علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۸، شماره ۲، ۱۳۹۹
صفحات ۲۱- ۳۰
مقاله عادی

نشریه علوم رایانش و فناوری اطلاعات

ارائه مدلی مبتنی بر بلاک‌چین قابل ویرایش برای ذخیره سازی و انتقال مدارک و اعتبارهای علمی

سعید شکرالهی [۱*]، محمد سعید مصلح نژاد [۲]

*نویسنده مسئول، دریافت: ۱۴۰۰/۰۲/۱۶، بازنگری: ۱۴۰۰/۰۳/۰۲، پذیرش: ۱۴۰۰/۰۳/۰۹

[۱] استادیار، گروه امنیت شبکه و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران
[۲] دانشجوی کارشناسی ارشد، رشته مخابرات امن و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران

چکیده

امروزه با پیشرفت علم و فناوری، اکثر دانشگاه‌ها، مؤسسات آموزشی و سازمان‌ها برای حوزه آموزش خود از یادگیری الکترونیکی استفاده می‌کنند که با ظهور بیماری کووید ۱۹ این موضوع بیش از پیش مورد توجه قرار گرفته است. یکی از فناوری‌هایی که در سال‌های اخیر در زیرساخت سیستم‌های یادگیری الکترونیکی مورد توجه قرار گرفته است فناوری بلاک‌چین است. صدور گواهینامه‌های دیجیتال، حقوق مالکیت فکری و امور مالی دانشگاه‌ها و مؤسسات آموزشی از جمله زمینه‌هایی است که از بلاک‌چین در زیرساخت‌های آنها استفاده شده است. زیرساخت انتقال نمرات و اعتبارهای علمی دانشجویان نیز ازجمله مواردی است که می‌توان از بلاک‌چین در آن بهره برد. در این مقاله مدلی مبتنی بر بلاک‌چین قابل ویرایش برای ذخیره‌سازی و انتقال اطلاعات دانشجویان و اعتبار علمی دانشجویان پیشنهاد شده است. این مدل می‌تواند یک سیستم سراسری قابل اعتماد، غیرمتمرکز و قابل ویرایش که استفاده از آن آسان بوده و به هیچ مدیریت مرکزی نیاز ندارد را در اختیار دانشجویان، دانشگاه‌ها و سازمان‌ها قرار دهد. استانداردها و الگوریتم‌های استفاده شده در مدل پیشنهادی، امنیت، انعطاف‌پذیری و مقیاس‌پذیری این مدل را در سطح مطلوبی قرار می‌دهد. نتایج پیاده‌سازی مدل پیشنهادی نشان می‌دهد که زمان تولید و تأیید تراکنش‌های دانشجویان، مدت زمان به‌روزرسانی و حجم آنها قابل قبول است.

کلمات کلیدی: بلاک‌چین قابل ویرایش، یادگیری الکترونیکی، الگوریتم درهم‌ساز آفتاب‌پرست، نظام اروپایی انتقال واحدهای درسی.

۱- مقدمه

در بسیاری از کشورهای دنیا، وابستگی حوزه‌های مختلف به آموزش سبب شده است که این حوزه از اهمیت خاصی برخوردار باشد. امروزه با پیشرفت علم و فناوری، اکثر دانشگاه‌ها، مؤسسات آموزشی و سازمان‌ها برای حوزه آموزش از یادگیری الکترونیکی استفاده می‌کنند. یادگیری الکترونیکی را می‌توان کاربرد هدفمند فناوری اطلاعات و ارتباطات در فرایند تدریس و یادگیری دانست [۱]. البته اصطلاحاتی همچون یادگیری برخط، یادگیری مجازی، یادگیری مبتنی بر وب نیز برای این شیوه از یادگیری مورد استفاده قرار می‌گیرد. یکی از فناوری‌هایی که در سال‌های اخیر در زیرساخت سیستم‌های یادگیری الکترونیکی مورد توجه قرار گرفته است، بلاک‌چین[۱] است [۲]. اولین ایده بلاک‌چین، در سال ۱۹۹۱ در کارهای دو دانشمند آمریکایی به نام استوارت هابر و اسکات استورنتا توصیف شد [۳]. در سال ۱۹۹۲، بایر، هابر و استورنتا از یک درخت درهم‌سازی استفاده کرده که اجازه می‌داد چندین سند در یک بلوک جمع‌آوری شود [۴،۵]. مفهوم اولیه بلاک‌چین توسط ساتوشی ناکاموتو در سال ۲۰۰۸ با افزودن ایده‌ای نوآورانه، یعنی استخراج ارز دیجیتال معرفی شد [۶]. این فناوری یک سال بعد به‌عنوان یک جزء اصلی از بیت‌کوین اجرا شد. در سال ۲۰۱۷ آتنی و همکاران [۱۶] با استفاده از درهم‌ساز آفتاب‌پرست[۲] اولین بلاک‌چین قابل ویرایش[۳] را ارئه داد. در سال‌های اخیر، بلاک‌چین در صدور گواهینامه‌های دیجیتال، حقوق مالکیت فکری، اقتصاد آموزشی و مسائل مالی مؤسسات آموزشی مورد توجه قرار گرفته است.

با توجه به مقررات کلی حفاظت از داده‌های اتحادیه اروپا[۴]، حق کنترل داده‌ها به شهروندان و ساکنان این منطقه داده شده است. این آیین‌نامه، از نظر قانونی دیگر امکان استفاده از بلاک‌چین‌های تغییرناپذیر در فرایندهایی که داده‌های شخصی در بلاک‌چین‌ها ثبت می‌شوند را نمی‌دهند. ذخیره‌سازی و انتقال نمرات،

مدارک تحصیلی و اعتبارهای علمی دانشجویان نیز ازجمله زیرساخت‌های مرتبط با سیستم‌های یادگیری الکترونیکی است. به دلیل احتمال بروز خطای انسانی در سطح دانشگاه‌ها در ثبت نمرات، مدارک تحصیلی و اعتبارهای علمی و با توجه به تغییرناپذیری بلاک‌چین‌های سنتی، ما می‌توانیم از بلاک‌چین قابل ویرایش برای ایجاد انعطاف‌پذیری بیشتر سیستم استفاده کنیم. در حال حاضر، بسیاری از دانشگاه‌ها رکوردهای مربوط به نمرات و اعتبار دانشجویان را در پایگاه داده‌ای متمرکز قرار می‌دهند که با قوانین سخت‌گیرانه‌ای برای دانشجویان قابل دسترسی هستند. از آنجایی‌که این داده با سایر دانشگاه‌ها به اشتراک گذاشته نمی‌شود معمولاً انتقال دانشجویان به سایر دانشگاه‌ها با مشکلاتی در این زمینه همراه است. این مشکل زمانی که دانشجو می‌خواهد به دانشگاهی در کشوری دیگر منتقل شود پررنگ‌تر می‌شود. با توجه به اینکه رکوردهای مربوط به نمرات و اعتبار دانشجویان با استانداردهای مختلفی ذخیره می‌شوند مشکلاتی را برای تبادل آنها بین دانشگاه‌ها به وجود می‌آورد. همچنین وقتی دانشجویان در کشورهای مختلف برای شغلی اقدام می‌کنند، برای دسترسی به نمرات و اعتبار علمی خود با مشکل روبرو هستند. آنها نیاز دارند مدارک و اعتبار علمی خود را ترجمه کرده که این موضوع هزینه و زمان را برای دانشجویان در پی خواهد داشت. برای حل مشکلات مطرح شده، در این مقاله، مدلی غیرمتمرکز مبتنی بر بلاک‌چین کنسرسیوم قابل ویرایش برای ذخیره‌سازی منسجم نمرات، مدارک تحصیلی و اعتبارهای علمی دانشجویان در سطح یک تراکنش ارائه خواهد شد. همچنین با کمک گرفتن از درهم‌ساز آفتاب‌پرست راهکاری برای امکان انتقال مدارک تحصیلی و اعتبارهای علمی دانشجویان ارائه خواهد شد. این مدل می‌تواند به عنوان یکی از زیرساخت‌ها در یادگیری الکترونیکی مورد استفاده قرار گرفته و نمرات، مدارک و اعتبارهای علمی را به‌صورت قابل اعتماد و غیرمتمرکز در اختیار دانشجویان، دانشگاه‌ها و سازمان‌ها قرار دهد.

ساختار ادامه مطالب این مقاله به شکل زیر است. در بخش دوم، برخی از کارهای مرتبط در زمینه استفاده از بلاک‌چین در زیرساخت‌های یادگیری الکترونیکی بررسی می‌شود. بخش سوم پس‌زمینه‌ای از بلاک‌چین کنسرسیوم قابل ویرایش و مفاهیم مرتبط را ارائه می‌کند. در بخش چهارم، مدلی مبتنی بر بلاک‌چین کنسرسیوم قابل ویرایش برای ذخیره‌سازی و انتقال نمرات، مدارک تحصیلی و اعتبارهای علمی دانشجویان در سیستم یادگیری الکترونیکی پیشنهاد می‌شود. بخش پنجم به ارزیابی مدل پیشنهادی می‌پردازد. در بخش ششم نتیجه‌گیری مقاله ارائه خواهد شد.

