکاری برای تشخیص گره‌های تقلبی، یک جزء تأیید مرکزی داده‌ها برای فیلتر کردن داده‌های مخرب و یک جزء برای تشخیص و جلوگیری از حملات DoS و DDoS می‌باشد (Shaikh & Iliev, ۲۰۱۸).

راهکارهای کاهش حملات DDoS در توده، توسط گوراو سومانی و همکاران پیشنهاد شده‌اند. به خصوص، مشاهده‌ی دقیق مکانیسم‌های کاهش، تشخیص، جلوگیری و تعیین مشخصات این حملات، به صورت جامع انجام شده است. علاوه بر این، یک طبقه‌بندی راهکار جامع از حملات DDoS ارائه شد. در نهایت، یک راهنمای مؤثر برای ایجاد یک راهکار مؤثر ارائه گردید که برای جامعه‌ی تحقیقاتی مفید واقع خواهد شد، در حالی که یک مکانیسم دفاعی طراحی می‌شود (Shaikh & Iliev, ۲۰۱۸).

خاندراکپام جانسون سینگ و تانمی دی، یک استراتژی منحصر به فرد چنین حمله‌ای را معرفی کردند و پارامترهای اصلی برجسته‌ی پروتکل‌ها را که در هر حمله‌ی لایه‌ای همراه بودند، معرفی کردند. در این روش، براساس مشخصه‌ی ورودی، بسته‌های ورودی را به عنوان یک دسته یا دسته‌ی نرمال حمله دسته‌بندی می‌کنیم. مجموعه داده‌ی حمله‌ی DDoS از مجموعه داده‌های CAIDA، HTTP – EPA برای بررسی ویژگی‌های این پروتکل‌ها استفاده شدند. بعد از آن، مجموعه‌ی ویژگی‌ها در سراسر طبقه‌بندی‌کننده‌های آماری معروف که برای مقایسه‌ی نرخ دقت، حساسیت، ویژگی و زمان برای طبقه‌بندی استفاده شده است، مورد آزمایش قرار گرفتند. نتایج تجربی برای قابلیت استفاده و قابلیت دوام برخی از الگوریتم‌های طبقه‌بندی نشان داده شده‌اند (Shaikh & Iliev, ۲۰۱۸).

فناوری بلاکچین، یک مکانیسم تراکنش غیرمتمرکز، مقاوم در برابر خطای بیزانسی را ارائه می‌دهد و نوید تبدیل شدن به زیرساخت برای نسل جدید تعامل اینترنتی، از جمله پرداخت‌های الکترونیکی بی‌نام، انتقال پول و تراکنش‌های دارایی‌های دیجیتال را داده است. کار مداوم به بررسی قراردادهای دیجیتال هوشمند می‌پردازد که طرفین بی نام را قادر می‌سازد، به

شکل برنامه‌ریزی شده، توافق‌های پیچیده را انجام دهند. با وجود این پتانسیل، پروتکل‌های بلاکچین برگرفته از بیت کوین نیز با یک مانع مقیاس‌پذیری قابل‌توجه مواجه هستند. بیت کوین دارای مسائل مربوط به مقیاس پذیری از نظر توان عملیاتی، نهفتگی، ظرفیت و پهنای باند شبکه است. برای مثال، افزایش اندازه‌ی بلوک می‌تواند توان عملیاتی را بهبود بخشد، اما باعث می‌شود که بلوک‌های بزرگ‌تر زمان بیشتری برای انتشار در شبکه پیدا کنند. کاهش فاصله‌ی بلوک، نهفتگی را کاهش می‌دهد، اما منجر به ناپایداری می‌شود که زنجیره را به شاخه‌ها می‌شکافد (Xie et al., ۲۰۱۸).

بسیاری از پروتکل‌های اجماع، از مکانیسم‌های تصادفی‌سازی، به خصوص برای گریز از عدم امکان FLP معروف در شبکه‌های ناهمگام قطعی استفاده می‌کنند. به طور کلی، بیان مجدد غیر قطعی از مشکل اجماع شامل قوانین لاس وگاس است: شبکه باید در نهایت به اجماع برسد، هر چند زمان صرف شده ممکن است نامحدود باشد. کینگ و سایا مشاهده کردند که قوانین لاس وگاس، برای شبکه‌های مقیاس بزرگ بسیار سختگیرانه هستند. از آنجا که اجماع قطعی، به حداقل بیت پیام نیاز دارد، هر پروتکل اجماع تصادفی با استفاده‌ی کمتر از پیغام‌های درجه دو باید یک پروتکل مونت کارلو با احتمال غیر صفر شکست باشد (Xie et al., ۲۰۱۸).

در جنبه‌های دیگر، زروکش و زروکوین، یک پرداخت بی نام را از طریق استفاده از یک نوع جدید اسناد رمزنگاری ارائه کردند. برخلاف بیت کوین، سیستم پرداخت بی نام است که می‌تواند حریم خصوصی بلاکچین را فراهم کند و در کل، دارای توان عملیاتی بالاتر است. با این حال، طرفینی که برای بی نام کردن تراکنش‌ها انتخاب شدند، هنوز هم می‌توانند از بی نامی کاربران تخطی کنند، حتی اگر آنها صادق اما کنجکاو باشند. ایتای ایال، بیت کوین NG، یک پروتکل بلاکچین جدید برگرفته از بیت کوین را نشان می‌دهد که برای یک مقیاس طراحی شده است. بیت کوین NG به تحمل خطای بیزانسی دست می‌یابد، در برابر برانگیختگی شدید مقاوم است و به اشتراک گذاری همان مدل اعتماد، از تغییرات کیفی در اکو سیستم استفاده می‌کند. هنگ جی هی، یک بلاکچین مبتنی بر طرح علامت‌گذاری بی اساس را برای حل مسئله‌ی امنیت و صحت مکان‌یابی آن پیشنهاد می‌کند (Xie et al., ۲۰۱۸).

٤. محرک های امنیتی

امروزه، تجارت الکترونیک، یک ضرورت است که می‌تواند در بازار رقابت کند. برای تجارت، حریم خصوصی و امنیت یک نگرانی عمده است. دسترسی غیرمجاز، نشت اطلاعات مشتری، مضحکه شدن کارت‌های اعتباری و غیره، نگرانی‌های امنیتی متعددی در تجارت الکترونیکی هستند. بدون آگاهی و همکاری از سوی قربانی، جرایم در قالب آینده‌ای نگران-کننده‌تر صورت خواهند گرفت. به جای احتیاط معمولی انسان، امنیت الکترونیکی قوی برای جلوگیری از جنایت سایبری در آینده لازم است. به دلیل مشکلات امنیتی و حریم خصوصی (مثل هک کردن اطلاعات مشتریان)، مشتریان برای مشارکت در تجارت الکترونیک، هوشیارتر شده‌اند. همچنین از نظر شبکه‌ی باز، بسیاری از حملات وجود دارند که برای اطلاعات مشتری هشداردهنده هستند. برای بسیاری از سازمان‌ها، ریسک مربوط به امنیت قابل‌توجه و حریم خصوصی، افشای عمومی تمام تراکنش‌ها است (Shaikh & Iliev, ۲۰۱۸).

