دوره شانزدهم، شماره پاییز و زمستان ۱۴۰۲

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://ited.sinaweb.net

ارایه مدلی مبتنی بر بلاک‌چین برای ذخیره و بازیابی سوابق تحصیلی داوطلبان کنکور سراسری

راحله مالکی[۱] داود بهره‌پور*[۲] سیده سمیه فاطمی‌نسب[۳]

(۱) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(۲) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران *

(۳) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(تاریخ دریافت : ۱۴۰۲/۰۲/۱۹ تاریخ پذیرش: ۱۴۰۲/۱۲/۲۷)

چکیده

در سال‌های اخیر موضوع حذف آزمون کنکور سراسری مطرح شده است، در این راستا، سال جاری تنها برای چند رشته‌ی خاص آزمون برگزار شده است، و در عین حال نمرات امتحانات نهایی پایه دوازدهم هم تا ۴۰ درصد در پذیرش داوطلب تاثیر مستقیم دارد و برای سایر رشته‌های تحصیلی، پذیرش بر اساس سوابق تحصیلی دانش‌آموز است. لذا ذخیره امن سوابق تحصیلی و ممانعت از تغییر و دستکاری نمرات دانش‌آموزان اهمیت بسزایی دارد. فناوری بلاک‌چین به دلیل ویژگی‌های منحصر به فرد از جمله تغییرناپذیری بلوک‌های داده، شفافیت و خاصیت غیرمتمرکز بودن مورد توجه است از طرفی قراردادهای هوشمند مبتنی بر بلاک‌چین، حریم خصوصی و کنترل دسترسی را فراهم می‌کنند. یک بستر برای اجرای قرادادهای هوشمند، شبکه بلاک‌چین هایپرلجر فابریک است. در این مقاله مدلی برای ذخیره و بازیابی سوابق تحصیلی دانش‌آموزان مبتنی بر بلاک‌چین هایپرلجر فابریک ارایه می‌شود. در این مدل سوابق تحصیلی دانش‌آموزان از جمله نمرات دروس تخصصی و عمومی سال دوازدهم، در قالب تراکنش نگهداری می‌شود. سازمان سنجش بعنوان سازمان متولی امر می‌تواند این سوابق را بازیابی و نتیجه سنجش (پذیرفته شدن و یا عدم پذیرفته شدن در رشته محل انتخابی داوطلب) را در اختیار داوطلب بگذارد. این مدل جامعیت، غیر متمرکز بودن، حفظ حریم خصوصی و کنترل دسترسی را در نظر گرفته است.

کلمات کلیدی: بلاک چین ، قرادادهای هوشمند، بستر هایپر لجر فابریک، ذخیره و بازیابی امن داده، سوابق تحصیلی دانش‌آموزان

*عهده‌دار مکاتبات:

داود بهره‌پور

نشانی: گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

پست الکترونیکی:bahrepour@mshdiau.ac.ir

۱- مقدمه

چالش کنکور سراسری همواره ذهن داوطلبان و خانواده‌های آنها را درگیر نموده است. در آبان ماه سال ۱۳۸۶ قانونی در مجلس شورای اسلامی برای پذیرش دانشجو در دانشگاه‌ها و مراکز آموزش عالی کشور به تصویب رسید که طی آن، تأثیر سوابق تحصیلی دانش‌آموز، هر ساله تا حذف کامل کنکور افزایش می‌یافت و این قانون در آزمون‌های سراسری سال‌های ۱۳۸۷ تا ۱۳۹۲ مورد استفاده قرار گرفت، اما با توجه به عدم افزایش پوشش سوابق تحصیلی و تقاضای زیاد داوطلبان برای برخی از رشته‌های تحصیلی، حذف کنکور محقق نشد. سوابق تحصیلی دانش‌آموز شامل نمرات دروس عمومی و تخصصی دوره دوم متوسطه در نظام آموزشی ۳-۳-۶ است که امتحانات آن مطابق اصول سنجش و اندازه‌گیری، به طور استاندارد و کیفی توسط وزارت آموزش و پرورش به صورت سراسری و نهایی در سنوات مختلف مطابق مصوبات شورای عالی آموزش و پرورش برگزار شده باشد [1].

در سال جاری سهم نمره کل سابقه تحصیلی پایه دوازدهم دانش‌آموز با لحاظ ضریب دروس ۴۰ در صد است. جدول ۱ به عنوان نمونه، ضرایب دروس عمومی و تخصصی را برای گروه آزمایشی تجربی نشان می‌دهد.