۲- کارهای مرتبط

در بیشترکارهای انجام شده، از بلاک‌چین برای ذخیره‌سازی نمرات و صدور گواهی‌های دیجیتال استفاده شده است. استفاده از سیستم گواهی دیجیتال بر بستر بلاک‌چین به دلیل امنیت بالا، تغییرناپذیری و اطمینان‌پذیری از عدم امکان جعل باعث افزایش اعتبار این گواهی‌ها می‌شود. دانشگاه و مؤسسه فناوری ماساچوست [۳] که در آموزش متخصصین در حوزه‌های مختلف فناوری‌های پیشرفته سرآمد است، یک سکوی آموزشی برای ذخیره‌سازی دیجیتال مدارک فارغ‌التحصیلان ارائه کرده است. دانشگاه نیکوسیا در قبرس و همچنین دانشگاه ملی لاپلاتا [۴] از بلاک‌چین برای ذخیره‌سازی اطلاعات مربوط به دانشجویان خود و مدارک تحصیلی آنها استفاده کرده‌اند. بخش آموزش متعلق به شرکت بزرگ سونی، یک سکو مبتنی بر بلاک‌چین برای ارزیابی نمره‌های افراد و ذخیره سازی اطلاعات آموزشی و سوابق تحصیلی راه‌اندازی کرده است [۷]. شارپلس و دومینگو [۸] سیستم توزیع‌شده‌ای ارائه داده‌اند که نه تنها فعالیت‌های دانشگاهی دانشجویان را ذخیره می‌کند بلکه نتایج فعالیت‌های غیرعلمی مانند سوابق کارآموزی و مهارت‌های فردی و دوره‌های تخصصی گذرانده شده را ذخیره و ارزیابی می‌کند. با این داده‌های ذخیره‌شده، کارفرمایان می‌توانند اطلاعات مربوط به یک کارمند را به‌راحتی، سریع و بدون هیچ تردیدی به دست آورند. یانگ [۹] در سال ۲۰۱۷ نرم‌افزاری را در زمینه آموزش بر پایه بلاک‌چین ارائه داده است که با به اشتراک‌گذاری داده‌های آموزشی با دیگر دانشگاه‌ها و مراکز استخدامی در هر نقطه از جهان، موجب دسترسی به سوابق تحصیلی و کاری افراد با سهولت و اطمینان بیشتر شده است. در [۱۰] یک سیستم بر پایه سکوی بلاک‌چین اتریوم برنامه‌ریزی شده است که گواهی دیجیتال صادر می‌کند. در این سیستم، مرکز آموزشی صادرکننده گواهی، دانش آموختگان و گروه پشتیبانی به گواهی‌های صادرشده دسترسی دارند. در [۱۱] سیستمی مبتنی بر بلاک‌چین ارائه شده است که ابتدا فایل الکترونیکی گواهینامه کاغذی و اطلاعات آموزشی و دیگر داده‌های مرتبط به دانشجویان را دریافت کرده و به همراه درهم‌ساز مربوط به هر فایل الکترونیکی در بلاک‌چین ذخیره می‌کند. در این سیستم پس از تأیید اطلاعات یک کد کیوآر و یک سریال مختص به هر گواهی ایجاد و در سیستم ذخیره می‌شود. دانشجویان در هر زمان می‌توانند با داشتن کد کیوآر یا سریال خود به گواهی و مدرک مورد نیاز خود دسترسی داشته باشند. همچنین با استفاده از این روش هزینه کاغذ و چاپ و نگهداری اسناد کاهش یافته و افراد به‌راحتی می‌توانند سوابق تحصیلی و کاری خود را با اطمینان برای کارفرمایان ارائه دهند. در بسیاری ازکارهای انجام‌شده، از بلاک‌چین و ارزهای دیجیتال مبتنی بر آن در امور مالی استفاده شده است که دانشگاه‌ها و مؤسسات آموزشی نیز می‌توانند از آن در امور مالی خود استفاده کنند [۱۲]. در این‌صورت محاسبه بورس دانشجویان و دستمزد استادان بهبود یافته و سازوکار شفاف و عادلانه‌ای برای کمک‌های مالی سرمایه‌گذاری فراهم شده است. در برخی دیگر از کارهای انجام‌شده، از بلاک‌چین برای حفاظت از حقوق مالکیت فکری استفاده شده است. فراسین گری، مدیر کل سازمان جهانی مالکیت فکری از فناوری بلاک‌چین به عنوان فرصتی برای حفاظت از حقوق مالکیت فکری نام برده است که عملکرد این فناوری می تواند بسیاری از مشکلات مربوط به حفاظت مالکیت معنوی را حل کند. فناوری بلاک‌چین می تواند یک پایگاه داده غیر متمرکز و امن را برای ذخیره محتوای الکترونیکی و دروس بارگذاری شده فراهم کند. به این صورت که کلیه داده ها در بلاک‌های مربوطه ثبت می‌شوند بنابراین این سیستم قادر است نشان دهد که محتوای مورد نظر دقیقاً در چه زمانی ایجاد شده، مالکیت اثر مربوط به کیست و همچنین می-تواند اصالت و اعتبار آنها را با سهولت و سرعت و دقت بیشتری تشخیص و تأیید کند. بنابراین، ثبت کلیه اطلاعات رسمی در سیستم بلاک‌چین موجب ایجاد بستری برای جلوگیری از استفاده غیر قانونی در اینترنت و به‌خصوص شبکه‌های اجتماعی برای مالکان و مدرسین خواهد شد[۵،۱۳].

۳- پس زمینه

در این بخش پس زمینه‌ای از بلاک‌چین قابل ویرایش و مفاهیم مرتبط با آن ارائه می‌شود.

۳-۱- بلاک‌چین

فناوری بلاک‌چین، پایگاه‌داده‌ای توزیع‌شده است که اطلاعات به‌صورت زنجیرشده و کاملا شفاف در آن نگهداری می‌شود و قادر به ذخیره و حسابرسی تمامی تعاملات است [۶]. در حقیقت این فناوری یک دفتر حسابرسی توزیع شده را ارائه می‌کند که حاوی تراکنش‌های مربوط به یک کاربرد است. این تراکنش‌ها قابل اعتماد، قابل‌حسابرسی و غیرقابل تغییر خواهند بود. با توجه به کاربردهای مختلف، بلوک‌های موجود در بلاک‌چین اطلاعات متفاوتی را در خود جای می‌دهند. یک بلوک، شامل مقدار درهم‌سازی شده‌ی بلوک قبل، سربار، امضای سازنده بلوک و مهر زمانی است. مقدار درهم سازی شده‌ی بلوک قبلی، باعث می‌شود که بلوک‌ها غیرقابل تغییر شوند. سربار بلوک‌ها، می‌تواند با توجه به

کاربردهای مختلف، شامل اطلاعات متفاوتی باشد که این اطلاعات می‌تواند یک تراکنش یا آدرس اشاره‌گر به اطلاعات اصلی باشد. در شبکه بلاک‌چین، استخراج‌کننده‌ها و اعتبارسنج‌ها دو نهاد ارزشمند هستند. استخراج‌کننده‌ها به نودهایی گفته می‌شوند که بلوک‌های جدیدی را تولید می‌کنند. البته در کاربردهای مختلف بلاک‌چین، استخراج‌کننده‌ها می‌توانند نقش متفاوتی داشته باشند. به‌عنوان‌مثال در بیت کوین، استخراج‌کننده‌ها، نودهایی هستند که عملیات درستی عملکرد را انجام می‌دهند. بلوک‌های جدید، پس از اعتبارسنجی توسط اعتبارسنج‌ها مجاز شناخته می‌شوند. عملیات تولید، اعتبارسنجی و افزودن بلوک جدید به بلاک‌چین را عملیات استخراج گویند. با توجه به حفظ امنیت و قابل‌اطمینان بودن عملیات استخراج، وجود الگوریتم‌های اجماع در بلاک‌چین حیاتی است که این الگوریتم موظف به انتخاب شخص نگه‌دارنده اطلاعات و نیز چگونگی اعتبارسنجی بلوک جدید است. با توجه به نیازمندی‌ها و کاربردهای مختلف، می‌توان بلاک‌چین را به سه دسته تقسیم کرد. بلاک‌چین عمومی که در آن هرکسی می‌تواند به اطلاعات دسترسی داشته باشد و تراکنش انجام دهد. این نوع بلاک‌چین بصورت آشکار در اینترنت قرار می‌گیرد. بلاک‌چین خصوصی که در آن مرجع یا سازمانی، حقوق دسترسی به اطلاعات را بررسی و کنترل می‌کند. بلاک‌چین کنسرسیوم[۵] که توسط سازمان‌های مختلفی مدیریت می‌شود و تنها سازمان‌های موجود در سیستم، توانایی دسترسی به بلاک‌چین را دارند. بلاک‌چین‌ها می‌توانند به‌صورت قابل ویرایش ارائه شوند که در اینصورت در دو سطح ارائه می‌شوند. بلاک‌چین‌هایی در سطح بلوک قابلیت ویرایش را دارند که در آنها امکان حذف یا افزودن تراکنش به یک بلوک در زنجیره بلاک‌چین وجود داشته باشد. همچنین، بلاک‌چین‌هایی در سطح تراکنش قابلیت ویرایش را دارند که در آنها امکان ویرایش تراکنش‌های هر بلوک در زنجیره بلاک‌چین وجود دارد.

۳-۲- درهم‌ساز آفتاب‌پرست

درهم‌ساز آفتاب‌پرست اولین بار توسط رابین و همکاران در سال ۲۰۰۰ پیشنهاد شد[۱۵]. درهم‌ساز آفتاب‌پرست یک عملکرد مهم در امضای آفتاب‌پرست محسوب می‌شود. این درهم‌ساز در ابتدا به این منظور طراحی شده بود که به گیرنده اجازه نمی‌داد که بدون رضایت امضاءکننده، محتوای اطلاعات امضاءشده را برای کسی فاش کند. درهم‌سازآفتاب‌پرست را می‌توان به‌عنوان یک تابع درهم‌ساز رمزنگاری‌شده در نظر گرفت که شامل یک دریچه است. اگر دریچه وجود نداشته باشد، تابع درهم‌ساز در برابر برخورد مقاوم خواهد بود اما با آگاهی از دریچه قابل انعطاف است. آتنی و همکاران [۱۶] روشی را پیشنهاد کردند که از درهم‌ساز آفتاب‌پرست برای جایگزینی عملکرد درهم‌سازی در بلوک استفاده می‌شد تا زنجیره بلوک‌ها قابل تغییر باشند. پس از آن، درلر و همکاران [۱۷] از تابع درهم‌ساز مبتنی بر قوانین برای اجرای بازنویسی در سطح تراکنش استفاده کردند. در نتیجه این روش از ویرایش ریزدانه و قابل کنترل در سطح تراکنش پشتیبانی می‌کند. درهم‌ساز آفتاب‌پرست که توسط آتنی و همکاران [۱۶] ارائه شده است به‌صورت زیر تعریف می‌شود.