تخطی از یکپارچگی، کنترل دسترسی، حمله‌ی DoS و DDoS و حملات زیرساخت برخی از تهدیدات امنیتی هستند که در سرتاسر اینترنت در دسترس می‌باشند و این خطرات، در دنیای امروز، به تروریسم دیجیتال تبدیل شده‌اند؛ زیرا امنیت و حریم خصوصی، مسائل اصلی در اینترنت برای توسعه‌ی تجارت الکترونیکی هستند. از این رو، ما باید برخی شرایط

حفاظت شده داشته باشیم تا بر مشکلات امنیتی مربوط به ماهیت کلی در تراکنش‌های تجارت الکترونیک غلبه کنیم و باید از اطلاعات تراکنش، به شکل قوی حفاظت شود (Shaikh & Iliev, ۲۰۱۸).

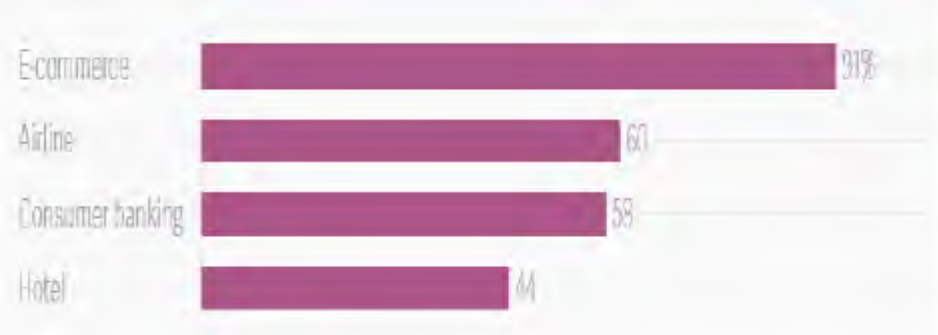
برای برنامه‌های کاربردی حساس مانند تجارت الکترونیکی، این روزها پروتکل لایه‌ی سوکت امن (SSL) استفاده می‌شود و این مورد برای تأمین امنیت تجارت الکترونیکی، محرمانه است. نقطه‌ضعف اصلی پروتکل SSL، زمان پاسخ کند بر روی سرور است و این دلیل اصلی ناکام ماندن برای کاربران تجارت الکترونیک است. پروتکل‌های موجود، نیازمندی‌های امنیتی جامع برنامه‌های کاربردی تجارت الکترونیک را برآورده نمی‌کنند، در حالی که ارتباط بین مشتریان و فروشندگان، نیازمند بهبود بیشتر است. طراحی یک سیستم احراز هویت، به دلیل ماهیت پیچیده‌ی برنامه‌های کاربردی تجارت الکترونیکی و الزامات امنیتی متنوع، یک کار چالش برانگیز است. این پروتکل، زمانی که در داخل یک شبکه‌ی بسته و امن به عنوان بلاکچین خصوصی شناخته می‌شود، مورد استفاده قرار می‌گیرد (Shaikh & Iliev, ۲۰۱۸).

۵. مرور ادبیات

تعدادی از تحقیقات برای داشتن یک منطق قوی برای راه‌حل پیشنهادی مورد بررسی قرار گرفتند. تجارت الکترونیک آنلاین، با استفاده از اینترنت رشد می‌کند و این امر به انجام کارهای روزمره‌ی مردم کمک کرده است. امروزه، مشتریان می‌توانند تقریباً هر چیزی را که از پلتفرم‌های آنلاین می‌خواهند، خریداری کنند. این کار برای کاربران آنلاین مناسب و در دسترس است، مشتریان می‌توانند هر جایی که به کالا یا خدمات نیاز دارند، به صورت آنلاین خرید کنند. همانطور که پلتفرم‌های تجاری آنلاین رشد می‌کنند، تعداد مجرمان سایبری در همان زمان افزایش می‌یابد. ریسک بالای ناشی از این واقعیت است که پایگاه‌های داده‌ی تجارت الکترونیک به ناچار مقدار زیادی از اطلاعات شخصی را ذخیره می‌کنند که ممکن است به طور مستقیم بر امنیت فردی تأثیر بگذارد؛ بنابراین، فناوری بلاکچین برای سیستم پایگاه داده‌ی پلتفرم‌های کسب و کار تجارت الکترونیک توصیه می‌شود (Xuan et al., ۲۰۲۰).

۵-۱. رخنه و شکاف در داده‌ها در تجارت الکترونیک

رابرتز، اس (۲۰۱۹) اشاره کرد که اغلب این شرکت‌ها خسارات ناشی از موارد رخنه و شکاف در داده‌ها را دست‌کم می‌گیرند و ممکن است منجر به عدم اقدامات پیشگیری از مشکلات شوند. بیش از ۹۰٪ از پلتفرم‌های کسب و کار آنلاین، تلاش‌های ورود به سیستم را از سوی هکرها تجربه کرده‌اند. این بدان معنی است که مسئله‌ی رخنه و شکاف در داده‌ها جدی است و کسب و کار تجارت الکترونیک توسط نهادهای غیر مجاز مورد هدف قرار می‌گیرد (Xuan et al., ۲۰۲۰).



شکل ۱ - سهم تلاش‌های ورود به سیستم که از حملات آسیب دیده‌اند (دتریکس، جی ۲۰۱۸).

شرکت‌های تجارت الکترونیک باید به این مسائل توجه کنند و راه‌حل‌های جایگزین برای آنها داشته باشند.

۵-۲. بهبود اعتماد عمومی در تجارت الکترونیک توسط بلاکچین

یکی از بزرگ‌ترین اثرات بر تجارت الکترونیک، معرفی راهکار بلاکچین است که مربوط به اعتماد عمومی و وفاداری است. مطالعه‌ی انجام شده توسط راجش راماچاندرین نشان داد که تحقیقات موجود بر مسائل مربوط به اعتماد بیشتر بر توانایی بلاکچین برای معرفی قوانین و سیاست‌ها بدون نیاز به کنترل خودسرانه (۲۰۱۸) متمرکز هستند. راهکار پیشنهادی می‌تواند اعتماد کاربران پلتفرم تجارت الکترونیک را با اعمال یک شبکه‌ی بلاکچین به سیستم پایگاه داده‌ی شرکت تضمین کند. تلفیق فناوری بلاکچین و سیستم پایگاه داده‌ی شرکت، شفافیت داده‌ها را ترویج می‌کند، چرا که تمام طرفین ممکن است اطلاعات خود، از جمله ارائه‌دهندگان پلتفرم تجارت الکترونیک، تأمین‌کنندگان و مشتریان را مشاهده کنند. در پایان، حریم خصوصی و محرمانگی کاربران پلتفرم تجارت الکترونیک را افزایش می‌دهد که در مقابل، بدون شک وفاداری و اعتماد به سازمان پشت آن را ارتقا می‌دهد (Xuan et al., ۲۰۲۰).