جدول ۱. ضرایب سوابق تحصیلی دیپلم علوم تجربی[1]

نوع	ردیف	نام درس سوابق تحصیلی دیپلم	ضریب
عمومی	۱	فارسی (۳)	۲۱/۶۳
	۲	عربی،زبان قرآن(۳)	۹/۰۵
	۳	تعلیمات دینی (۳)	۱۶/۵۲
	۴	زبان خارجه (۳)	۱۱/۸۰
	۵	سلامت و بهداشت	۳/۴۴
	۶	علوم اجتماعی	۲/۵۶
تخصصی	۷	ریاضی (۳)	۶/۸۸
	۸	زیست شناسی (۳)	۱۲/۰۲
	۹	فیزیک (۳)	۶/۱۹
	۱۰	شیمی (۳)	۹/۹۱

بلاک‌چین یک فناوری نوظهور است که در سال ۲۰۰۸ معرفی شد[2-4]که برای اولین بار به عنوان یک دفتر کل همتا به همتا[1] برای ثبت تراکنش‌های ارز دیجیتال بیت‌کوین مورد استفاده قرار گرفت. هدف از این فناوری از بین بردن هرگونه واسطه شخص ثالث و اجازه دادن به کاربران برای انجام تراکنش مستقیم بود. در بلاک‌چین، هر بلوک تراکنش با هش[2] خود به بلوک قبلی اشاره

[1] نوعی معماری شبکه کامپیوتری است که مشتری و خدمتگزار در یک سطح کار می‌کنند.

۲ به هر رویه خوش تعریف یا تابع ریاضی می‌گویند که حجم زیادی از داده (احتمالاً حجم نامشخصی از داده) را به یک عدد طبیعی تبدیل کند.

می‌کند که جامعیت داده‌ها را تضـمین می‌کند. به عبارتی دیگر با استفاده از تابع هش امکان حذف و یا دستکاری اطلاعات ثبت شده تقریبا غیرممکن اسـت. علاوه بر این، بلاک‌چین امکان استفاده از قراردادهای هوشمند را فراهم می‌کند که قرادادهای خود حکمران هسـتند که صـحت تراکنش را کنترل می‌کند و برای اجرای آن نیازی به واسطه ندارد[5]. دو نوع مهم و مرسوم قراردادهای هوشمند اتریوم[6,7] و هایپر لجر فابریک[8] هسـتند. این مقاله یک مدل مبتنی بر بسـتر هایپرلجر فابریک برای ثبت سـوابق تحصـیلی دانش آموزان و اعلام نتیجه پذیرش یا عدم پذیرش آنها در یک رشته محل انتخابی ارایه شده است. مقاله به شرح زیر سازماندهی شده است. بخش ۲ مرور ادبیات، بخش ۳ بیان مسـئله، بخش ۴ الگوریتم‌های قرارداد هوشـمند و بخش ۵ ارزیابی مدل پیشـنهادی و در نهایت، نتیجه‌گیری و جهت گیری‌های آینده در بخش ۶ آورده شده است.

۲- مرور ادبیات

با توسعه فناوری اطلاعات، سوابق آموزشی دیجیتالی شده است، که روی انواع فضاهای ذخیره‌سازی نگهداری می‌شوند و به راحتی قابل انتقال و اشتراک‌گذاری هستند. سیستم‌های متمرکز در ذخیره و بازیابی داده‌های با اهمیت با چالش‌هایی ازجمله جامعیت، غیر متمرکز بودن، حریم خصوصی، کنترل دسترسی و مقیاس پذیری مواجه هستند[9].

بلاک‌چین به عنوان یک فن‌آوری نوظهور می‌تواند مشکل جامعیت و غیر متمرکز بودن را برطرف کند، در واقع به عنوان یک دفترکل غیر قابل تغییر توصیف می‌شود که برای ذخیره تراکنش‌ها مورد استفاده قرار می‌گیرد و به صورت توزیع شده توسط گره‌های مختلف نگه‌داری می‌شود. هر عضو شبکه یک کپی از این دفترکل را نگه‌داری می‌کند و برای اعتبارسنجی تراکنش‌ها از پروتکل اجماع استفاده می‌شود و سپس تراکنش‌ها در بلوک‌های مختلف قرار می‌گیرند. هش داده‌های ذخیره شده در هر بلوک توسط یک تابع ریاضی محاسـبه شـده و از این مقدار به عنوان اشاره‌گر استفاده شده است و بلوک‌های مختلف به یکدیگر زنجیر می‌شوند. بلاکچین در سال 1990 با هدف زمانبندی اسناد دیجیتال مورد استفاده قرارگرفت [10] و پس از معرفی بیت‌کوین به صورت گسترده در صدر توجهات محققین و توسعه دهندگان جای گرفت. در بلاک‌چین استفاده شده در بیت‌کوین تمامی افراد بدون استفاده از هویت مشخص و تایید شده امکان مشارکت در فرآیند اجماع دارند و در اصطلاح بلاک‌چین استفاده شده در بیت‌کوین یک بلاک‌چین عمومی و بدون نیاز به مجوز است. هویت غیر مشخص در یک سیستم توزیع شده، حملات امنیتی مختلفی از جمله حمله سیبل [11] را محتمل می‌کند.