- الگوریتم تولید کلید: الگوریتم تولید کلید، پارامتر امنیتی $k \epsilon N$ را به‌عنوان ورودی می‌گیرد و یک کلید درهم‌ساز عمومی hk و یک کلید مخفی tk را در خروجی می دهد.
- الگوریتم تولید درهم‌ساز آفتاب‌پرست: الگوریتم درهم‌ساز آفتاب‌پرست به‌عنوان ورودی یک کلید درهم‌ساز عمومی hk ، یک پیام m و (r,s) را می‌گیرد، به‌طوری که r و s عددهای تصادفی هستند و در خروجی یک درهم‌ساز آفتاب‌پرست h را تولید می‌کند.
- الگوریتم تأیید درهم‌ساز آفتاب‌پرست: الگوریتم تأیید در ورودی یک کلید درهم‌ساز hk ، یک پیام m و (s,r,h) را می‌گیرد. اگر و فقط اگر $h = CH.Hash(s,r;m,hk)$ باشد d=1 را برمی‌گرداند و در غیر این صورت، d برابر صفر خواهد بود.
- الگوریتم پیدا کردن برخورد تصادفی: الگوریتم پیدا کردن برخورد تصادفی به‌عنوان ورودی یک کلید دریچه tk، یک درهم‌ساز آفتاب‌پرست h و یک پیام جدید m' را به‌عنوان ورودی می‌گیرد و یک جفت دوتایی جدید (s',r') را به گونه‌ای که رابطه $h = CH.Hash(s',r';m',hk)$ صدق کند، برمی‌گرداند. اگر (m,h,tk) نامعتبر باشد، الگوریتم NULL را برمی‌گرداند.

۳-۳- لگاریتم گسسته

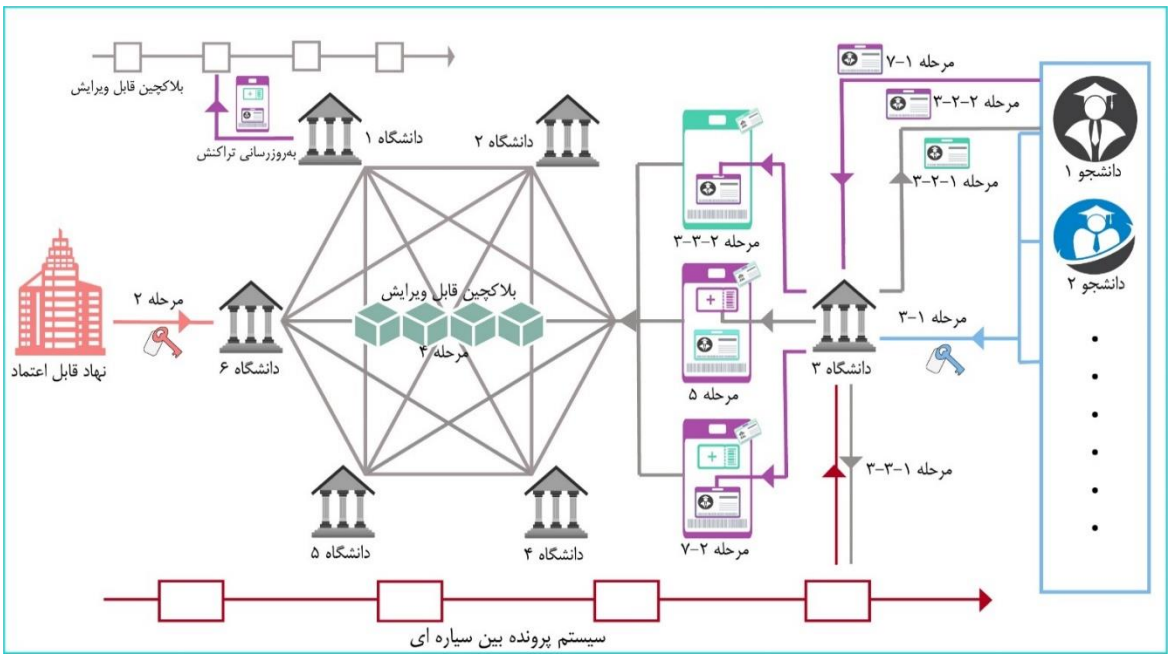
مسئله لگاریتم گسسته (DLP): فرض کنید، G یک گروه ضرب دوری است که توسط g با مرتبه‌ی اول q تولید شده است. برای هر دشمن زمان چند جمله‌ای احتمالی (PPT) A، احتمال یافتن $x \epsilon \mathbb{Z}_q^*$ برای برآوردن معادله $y = g^x$ با آگاهی از پارامترهای g و y ناچیز است.

۳-۴- سیستم پرونده بین سیاره‌ای

سیستم پرونده بین سیاره‌ای[۶] (IPFS)، یک سیستم فایل توزیع‌شده نظیربه‌نظیر است که به دنبال اتصال همه دستگاه های محاسباتی با همان سیستم پرونده‌ها است. IPFS یک مدل ذخیره‌سازی با کارایی بالا برای ذخیره‌سازی داده درون بلوک است. IPFS بین داده و آدرس ذخیره‌سازی داده پیوند ایجاد می‌کند. این فناوری از جمله جداول درهم‌ساز توزیع شده (DHT) و تبادل بلوک با انگیزه ترکیب شده است. مزیت IPFS نسبت به فضای ذخیره‌سازی ابری موجود این است که سرور مرکزی وجود ندارد و داده‌ها در مکان‌های مختلف جهان توزیع و ذخیره می‌شوند. با بارگذاری پرونده در سیستم IPFS، یک رشته درهم‌سازی شده منحصر به فرد مرتبط با پرونده دریافت می‌کنیم که از طریق آن می‌توان پرونده را بازیابی کرد. رشته درهم‌سازی شده را می‌توان به‌عنوان یک منبع‌یاب یکنواخت (URL) در وب فرض کرد. در مدل پیشنهادی از رشته درهم‌سازی شده به عنوان محل قرارگیری پرونده مدارک تحصیلی مرتبط با دانشجو اشاره خواهیم کرد. در کاربردهای عملی، بلاک‌چین برای ذخیره پرونده‌های بزرگ مناسب نیست. بنابراین، در این طرح، پرونده تحصیلی دانشجو توسط دانشگاه رمزگذاری شده و در IPFS ذخیره می‌شود.

۴- مدل پیشنهادی

در این بخش به ارائه یک مدل غیرمتمرکز مبتنی بر بلاک‌چین کنسرسیوم قابل ویرایش برای ذخیره‌سازی منسجم نمرات، مدارک تحصیلی و اعتبارهای علمی هر دانشجو در سطح یک تراکنش می‌پردازیم. درواقع در این مدل، با استفاده از بلاک‌چین قابل ویرایش در سطح تراکنش، بین هر دانشجو و یک تراکنش مشخص پیوند ایجاد می‌شود. این پیوند به‌نحوی است که فرایندهای مرتبط با دانشجو از جمله ثبت درخواست‌های دانشجو، ثبت اعتبارهای علمی و غیره در طول مدت زمان تحصیل دانشجو با به‌روزرسانی تراکنش دانشجو در تراکنش قرار می‌گیرند. همچنین نشان خواهیم داد که در مدل ارائه شده فرایند انتقال مجوز ویرایش تراکنش دانشجو از دانشگاهی به دانشگاه دیگرچگونه خواهد بود. باید توجه داشت که انتقال نمره و اعتبار در این مدل طبق نظام اروپایی انتقال واحدهای درسی[۷] (ECTS) صورت می‌گیرد. در مدل ارائه شده برای افزایش امنیت، انعطاف‌پذیری و مقیاس‌پذیری بلاک‌چین از الگوریتم اجماع تحمل خطای بیزانس عملی (PBFT) استفاده شده است. شکل ۱ شمای کلی از مدل پیشنهادی را ارائه می‌کند. در مدل ارائه شده دو نوع تراکنش وجود دارد. نوع اول به تراکنشی گفته می‌شود که برای ثبت دانشجو جدید یا انتقال دانشجو از دانشگاهی به دانشگاه دیگر توسط دانشگاه در شبکه بلاک‌چین ارسال می‌شود. از این پس در این مقاله



شکل ۱- شمای کلی از مدل پیشنهادی

این نوع از تراکنش با عنوان تراکنش دانشجو بیان خواهد شد. نوع دوم، تراکنشی است که برای ویرایش یا به‌روزرسانی تراکنش دانشجو در شبکه ارسال می‌شود و با عنوان تراکنش به‌روزرسانی بیان خواهد شد.

۴-۱- روش انتقال نمره و اعتبار در مدل پیشنهادی

در مدل پیشنهادی برای انتقال نمره و اعتبار از نظام اروپایی انتقال واحدهای درسی استفاده می‌شود. امروزه تحصیل در خارج از کشور به دلیل برخوداری از کیفیت آموزشی بهتر و ایجاد فرصت‌های شغلی مناسب‌تر علاقمندانی را در بین دانشجویان کشورهای مختلف دارد. سالانه دانشجویان بی‌شماری در سراسر دنیا اقدام به ارسال مدارک تحصیلی خود برای دریافت پذیرش از دانشگاه‌های کشورهای دیگر می‌نمایند. این دانشجویان لازم است رزومه تحصیلی و علمی خود را برای دانشگاه‌های مورد نظر ارسال نمایند. یکی از چالش‌های اساسی در این زمینه این است که رزومه تحصیلی ارائه شده که حاوی نمرات و تعداد واحدهای گذرانده شده بر طبق سیستم آموزشی یک کشور است ممکن است که در کشور دیگر قابل پذیرش نباشد. هر کشوری بر طبق آیین نامه‌های آموزشی خود ممکن است دارای نوع نمره‌دهی و تعداد واحدهای متفاوتی نسبت به سایر کشورها باشد. بر این اساس دانشجویان لازم است در جریان ارسال مدارک خود نمرات و تعداد واحدهای گذرانده شده خود را نیز از واحدهای کشور مبدأ به واحدهای کشور مقصد محاسبه نموده و آنگاه اقدام به ارسال مدارک خود نمایند. یکی از بهترین سیستم‌ها برای تبدیل تعداد واحدها و نمرات دروس پاس شده بر طبق نظام اروپایی انتقال واحدهای درسی است[۱۴]. این نظام نوعی سیستم انتقال نمره و تعداد واحدها بر اساس نظام آموزشی کشورهای اتحادیه اروپا را ارائه می‌کند که به ارزیابی مدارک تحصیلی و دوره‌های آموزشی کشورهای دیگر برای انتقال به دانشگاه‌ها در محدوده اتحادیه اروپا می‌پردازد. مقیاس این سیستم بر مبنای نمره ۵ است که در کشورهای مختلف نمادهای آن متفاوت است. مهمترین کاربرد این سیستم تبدیل تعداد واحدهای گذرانده شده در کشور مبدأ بر طبق نظام آموزشی اتحادیه اروپا است که نقش مهمی را در جریان پذیرش دانشجویان در مقاطع ارشد و دکتری توسط دانشگاه‌های اروپایی دارد. در این سیستم هر سال تحصیلی ۶۰ واحد آموزشی است که در کشورهای انگلستان، ایرلند و اسکاتلند این تعداد واحد ۱۲۰ محاسبه می‌شود. متقاضیانی که به دنبال ادامه تحصیل در مقاطع بالاتر در اروپا هستند لازم است تعداد واحدهای گذرانده شده خود را بر اساس این سیستم محاسبه نمایند. در این صورت دانشگاه مقصد می‌تواند برآورد نماید که متقاضی دروس پیش نیاز لازم مورد تأیید برای ورود به مقطع ارشد یا دکترا در دانشگاه مبدأ را گذرانده است. با استفاده از فناوری بلاک‌چین و بر اساس نظام آموزشی کشورهای اتحادیه اروپا می‌توان یک سیستم توزیع‌شده و قابل اعتماد طراحی کرد که دیدی واحد از نمره و اعتبار علمی برای دانشجویان، دانشگاه‌ها و سازمان‌ها ایجاد نماید.