۵-۳. عملکرد بلاکچین

همان طور که در یک مطالعه‌ی دیگر توسط محمد جابد مرشد چودوری و همکاران نیز اشاره شد، یکی از ویژگی‌های برجسته‌ی یک راهکار بلاکچین، تغییرناپذیری آن است که با مفهوم غیرمتمرکزسازی به دست می‌آید که نوعی دموکراسی سیستمی را معرفی می‌کند. همراه با آن، این واقعیت وجود دارد که داده‌هایی که با مفهوم بلاکچین ذخیره می‌شوند، از رویکرد رمزنگاری کلید عمومی استفاده می‌کنند. با این حال، یکی از نگران‌کننده‌ترین محدودیت‌های کاربرد فناوری بلاکچین، عملکرد است. طبق این مطالعه، تراکنش‌هایی که با استفاده از بلاکچین اتفاق می‌افتند، در مقایسه با روش‌های سنتی بسیار کند هستند. بازه‌ی زمانی می‌تواند به ۱۰ دقیقه برسد، در حالی که یک سیستم پایگاه داده‌ی قراردادی می‌تواند هزاران تراکنش را در هر ثانیه با یک ساختار مناسب مورد رسیدگی قرار دهد. با این حال، محقق بیان می‌کند که الگوریتم‌های مختلف مورد مطالعه قرار گرفته‌اند و ۱۰ تا ۲۰ ثانیه در هر تراکنش قابل حصول است. این آسیب‌پذیری قبل از پیاده‌سازی شبکه‌ی بلاکچین به پایگاه داده‌ی تجارت الکترونیک در نظر گرفته خواهد شد (Xuan et al., ۲۰۲۰).

۵-٤. فناوری بلاکچین را با روش ذخیره‌سازی سنتی ترکیب کنید.

در تحقیقات انجام شده توسط جیان چن و همکاران، عیب اصلی بلاکچین پیدا شد، فضای ذخیره‌سازی محدود هر گره/بلوک که ذخیره‌سازی داده‌های بزرگ و مشکل افزونگی اطلاعاتی در شبکه‌ی بلاکچین را تقریباً غیر ممکن می‌سازد. راهکار پیشنهادی برای این مسئله، ترکیب فناوری بلاکچین با روش ذخیره‌سازی سنتی است که به جداسازی داده‌ها در بلاکچین و ذخیره‌ی آن در پایگاه داده مرکزی نیاز دارد تا کارایی فرآیند ذخیره‌سازی داده را بهبود بخشد. راهکار پیشنهادی می‌تواند مشکلات ذخیره‌ی ناکافی و افزونگی اطلاعات بلاکچین را حل کند (Xuan et al., ۲۰۲۰).

۵,٤. سیستم پایگاه داده‌ی مبتنی بر بلاکچین

براساس مطالعه‌ی انجام شده توسط محمد مزمل و همکاران، مشخص شد محدودیت پایگاه داده‌های بلاکچین به همان میزان اصلاح و اضافه کردن داده‌ها دشوار است. علاوه بر این، سیستم پایگاه داده‌ی بلاکچین یک منبع بازیابی در سطح داده و میان‌افزار حسابرسی می‌باشد؛ بنابراین، CHAINSQL برای افزایش ضعف شبکه‌ی بلاکچین توصیه شده است. این سیستم می‌تواند داده‌ها را در یک سیستم پایگاه داده‌ی مبتنی بر بلاکچین ذخیره کند که در آن ساختار چند به یک، اجازه‌ی پشتیبانی داده‌ها را در چندین گره تولید کارآمد می‌دهد. این روش، نقاط قوت اصلی دو سیستم پایگاه داده‌ی

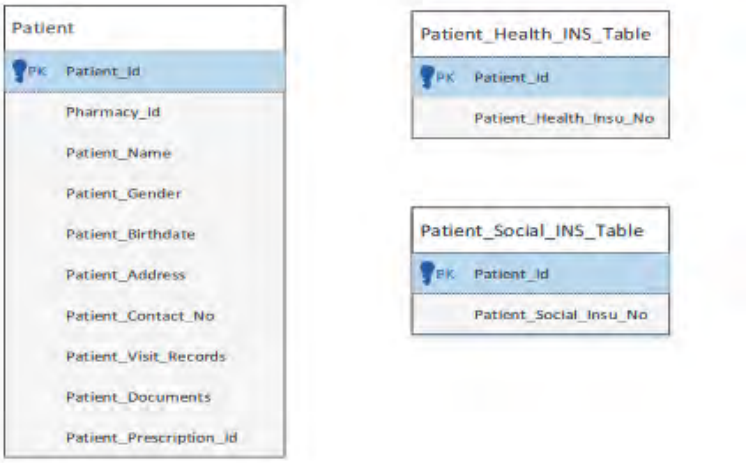
متفاوت را ترکیب می‌کند که انعطاف‌پذیری برای مدیریت و کنترل، توان عملیاتی بالا و ظرفیت بالا در پایگاه داده‌های توزیع شده و امنیت با ویژگی‌های قابلیت استماع در پایگاه داده‌های بلاکچین است. علاوه بر این، این روش، یکپارچگی داده‌ها و مسائل مربوط به قابلیت اطمینان در سیستم‌های پایگاه داده‌ی توزیع شده را بهبود می‌بخشد و در عین حال، مسائل مربوط به دستکاری در پایگاه داده‌ی بلاکچین نیز بهبود می‌یابد. این روش برای پلتفرم کسب و کار تجارت الکترونیک مناسب است، داده‌های ذخیره شده تطبیقی هستند تا تغییرات را برای دستیابی مجاز ایجاد نمایند، علاوه بر این، امنیت داده‌ها را می‌توان برای سازمان‌ها و مشتریان تضمین کرد. این سیستم به عنوان مرجع در هنگام توسعه و طراحی سیستم پیشنهادی به کار گرفته خواهد شد. صالح (۲۰۲۰) دریافت که یک رابطه بین وب و سیستم پشتیبانی تصمیم‌گیری وجود دارد که آن را مقرون به صرفه می‌سازد (Xuan et al., ۲۰۲۰).