در مقابل در بلاک‌چین دارای مجوز اجرای تراکنش‌ها صـرفا توسـط گروه مشـخصی از اعضا قابل انجام است. بلاک‌چین دارای مجوز را می‌توان بـه دو گروه کلی بلاک‌چین فدرالی و بلاک‌چین خصـوصـی تقسـیم بندی کرد. در بلاک‌چین فدرالی که کنسرسیومی نیز نامیده می‌شود گروهی از گره‌های از قبل تعیین شده قوانین شبکه را تعیین می‌کنند که این گروه می‌توانند نسبت به هم بی اعتماد باشـند و تایید تراکنش‌ها با تایید این گروه تعیین شده از گره‌ها انجام می‌شود. در بلاک‌چین خصوصی یک عضو خاص یا یک گروه خاص قوانین شبکه را تعیین می‌کنند.[12]

در ادامه نمونه‌هایی از کاربرد فناوری بلاک‌چین در ذخیره‌سازی اطلاعات ارایه شده است.

- حوزه سـلامت: فناوری بلاک‌چین در این حوزه مورد توجه قرار گرفته اسـت چرا که نگهداری و به اشـتراک‌گذاری پرونده سلامت یکی از وظایف ضروری در سیستم‌های مراقبت بهداشتی است و ایمن‌سازی پرونده الکترونیک سلامت از اهمیت بالایی برخوردار است [13-19].

- حوزه دادگستری: فناوری بلاک‌چین به تدریج جایگزین قضات و شاهدان متخصص شده است که نقش اصلی را در شناسایی اصالت و جامعیت شواهد الکترونیکی ایفا کرده‌اند [20].
- حوزه رای‌گیری و انتخابات: یک کاربرد دیگر، سیستم رای‌گیری الکترونیکی است که امنیت آرا را در برابر دستکاری تضمین می‌کند [21].
- حوزه بیمه: حوزه پرکاربرد دیگر گسترش و نفوذ بلاک‌چین در صنعت بیمه است چراکه کسب و کار بیمه نقش بسزایی در زندگی مردم دارد، اما در فرآیند تسویه خسارت احتمال تقلب وجود دارد که از آن جمله می‌توان از امتناع شرکت‌های بیمه در پرداخت خسارت و یا کلاهبرداری سوء مشتریان برای دریافت غرامت نام برد [28-22].

بطور خلاصه نمونه‌های مطرح شده فوق از کاربرد فناوری اطلاعات در ذخیره و بازیابی اطلاعات با مشکلاتی همچون حریم خصوصی[14,23,28]، کنترل دسترسی[15,14,30,23,28] و مقیاس‌پذیری [19,14,30,27,23,28] مواجه‌اند، از آنجاکه این چالش‌ها را فناوری بلاک‌چین حل نمی‌کند، یک راه‌حل، استفاده از قرارداد هوشمند است. از طریق قرارداد هوشمند می‌توان سطح حریم خصوصی و کنترل دسترسی [33-29] را تعریف کرد اما مشکل مقیاس پذیری باقی می‌ماند.

شبکه فابریک یک سیستم ماژولار، قابل توسعه، و منبع باز[1] است که امکان مدیریت و اجرای قراردادهای هوشمند مبتنی بر بلاک‌چین خصوصی را فراهم می‌کند. شبکه فابریک یکی از پروژه‌های هایپرلجر میزبانی شده توسط بنیاد لینوکس است[34] . یکی از مهمترین مزایای فابریک پشتیبانی از زبان‌های برنامه‌نویسی همه‌منظوره بدون وابستگی به رمزارز مبتنی بر شبکه است که با سایر شبکه‌های بلاک‌چین که صرفا از زبان‌های برنامه نویسی با دامنه محدود برای توسعه قرارداد هوشمند استفاده می‌کنند، متفاوت است. برای مثال برای توسعه قرارداد هوشمند در بلاک‌چین اتریوم از رمزارز بومی اتر استفاده می‌شود و برای توسعه قرارداد هوشمند فابریک صرفا از زبان برنامه‌نویسی solidity استفاده می‌شود. این امر توسعه قرارداد هوشمند را برای توسعه‌دهندگان تسهیل می‌کند و چالش‌های پیاده سازی قرارداد هوشمند با یک زبان برنامه‌نویسی جدید را بر طرف می‌کند.

اجزا اصلی در بستر هایپرلجرفابریک عبارتند از:

- یک سیستم ترتیب‌دهی، مسئولیت ترتیب‌دهی تراکنش‌ها را بر عهده می‌گیرد و تمامی همتایان به یک لیست از تراکنش‌های یکسان دسترسی پیدا می‌کنند.
- یک ارائه‌دهنده خدمات عضویت[2] مسئول مرتبط کردن همتایان با هویت رمزنگاری است. این ماهیت خصوصی بودن و نیاز به مجوز در شبکه فابریک را حفظ می‌کند.
- از یک سرویس انتقال شایعه[3] همتا به همتا برای توزیع بلوک‌های خروجی سیستم ترتیب‌دهی به همتایان استفاده می‌شود.
- هر همتا به صورت محلی دفترکل را نگه‌داری می‌کند و همتایان در شبکه فابریک مانند گره‌های شبکه در شبکه بلاک‌چین بیت‌کوین هستند.

[1] یک کد منبع است که برای اصلاح و توزیع مجدد احتمالی آزادانه در دسترس قرار می‌گیرد.

