بررسی سیستم های مدیریت هویت مبتنی بر پایگاه دانش و بلاک چین

مهساشکاری-تکتم پازش-حمید طباطبایی

گروه مهندسی کامپیوتر, واحد مشهد ,دانشگاه آزاد اسلامی , مشهد,ایران

Department Of Computer Engineering , Mashhad Branch ,Islamic Azad University , Mashhad ,Iran

چکیده

راه حل های مدیریت هویت عموما برای تسهیل مدیریت هویت های دیجیتال و عملیاتی مانند احراز هویت طراحی شده و به طور گسترده در برنامه های کاربردی دنیای واقعی استفاده می گردند. در سال‌های اخیر، تلاش‌هایی برای معرفی راه‌حل‌های مدیریت هویت مبتنی بر بلاک چین صورت گرفته که به کاربر اجازه می‌دهد کنترل هویت خود (یعنی هویت خودمختار) را در دست بگیرد. در این مقاله، یک بررسی عمیق از مقالات مدیریت هویت مبتنی بر بلاک چین و مدیریت پایگاه دانش منتشر شده بین ماه می ۲۰۱۷ تا ژانویه ۲۰۲۰ ارائه خواهیم نمود. از جمله نتایج مهم این پژوهش ذکر این مورد می باشد که سیستم های I DM مبتنی بر بلاک چین بر تعدادی از محدودیت های ذاتی سیستم های I DMمعمولی غلبه می کنند. چنین سیستم های مبتنی بر بلاک چین را می توان به عنوان یک انقلاب هویت توصیف کرد.

بلاک چین بر روی مفهوم "دفترکل/پایگاه داده توزیع شده" کارمی‌کند. تراکنش‌ها ثبت می‌شوند و به صورت زمانی برای همه طرف های شرکت کننده تکرار می‌شوند. بلاک چین ثابت شده است که تغییرناپذیراست و از طریق یک جفت کلید خصوصی و عمومی، مسئولیت‌پذیری، یکپارچگی و محرمانه بودن بسیار زیادی را ارائه می‌دهد.

کلیدواژه ها: سیستم مدیریت، پایگاه دانش، بلاک چین

۱- مقدمه

هویت دیجیتال نقش مهمی را در جامعه به هم پیوسته و دیجیتالی ما ایفا می نماید. برای مثال، بسیاری از ما تعدادی هویت دیجیتالی داریم که با محل کار، زندگی شخصی و سایر فعالیت‌های مرتبط با حرفه‌ای مرتبط می باشد. این امر تا حدی به اتکای فزاینده به مدیریت اطلاعات هویت (که در ادبیات به آن مدیریت هویت، مدیریت هویت و کنترل دسترسی و غیره نیز گفته می‌شود) کمک می‌کند که برای مدیریت و ایمن کردن اطلاعات هویتی ما و ارائه خدمات مرتبط طراحی شده است. در یک سیستم مدیریت هویت مبتنی بر بلاک چین، تعداد زیادی گره توزیع شده وجود دارد(۱۰).

چنین گره هایی را می توان برای ارائه ذخیره سازی توزیع شده، دسترسی قابل اعتماد و قابلیت های محاسباتی مورد استفاده قرار داد. کاربر در چنین سیستمی به عنوان یک گره در شبکه عمل می کند. بنابراین، اجازه می دهد تا ذخیره سازی داده های کاربر حساس از سرورها (در راه حل های مدیریت هویت مرسوم) به کاربر تغییر کند در یک سیستم مدیریت هویت مبتنی بر بلاک چین معمولی، تعداد زیادی گره توزیع شده وجود دارد (۱۰).