۵-۵. افزایش امنیت داده‌ها از طریق فناوری بلاکچین

در تحقیق دیگر که توسط الکس آر ماتو نوشته شد، مشخص گردید که امنیت سیستم‌های مدیریت داده‌های قراردادی، برای مهاجمان سایبری، آسیب‌پذیر است. این تحقیق، ماهیت متمرکز سیستم‌های مدیریت داده‌های مورد استفاده‌ی فعلی را به طور خاص جهت پرداختن به استفاده‌ی مشابه از یک سیستم امنیت واحد و وابسته که مستعد حملاتی مانند DDoS (توزیع تکذیب خدمات) است، مورد بحث قرار می‌دهد که هکرها یک سیستم امنیت واحد را مورد هدف قرار می‌دهند، آن را کنار می‌گذارند و سپس کار را جهت گردآوری داده‌ی شخصی با ارزش ادامه می‌دهند. در مقابل، این تحقیق بیان می‌کند که فناوری بلاکچین دارای پتانسیل بهبود سیستم‌های امنیت فعلی و دستیابی به ذخیره‌سازی داده‌های حفاظت شده برای ماهیت توزیع شده‌ی همتا به همتا است. این مطالعه نتیجه می‌گیرد که بزرگ‌ترین ضعف سیستم مدیریت داده‌ی فعلی، وجود یک نقطه‌ی واحد از شکست یا سازگاری است و استفاده از بلاکچین را به دلیل زیرساختار قوی بسیار دقیق آن پیشنهاد می‌دهد. از آنجا که هر بلوک داده‌ی مشترک هش شده و متصل به گره بعدی است، برای اشخاص ثالث، دسترسی به آن غیرممکن است، تنها دو طرف قادر به خواندن و دستکاری داده‌ها هستند، از این رو، توسط اشخاص ثالث در مورد نشت غیرقابل استفاده خواهد شد. الکس آر ماتو اشاره می‌کند که محققان امنیتی مشخص کرده‌اند که فناوری بلاکچین می‌تواند به طور بالقوه روزنه‌های امنیتی کنونی را محصور کند که فراتر از محدوده‌ی اقدامات امنیتی فعلی است. در عین حال، امنیت داده‌ها در بلاکچین می‌تواند با استفاده از کلیدهای خصوصی و کیف پول افزایش یابد. کیف پول کاغذی و کیف پول سخت‌افزاری برای افزایش سطح امنیت در پایگاه داده‌های بلاکچین پیشنهاد شده‌اند (Xuan et al., ۲۰۲۰).

۵-۶. تفکیک فراداده در سیتم پایگاه داده

براساس مطالعه‌ی انجام شده توسط دوانشو تریودی و همکاران، ۲۰۱۶، فراداده در پایگاه داده، به عنوان جزئیات داده‌ها ارائه شده است. براساس این تحقیق، ستون‌های پایگاه داده براساس سطح حساسیت تفکیک خواهند شد و انسجام ارجاعی را در زمان اجرا ایجاد خواهند کرد تا اطمینان حاصل شود که تمام فراداده‌ها از یکدیگر جدا شده‌اند و در نتیجه دشواری دسترسی غیر مجاز به سیستم پایگاه داده را افزایش می‌دهند. هنگامی که اطلاعات از یکی از جداول به وسیله‌ی هکرها مورد حمله قرار می‌گیرد، فراداده از طریق محدودیت‌های مربوط به یکپارچگی ارجاعی تفکیک خواهد شد؛ بنابراین، می‌توان از خطر افتادن دیگر جداول، توسط مهاجمین جلوگیری کرد و اتصال اشیای پایگاه داده و جمع‌آوری یا انتقال داده‌ها برای هکرها دشوار است (Xuan et al., ۲۰۲۰).



شکل ۲ – جداول تفکیک شده در سیستم پایگاه داده (تریودی و همکاران ۲۰۱۶)

این روش برای حفاظت از داده‌ها از دسترسی غیر مجاز بسیار قدرتمند است، با این حال، سطوح مختلف حساسیت و انواع مختلف رابطه بین جداول داده‌ها، دشواری در بازیابی داده‌ها بعد از فرآیند تفکیک را افزایش می‌دهد. پیاده‌سازی، برای سیستم پایگاه داده‌ی تجارت الکترونیک مناسب نیست، چون پلتفرم تجارت الکترونیک انواع مختلف داده و برنامه‌های کاربردی مانند جزئیات تراکنش، جزئیات مشتریان و یا حتی داده‌های رقبا را دارد. علاوه بر این، استفاده از این روش در ساختار شبکه‌ی کسب و کار الکترونیک به عنوان سرورهایی که در مناطق جغرافیایی متمایز واقع شده‌اند، بسیار دشوار است و نیازمند تلاش غیرضروری و هزینه‌ی بالا است (Xuan et al., ۲۰۲۰).

٦. مروری بر چارچوب تجارت مورد اعتماد با استفاده از تجارت الکترونیک بلاکچین

ما همتا را با p نشان می‌دهیم. هویت همتایان، با استفاده از رمزنگاری کلید عمومی به صورت زیر ایجاد می‌شود: زمانی که همتا برای اولین بار، به شبکه ملحق می‌شود، p یک جفت کلید عمومی و خصوصی را تولید می‌کند. در تجارت الکترونیک، هر همتا یک پلتفرم پرداخت شخص ثالث، پلت فرم لجستیک و یا پلتفرم نظارت ترکیبی را نشان می‌دهد. ما سه نوع همتا را معرفی می‌کنیم: همتای تولید بلاکچین جهانی (gp)، همتای اعتبار سنجی بلاکچین جهانی (vp) و همتای عادی (op). فقط gp مجوز برای تولید بلوک جهانی دارد، فقط vp اجازه دارد که قانونی بودن بلوک جهانی را تأیید کند. هر همتا می‌تواند با تراکنش‌ها مواجه شود. تمام همتایان، شبکه‌ی تجارت مورد اعتماد مبتنی بر ETTF (ETTN) را تشکیل می‌دهند (Xie et al., ۲۰۱۸).

ETTF در دوره‌ی بعدی ادامه می‌یابد. در هر دوره، ابتدا هر همتا تراکنش‌ها را برای بلوک‌ها می‌نویسد. در این میان، بر اساس صداقت همتا که احتمال دستکاری تراکنش را نشان می‌دهد، یک قدرت کاوش در دسترس وجود دارد که قدرت محاسبه‌ی همتا را نشان می‌دهد، ETTF مجموعه‌ی gp و vp را از تمام همتایان نشان می‌دهد. دوم، تمام gp ها یک بلوک جهانی تجارت الکترونیک را تولید می‌کنند و یک بلوک جهانی را به مجموعه‌ی vp می‌فرستند. سوم، مجموعه‌ی vp، بلوک‌های متعدد را برای یک واحد ادغام و قانونی بودن بلوک جهانی تأیید می‌کند. در TTEN، هر همتا باید تمامی بلوک‌های جهانی را نگه دارد. op، فقط بلوک‌های همتا را مدیریت می‌کند و gp تمام بلاکچین‌های همتا را تحت مدیریت دارد (Xie et al., ۲۰۱۸).