Fabric based Framework as a Service

در شبکه بلاکچین فابریک از یک معماری موسوم به execute-order-validate استفاده می‌شود که جریان تراکنش را به سه فاز مختلف تقسیم بندی می‌کند. که توسط موجودیت‌های مختلف سیستم اجرا می‌شود. در فاز (۱) اجرا تراکنش‌ها انجام می‌شود و صحت و درستی منطق برنامه مورد بررسی قرار می‌گیرد. در فاز (۲) مستقل از منطق قرارداد هوشمند ترتیب‌دهی تراکنش‌ها توسط فرآیند اجماع انجام می‌شود. در فاز(۳) با توجه به سیاست‌ها و فرض‌های از قبل تعیین شده ارزیابی تراکنش‌ها توسط همتایان مختلف و تعیین‌شده شبکه انجام می‌شود. بر خلاف معماری مرسوم order-execute، تراکنش‌ها قبل از رسیدن به توافق نهایی در شبکه فابریک اجرا می‌شوند. برای بررسی دقیقتر معماری execute-order-validate به[35] مراجعه شود.

در این بخش چند مقاله از کاربرد قراردادهای هوشمند در ذخیره و بازیابی اطلاعات مرور شده است:

در [36] برای بهبود کارایی زنجیره تامین، یک سیستم زنجیره تامین پورت مبتنی بر بلاک‌چین هایپر لجر فابریک طراحی و اجرا شده است. در سیستم پیشنهادی، چهار قرارداد هوشمند با بهره‌گیری از توافق غیرمتمرکز، بدون دستکاری، توزیع شده بلاک چین، همراه با سیاست کنترل دسترسی مبتنی بر نقش (RBACP)، ارایه شده است.

در مرجع [37] سیستم بلاک‌چین پرونده الکترونیکی سلامت بیماران، گره‌های همتا از سازمان‌های مختلف (ذینفعان) یک شبکه دفتر کل ایجاد می‌کنند، که در آن کانال‌هایی ایجاد می‌شوند تا ارتباط امن و خصوصی ایجاد کنند. بیماران انفرادی و سایر ذینفعان توسط گواهی های دیجیتال منحصر به فرد صادر شده توسط مؤلفه ارائه دهنده خدمات عضویت (MSP) در معماری هایپر لجر فابریک شناسایی و در شبکه ثبت می‌شوند.

در مرجع [38]، یک راه ایمن رای‌گیری با کمک بلاک‌چین با استفاده از چارچوب مبتنی بر هایپر لجر فابریک به عنوان یک سرویس (FaaS)[۱] پیشنهاد شده است که می‌تواند برای اجرای رای‌گیری الکترونیکی با قابلیت نگهداری، مقیاس بزرگ و مقرون به‌صرفه استفاده شود.

مرجع[39] اجرای قراردادهای هوشمند برای خدمات بیمه را بر اساس بلاک‌چین هایپرلجر فابریک ارائه می‌کند. از طریق قراردادهای هوشمند می‌توان بیمه نامه ایجاد کرد، ریسک بیمه را تعیین کرد و خسارت‌های بیمه‌ای را اجرا کرد.

نمونه‌های فوق زمینه‌های کاربردی استفاده از قراردادهای هوشمند را نشان می‌دهند از آنجا که در حیطه سنجش و پذیرش داوطلبان کنکور و آزمون ورودی دانشگاه‌ها کار مشابهی صورت نگرفته، در مرور این مقالات تمرکز بر نحوه ذخیره و بازیابی اطلاعات بوده است.

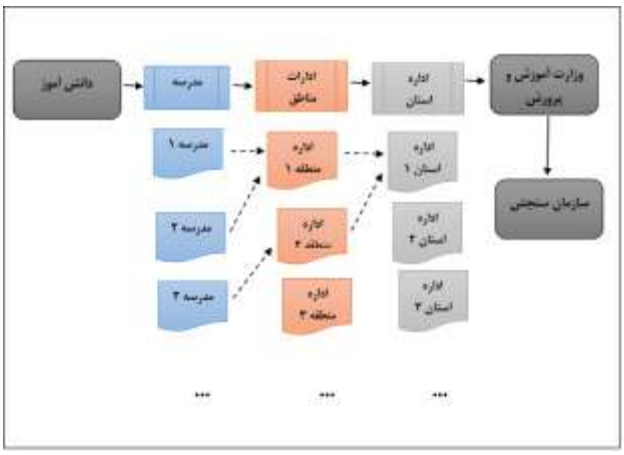
۳- مدل پیشنهادی

در این بخش ابتدا مدل را برای نمایش عملکرد بصورت بلوک دیاگرامی از موجودیت‌ها شامل دانش‌آموز، وزارت آموزش و پرورش و سازمان سنجش نمایش می‌دهیم، سپس آن را به موجودیت‌های شبکه فابریک نگاشت می‌دهیم.

سه موجودیت اصلی سیستم از چهار سطح مدرسه و ادارات مناطق، اداره استان و وزرات آموزش و پرورش در شکل ۱ نشان داده شده است. هر یک از سطوح مدارس و ادارات می‌تواند شامل تعداد زیادی پرونده باشد که به صورت موازی ایجاد و برای ارسال به وزارتخانه آماده می‌شود.