۴-۲- فرایندهای مدل پیشنهادی

مدل پیشنهاد شده شامل هشت فرایند است که در ادامه به تشریح این فرایندها می‌پردازیم.

۱) راه‌اندازی مدل: نهاد قابل اعتماد به‌عنوان یک نود قابل اعتماد برای همه اعضای شبکه، پارامترهای عمومی شبکه pk را برای ایجاد بستری مناسب برای استفاده از تابع درهم‌ساز آفتاب‌پرست مطابق با الگوریتم ۱ ایجاد می‌کند. همچنین کلید اصلی مخفی β^8 و g^{β} را ایجاد می‌کند.

Algorithm 1: Initialization.
Input: Security parameter κ;
Output: Public parameter p, q, g, H and Master secret key β;
1: Select prime p, q, where $p = 2q + 1$;
2: Select g, which is a generator for the subgroup of quadratic residues $\mathbb{QR}_p$ of $\mathbb{Z}_q^*$;
3: $H : \{1,0\}^* \longrightarrow \mathbb{Z}_q$ is a standard-collision resistant hash function;
4: Select a value $\beta \in [1, q-1]$ as the master secret key and compute g^{β};
5: **return** $(p, q, g, H, \beta, g^{\beta})$;

۲) تولید کلید برای دانشگاه‌ها: نهاد قابل اعتماد، اطلاعات دانشگاه ها را که به عنوان نودهای نیمه قابل اعتماد[۹] شبکه بلاک‌چین کنسرسیوم شناخته می‌شوند دریافت می‌کند. سپس با استفاده از الگوریتم تولید کلید درهم‌ساز آفتاب‌پرست الگوریتم ۲ یک جفت کلید خصوصی و عمومی (X_{u_i}, Y_{u_i}) برای هر نود ایجاد می‌کند. نهاد قابل اعتماد با استفاده از کلید اصلی خود β و کلید خصوصی X_{u_i}،

کلید دریچه خصوصی[۱۰] $\alpha_{u_i} = X_{u_i} + \beta$ را محاسبه و به همراه g^{β} از طریق کانال امن برای هر نود در شبکه بلاک‌چین ارسال می‌کند. همچنین کلید عمومی به همراه شناسه دانشگاه‌ها (ID_{u_i}, Y_{u_i}) را به‌صورت عمومی اعلام می‌کند.

Algorithm 2: Key Generation.
Input: All the authorized universities 'identities, Public parameter *p, q, g, H;*
Output: Secret key X_{u_i} and public key Y_{u_i};
foreach university ID_{u_i}:
1: Select a random value $X_{u_i} \epsilon [1, q-1]$ as the secret key;
2: Set the public key $Y_{u_i} = g^{X_{u_i}}$;
3: **return** (X_{u_i}, Y_{u_i});

۳) ثبت نام دانشجو: ثبت نام دانشجو از ۲ مرحله تشکیل می‌شود این مراحل به شرح زیر هستند.

۳-۱) تولید شناسه و کلید: دانشجو S_j هنگام ثبت نام در دانشگاه یک شناسه ID_{s_j} و یک جفت کلید خصوصی و عمومی (X_{s_j}, Y_{s_j}) مرتبط را به کمک الگوریتم تولید کلید درهم‌ساز آفتاب‌پرست و pk ایجاد می‌کند. دانشجو کلید دریچه خصوصی $\alpha_{s_j} = X_{s_j}$ را به‌صورت امن ذخیره سازی می‌کند. دانشجو همچنین یک کلید خصوصی ۱۲۸ بیتی K_{s_j} را ایجاد و پیام $(ID_{s_j}, Y_{s_j}, K_{s_j})$ را از طریق کانال امن برای دانشگاه ارسال می‌کند.

۳-۲) احراز هویت دانشجو: دانشگاه پس از دریافت پیام، شناسه دانشجو را بررسی می‌کند، اگر این شناسه در بلاک‌چین ثبت شده باشد، آن را رد می‌کند، در غیر این صورت دانشجو را احراز اصالت می‌کند. مراحل احراز اصالت دانشجو به شرح زیر است:

۳-۲-۱) تولید لیست درخواست: دانشگاه یک لیست درخواست RL_{s_j} برای ثبت درخواست‌های دانشجو ایجاد می‌کند (شکل ۲-الف). دانشگاه برای ایجاد لیست درخواست یک پیام m_1 ایجاد می‌کند. پیام به دو قسمت شناسه زمانی و درخواست‌های دانشجو تقسیم می‌شود. باید توجه داشت که هنگام ثبت نام دانشجو مقادیر مرتبط با درخواست دانشجو در پیام به دلیل عدم درخواست توسط دانشجو خالی است. دانشگاه m_1 را مطابق با الگوریتم ۳ با استفاده از $y = g^{\alpha_{s_j}} = Y_{s_j}$ و pk درهم‌سازی می‌کند. دانشگاه با استفاده از مقدار درهم سازی شده پیام h_1 و (r_1, s_1, Y_{s_j}, m_1) لیست درخواست $RL_{s_j} = \{h_1, m_1, Y_{s_j}, r_1, s_1\}$ را ایجاد و برای دانشجو ارسال می‌کند.

۳-۲-۲) درخواست ثبت نام: دانشجو برای انجام فرایند ثبت نام و احراز اصالت خود یک در خواست ثبت نام ایجاد می‌کند. دانشجو برای اضافه کردن درخواست ثبت نام به لیست درخواست، یک پیام جدید m'_1 ایجاد می‌کند. اطلاعات موجود در m'_1 مانند m_1 است فقط درخواست ثبت نام در قسمت درخواست‌ها اضافه شده است (شکل ۲-ب). دانشجو از α_{s_j} خود برای یافتن (r'_1, s'_1) مطابق با الگوریتم ۴ استفاده می‌کند. دانشجو پس از به دست آوردن (r'_1, s'_1) یک لیست درخواست جدید $RL'_{s_j} = \{h_1, m'_1, Y_{s_j}, r'_1, s'_1\}$ ایجاد و برای دانشگاه ارسال می‌کند.

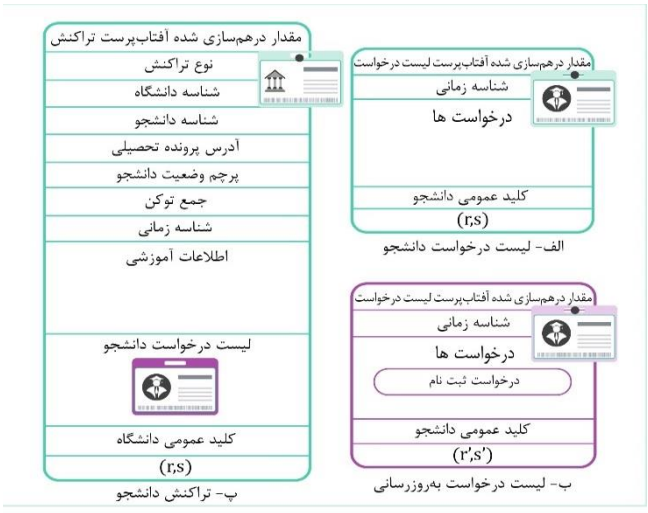
۳-۲-۳) احراز اصالت دانشجو: دانشگاه پس از دریافت لیست بروزرسانی RL'_{s_j}، صحت آن را با استفاده از الگوریتم ۵ بررسی می‌کند. اگر مقدار خروجی الگوریتم $d = 1$ باشد، دانشگاه اصالت دانشجو را تأیید و اطلاعات دانشجو را ذخیره‌سازی می‌کند.

۳-۳) ذخیره‌سازی اطلاعات دانشجو: دانشگاه پس از احراز اصالت دانشجو اطلاعات دانشجو را ذخیرسازی می‌کند. مراحل ذخیره‌سازی اطلاعات دانشجو به شرح زیر است:

۳-۳-۱) ذخیره سازی پرونده تحصیلی دانشجو: دانشگاه در این مرحله اطلاعات مورد نیاز را از دانشجو دریافت و پس از تأیید برای دانشجو پرونده تحصیلی ایجاد می‌کند. دانشگاه پرونده مورد نظر را به‌صورت یک پوشه، با استفاده از الگوریتم رمزنگاری متقارن AES و کلید K_{s_j} رمزنگاری و در IPFS ذخیره سازی می‌کند.

۳-۳-۲) تولید تراکنش دانشجو: دانشگاه یک تراکنش جدید TX_{s_j} (شکل ۲-پ) برای تکمیل فرایند ثبت نام دانشجو و ثبت اطلاعات دانشجو در بلاک‌چین ایجاد می‌کند. دانشگاه برای ایجاد تراکنش یک پیام m_2 ایجاد می‌کند. اطلاعات ذخیره شده در m_2 شامل موارد زیر است:

- نوع تراکنش: پرچمی یک بیتی است که باعث تمایز بین تراکنش دانشجو و تراکنش به‌روزرسانی در نودها می شود. در تراکنش دانشجو مقدار این پرچم صفر است.
- شناسه دانشگاه: شناسه‌ای یکتا است که به هر دانشگاه اختصاص دارد.
- شناسه دانشجو: شناسه‌ای یکتا است که توسط دانشگاه ایجاد شده است.
- آدرس پرونده تحصیلی دانشجو: آدرس پرونده تحصیلی دانشجو در IPFS است.
- وضعیت دانشجو: پرچمی یک بیتی است که باعث تمایز بین دانشجویان در حال تحصیل و فارغ التحصیلان می شود. در هنگام تحصیل دانشجو مقدار این پرچم صفر است.
- جمع توکن‌ها: مجموعه اعتبارهای کسب شده توسط دانشجو است.
- مهر زمانی: بیانگر زمان ارسال تراکنش توسط دانشگاه است.
- اطلاعات آموزشی دانشجو: در این قسمت توکن و شناسه درس‌هایی که توسط دانشجو گذرانده شده است قرار می‌گیرد.
- توکن: مقدار اعتبار درس است که برای درس‌های با موفقیت به اتمام رسیده اختصاص داده می‌شود.
- شناسه درس: شناسه‌ای یکتا است که به هر درس اختصاص داده می‌شود.
- لیست درخواست دانشجو: در این قسمت لیست درخواست دانشجو قرار می‌گیرد.