ETTF شامل دو بخش است: پروتکل بلاکچین همتا (PBP) و یک الگوریتم اجماع قوی در تجارت الکترونیک (ECA). PBP یک پروتکل بلاکچین برای حفاظت از امنیت تراکنش‌ها در همتا است. ECA فقط برای جلوگیری از نادرستی همتایان برای مداخله‌ی تراکنش‌های همتای دیگر استفاده می‌شود.

٦-١. چارچوب تجارت مورد اعتماد با استفاده از بلاکچین در تجارت الکترونیک

الف. پروتکل بلاکچین همتا

برای محافظت از امنیت و اعتماد تراکنش‌ها در هر همتا، این مقاله یک پروتکل بلاکچین همتا (PBP) را ارائه می‌دهد. هر همتا دارای یک بلاکچین همتا است که تنها تراکنش‌های درگیر در انتقال دارایی‌ها را نگه می‌دارد. در PBP، وضعیت هر بلوک، سه نوع را معرفی می‌کند: غیرقطعی، معتبر و نامعتبر. در بلاکچین همتا، هر بلوک ریز همتا (PMB) حاوی یک دسته از تراکنش‌ها، یک فهرست رأی توسط مجموعه‌ی vp و شامل یک فهرست امضا است که در شکل ۳ الف نشان داده شده است. هر بلوک کلید همتا (PKB) حاوی گروهی از PMB می‌باشد که در شکل ۳ ب نشان داده شده است. اکثریت زیادی از رأی‌های مثبت یا منفی برای PMB در مجموعه‌ی vp وجود دارند، این PMB می‌تواند به صورت غیرقطعی به سمت معتبر یا نامعتبر حرکت کند. این یک قانون است که تنها PMB معتبر را می‌توان در یک PKB نوشت. اگر PMB، معتبر در نظر گرفته شود، آن تراکنش‌هایی که گنجانده شده‌اند، نیز معتبر خواهند بود و تراکنش‌ها به شیوه‌ای مؤثر به اجرا درخواهند آمد (Xie et al., ۲۰۱۸).

PBP در طول دوره‌ها تداوم دارد. هر تراکنش و PMB از وضعیت غیرقطعی به وضعیت معتبر یا نامعتبر حرکت می‌کند. برای تضمین زمان، از وقوع تراکنش به تراکنش در اثر کمتر از یک دوم، چندین PMB در یک زمان تولید خواهند شد، اما فقط یک PKB در یک زمان تولید خواهد شد. جهت حفاظت از امنیت تراکنش‌ها و اعتماد به آنها، هر PMB باید با مجموعه‌ی vp امضا شود. همانطور که در الگوریتم ۱ نشان داده شده است: PBP می‌تواند به سه مرحله تقسیم شود: اول اینکه، PBP قانونی بودن تراکنش‌ها را بررسی می‌کند. دوم، PBP تراکنش‌های معتبر را به PMB می‌نویسد و به مجموعه‌ی vp ارسال می‌کند. سوم، PBP، PMB معتبر را به PKB می‌نویسد.

به طور کلی، اگر یک vp، یک PMB را دریافت کند، vp قانونی بودن این PMB را بررسی می‌کند و این PMB را با امضای خود به هر vp همتا می‌فرستد. اگر اکثریت vp رأی دادند که بلوک معتبر است، تمام vp این PMB را به صورت بلاکچین همتای خود نگاه می‌دارند. مکانیسم پخش p2p سنتی، پهنای باند شبکه‌ی بسیار بیشتری را مصرف خواهد کرد. اگر هر همتا، PMB را به ترتیب با امضای یک به یک ارسال کند، گاهی اوقات، اولین همتا هرگز، نتیجه‌ی رأی‌گیری را دریافت نخواهد کرد، البته در صورتی که هر همتا تجزیه شده و فرایند رأی گیری متوقف شود؛ بنابراین، این مقاله یک مکانیسم پخش جدید EPA را توسعه می‌دهد که هزینه‌های ارتباطات پایینی دارد. هدف ما کاهش هزینه‌های ارتباطات از N^N به $K \bullet N$ است که N تعداد همتایان در ETTN را نشان می‌دهد و $1 \le K \le N$. ایده‌ی اصلی در EPA این است که هر هویت را به یک گروه تصادفی اختصاص دهیم. اول، تمام vp را به m گروه g_i تقسیم می‌کنیم. دوم، هر همتا، یک فهرست ارسال بعدی را با انتخاب تصادفی یک قالب از گروه‌ها تولید می‌کند، فرض کنید تعداد همتایان در یک گروه N/m است، حداکثر فرکانس انتشار، $m \bullet N + m^2$ می‌باشد. از آنجا که $m \bullet N + m^2 \le 2N^2$ و $m \ll N$ است، بنابراین $m \bullet N + m^2 \le K \bullet N$ خواهد بود. علاوه بر این، اگر هر vp، اکثریت vp های رأی داده را بیابد، PMB نامعتبر یا معتبر است، این vp، PMB را به همتا بازمی‌گرداند که این PMB را ابتدا ارسال می‌کند و به

سراغ vp دیگر می‌رود. اگر همتا، این PMB را در ابتدا ارسال کند، PMB کافی را با امضا دریافت می‌کند، این همتا یک پیام را به تمام vp ارسال خواهد کرد تا فرایند رأی‌گیری PMB را متوقف کند. ؛بنابراین، EPA عملکرد بهتری نسبت به مکانیسم سنتی دارد.

در PBP، فقط اگر تراکنش‌ها به یک PMB نوشته شده باشند، هر کس نمی‌تواند به هر طریقی این اطلاعات را دستکاری کند؛ زیرا هر PMB باید با اکثریت همتایان پیشنهاد شود، این PMB می‌تواند معتبر باشد. علاوه بر این، اکثر vp ها باید این PMB را برای بلاکچین خود نگه دارند. اگر یک همتا تمایلی به مداخله در یک تراکنش موجود داشته باشد، دستکاری تمام اطلاعات در همتایان دیگر، به طور همزمان غیرممکن است.

الگوریتم ۱ PBP

Input: Text:All Transactions
Output: Peer Key Block

1: **for** each transaction T, whose status(T) == *undecided* **do**
2: Check legality of T and assigned invalid or valid
3: **if** status(T) == *invalid* **then**
4: Remove T
5: **end if**
6: **end for**
7: **for** each time epochs **do**
8: Select $VTset$, in which each T satisfies status(T) == *valid*
9: **if** size($VTset$) $\leq$ 1M **then**
10: Write $VTset$ into a new PMB
11: **else**
12: ($VTset$) will be divided, and writen into several PMB with a size of 1M
13: **end if**
14: **end for**
15: **for** each PMB **do**
16: **if** status(PMB) == *undecided* **then**
17: Send PMB to *vp* set
18: **else if** status(PMB) == *invalid* **then**
19: Delete the PMB
20: Reassign each T to undecided
21: Return to step 1
22: **else if** status(PMB) == *valid* **then**
23: Each T is in effect
24: Write PMB into a new PKB
25: **end if**
26: **end for**

ب. الگوریتم اجماع تجارت الکترونیک

بعد از اینکه هر همتا PKB را تولید می‌کند، ساخت یک بلاکچین جهانی (بلاکچین E) برای حفظ تمام PKB در ETTN ضروری است. در ETTN، بلاکچین E یک شاخص برای تمام بلاکچین‌های همتا فراهم می‌کند، به طوری که هر همتا بتواند PMB دریافت شده از همتایان دیگر را تأیید کند. شکل ۴ ساختار بلوک را در بلاکچین E نشان می‌دهد. هر بلوک جهانی (EGB) حاوی یک گروه PKB، ساختار و فهرست رأی‌دهنده است.