چنین گره هایی را می توان برای ارائه ذخیره سازی توزیع شده، دسترسی قابل اعتماد و قابلیت های محاسباتی مورد استفاده قرار داد. کاربر در چنین سیستمی به عنوان یک گره در شبکه عمل می کند. بنابراین، اجازه می دهد تا ذخیره داده های کاربر حساس از سرورها (در راه حل های مدیریت هویت مرسوم) به دستگاه ها/گره های کاربر (در پارادایم جدید مبتنی بر بلاک چین) تغییر کند. این امر هویت خودمختار (SSI) را تسهیل کرده، زیرا کاربران اکنون این قابلیت را خواهند داشت که کنترل هویت خود را دوباره به دست آورند. در نتیجه، این امر خطرات مختلف ذاتی راه‌حل‌های مدیریت هویت مرسوم (مانند سوء استفاده از هویت کاربر) را به حداقل خواهد رساند(۲۲).

۲- بررسی مفاهیم

مدیریت هویت

همانطور که قبلاً بحث شد، مدیریت هویت (IDM) همچنین به عنوان مدیریت هویت و دسترسی (IAM) در ادبیات شناخته می شود. به طور کلی، IDM به چارچوبی از سیاست‌ها و فناوری‌ها برای اطمینان از اینکه فقط افراد مجاز می‌توانند به منابع مرتبط در یک سازمان دسترسی داشته باشند، اشاره دارد (۱۲).

با این حال، همانطور که جامعه ما بیشتر به هم پیوسته و دیجیتالی می شود، با افزایش قابل توجهی در تعداد و انواع سیستم ها و هویت هایی که باید مدیریت شوند، نیاز به بازنگری مجدد پارادایم های IDM مرسوم نیز وجود دارد. به عنوان مثال، همانطور که قبلاً بحث شد، تلاش‌هایی برای استفاده از ویژگی‌های بلاک چین (به عنوان مثال عدم تمرکز، باز بودن، قابل اعتماد بودن و امنیت) در طراحی نسل بعدی IDM صورت گرفته است.

بلوک های ساختمان

برای سادگی، اجازه دهید سناریویی را در نظر بگیریم که در آن کاربر از یک ارائه‌دهنده هویت درخواست اثبات هویت می‌کند و ارائه‌دهنده هویت به توکن پاسخ می‌دهد. در این محیط ساده، تبادل اطلاعات بین هر دو نهاد (به عنوان مثال فرد واقعی یا برخی از موجودیت ها) وجود دارد. اگر ارائه دهندگان هویت موجودیت های جداگانه ای باشند، آنگاه این به یک مدل مدیریت هویت سه جانبه متشکل از کاربران، ارائه دهندگان هویت و وابستگان هویت تبدیل می شود. در چنین مدلی، از آنجایی که

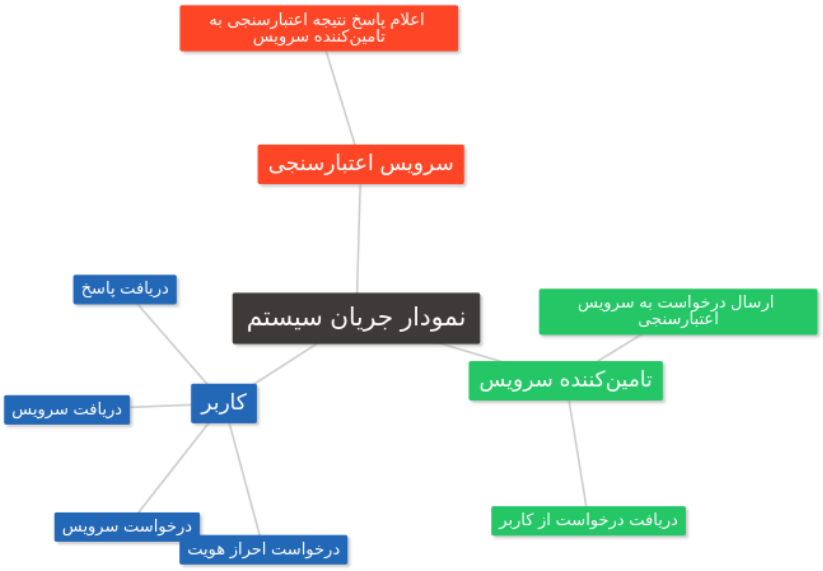
ارائه‌دهنده هویت یک موجودیت جداگانه است، منبع هویتی که برای احراز هویت استفاده می‌شود فقط در ارائه‌دهنده هویت ذخیره می‌شود و وابسته به هویت تنها می‌تواند با پرس و جو از ارائه‌دهنده هویت، احراز هویت کاربر را تأیید کند. علاوه بر ارائه هویت کاربر، ارائه دهندگان هویت باید مدیریت هویت، بازنشانی هویت، ابطال هویت و سایر عملکردهای مرتبط را نیز داشته باشند (۲۱).