---

[۱] Fabric based Framework as a Service



شکل ۱. بلوک دیاگرام موجودیت ها

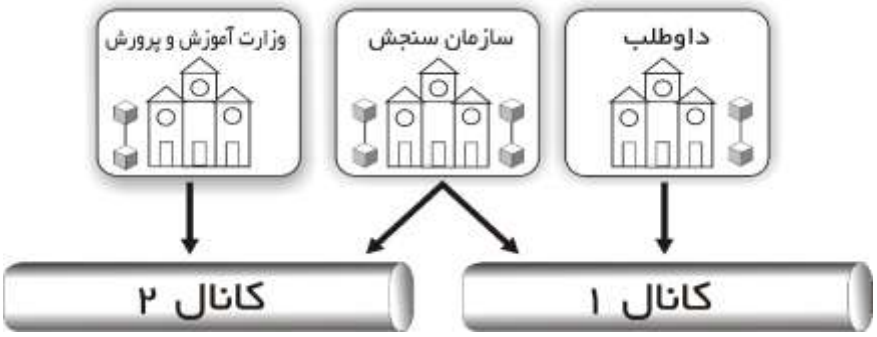
همانطور که شکل ۱ نشان می‌دهد ادارات استان که در سطح اول قرار می‌گیرند بیشترین ارتباط با وزارت‌خانه را دارند و نسبت به سایر سطوح پرونده‌های بیشتری دارند که به صورت مستقیم به وزارت‌خانه ارسال می‌شوند.

کلی‌ترین موجودیت در شبکه فابریک، یک سازمان است هرسازمان از بخش‌های مختلفی تشکیل شده است که عبارتند از:

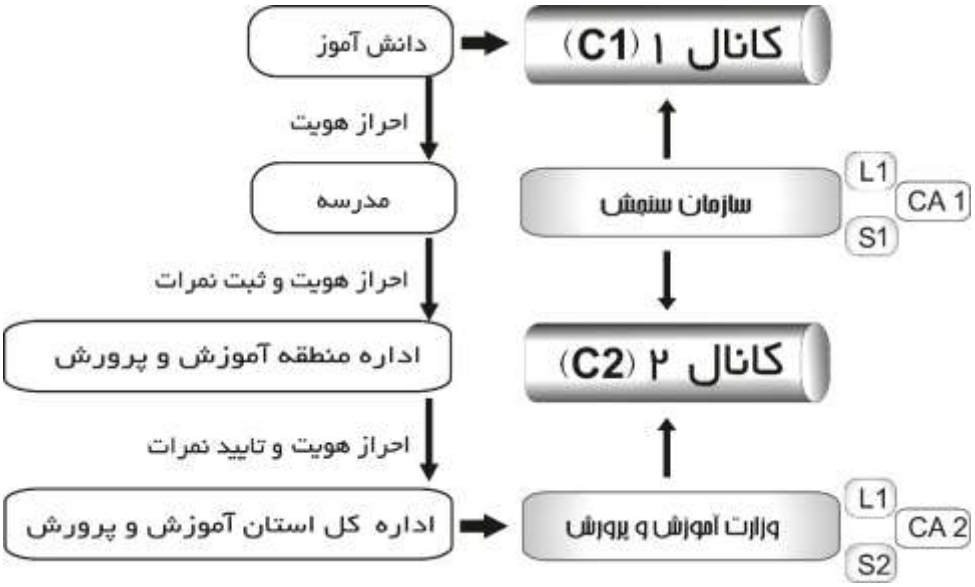
- سرویس خدمات عضویت
- ادمین(ها)
- کاربران
- همتایان
- کانال‌ها

سرویس خدمات عضویت هویت افراد را تایید می‌کند و موجودیتی است که برای مدیریت بلاک‌چین دارای نیاز به مجوز، ضروری است و سطوح دسترسی مختلف را تعیین می‌کند. هر یک از بخش‌های مختلف سازمان از جمله کاربران، ادمین، همتایان دارای هویت مخصوص به خود هستند. این هویت‌ها توسط Certificate Authority که به اختصار CA نامیده می‌شود صادر می‌شود. هر زمانی که یک کاربر با بلاک‌چین تعامل انجام می‌دهد با امضای تراکنش هویت خود را اثبات می‌کند و این امضا توسط همتایان سیستم ارزیابی می‌شود. هر سازمان می‌تواند یک یا چند ادمین داشته باشد که وظایفی از جمله وارد کردن همتایان به شبکه، کمک به اتصال همتایان به یک کانال، نصب قرارداد هوشمند از طرف این افراد و همچنین ممکن است سرویس ترتیب‌دهی تراکنش‌ها را اجرا کنند. علاوه بر آن هر سازمان می‌تواند حاوی یک یا چند همتا باشد که می‌توانند نقش اعتبارسنجی تراکنش، طبق سیاست از پیش تعیین شده را داشته باشند و یا صرفا قرارداد هوشمند و آخرین وضعیت شبکه را نگهداری کنند. همچنین هر سازمان می‌تواند در یک یا چند کانال در شبکه بلاک‌چین مشارکت کند. در اینجا کانال‌ها برای درج سوابق تحصیلی دانش‌آموز مابین وزارت آموزش و پرورش و سازمان سنجش و برای اعلام پذیرش یا عدم پذیرش داوطلب مابین سازمان سنجش و داوطلب در نظر گرفته شده‌اند. وجود کانال به واسطه حفظ امنیت اطلاعات ضروری است در واقع همانطور که شکل ۲ نشان می‌دهد کانال ۱ مابین وزرات آموزش و پرورش و سازمان سنجش برای ارسال سوابق و کانال ۲ بین سازمان سنجش و داوطلب برای اعلام نتیجه پذیرش در نظرگرفته شده