در تجارت الکترونیک، اگر ما مکانیسم اثبات کار را برای تضمین EGB اتخاذ کنیم، منابع زیادی را مصرف خواهد کرد که نیازی به هدر دادن ندارند.

Hash value: <sha3 hash> Timestamp: <block creation timestamp> Owner: <public key of the node creating the block > Voter List: <list of federation nodes public keys> signature : <ECDSA signature of vote block >
Transaction List: <list of transactions >

(a) ساختار بلوک ریز همتا

Hash value: <sha3 hash> Timestamp: <block creation timestamp> Owner: <public key of the node creating the block >
Peer micro block List: <list of Micro block >

(b) ساختار بلوک کلید همتا

شکل ۳ – مدل بلوک در بلاکچین همتا

Hash value: <sha3 hash> Timestamp: <block creation timestamp> Constructor: <public key of the node creating the block > Voter List: <list of federation nodes public keys> signature : <ECDSA signature of vote block >
PKB List: <list of PKB >

شکل ٤ – مدل بلوک در بلاکچین E

به عبارت دیگر، هزینه‌ی پلتفرم تجارت الکترونیک افزایش خواهد یافت. به علاوه، مکانیسم اثبات کار باید مراقب مشکل معمای رمز باشد. در بیت کوین، مشکل معمای رمز که با این مقدار مشخص می‌شود، به طور پویا تطبیق داده می‌شود، طوری که بلوک‌ها در یک نرخ متوسط هر ده دقیقه یک بار تولید می‌شوند. هر چه مشکل دشوارتر باشد، به زمان بیشتری نیاز دارد. در تجارت الکترونیکی، برای پشتیبانی از تراکنش های فوری، لازم است که از یک مکانیسم مشارکتی بدون قربانی کردن امنیت استفاده شود که می‌تواند نهفتگی اجماع را کاهش دهد؛ بنابراین، ما یک مکانیسم مشارکتی را برای تولید EGB در هر دوره اتخاذ می‌نماییم. ابتدا، انتخاب یک یا تعداد بیشتری از گره‌ها از هر همتا برای تشکیل یک گروه gp که گروه ساخت و ساز جهانی (GCG) نامیده می‌شود و سپس، یک گره اولیه از تمام گره‌ها در GCG انتخاب خواهد شد، در نهایت در گره اولیه، الگوریتم PBFT برای تولید EGB اتخاذ می‌شود.

همان طور که در الگوریتم ۲ نشان داده شده است، ECA را می‌توان به دو مرحله تقسیم کرد: اول، ما باید یک گروه ساخت و ساز جهانی (GCG) ایجاد کنیم. هر گره (n) در شبکه، به طور تصادفی یک مجموعه از گره‌ها (nset) را از کل شبکه انتخاب می‌کند، سپس نتایج انتخاب را به سایر گره‌ها در شبکه ارسال می‌نماید. به علاوه، گره‌ها باید به همتایان بالای ۲/۳ از کل شبکه تعلق داشته باشند و نمی‌تواند بیش از ۲ برابر تعداد کل همتایان در کل شبکه باشد (فرض کنید که این شبکه شامل M همتا است و تعداد m گره انتخابی باشد، سپس $2/3M < m <= 2M$). پس از اتمام این فرآیند، تمام گره‌ها آرا را شمارش خواهند کرد و ۲M گره با بیش‌ترین تعداد آرا را به عنوان یک گروه ساخت و ساز جهانی در اختیار دارند. در این حالت، هویت هر گره تعیین خواهد شد. دوم، انتخاب یک گره اولیه (Pnode) از GCG برای ساخت EGB، یک روش مشابه ساخت GCG می‌باشد. هر گره در GCG، گره ساخت و ساز (cn) نامیده می‌شود. هر گره ساخت و ساز به طور تصادفی، یک گره ساخت و ساز را به عنوان هدف پیش انتخاب شده برای گره اولیه انتخاب می‌کند

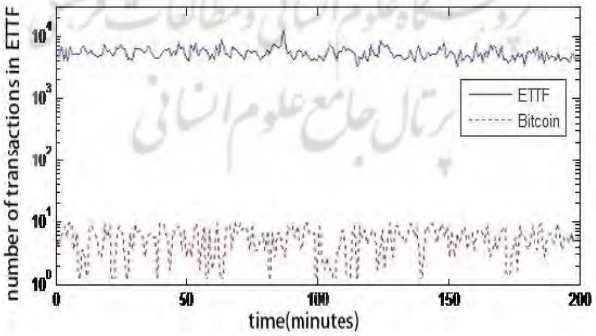
و نتیجه را به گره‌های ساخت و ساز دیگر ارسال می‌کند. پس از رأی‌گیری، گره ساخت و ساز که بیش‌ترین آرا را کسب می‌کند، به عنوان گره اولیه در نظر گرفته خواهد شد و مجوز تولید EGB را دارد. گره اولیه یک EGB می‌سازد و به گره‌های ساخت و ساز می‌فرستد. هر گره ساخت و ساز، قانونی بودن EGB را از EGB دریافت می‌کند. اگر EGB معتبر باشد، به گره‌های دیگر شبکه ارسال خواهد شد و گره اولیه بعه ساخت EGB بعدی ادامه می‌دهد. اگر EGB نامعتبر باشد، حذف خواهد شد و یک گره اصلی جدید برای ادامه انتخاب خواهد شد.