شکل ۲- تراکنش ثبت نام دانشجو

دانشگاه لیست درخواست RL'_{s_j} را در m_2 قرار می‌دهد. دانشگاه پیام m_2 را مطابق با الگوریتم ۳ با استفاده از $y = g^{\alpha_{u_i}} = g^{\beta} \times y_{u_i}$ و pk درهم‌سازی می‌کند. دانشگاه با استفاده از مقدار درهم‌سازی شده پیام h_2 و (r_2, s_2) یک تراکنش جدید دانشجو (Y_{u_i}, m_2) ایجاد $TX_{s_j} = \{h_2, m_2, Y_{u_i}, r_2, s_2\}$ و تراکنش را در شبکه کنسرسیوم پخش می‌کند.

Algorithm 3: Chameleon Hash.

Input: Message m, y, Public parameter p, q, g, H;
Output: Chameleon hash h;

1: Select random value r and s, where $r, s \in \mathbb{Z}_q$;
2: Compute chameleon Hash value
3: $r - \left(y^{H(m\|r)} \times g^s \bmod p\right) \bmod q = h$, where $H : \{1,0\}^* \longrightarrow \mathbb{Z}_q$ is a standard-collision resistant hash function;
4: **return** (h, r, s);

۴) اجماع: پس از ایجاد تراکنش، دانشگاه تراکنش را برای سایر دانشگاه‌ها در کنسرسیوم پخش می‌کند. با توجه به اینکه بلاک‌چین یک سیستم توزیع شده است که به یک مقام مرکزی بستگی ندارد، الگوریتمی لازم است تا دانشگاه‌ها در کنسرسیوم بتوانند به اجماع برسند. در مدل ارائه شده برای افزایش امنیت، انعطاف‌پذیری و مقیاس‌پذیری بلاک‌چین از الگوریتم اجماع تحمل خطای بیزانس عملی (PBFT) استفاده شده است. فرض می‌کنیم که 3f+1 نود در مجموعه کنسرسیوم وجود دارد. در هر دوره زمانی فقط یک رهبر وجود دارد و رهبر توسط نودها چرخانده می‌شود. نودهای شبکه پس از دریافت تراکنش با بهره‌گیری از y_{u_i} موجود در تراکنش و مقدار g^{β} را محاسبه و صحت تراکنش را با $y = g^{\beta} \times y_{u_i}$ استفاده از الگوریتم ۵ بررسی می‌کند. اگر مقدار خروجی الگوریتم $d = 1$ باشد، نودها تراکنش را تأیید و دانشگاه ID_{u_i} را احراز اصالت می‌کنند. پس از مراحل پیش آماده سازی، آماده سازی، تعهد و پاسخ اجماع PBFT، تراکنش‌های قانونی به زنجیره بلوکی کنسرسیوم که توسط همه نودهای شبکه نگهداری می‌شود، اضافه می‌شوند. سپس، هر گره شبکه نتایج تأیید تراکنش ها را پخش می‌کند. تراکنش‌های قانونی به زنجیره بلاک‌چین کنسرسیوم که توسط همه گره‌های شبکه نگهداری می‌شود اضافه می‌شود. بعد از قرار گرفتن تراکنش در بلاک‌چین دانشگاه شناسه تراکنش (ارتفاع بلوک و عمق تراکنش) که بیانگر موقعیت مکانی تراکنش در شبکه بلاک‌چین است را به دانشجو می‌دهد. دانشجو با ارائه شناسه تراکنش خود قادر خواهد بود که بدون دخالت هیچ مدیریتی، اعتبار علمی خود را به دیگران اثبات کند. دانشگاه برای به‌روزرسانی این تراکنش در مراحل بعد، شناسه تراکنش را در حافظه داخلی خود ذخیره سازی می‌کند.

Algorithm 4: Chameleon Collision.

Input: Updated message m', chameleon hash h, secret trapdoor key α ;
Output: updated (r', s');

1: Select a random value $k \in [1,\ q-1]$;
2: Compute updated $r' = h + (g^k \bmod p) \bmod q$;
3: Compute updated $s' = k - H(m' \parallel r') \times \alpha \bmod q$;
4: **return** (r', s');

۵) به‌روزرسانی اعتبار علمی دانشجویان: در مدل پیشنهادی از فناوری بلاک‌چین برای پردازش، مدیریت و کنترل توکن‌ها به‌عنوان اعتبار علمی دانشجویان استفاده شده است. توکن‌ها معادل اعتبار درس‌های به اتمام رسیده بر اساس نظام آموزشی کشورهای اتحادیه اروپا در نظر گرفته می‌شوند. هر دانشجو در این بلاک‌چین یک تراکنش مشخص خواهد داشت. اعتبارهای علمی دانشجو در کنار سایر اطلاعات همانطور که در بخش ۳-۲-۳ توضیح داده شد، در آن تراکنش نگهداری می‌شود. این اعتبار توسط دانشگاه مربوطه برای درس‌های به اتمام رسیده اختصاص پیدا می‌کند. هر زمان که یک دانشجو یک درس را با موفقیت به اتمام می‌رساند، دانشگاه مربوطه توکن‌های متناسب آن درس را در تراکنش آن دانشجو در بلاک‌چین قرار می‌دهد. به این منظور دانشگاه یک تراکنش جدید برای به‌روزرسانی تراکنش دانشجو ایجاد می‌کند (شکل-۳). تراکنش به‌روزرسانی درواقع یک کپی از اطلاعات تراکنش دانشجو است و فقط شناسه و توکن درس‌هایی که به‌تازگی توسط دانشجو گذرانده شده به همراه شناسه زمانی در آن اضافه شده است تا بعد از تأیید صحت تراکنش به‌روزرسانی توسط نودها، شناسه و توکن درس‌های جدید در کنار شناسه زمانی در تراکنش دانشجو به‌روزرسانی شوند.

شکل ۳- تراکنش به‌روزرسانی

مراحل ساخت تراکنش جدید به شکل زیر است.

- دانشگاه برای به‌روزرسانی تراکنش دانشجو یک پیام جدید m'_2 ایجاد می‌کند. اطلاعات موجود در m'_2 مانند m_2 است و فقط شناسه وتوکن درس‌های جدید به همراه شناسه زمانی در قسمت اطلاعات آموزشی دانشجو اضافه شده است
- دانشگاه از α_{u_i} خود برای یافتن $(r'_2,\ s'_2)$ مطابق با الگوریتم ۴ استفاده می‌کند.
- دانشگاه پس از به دست آوردن $(r'_2,\ s'_2)$ یک تراکنش جدید $TX'_{s_j} = \{h_2, m'_2, Y_{u_i}, r'_2, s'_2\}$ ایجاد و تراکنش را در شبکه کنسرسیوم پخش می‌کند.
- سایر نودها پس از دریافت تراکنش مقدار $y = g^{\beta} \times y_{u_i}$ را محاسبه و صحت تراکنش را با استفاده از الگوریتم ۵ بررسی می‌کنند. اگر مقدار خروجی الگوریتم $d = 1$ باشد، نودها تراکنش را تأیید کرده و تراکنش دانشجو را در بلاک‌چین خود با تراکنش جدید جایگزین می‌کنند.

Algorithm 5: Verification.

Input: message m, chameleon hash h, $(r, s), y$;
Output: d;

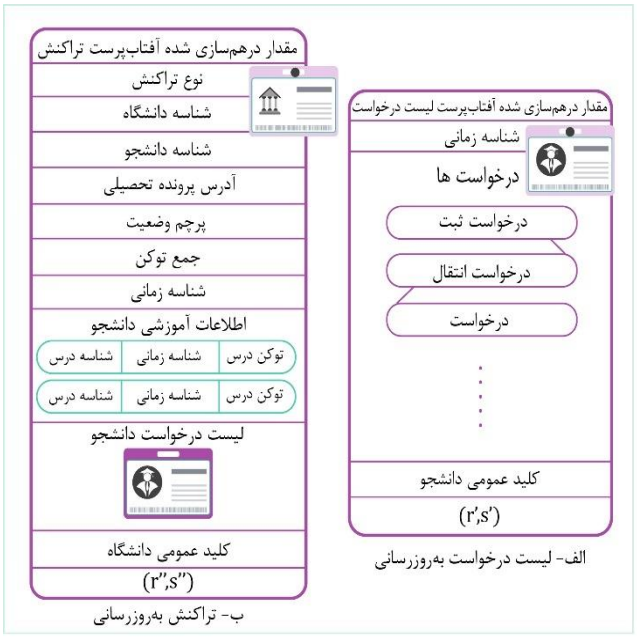
5: Compute $h' = \mathrm{r} - \left(y^{H(\mathrm{m}\,\|\,\mathrm{r})} \times g^s \bmod p\right) \bmod q$;
If $h == h'$:
6: **return** $d = 1$;
else:
7: **return** $d = 0$;

۶) به‌روزرسانی پرونده علمی دانشجویان: دانشگاه برای دانشجویانی که دوره تحصیلی خود را با موفقیت به پایان رسانده‌اند، گواهی تحصیلی صادر می‌کند. دانشگاه با قرار دادن گواهی تحصیلی دانشجو در پرونده تحصیلی دانشجو آن را تکمیل می‌کند. برای به‌روزرسانی پرونده دانشجو در تراکنش دانشجو، دانشگاه پرونده تحصیلی دانشجو را دوباره در IPFS بارگذاری می‌کند و یک آدرس جدید دریافت می‌کند. دانشگاه با تغییر آدرس پرونده تحصیلی در تراکنش به‌روزرسانی و ارسال آن در شبکه بلاک‌چین می تواند آدرس پرونده دانشجو را در تراکنش دانشجو به‌روزرسانی کند.