- کاربر: کاربران توانمندسازهای اولیه سیستم هستند که از خدمات مختلف ارائه شده توسط ارائه دهنده خدمات و ارائه دهنده هویت لذت می برند. همه کاربران از امتیاز یکسانی برخوردار نیستند.

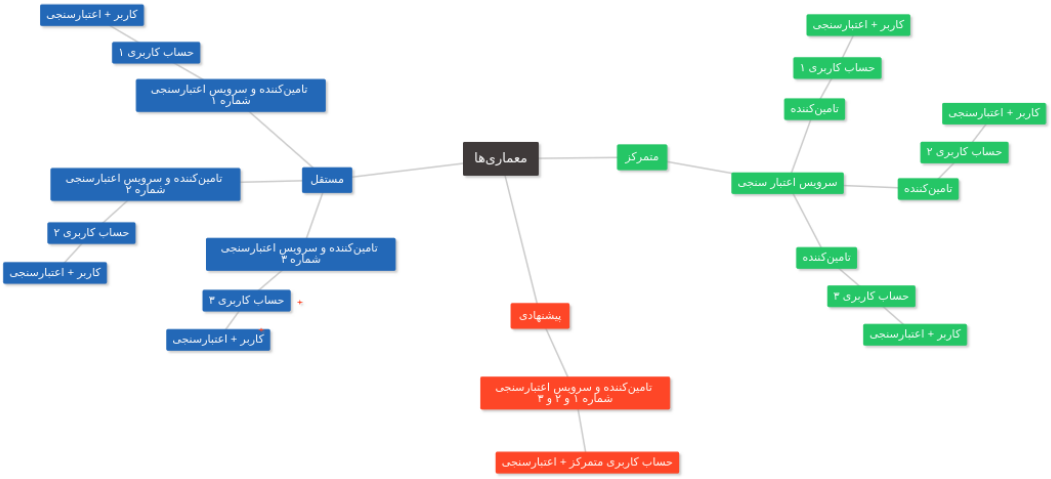
- ارائه دهنده هویت: ارائه‌دهنده هویت، هسته اصلی سیستم، وظیفه ارائه خدمات هویتی (مانند ثبت نام، احراز هویت و مدیریت) را بر عهده دارد. این موجودیت همچنین احراز هویت کاربر را فراهم می کند.

- ارائه دهنده خدمات: ارائه‌دهنده خدمات بخش مهمی از سیستم است و عمدتاً مسئول ارائه خدمات برای کاربران (پس از احراز هویت با موفقیت) است.

نمودار جریان سیستم در شکل ۱ ارائه شده و در زیر توضیح داده شده است:



شکل ۱. یک عملیات معمولی از یک سیستم مدیریت هویت (۱۸).



شکل ۲. معماری مدیریت هویت: یک نمای کلی (۱۸).

برای بهره مندی از خدمات مورد نظر، کاربر باید از مدیر هویت درخواست هویت ارسال کند. سپس مدیر هویت بر اساس اطلاعات ارائه شده توسط کاربر یک هویت منحصر به فرد ایجاد می کند و به کاربر پاسخ می دهد. کاربر یک سرویس خاص از ارائه دهنده خدمات درخواست می کند و ارائه دهنده خدمات اطلاعات هویتی را از کاربر درخواست می کند. کاربر درخواست را دریافت کرده و با داده های مربوطه پاسخ می دهد.