اســـت. اطلاعات هر ســـازمان در بلوک genesis که پیکربندی کانال انجام می‌شـــود نگه داری می‌شـــود. کاربران در ســـیســـتم، موجودیت‌هایی هســـتند که از طریق برنامه کاربر با بلاک‌چین ارتباط برقرار می‌کنند و به طور مســـتقیم با معماری بلاک‌چین و تایید تراکنش‌ها در ارتباط نیستند. تجمیع موجودیت‌ها و بلوک دیاگرام نهایی عملکرد مدل در شکل ۳ آمده است.



شکل ۲. دو کانال به کار رفته در مدل



شکل ۳. مدل معرفی شده برای پذیرش داوطلبان کنکور سراسری بر اساس سوابق تحصیلی در بستر هایپر لجر فابریک

با توجه به شکل ۳، دانش‌آموز ابتدا توسط مدرسه ثبت نام و احراز هویت می‌شود، مدرسه سوابق تحصیلی دانش آموز را به اداره منطقه (نواحی) آموزش و پرورش ارسال می‌کند. سپس ادارات آموزش و پرورش به اداره کل استان و نهایتا به وزرات آموزش و پرورش ارسـال می‌شـود. وزارت آموزش و پرورش به عنوان بالاترین مرجع متولی آموزش متوسـطه دوم در راس سطوح دسترسی به پایگاه داده نمرات و سوابق تحصیلی دانش آموزان قرار می‌گیرد. در این ارگان نمرات دروس عمومی و تخصصی دانش آموز در قالب

تراکنش از طریق کانال ۲ (C2) به سـازمان سـنجش ارسال می‌شود. سازمان سنجش می‌تواند بر اساس ضریب نمرات ارسالی و نمره کنکور سـراسری برای رشته‌های تحصیلی که کنکور برگزار می‌شود و یا معدل دیپلم برای رشته‌های تحصیلی بدون کنکور سنجش را صورت دهد و نتیجه را از طریق کانال ۱ (C1) به داوطلب اعلام کند.

۴- قراردادهای هوشمند

قرارداد هوشمند در سطح وزارت آموزش و پرورش(S1) دو وظیفه را به عهده دارد: اول: احراز هویت ، ثبت نام دانش‌آموز و ثبت نمرات. دوم: پیش پردازش سوابق تحصیلی دانش آموزان و ایجاد تراکنش. این تراکنش در شکل نشان۴ داده شده است.

TX ID	TX *index*	STID	NUM	…	NUM	Average

شکل ۴. تراکنش در سطح وزارت آموزش و پرورش

فیلدهای نمایش داده شده در شکل ۴ عبارتند از :

- TX ID : شناسه تراکنش
- TX index : شاخص تراکنش
- STID : شماره دانش آموزی
- NUM : نمره درس
- Average: معدل دیپلم

سـازمان سـنجش در قالب یک قراداد هوشمند(S2) دیگر بر اساس داده‌های دریافتی و نتایج آزمون کنکور سراسری برای برخی رشته محل‌ها که کنکور برگزار شده است نتیجه پذیرش یا عدم پذیرش را از طریق کانال دیگر به داوطلب اعلام می‌کند. شکل ۵ فیلدهای این تراکنش را نشان می‌دهد.

TX ID	TX index	STID	Result

شکل ۵. تراکنش در سطح سازمان سنجش

همانطور که شکل ۵ نشان می‌دهد فیلدها عبارتند از :

- TX ID :شناسه تراکنش
- TX index : شاخص تراکنش
- STID : شماره دانش‌آموزی
- Result : نتیجه قبولی یا رد شدن

۵- ارزیابی مدل پیشنهادی

ویژگی‌های مدل معرفی شده عبارتند از:

- **احراز هویت** : در هر دو قرارداد هوشمند، احراز هویت با استفاده از مراکز احراز هویت مستقر در نودهای سازمان سنجش و وزارت آموزش و پرورش صورت می‌گیرد. در سطح آموزش و پرورش برای مدرسه و منطقه و استان و در سطح سازمان سنجش برای دانش آموز احراز هویت انجام می‌شود.
- کنترل دسترسی : یک کانال بین وزارت آموزش و پرورش و سازمان سنجش برای ارسال سوابق تحصیلی دانش‌آموز و یک کانال میان سازمان سنجش و دانش آموز برای دریافت نتیجه کنکور سراسری لحاظ شده است تا اطلاعات بصورت محرمانه در دسترس قرار گیرد.
- محرمانگی : اطلاعات دانش آموز با شماره دانش آموزی به جای نام و نام‌خانوادگی ذخیره می‌شود و از طریق کانال امن ارسال و دریافت اطلاعات صورت می‌گیرد.