الگوریتم ۲ ECA

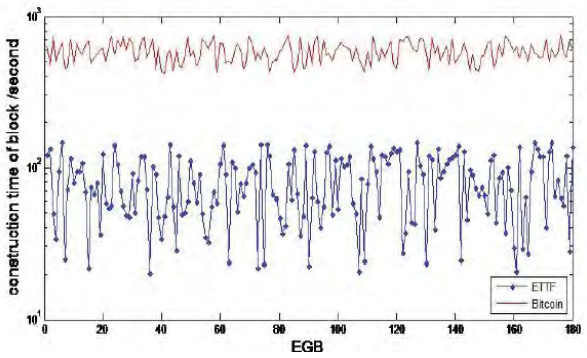
```
for each time epochs do
  for n_i in {n_1, ..., n_m} do
    votes ← Rselect nset, 2/3M ≤ Size(nset) ≤ 2M
    voteList ← GeneratevoteList(votes)
    SendcvoteList()
  end for
  voteList' ← AddvoteList(all voteList)
  GCG ←— top 2M nodes(voteList')
  for cn_i in GCG do
    cvotes ← Rselect cn_j, (1 ≤ j ≤ 2M)
    cvoteList ← GeneratecvoteList(cvotes)
    SendcvoteList()
  end for
  cvoteList' ← AddcvoteList(all cvotes)
  Pnode ← Select cn_i (Max(cvotes'))
  EGB ← constructEGB(Pnode)
  sendEGB()
  for cn_i in GCG do
    ValidateEGB()
    if status(EGB) == valid then
      SendEGB()
      NextEGB ← constructnextEGB(Pnode)
    else if status(EGB) == invalid then
      DeleteEGB()
      NextPnode ← selectNextPnode()
    end if
  end for
end for
```

۷. آزمایش‌ها

در این مقاله، ما برای پیاده‌سازی ETTF به فابریک و اترنت فنگ اشاره می‌کنیم.



شکل ۵ – تعداد تراکنش‌ها در هر ثانیه

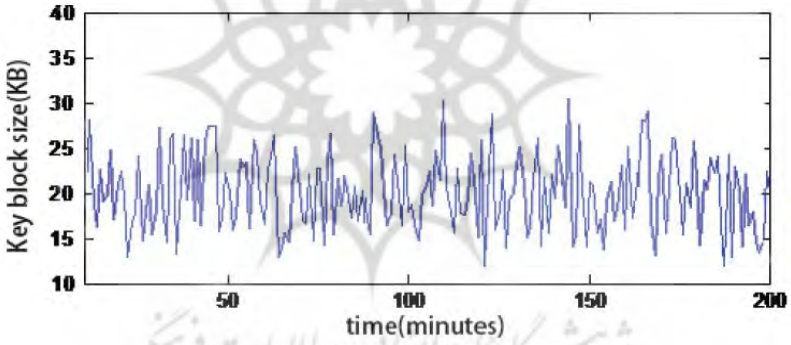


شکل ٦ – زمان ساخت EGB

محیط آزمایش به شرح زیر است: ۲۰ سرور، هر سرور با حافظه‌ی ۱۲۸G، CPU ۳۲ هسته‌ای، فضای ذخیره‌سازی ۱۰T و ارتباطات شبکه‌ی گیگابیت بین سرورها پیکربندی شده است و گره‌های بلاکچین از طریق فناوری داکر گنجانده شده‌اند. در این بخش، مجموعه‌ای از آزمایش‌ها را برای ارزیابی عملکرد ETTF توسط تغییر توان عملیاتی تراکنش، نهفتگی تراکنش و اندازه‌ی بلوک انجام دادیم. این بار ما ۳۰۰ گره را برای اجرای آزمایش انتخاب کردیم تا به طور کامل، بهبود عملکرد در ETTF را مورد مشاهده قرار دهیم.

الف. توان عملیاتی تراکنش

توان عملیاتی تجاری یک شاخص عملکرد مهم است. ویژگی‌های اصلی ETTF دو مورد هستند. اول، ETTF به هر تراکنش با همتای دیگر تخصیص می‌یابد و GP تنها مسئول حفظ مقدار هش بلوک در هر همتا می‌باشد.



شکل ۷ – اندازه‌ی EGB

بر این اساس: اطلاعات مربوط به تراکنش‌های نوشته شده در PMB، مقدار هش PMB در PKB ذخیره می‌شود و PKB، مقدار هش PMB را ذخیره می‌کند، کاملاً مشخص است که اندازه‌ی مقدار هش بسیار کوچک‌تر از هش قبل از داده‌های تراکنش است، بنابراین، به طور منطقی، EGB می‌تواند مقدار زیادی داده‌ی تراکنش را به کار ببرد. همان طور که در شکل ۶ نشان داده شده است، عملکرد ETTF در توان عملیاتی بهتر است و می‌تواند به توان عملیاتی بالاتری دست یابد.

ب. فرکانس بلوک

برای بیت کوین، اگر ما فرکانس تولید بلوک را با کاهش دشواری مدارک کار تغییر دهیم، امنیت تراکنش‌ها ممکن است کاهش پیدا کند. برای ETTF، ما فرکانس تولید قطعات ریز را تغییر می‌دهیم. برای هر فرکانس، ما اندازه‌ی بلوک را طوری انتخاب می‌کنیم که توان عملیاتی بار مفید با سیستم عملیاتی بیت کوین یکسان باشد.

در ETTF، به جای POW، ما در این مقاله، بلوک‌های مبتنی بر PBFT را می‌سازیم و و وضعیت ارتباطات شبکه نسبتاً خوب است، بنابراین، تأخیر بسیار کمتر خواهد بود. شکل ۶ نشان می‌دهد که تولید یک EGB در ETTF زمان کمتری نسبت به ساخت در بلاکچین برگرفته از بیت کوین مصرف می‌کند.

ج. اندازه‌ی بلوک

در ETTF، هر کاربر می‌تواند یک تراکنش را در یک زمان انجام دهد؛ و محتوای هر EGB فقط شامل یک مجموعه از مقدار هش است، درست مانند PKB و PMB، به طوری که اندازه‌ی بلوک جهانی خیلی کوچک است، فقط چند KB به صورت نشان داده شده در شکل ۷ است.

۸. نتیجه‌گیری

با توسعه‌ی داده‌های پلتفرم تجارت الکترونیک، مدیریت داده‌های پلتفرم تجارت الکترونیک بیش از پیش مورد توجه قرار گرفته است. برای این مقاله، می‌توان به طور خلاصه، ادغام فناوری بلاکچین در سیستم پایگاه داده‌ی پلتفرم کسب و کار تجارت الکترونیک را بیان کرد که برای حفاظت داده‌ها از مسائل رخنه و شکاف در داده‌ها ضروری است. این روش به طور قابل‌توجهی بهتر از پیاده‌سازی یک سیستم پایگاه داده‌ی سنتی است چرا که توسط هکرها به راحتی مورد حمله قرار می‌گیرد و یا از فناوری بلاکچین، به عنوان سیستم پایگاه داده استفاده می‌شود که برای فرآیند کسب و کار روزانه ناکارآمد است. سیستم پیشنهادی می‌تواند از عملیات کسب و کار خرده‌فروشی‌های آنلاین با یک مخزن کارآمد و با ثبات با مشخصات آن پشتیبانی کند. با این حال، محدودیت تحقیقات از جمله هزینه‌های بالا، باید با مطالعه‌ی بیشتر در مورد فناوری بلاکچین بهبود یابند. علاوه بر این، این سیستم نیازمند تیم‌های فنی بسیار ماهر برای پشتیبانی از این سیستم است که یکی از چالش‌ها برای سازمان‌ها باید از طریق تحقیقات عمیق آتی حل شود.