ارائه دهنده خدمات از ارائه دهنده هویت درخواست می کند تا اعتبار هویت کاربر را تأیید کند. ارائه‌دهنده هویت، نتایج احراز هویت را برمی‌گرداند و ارائه‌دهنده خدمات، سرویس را بر اساس نتایج تأیید اعتبار دریافت‌شده ارائه می‌کند (۱۷).

معماری

بسیاری از سیستم‌ها و معماری‌های مدیریت هویت مختلف در ادبیات وجود دارد (۱۸) که می‌توان آن‌ها را به طور کلی در معماری مدیریت هویت مستقل (IIMA) طبقه‌بندی کرد. معماری مدیریت هویت فدرال و معماری مدیریت هویت متمرکز (شکل ۲ را ببینید).

جدول ۱: معماری‌های مدیریت هویت مستقل، فدرال و متمرکز: خلاصه‌ای مقایسه‌ای

استاندارد	معماری سیستم		
	IIMA	CIMA	FIMA
پیچیدگی	کم	متوسط	بالا
پیاده سازی	ساده	متوسط	سخت
مقیاس پذیری	بالا	متوسط	کم
الزامات کاربران	قابل توجه (به عنوان مثال ذخیره سازی)	سبک	متوسط
SSO	پشتیبانی نشده	پشتیبانی	پشتیبانی

- IMA مستقل: در این معماری، هر ارائه‌دهنده خدمات داده‌های هویت کاربر خود را دارد. به عبارت دیگر، هویت ارائه دهندگان خدمات مختلف قابل تعامل نیست. اگرچه ساختار ساده است، اما با افزایش تعداد ارائه دهندگان خدمات، مقیاس پذیر نیست (مثلاً پیامدهایی برای نیازهای ذخیره سازی در ارائه دهندگان خدمات). همچنین، برای کاربران عملی نیست که اطلاعات هویتی خود را برای هر ارائه دهنده خدمات بدون استفاده مجدد یا بازیافت اعتبار کاربری خود به خاطر بسپارند.
- IMA متمرکز: IMA متمرکز تنها یک شناسه و ارائه دهنده هویت در دامنه مورد اعتماد دارد. این بدان معنی است که همه ارائه دهندگان خدمات در یک دامنه مورد اعتماد هویت کاربران را به اشتراک خواهند گذاشت. از این رو، شناسه باید با دقت انتخاب شود و هویت منحصر به فرد در دامنه مورد اعتماد یک انتخاب معمولی است (۱۳).

۳- بلاک چین

اتریوم، اولین پلتفرمی که قرارداد هوشمند کامل تورینگ را اجرا کرد، در حال حاضر یکی از محبوب‌ترین پلتفرم‌ها برای برنامه‌های بلاک چین است. بنابراین، ما از اتریوم به عنوان مثال برای توضیح معماری بلاک چین استفاده خواهیم کرد. یک نمای کلی از ساختار اتریوم در شکل ۳ ارائه شده است.

شکل ۳. ساختار اتریوم.

لایه داده پایه و اساس همه عملکردها از جمله ذخیره سازی داده ها و تضمین امنیت است. ذخیره سازی داده ها از طریق بلوک ها و زنجیره محقق می شود. ذخیره سازی بر اساس درخت Merkle برای اطمینان از پایداری داده ها است. ضمانت امنیت متکی به عملکرد هش لایه داده، امضای دیجیتال و سایر فناوری‌های رمزنگاری است که در مجموع امنیت حساب و تراکنش را تضمین می‌کنند. امضا و هش زیربنایی الگوریتم امضای الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA) و الگوریتم هش SHA۳ را اتخاذ می‌کند (۶).