۷) فرایند انتقال مجوز ویرایش تراکنش دانشجو: این فرایند از ۳ مرحله تشکیل می‌شود که این مراحل به شرح زیر هستند.

۷-۱) درخواست انتقال: دانشجو اگر قصد انتقال به دانشگاه دیگر در هنگام تحصیل را داشته باشد و یا اگر قصد ادامه تحصیل در مقاطع بالاتر دانشگاهی را داشته باشد. برای انتقال مجوز ویرایش تراکنش خود به دانشگاه مقصد، یک درخواست انتقال ایجاد می‌کند (شکل ۴- الف). این درخواست شامل شناسه دانشجو، شناسه دانشگاه مبدأ، شناسه دانشگاه مقصد، کلید عمومی دانشگاه مقصد و نشانه‌گر زمانی است. دانشجو برای اضافه کردن درخواست انتقال به لیست درخواست، یک پیام جدید m''_1 ایجاد می کند. اطلاعات موجود در m''_1 مانند m'_1 است و فقط درخواست انتقال در قسمت درخواست‌ها اضافه شده است. دانشجو از α_{s_j} خود برای یافتن (r''_1, s''_1) مطابق با الگوریتم ۴ استفاده می‌کند. دانشجو پس از به دست آوردن (r''_1, s''_1) یک لیست درخواست جدید به‌صورت $RL''_{s_j} = \{h_1, m''_1, Y_{s_j}, r''_1, s''_1\}$ ایجاد و برای دانشگاه ارسال می‌کند.

۷-۲) تأیید و ثبت درخواست انتقال: دانشگاه صحت RL''_{s_j} را با استفاده از الگوریتم ۵ بررسی می‌کند. اگر مقدار خروجی الگوریتم $d = 1$ باشد، دانشگاه اصالت دانشجو را تأیید می‌کند. دانشگاه در صورت موافقت با درخواست انتقال دانشجو یک پیام جدید m''_2 ایجاد می کند. اطلاعات موجود در m''_2 مانند m'_2 است و فقط RL''_{s_j} در آن جایگزین شده است. دانشگاه از α_{u_i} خود برای یافتن (r''_2, s''_2) مطابق با الگوریتم ۴ استفاده می‌کند. دانشگاه پس از به دست آوردن (r''_2, s''_2) یک تراکنش جدید $TX''_{s_j} = \{h_2, m''_2, Y_{u_j}, r''_2, s''_2\}$ ایجاد و در شبکه کنسرسیوم ارسال می‌کند (شکل ۴- ب). سایر نودها پس از تأیید صحت تراکنش و احراز اصالت دانشگاه TX''_{s_j} را در بلاک‌چین خود جایگزین می‌کنند.



شکل ۴- تراکنش انتقال دانشجو

۷-۳) انتقال مجوز ویرایش: دانشگاه مبدأ بعد از انجام فرایندهای به‌روزرسانی و قرار گرفتن درخواست انتقال در تراکنش دانشجو، برای انجام فرایند انتقال به روش زیر عمل می‌کند.

دانشگاه یک پیام جدید m_3 ایجاد می‌کند. اطلاعات موجود در m_3 مانند m''_2 است و فقط شناسه دانشگاه مقصد ID_{u_i} در قسمت شناسه دانشگاه جایگزین می‌شود. دانشگاه با استفاده از کلید عمومی دانشگاه مقصد Y_{u_j} و g^β مقدار $y = g^\beta \times Y_{u_j}$ را محاسبه و m_3 را مطابق با الگوریتم ۳ درهم‌سازی می‌کند. دانشگاه با استفاده از مقدار درهم‌سازی شده پیام h_3 و (r_3, s_3, Y_{u_j}, m_3) یک تراکنش جدید دانشجو $TX_{s_j} = \{h_3, m_3, Y_{u'_j}, r_3, s_3\}$ ایجاد و تراکنش را در شبکه کنسرسیوم پخش می‌کند.

دانشگاه مبدأ بعد از قرار گرفتن تراکنش در بلاک‌چین، شناسه تراکنش جدید را به دانشجو می‌دهد. از این پس دانشگاه مقصد فقط توانایی به‌روزرسانی تراکنش جدید دانشجو را دارد. دانشجو با ارائه شناسه تراکنش دانشجویی جدید و کلید رمزنگاری پرونده تحصیلی خود به دانشگاه مقصد فرایند انتقال یا ثبت نام در دانشگاه جدید را به اتمام می‌رساند. در این روش دانشگاه مبدأ درواقع با ایجاد تراکنش جدید دانشجو و استفاده از کلید عمومی دانشگاه مقصد فرایند انتقال مجوز ویرایش تراکنش دانشجو را انجام داده است. چراکه تنها دانشگاه مقصد می‌تواند با استفاده از کلید خصوصی خود تراکنش مذکور را ویرایش یا به‌روزرسانی کند.

۸) اعتبارسنجی دانشجو توسط سازمان‌ها: برای اعتبارسنجی دانشجو توسط سازمان‌ها لازم است که دانشجو شناسه تراکنش خود را در اختیار سازمان قرار دهد. برای آنکه سازمان از صحت شناسه دانشجو اطمینان حاصل کند دو پیام m_1 و m_2 دلخواه را انتخاب می‌کند، سپس مقدار درهم‌سازی شده آفتاب‌پرست m_1 را با استفاده از کلید عمومی دانشجو $y = Y_{s_j}$ مطابق با الگوریتم ۳ محاسبه می‌کند و مقادیر (r_1, s_1, h_1, m_1) را در اختیار دانشجو قرار می دهد. سازمان از دانشجو می خواهد که (r_1', s_1') را به‌نحوی پیدا کند که مقدار درهمسازی شده آفتاب‌پرست m_2 با h_1 برابر شود. به این منظور دانشجو به کمک کلید دریچه خصوصی خود α_{s_j} و مطابق با الگوریتم ۴ مقدار (r_1', s_1') را محاسبه و برای سازمان ارسال می‌کند. سازمان صحت (r_1', s_1') را با استفاده از الگوریتم ۵ بررسی می کند. اگر مقدار خروجی الگوریتم $d = 1$ باشد، سازمان می‌تواند مطمئن شود که شناسه تراکنش دانشجو و اعتبارهای موجود در آن متعلق به همان دانشجو است.

۵- ارزیابی مدل پیشنهادی

در این بخش به ارزیابی عملکرد مدل پیشنهادی می‌پردازیم. تحلیلی بر روی مدل پیشنهادی نشان می‌دهد که ویژگی‌هایی همچون امنیت شناسه، احراز اصالت، عدم انکار، یکپارچگی و تمرکززدایی به خوبی در این مدل فراهم شده است که در ادامه به تشریح این ویژگی‌ها در مدل پیشنهادی می‌پردازیم. سپس در بخش ۵-۱ نتایج حاصل از پیاده‌سازی مدل پیشنهادی را مورد ارزیابی قرار خواهیم داد.

امنیت شناسه: شایان ذکر است در طرح پیشنهادی شناسه دانشجویی ID_{s_j} ، کلید عمومی Y_{s_j} و کلید خصوصی X_{s_j} توسط خود دانشجو تولید می‌شود. دانشگاه دانشجو را احراز اصالت می‌کند و یک تراکنش دانشجو را که شامل ID_{s_j} و Y_{s_j} است را به بلاک‌چین اضافه می‌کند. پس از آن هیچ دشمنی نمی‌تواند ID_{s_j} و Y_{s_j} را دستکاری کند. به این شکل هر دانشجو با یک شناسه قانونی ID_{s_j}، فقط یک جفت کلید خصوصی و عمومی (X_{s_j}, Y_{s_j}) احراز اصالت شده دارد. برای هر دشمن زمان چند جمله‌ای احتمالی (PPT) [11]، امکان استخراج کلید خصوصی X_{s_j} با توجه به کلید عمومی Y_{s_j} وجود ندارد. علاوه بر این، در طرح ارائه شده به دلیل استفاده از تابع درهم‌ساز آفتاب‌پرست با آزادی دربرابر افشای کلید[12]، X_{s_j} در هنگام استفاده از الگوریتم پیدا کردن برخورد تصادفی فاش نمی‌شود. بنابراین X_{s_j}

فقط توسط دانشجو کنترل می‌شود. در نتیجه، طرح پیشنهادی می‌تواند امنیت شناسه را فراهم کند.

احراز اصالت: دانشجو در هنگام ثبت درخواست جدید، لیست درخواست RL_{s_j} را با استفاده از کلید دریچه خصوصی خود α_{s_j} و الگوریتم پیدا کردن برخورد تصادفی به‌روزرسانی می‌کند. دانشگاه با تأیید صحت RL'_{s_j} دانشجو را احراز اصالت می کند. از آنجایی که ثابت کردیم X_{s_j} تنها تحت کنترل دانشجو است هیچ دشمنی توانایی جعل RL'_{s_j} را ندارد. دانشگاه در مرحله تولید تراکنش دانشجو TX_{s_j} از $y = g^{\beta} \times y_{u_i}$ را برای درهم‌سازی پیام استفاده می‌کند. با توجه به اینکه نهاد قابل اعتماد پارامتر خصوصی g^{β} را به‌صورت امن برای دانشگاه‌ها که نودهای نیمه قابل اعتماد شبکه هستند ارسال کرده است و با فرض امن بودن g^{β} هیچ دشمنی توانایی جعل و حتی تأیید تراکنش دانشجو را ندارد. دانشگاه هنگام تولید تراکنش به‌روزرسانی دانشجو TX_{s_j}' از کلید دریچه خصوصی خود $\alpha_{u_i} = X_{u_i} + \beta$ برای یافتن (s', r') مطابق با الگوریتم ۴ استفاده می‌کند. سایر نودها، TX'_{s_j} را با استفاده از $y = g^{\beta} \times y_{u_i}$ تأیید و دانشگاه را احراز اصالت می‌کنند. با فرض امن بودن α_{u_i} هیچ دشمنی توانایی جعل TX_{s_j}' را ندارد.