سیستم پردازش تراکنش با استفاده از فناوری بلاکچین، اثبات عدم آگاهی و رمزنگاری پنهان منحنی بیضوی اصلاح شده طراحی شده است. سیستم پردازش تراکنش، امنیت تراکنش‌های تجارت الکترونیک را با ارائه‌ی خدمات محرمانگی و یکپارچگی افزایش می‌دهد. روش تشخیص حمله‌ی DoS پیشنهاد شده است که از بهینه‌سازی ازدحام کرم شب‌تاب مبتنی بر اجازه‌ی شبکه‌ی عصبی بردار پشتیبان برای تشخیص حمله‌ی DoS استفاده می‌کند. طراحی GSO – SVNN می‌تواند بر تمام اشکالات مذکور در مقالات فایق آید. روش پیشنهادی تشخیص حمله‌ی DoS، عملکرد بهتری را از لحاظ صحت و دقت در مقایسه با سایر روش‌های موجود نشان می‌دهد. با ارائه‌ی دو مدل راهکار امنیتی، حفظ محرمانگی و یکپارچگی تراکنش‌های تجارت الکترونیکی آسان است.

در جامعه‌ی امروز، تجارت الکترونیک نقش مهمی در زندگی ما، از پرداخت موبایل گرفته تا سپرده بانکی دارد، بنابراین، امنیت و کارایی آن به یک موضوع مهم تبدیل شده است. رمزنگاری، بعد اصلی تحقیق در خصوص مسائل مربوط به آن است. بلاکچین برگرفته از بیت کوین با مجموعه‌ای از ترکیبات فناوری مانند ذخیره‌سازی توزیع شده، برچسب زمان، رمزنگاری هش و غیره، محیط تجارت الکترونیک مورد اعتماد را فراهم می‌کند؛ اما امنیت با قربانی کردن کارایی بازمی-گردد، برای مثال، تولید یک بلوک داده هر ۱۰ دقیقه، از انشعاب بلاکچین جلوگیری می‌کند. علاوه بر این، اندازه‌ی بلوک‌ها به شدت محدود است که تعداد و فرکانس تراکنش‌ها را محدود می‌کند.

برای برطرف کردن این عامل کندکننده، تجارت فوری و مقیاس بزرگ بدون قربانی کردن اعتبار لازم است. این مقاله، یک چارچوب تجاری مورد اعتماد در تجارت الکترونیک (ETTF) را ارائه می‌دهد. ETTF، بر مبنای ساختار بلاکچین

و یک الگوریتم اجماع قوی است، اندازه‌ی بلوک‌ها را محدود نمی‌کند، از تراکنش‌های فوری پشتیبانی می‌کند و هیچ انشعابی در بلاکچین ندارد. ETTF شامل دو بخش است: اول، پروتکل بلاکچین همتا (PBP) که در هر دوره پیش می‌رود و می‌تواند از امنیت تراکنش‌ها در همتا حفاظت کند. در بین آنها، یک الگوریتم انتشار (EPA)، از مکانیسم رأی‌گیری و مکانیسم چرخش استفاده می‌کند و مجموعه‌ی vp به جای تمام نقاط، به طور موثر هزینه‌های ارتباطات را کاهش می‌دهد. دوم، الگوریتم اجماع جهانی (ECA) از عدم صداقت همتاها برای دستکاری تراکنش همتای دیگر با نوشتن مقدار هش یک بلوک به بلوک جهانی در هر دوره جلوگیری می‌کند و تراکنش های فوری را انجام می‌دهد. ETTF، دستیابی به توان عملیاتی بالاتر و نهفتگی اجماع پایین‌تر را توسط بهبود مقیاس‌پذیری پروتکل بلاکچین ممکن می‌سازد که در آن کلید نهفتگی، توانایی یک همتای واحد است. ETTF به تمام همتایان در شبکه کمک می‌کند تا با یک سیستم عمومی، مورد اعتماد مستقل غیرمتمرکز همکاری کنند که عملکرد بهتر در تجارت الکترونیک را نشان می‌دهد.

۹. منابع و ماخذ

1. Gao, F. (۲۰۱۹). Data encryption algorithm for e-commerce platform based on blockchain technology. Discrete & Continuous Dynamical Systems-S, ۱۲(٤&٥), ۱٤٥٧.
2. Shaikh, J. R., & Iliev, G. (۲۰۱۸). Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security. ۲۰۱۸IEEE Global Conference on Wireless Computing and Networking (GCWCN),
3. Xie, W., Zhou, W., Kong, L., Zhang, X., Min, X., Xiao, Z., & Li, Q. (۲۰۱۸). Ettf: A trusted trading framework using blockchain in e-commerce. ۲۰۱۸IEEE ۲۲nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)),
4. Xuan, T. M., Alrashdan, M. T., Al-Maatouk, Q., & Alrashdan, M. T. (۲۰۲۰). Blockchain Technology in E-Commerce Platform. International Journal of Management.۱٦۹۷-۱٦۸۸ ,(۱۰)۱۱ ,

Investigate the security improvement of online businesses using blockchain technology

Mahshid Soltansalimi [1]

Date of Receipt: 2021/05/15 Date of Issue: 2021/05/27

Abstract

The growth of the Internet introduced new ways on how customers receive services and how companies run their operations. In the current days internet connection and relevant services that it provides are essential for the majority of people. One of those services or industries is ecommerce In recent years, Electronic Commerce (E-commerce) applications are attracting many users and merchants to conduct their daily business online which includes payment of bills, online banking, buying tickets and purchasing goods etc. E-commerce transaction security is a major concern for E-commerce websites along with its customers. In E-commerce, the security technology has become a major issue restricting the rapid development and popularization of E-commerce. Existing solutions leverage blockchain protocols to improve the credibility of transactions, but most of them have some limitations, such as a lower throughput and higher consensus latency, and these problems make blockchain technology difficult to be widely used. This paper presents a trusted framework (ETT F) using blockchain protocol in E-commerce to achieve a higher credible trading. ETTF includes a peer blockchain protocol (PBP) based on a peer blockchain architecture to support the storage of massive transactions and instant transactions. In PBP, the throughput scales are nearly linearly increased with the computation: the more computing power available, the more blocks are selected per unit time. Besides, in order to ensure a higher security of transactions we have introduced a strong consensus algorithm(ECA) in E-commerce. ETTF is also efficient because the number of messages it requires is nearly linear in the network size. Compared to Bitcoin-derived blockchain, ETTF shows better performance on throughput, latency, and capacity in E-commerce.

Keyword

Blockchain, consensus mechanism, instant, trusted, Blockchain, E-Commerece, Cybersecurity, DoS, ECC

1. A master's degree in IT management, Faculty of Humanities, Payame Noor University, Tehran, Iran (mahshid.ssalimi@gmail.com).