لایه شبکه یک لایه است که با استفاده از فناوری همتا به همتا (P۲P) پیاده سازی شده است. در یک شبکه P۲P، هیچ سرور متمرکزی وجود ندارد و هر کاربر یک گره با عملکرد سرور است. این لایه تجسم عدم تمرکز و استحکام شبکه است.

۴- چالش های مدیریت هویت

تعدادی از چالش‌ها پشت سر یک سیستمIDM وجود دارد، و در اینجا ما فقط روی موارد زیر تمرکز می‌کنیم. اول، سطح مورد نیاز اعتماد بین سناریوهای مختلف برنامه واقعی متفاوت است. از این رو، الزامات عملی در طراحی سیستم هایIDM باید در نظر گرفته شود.

دسترسی و منبع: سیستم باید چندین سطح دسترسی را از پیش تعریف کند، مثلاً برای نقش های مختلف یا برای منابع مختلف. به عنوان مثال، یک سیستمIDM در یک موسسه آموزشی، این سیستم ممکن است شامل هویت‌هایی مانند اعضای هیئت علمی (مسئولیت رسمی و غیرحضوری)، کارکنان اداری (به عنوان مثال اعضای غیرهیئت علمی) و دانشجویان باشد. در چنین سیستمی، اعضای هیئت علمی دارای نقش‌ها و دسترسی‌های خاصی هستند (مانند دسترسی خواندن/ویرایش به تکالیف، امتحانات و مواد درسی)، و به طور مشابه، یک دانشجو دارای نقش‌ها و دسترسی‌های متفاوتی است (مثلاً برای بارگذاری تکلیف و مشاهده تکالیف و نمرات علامت‌گذاری شده.). یک مدیر همچنین باید دسترسی های متفاوتی داشته باشد(۱۲).

جدول ۲: چگونه Sovrin، uPort، ShoCard با قوانین هویت کامرون مرتبط است (۲۳).

قانون	مورد		
	Sovrin	uPort	ShoCard
۱. کنترل و رضایت کاربر	کاربران می توانند شناسه را برای استفاده و ویژگی هایی را برای آشکار کردن انتخاب کنند. امکان استفاده از وب اعتماد برای جلوگیری از فریب کاربران	ایجاد و افشای uPortIDs ها به طور کامل توسط کاربران کنترل می شود و کاربران می توانند مالکیت خود را ثابت کنند. احتمال نشت ویژگی ها در رجیستری.	کاربران ایجاد و افشای ShoCardIDs ها را کنترل می کنند. فقط طرف دعوت شده توسط مالک ShoCardIDs می تواند به ویژگی ها دسترسی داشته باشد و همه ویژگی ها توسط سرورهای ShoCard تأیید می شوند.
۲. حداقل افشا برای استفاده محدود	اعتبارنامه های ناشناس مبتنی بر شواهد دانش صفر، اصل افشای "کمترین مقدار اطلاعات شناسایی" را تضمین می کند.	هنگام دستیابی به شناسه uPort، نیازی به افشای ویژگی های شخصی نیست.	سند هویت قابل اعتماد برای بوت استرپ ShoCardIDs استفاده می شود.
۳. احزاب قابل توجیه	فقط احزاب و آژانس های مجاز می توانند به ویژگی ها دسترسی داشته باشند.	همه می توانند به ویژگی های موجود در رجیستری دسترسی داشته باشند. احتمال درز داده های رمزگذاری شده	فقط طرف دعوت شده توسط مالک ShoCardIDs می تواند به ویژگی ها دسترسی داشته باشد و سرورهای ShoCard نیز می توانند بدون دعوت به ویژگی ها دسترسی داشته باشند.
۴.هویت کارگردانی شده	از شناسه های همه جانبه پشتیبانی می کند.	از اشتراک گذاری یک طرفه شناسه ها بین طرفین پشتیبانی می کند.	از اشتراک گذاری یک طرفه شناسه ها بین طرفین پشتیبانی می کند.