با توجه به حساسیت داده‌ها و پیشرفت تکنولوژی، اولویت و دقت معیارهای سنجش متحول شده‌اند. مدل پیشنهادی با استفاده از قرادادهای هوشمند، کانال‌ها و مراکز احراز هویت مجزا در بستر هایپر لجر فابریک، کنترل دسترسی و حریم خصوصی را مد نظر قرار داده است.

۶- نتیجه‌گیری

در این مقاله در راستای حذف کنکور سراسری و ذخیره و بازیابی امن سوابق تحصیلی دانش‌آموزان در برابر دستکاری، تقلب و جعل هویت مدلی مبتنی بر فناوری ایمن و تغییر ناپذیر بلاک‌چین هایپر لجر فابریک ارایه شده است. با در نظر گرفتن نقش‌ها، کانال‌ها، قراردهای هوشمند و مراکز احراز مجوز، سوابق تحصیلی دانش‌آموز به صورت امن در قالب تراکنش ذخیره و ارسال می‌شود و نتیجه کنکور هم بطور محرمانه به دانش آموز اعلام می‌شود. بستر بلاک‌چین هایپرلجرفابریک مزیت‌های فراوانی نسبت به سایر بلاکچین‌های خصوصی دارد. یکی از این مزیت‌ها امکان استفاده از زبان‌های برنامه‌نویسی چند منظوره برای توسعه قرارداد هوشمند است و نیازی به استفاده از زبان‌های برنامه نویسی با دامنه محدود نیست که توسعه و تغییر برنامه را تسهیل می‌کند. در این مدل جامعیت، حریم خصوصی، کنترل دسترسی در نظر گرفته شده است. در کارهای آینده می‌توان امکان ملاحظه سوابق دانش‌آموزی را با هدف استخدام و یا ادامه تحصیل در سایر موسسات آموزش عالی فراهم نمود.

مراجع

[۱] https://www.sanjesh.org

[۲] S. Nakamoto, “Bitcoin: A Peer-to-peer Electronic Cash System,” vol. 15, no. 4, 2008

[۳] Morgen E Peck, "Blockchains: How they work and why they’ll change the world". IEEE Spectrum 54, 10 (2017), 26–35, 2017

[۴] Meng Han Zhigang Li Jing (Selena) He, “A Novel Blockchain-based Education Records

Verification Solution", Session 6A: Papers SIGITE'18, October 3-6, 2018, Fort Lauderdale, FL, USA

[۵] Mehdi Sookhak , Mohammad Reza Jabbarpour , Nader Sohrabi Safa , F. Richard Yu ," Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues", Journal of Network and Computer Applications Volume 178, 15 March 2021, 102950

[۶] https://ethereum.org/

[۷] Zeli Wang, Hai Jin, Weiqi Dai, Kim-Kwang Raymond Choo & Deqing Zou "Ethereum smart contract security research: survey and future research opportunities", Frontiers of Computer Science volume 15, Article number: 152802 (2021)

[۸] www.hyperledger.org

[۹] Hongzhi Li Dezhi Han, (Member, IEEE)," EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme, date of publication", November 27, 2019, date of current version December 23, 2019

[۱۰] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," J. Cryptol., vol. 3, no. 2, pp. 99–111, 1991

[۱۱] S. Zhang and J. H. Lee, "Double-Spending with a Sybil Attack in the Bitcoin Decentralized Network," IEEE Trans. Ind. Informatics, vol. 15, no. 10, pp. 5715–5722, 2019

[۱۲] O. Dib, K. Brousmiche, A. Durand, E. Thea, and B. Hamida, "Consortium blockchains: Overview, applications and challenges," Int. J. Adv.

[۱۳] Jin Sun; Xiaomin Yao; Shangping Wang; Ying Wu All Authors," Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS", accepted August 19, 2020, date of publication August 24, 2020, date of current version September 3, 2020.

[۱۴] Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya Balamurugan Balusamy," Securing e-health records using keyless signature infrastructure
blockchain technology in the cloud", Intelligent Biomedical Data Analysis and Processing Published: 30 November 2018

[۱۵] Jayapriya Jayabalan, N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," Journal of Parallel and Distributed Computing Volume 164, June 2022, Pages 152-167

[۱۶] Shivansh Kumar, Aman Kumar Bharti, Ruhul Amin," Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions" Volume4, Issue5 September/October 2021 e162

[۱۷] Anton Hasselgren , Katina Kralevska , Danilo Gligoroski , Sindre A. Pedersen , Arild Faxvaag "Blockchain in healthcare and health sciences—A scoping review", International Journal of Medical Informatics Volume 134, February 2020, 104040

[۱۸] Mohsen Attaran, ” Blockchain technology in healthcare: Challenges and opportunities” , INTERNATIONAL JOURNAL OF HEALTHCARE MANAGEMENT https://doi.org/10.1080/20479700.2020.1843887

[۱۹] Rateb Jabbar; Noora Fetais; Moez Krichen; Kamel Barkaoui, “Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity”, Conferences >2020 IEEE International Confe...