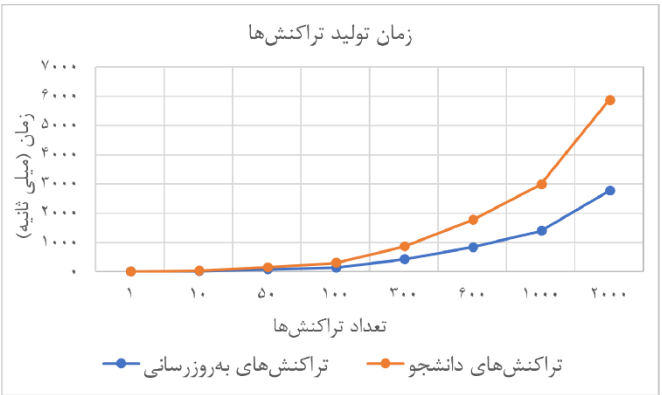
عدم انکار و یکپارچگی: دانشجو برای ثبت در خواست خود در تراکنش دانشجو، لیست درخواست RL_{s_j} را با استفاده از کلید دریچه خصوصی خود α_{s_j} به‌روزرسانی می‌کند. دانشگاه شناسه دانشجو را بررسی می‌کند و فقط در صورت تأیید شناسه دانشجو، RL'_{s_j} را در تراکنش دانشجو به‌روزرسانی می‌کند. دانستن شناسه فرستنده RL'_{s_j} بر اساس الگوریتم تأیید درهم ساز آفتاب‌پرست، باتوجه به امنیت شناسه، عدم انکار درخواست را تضمین می‌کند. دانشگاه تراکنش دانشجو TX_{s_j} را با استفاده از کلید دریچه خصوصی خود به‌روزرسانی و در شبکه کنسرسیوم پخش می‌کند. سایر نودها، شناسه دانشگاه را بررسی و فقط در صورت تأیید شناسه دانشگاه TX'_{s_j} را در بلاک‌چین خود به‌روزرسانی می‌کنند. دانستن شناسه فرستنده TX'_{s_j} بر اساس الگوریتم تأیید درهم‌ساز آفتاب‌پرست، باتوجه به امنیت شناسه، عدم انکار TX'_{s_j} را تضمین می‌کند. همچنین همه تراکنش ها در مرحله اجماع حسابرسی می‌شوند و در صورت تغییر یا ناقص بودن تراکنش‌ها، مرحله اجماع تصویب نخواهد شد. این امر صحت تراکنش‌های ارسال شده را تضمین می‌کند.

تمرکز زدایی: برخلاف روش سنتی ذخیره‌سازی داده، ما از یک طرح ذخیره سازی توزیع شده مبتنی بر بلاک‌چین قابل ویرایش کنسرسیوم استفاده کردیم. طرح ما به یک شخص ثالث قابل‌اعتماد برای ذخیره‌سازی متمرکز داده نیاز ندارد. اینگونه ما هزینه ایجاد یک پایگاه داده متمرکز قابل اعتماد را کاهش دادیم و از آسیب‌پذیری‌های این گلوگاه امنیتی در برابر حملات مخرب متمرکز جلوگیری کردیم.

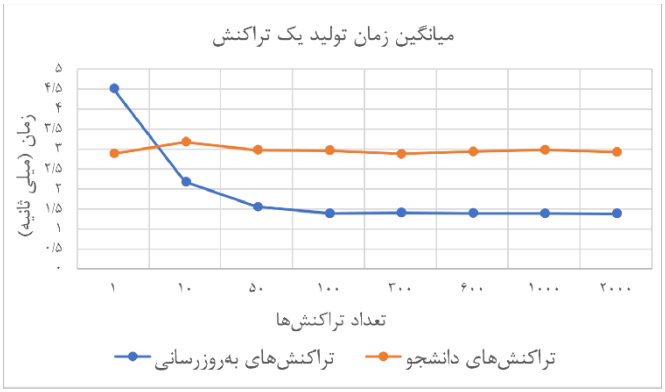
۵-۱- ارزیابی عملکرد

ما طرح خود را به منظور نمایش اثبات عملکرد و کارایی پیاده‌سازی کردیم. پیاده سازی بر روی یک رایانه با سیستم عامل Ubuntu 18.04 LTS مجهز به پردازنده Intel Core i7-4720HQ @ 2.60GHz و رم 12GB انجام شده است. از زبان برنامه نویسی پایتون ۳.۶ برای پیاده سازی بستر بلاک‌چین استفاده شده است. در این پیاده‌سازی ما از چارچوب خرد Flask برای ایجاد یک بلاک‌چین تحت وب استفاده کردیم. همچنین از کتابخانه PubNub برای ایجاد کانال ارتباطی بین نودهای شبکه بلاکچین استفاده شده است. به‌منظور پیاده‌سازی درهم‌ساز آفتاب‌پرست در بستر بلاک‌چین از چارچوب Charm [۱۹] استفاده کردیم. شکل ۲ تراکنش دانشجو که در زنجیره بلاک‌چین قرار گرفته را نشان می‌دهد.

ما برای ارزیابی مدل پیشنهادی، ۲۰ نود را به‌عنوان نودهای بلاک‌چین قابل ویرایش به‌صورت هم‌زمان اجرا کردیم. چهار نود را به‌عنوان نودهای اعتبارسنج در الگوریتم اجماع PBFT مشخص کردیم. در شبکه بلاک‌چین یکی از پارامترهای مهم مدت زمان تولید تراکنش توسط نودهای شبکه است. به این منظور ما مجموعه‌ای از تراکنش‌های دانشجو و تراکنش‌های به‌روزرسانی را به‌صورت مجموعه‌های جداگانه توسط یکی از نودهای شبکه تولید کردیم. مدت زمان تولید هر مجموعه از تراکنش‌ها در شکل ۵ نشان داده شده است که بیانگر خطی بودن نسبت زمان مورد نیاز برای تولید تراکنش‌ها به تعداد تراکنش‌ها است. میانگین زمان مورد نیاز برای تولید یک تراکنش در شکل۶ نشان داده شده است. میانگین زمان تولید تراکنش دانشجو و تراکنش به‌روزرسانی با افزایش تعداد تراکنش ها به ترتیب به عدد ۳ و ۱.۵ میلی ثانیه میل می‌کند. اختلاف زمانی ایجاد شده به دلیل ایجاد لیست درخواست در هنگام تولید تراکنش دانشجو توسط دانشگاه است.



شکل ۵- زمان تولید تراکنش‌ها

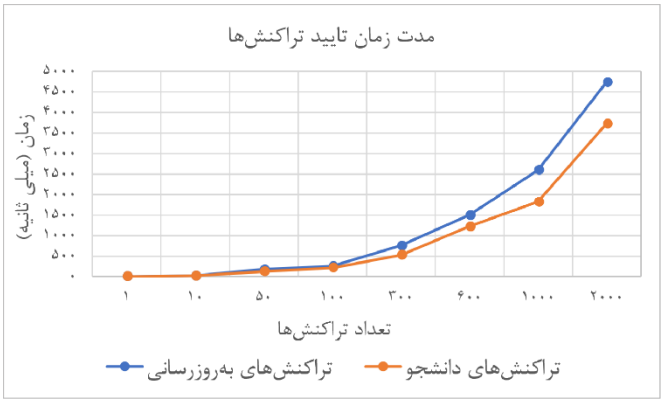


شکل ۶- میانگین زمان تولید تراکنش

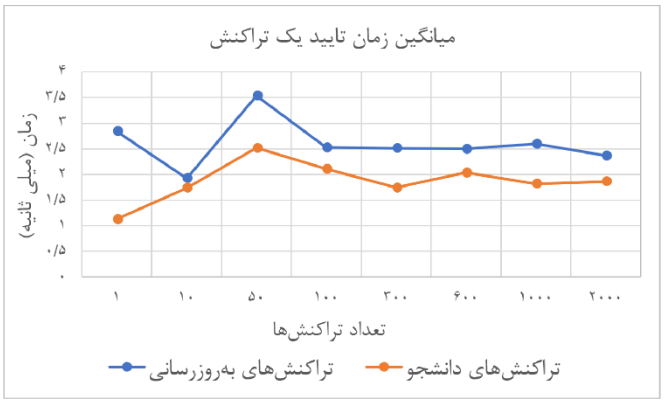
در شبکه بلاک‌چین یکی دیگر از پارامترهای مهم مدت زمان تأیید صحت تراکنش توسط نودهای شبکه است. به این منظور ما مجموعه‌های جداگانه تولید شده را به شبکه بلاکچین ارسال کردیم. مدت زمان تأیید صحت هر مجموعه از تراکنش‌ها توسط نودهای شبکه بلاک‌چین در شکل ۷ نشان داده شده است که بیانگر خطی بودن نسبت زمان مورد نیاز برای تأیید صحت تراکنش‌ها به تعداد تراکنش‌ها است. میانگین زمان مورد نیاز برای تأیید صحت یک تراکنش در شکل ۸ نشان داده شده است. میانگین زمان تأیید تراکنش دانشجو و تراکنش به‌روزرسانی با افزایش تعداد تراکنش ها به ترتیب عدد ۲ و ۲.۵ میلی ثانیه میل می‌کند. اختلاف زمانی ایجاد شده به دلیل افزایش توکن ها و درخواست‌ها در تراکنش به‌روزرسانی است.

در بلاک‌چین کنسرسیوم قابل ویرایش، نودها پس از تأیید صحت تراکنش به‌روزرسانی تراکنش دانشجو را در بلاک‌چین خود به‌روزرسانی می‌کند. به‌روزرسانی تراکنش درواقع جستجوی تراکنش در بلاک‌چین و جایگزینی تراکنش جدید است.

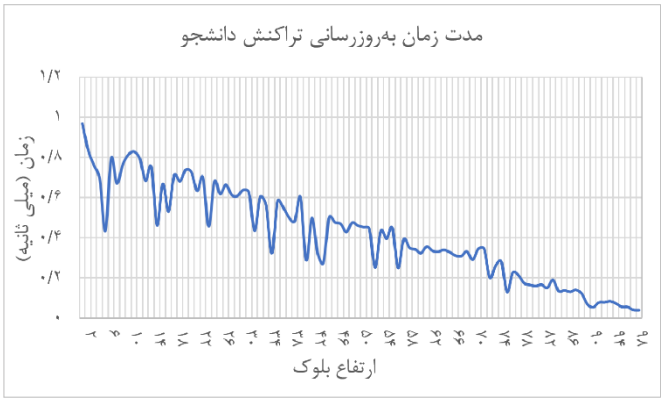
مدت زمان به‌روزرسانی تراکنش دانشجو به ارتفاع بلوکی که تراکنش در آن قرار دارد وابسته است. ما برای ارزیابی این پارامتر یک بلاک چین با ارتفاع ۱۰۰ ایجاد کردیم، سپس در هر بلوک یکی از تراکنش ها را به‌روزرسانی و مدت زمان بروزرسانی را اندازه‌گیری کردیم. همانطور که در شکل ۹ - نشان داده شده است، با افزایش ارتفاع بلوک مدت زمان به‌روزرسانی تراکنش کاهش می‌یابد.