۵. کثرت گرایی اپراتورها و فناوری ها	بستری برای واسطه ها بین کاربران و شبکه خود ایجاد می کند و رابط برای سایر سیستم های هویتی نیز پشتیبانی می شود.	امکان سفارشی سازی انواع را فراهم می کند، اگرچه استفاده از یک قالب داده خاص ترجیح داده می شود.	طرفین می توانند اعتبارنامه های مورد اعتماد موجود را پس از ادغام با سرورهای متمرکز ShoCard تجزیه کنند.
۶. ادغام انسانی	در مورد قابلیت استفاده و درک کاربر از حریم خصوصی در Sovrin مشخص نیست	برنامه موبایل ارائه شده است اما قابلیت استفاده و درک کاربر از حریم خصوصی مشخص نیست.	برنامه موبایل ارائه شده است اما قابلیت استفاده و درک کاربر از حریم خصوصی مشخص نیست.
۷.تجربه ثابت در سراسر زمینه ها	گفتنش سخت است، زیرا بستگی دارد که Sovrin چندین پلتفرم را انتخاب کند یا خیر.	کاربران با اپلیکیشن موبایل تعامل دارند و اسکن کد QR در دسترس است.	کاربران با اپلیکیشن موبایل تعامل دارند و اسکن کد QR در دسترس است.

۵- سیستم های مدیریت هویت مبتنی بر بلاک چین

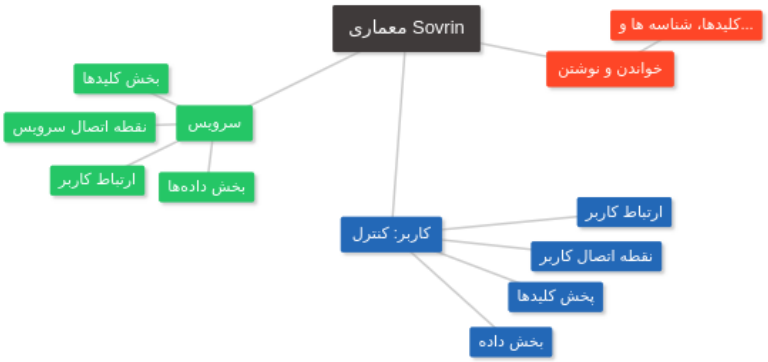
در این بخش، سه سیستمIDM مبتنی بر بلاک چین را بررسی خواهیم کرد:

۱- سوورین. Sovrin (Tobin and Reed) برای استفاده از اعتبار دیجیتال در دنیای آفلاین طراحی شده است. سوورین دارای یک هویت خودمختار است که به هیچ مرجع متمرکزی وابسته نیست و نمی توان آن را حذف کرد. ویژگی های Sovrin شامل حاکمیت، مقیاس پذیری و دسترسی است. مهمتر از آن، Sovrin یک زنجیره عمومی جهانی مبتنی بر Hyperledger است که حریم خصوصی طراحی را امکان پذیر می کند، مانند شناسایی مشتریان خصوصی با نام مستعار. برای تضمین انتخابی حریم خصوصی، از رمزگذاری اثبات دانش صفر استفاده می کند(۲).