[۲۰] Hong Wu , Guan Zheng,” Electronic evidence in the blockchain era: New rules on authenticity and integrity”, Computer Law & Security Review Volume 36, April 2020, 105401

[۲۱] Roopak T M Dr. R Sumath,” Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology”, Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020) IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1

[۲۲] Ankitha Shetty , Adithya D. Shetty, Rashmi Yogesh Pai1, Rohini R. Rao, Rakshith Bhandary, Jyothi Shetty, Santosh Nayak, Tantri Keerthi Dinesh, and Koma Jenifer Dsouza, “Block Chain Application in Insurance Services: A Systematic Review of the Evidence”, Artificial Intelligence for Smart Society - Literature Review

[۲۳] Anokye Acheampong AMPONSAH Professor Adebayo Felix ADEKOYA,” Blockchain in Insurance: Exploratory Analysis of Prospects and Threats”, International Journal of Advanced Computer Science and Applications, Vol. 12, No. 1, 2021

[۲۴] Lanqing Zhao,” The Analysis of Application, Key Issues and the Future Development Trend of Blockchain Technology in the Insurance Industry” American Journal of Industrial and Business Management > Vol.10 No.2, February 2020

[۲۵] Zhe Xiao; Zengxiang Li; Yechao Yang; Piao Chen; Ryan Wen Liu; Wei Jing; Yauheni Pyrlo,” Blockchain and IoT for Insurance: A Case Study and Cyberinfrastructure Solution on Fine-Grained Transportation Insurance” , IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, VOL. 7, NO. 6, DECEMBER 2020

[۲۶] Abid Hassan , Md. Iftekhar Ali , Rifat Ahammed , Mohammad Monirujjaman Khan , Nawal Alsufyani , and Abdulmajeed Alsufyani ,” Secured Insurance Framework Using Blockchain and Smart Contract”, Hindawi Scientific Programming Volume 2021, Article ID 6787406, 11 pages

[۲۷] Jin Sun; Xiaomin Yao; Shangping Wang; Ying Wu All Authors,” Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS”, accepted August 19, 2020, date of publication August 24, 2020, date of current version September 3, 2020.

[۲۸] Simon Grima, Jonathan Spiteri Inna Romānova, ” A STEEP framework analysis of the key factors impacting the use of blockchain technology in the insurance industry”, Published: 23 March 2020

[۲۹] Liam Bell,1 William J Buchanan,1 Jonathan Cameron,2 Owen Lo1, "Applications of Blockchain Within Healthcare", https://doi.org/10.30953/bhty.v1.8

[۳۰] Xiaodong Yang; Ting Li; Xizhen Pei; Long Wen; Caifen, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology", March 16, 2020. Digital Object Identifier 10.1109/ACCESS.2020.2976894

[۳۱] F. B. Schneider," Implementing fault-tolerant services using the state machine approach: A tutorial. ACM" Comput. Surv., 22(4):299–319, 1990

[۳۲] Mohsin Ur Rahman, Fabrizio Baiardi, Barbara Guidi, Laura Ricci ," Protecting Personal Data Using Smart Contracts" , Internet and Distributed Computing Systems pp 21–32

[۳۳] Richa Gupta; Vinod Kumar Shukla; Sindhu Suresh Rao; Shaista Anwar; Purushottam Sharma; Ruchika ," Enhancing Privacy through "Smart Contract" using Blockchain-based Dynamic Access Control", 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)

[۳۴] Seyedeh Somayeh Fatemi Nasab; Davoud Bahrepour; Seyed Reza Kamel Tabbakh ," A Review on Secure Data Storage and Data Sharing Technics in Blockchain-based IoT Healthcare Systems", 2022 12th International Conference on Computer and Knowledge Engineering (ICCKE)

[۳۵] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proceedings of the 13th EuroSys Conference, EuroSys 2018, Apr. 2018

[۳۶] Na Gao, Dezhi Han, Tien-Hsiung Weng, Benhui Xia, Dun Li, Arcangelo Castiglione, Kuan-Ching Li ," Modeling and analysis of port supply chain system based on Fabric blockchain", Computers & Industrial Engineering 173 (2022) 108716

[۳۷] Mueen Uddin1, M. S. Memon , Irfana Memon , Imtiaz Ali , Jamshed Memon , Maha Abdelhaq and Raed Alsaqour," Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records", Computers, Materials & Continua DOI:10.32604/cmc.2021.015354

[۳۸] Prodipta Promit Mukherjee Arika Afrin Boshra Mallik Mohammad Ashraf Milon Biswas," A Hyper-ledger Fabric Framework as a Service for Improved Quality E-voting System", 2020 IEEE Region 10 Symposium (TENSYMP), 5-7 June 2020, Dhaka, Bangladesh

[۳۹] Veneta Aleksieva, Hristo Valchanov Anton Huliyan , "Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain" , 978-1-7281-4346-0/20/$31.00 ©2020 IEEE