شکل ۷- زمان تأیید تراکنش‌ها

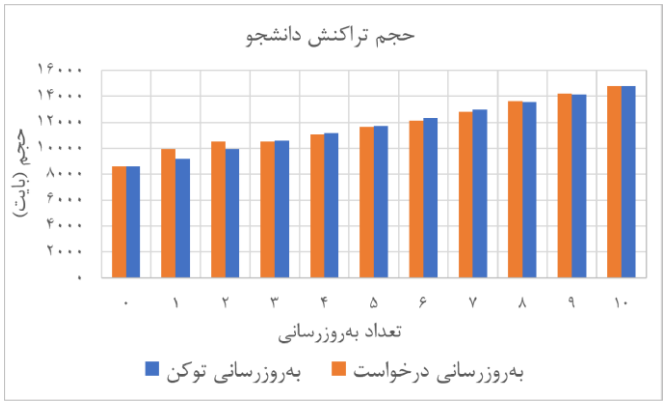


شکل ۸- میانگین زمان تأیید تراکنش



شکل ۹- زمان به‌روزرسانی تراکنش دانشجو

در مدل پیشنهادی، حجم تراکنش دانشجو در هر بار به‌روزرسانی افزایش می‌یابد. افزایش حجم تراکنش دانشجو با توجه به نوع به‌روزرسانی متفاوت است. برای ارزیابی این پارامتر ما شبکه بلاک‌چین را با دو روش آزمایش کردیم. در روش اول، تراکنش دانشجو، ۱۰ مرتبه و هر بار فقط با اضافه شدن یک شناسه و توکن درس جدید به همراه شناسه زمانی به‌روزرسانی شد. حجم تراکنش در هر به‌روزرسانی بین ۴۰۰ تا ۸۰۰ بایت افزایش یافت (شکل ۱۰ - ستون آبی). در روش دوم، تراکنش دانشجو، ۱۰ مرتبه و هر بار فقط با اضافه شدن یک درخواست در لیست درخواست دانشجو به‌روزرسانی شد. باتوجه به تعداد کاراکترهای موجود در هر درخواست، حجم تراکنش افزایش یافت (شکل ۱۰ - ستون نارنجی). با توجه به تغییر حجم تراکنش دانشجو و قرار گرفتن پرونده تحصیلی دانشجو در IPFS حجم تراکنش در مدل ارائه شده مطلوب به نظر می‌رسد.



شکل ۱۰- حجم تراکنش دانشجو

۶- نتیجه گیری

در این مقاله مدلی مبتنی بر بلاک‌چین کنسرسیوم قابل ویرایش برای ذخیره‌سازی و انتقال نمرات، مدارک تحصیلی و اعتبارهای علمی دانشجویان پیشنهاد شد. این مدل می‌تواند یک سیستم سراسری قابل اعتماد، غیرمتمرکز و قابل ویرایش که استفاده از آن آسان بوده را در اختیار دانشجویان، دانشگاه‌ها و سازمان‌ها قرار دهد. در مدل پیشنهادی درخواست‌ها، مدارک و اعتبارهای علمی دانشجویان در طول دوره تحصیل با به‌کارگیری بلاک‌چین قابل ویرایش به‌صورت منسجم در یک تراکنش از زنجیره بلاک‌چین قرار گرفته و به‌روزرسانی می‌شود. همچنین انتقال نمره و اعتبار در این مدل طبق نظام اروپایی انتقال واحدهای درسی صورت می‌گیرد. استفاده از این استانداردها و الگوریتم‌ها سبب می‌شود که مدل پیشنهادی از امنیت، انعطاف‌پذیری و مقیاس‌پذیری مطلوبی برخوردار شود. نتایج پیاده‌سازی مدل پیشنهادی نشان می‌دهد که زمان تأیید تراکنش‌های دانشجویان و حجم آنها قابل قبول است.

۷- مراجع

[1] A. Alhabeeb, and J. Rowley, "E-learning critical success factors: Comparing perspectives from academic staff and students," *Computers & Education*, Vol.127, pp.1-12, 2018.

[2] M. Jirgensons, and J. Kapenieks, "Blockchain and the future of digital learning credential assessment and management," *Journal of Teacher Education for Sustainability*, Vol.20, No.1, pp.145-156, 2018.

[3] Z. Qiu, *Digital certificate for a painting based on blockchain technology. Department of Information and Finance Management*, National Taipei University of Technology, Taiwan, ROC, 2017.

[4] A. Third, A., J. Domingue, M. Bachler, and K. Quick, "Blockchains and the Web position paper," *In Proc. W3C Workshop Distrib. Ledgers Web*, 2016.

[5] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," *In 2017 IEEE 13th international symposium on autonomous decentralized system (ISADS)*, pp. 128-133, IEEE, 2017.

[6] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2019.

[7] S.G. Education, *Sony global education develops technology using Blockchain for open sharing of academic proficiency and progress records*, 22 February 2016.

[8] M. Sharples, and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," *In European conference on technology enhanced learning*, Springer, Cham, pp. 490-4962016.

[9] X.M. Yang, X. Li, H.Q. Wu, and K.Y. Zhao, "The application model and challenges of blockchain technology in education," *Modern distance education research 2*, pp.34-45, 2017.

[10] C. Dannen, *Introducing Ethereum and Solidity,* Berkeley: A press, 2017.
[11] J.C. Cheng, N.Y. Lee, C. Chi, and Y.H. Chen, "Blockchain and smart contract for digital certificate," *In 2018 IEEE international conference on applied system invention (ICASI)*, pp. 1046-1051, 2018.
[12] K. Fanning, and D.P. Centers, "Blockchain and its coming impact on financial services," *Journal of Corporate Accounting & Finance*, Vol.27, No.5, pp.53-57, 2016.
[13] K. Ito, and M. O'Dair, "A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management," *In Business transformation through blockchain,* Palgrave Macmillan, Cham, pp. 317-335, 2019.
[14] T. Grosges, and D. Barchiesi, "European credit transfer and accumulation system: An alternative way to calculate the ECTS grades," *Higher Education in Europe*, Vol.32, No.2, pp.213-227, 2017.
[15] H. Krawczyk and T. Rabin, "Chameleon signatures," *In Proc. 7th Netw. Distrib. Syst. Secur. Symp.*, pp. 143–154, 2000.
[16] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain–or–rewriting history in bitcoin and friends," *In 2017 IEEE European symposium on security and privacy (EuroS&P)*, pp. 111-126, IEEE, 2017.
[17] D. Derler, K. Samelin, D. Slamanig, and C. Striecks, "Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based," *IACR Cryptol. ePrint Arch.*, p.406, 2019.
[18] J.C. Choon, and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *In International workshop on public key cryptography*, Springer, Berlin, Heidelberg, pp. 18-30, 2003.
[19] J.A. Akinyele, C. Garman, I. Miers, M.W. Pagano, M. Rushanan, M. Green, and A.D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, Vol.3, No.2, pp.111-128, 2013.

سعید شکرالهی تحصیلات خود را در مقطع کارشناسی کامپیوتر- نرم افزار در سال ۱۳۸۱ از دانشگاه اصفهان و در مقاطع کارشناسی ارشد و دکتری کامپیوتر- نرم افزار به ترتیب در سالهای ۱۳۸۴ و ۱۳۹۳ از دانشگاه شهید بهشتی به پایان رسانده است. ایشان دوره فرصت مطالعاتی خود را در سال ۱۳۹۱ در آزمایشگاه امنیت دانشگاه میلان سپری کرده است. وی در حال حاضر استادیار گروه امنیت شبکه و رمزنگاری پژوهشکده فضای مجازی در دانشگاه بهشتی است. زمینه های تحقیقاتی مورد علاقه ایشان عبارتند از: سیستمهای فوق مقیاس وسیع، معماری نرم افزار، معماری سرویس گرا، معماری سازمانی، امنیت و کنترل دسترسی، اینترنت اشیاء، میان افزارهای مبتنی بر رویداد و شبکه های بین خودرویی. آدرس پست الکترونیکی ایشان عبارت است از:

s_shokrollahi@sbu.ac.ir

محمد سعید مصلح نژاد دانشجوی کارشناسی ارشد مهندسی برق گرایش مخابرات امن و رمزنگاری در دانشگاه شهید بهشتی تهران است. از جمله زمینه های پژوهشی مورد علاقه او می‌توان به امنیت و کنترل دسترسی، زنجیره بلوکی و شبکه‌های بین خوردویی اشاره کرد. آدرس پست الکترونیکی ایشان عبارت است از:

m.moslehnejad@mail.sbu.ac.ir

[1] Blockchain
[2] Chameleon Hash
[3] Redactable
[4] General Data Protection Regulation
[5] Consortium
[6] Inter Planetary File System
[7] European Credit Transfer and Accumulation System
[8] Master Secret Key
[9] Semi Trusted
[10] Secret Trapdoor Key
[11] Probabilistic Polynomial-Time (PPT) Adversary
[12] Chameleon Hash with Key Exposure Freeness

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 18, No.2, 2021

A Redactable Blockchain Model for Storing and Transferring Scientific Documents and Credits

Saeed Shokrollahi, Mohamad Saeed Mosleh Nejad

Cyberspace Research Institute, Shahid Beheshti University (SBU), Tehran, Iran

Abstract

Today, with the advancement of science and technology, most universities, educational institutions, and organizations use e-learning for their field of education, which has become more and more important with the advent of Covid-19. One of the technologies that has been considered in recent years in the infrastructure of e-learning systems is blockchain technology. Digital certification, intellectual property rights, and finance of universities and educational institutions are some of the areas in which blockchain has been used. The infrastructure for transferring students' grades and academic credits is also one of the cases in which blockchain can be used. This paper proposes a redactable blockchain model for storing and transmitting student information and student academic credentials. This model can provide students, universities, and organizations with a reliable, decentralized, and redactable global system that is easy to use and requires no central management. The standards and algorithms used in the proposed model put the security, flexibility, and scalability of this model at the desired level. The implementation results of the proposed model show that the production time and confirmation of students' transactions, the duration of the update, and their volume are acceptable.

Keywords: Redactable blockchain, E-learning, Chameleon hash algorithm, European system of course transfer