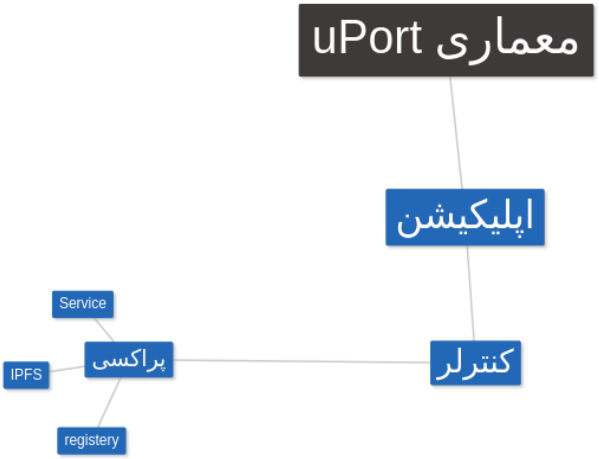
۲- uPort. uPort یک سیستم هویت خودمختار است. این به اتریوم بستگی دارد، بنابراین ماهیت هویت uPort آدرس حساب اتریوم است که کاربران با آن تعامل دارند و هویت دائمی است. جدول uPort قراردادی هوشمند برای همه هویت‌های uPort است و مبنایی برای احراز هویت و اشتراک‌گذاری دسترسی آفلاین به داده‌ها است. از دیدگاه کاربر، uPort برنامه‌های کاربردی Ethereumbased را بهینه می‌کند، به طوری که کاربران به جای پرداختن به آدرس‌های هگزا دسیمال، با افراد واقعی در تعامل هستند(۱۳).

۳- ShoCard (Shocard). ShoCard یک سیستمIDM مبتنی بر بلاک چین است که در آن کاربران می توانند هویت دیجیتالی خود را حفظ کرده و از آن محافظت کنند. اطلاعات هویت کاربر همیشه همراه با کلید کاربر برای اطمینان از حفظ حریم خصوصی استفاده می شود. این امر نیاز به پایگاه داده شخص ثالث را از بین می برد. ShoCard کد احراز هویت داده های کاربر را روی بلاک چین نگه می دارد که می تواند مشروعیت هویت شخصی را تضمین کند و تأیید شخص ثالث را تسهیل کند. ShoCard همچنین برای پرداخت ها سکه های SFN صادر می کند(۱۵).

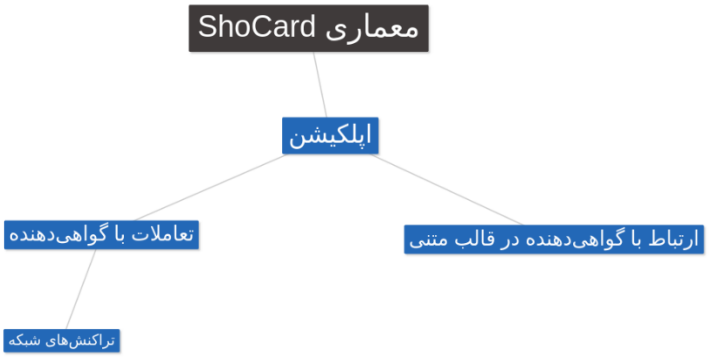
اکنون از قانون هویت کامرون (کامرون، ۲۰۰۵) برای کمک به مقایسه Sovrin، uPort و ShoCard استفاده خواهیم کرد - جدول ۲ را ببینید. ساختارهای Sovrin، uPort و ShoCard به ترتیب در شکل ۴، شکل ۵ و۶ شکل نشان داده شده اند.



شکل ۴. معماری (۲) Sovrin.



شکل ۵. معماری (۲) uPort.



شکل ۶. معماری (۲) ShoCard.

به وضوح بسیاری از سیستم‌های IDM مبتنی بر بلاک چین، از جمله مواردی که در ادبیات پیشنهاد شده‌اند، وجود دارد.

۶- یافته های پژوهش

در حالی که مدیریت هویت به طور گسترده مورد مطالعه قرار گرفته و در عمل به تصویب رسیده است، تعدادی محدودیت و چالش باقی مانده است(۴). در حالی که بلاک چین ممکن است بتواند برخی از این محدودیت ها را کاهش دهد، تعدادی از مسائل و پیامدها باقی مانده است.

جدول ۳: نمونه هایی از سیستم های مبتنی بر اعتماد (براساس یافته های پژوهش)

راه حل	موارد			
	توسعه	شرح	ضعف	استحکام – قوت
Borse et al. (Borse et al., ۲۰۱۶)	شبیه سازی	سیستمی برای هویت خودمختار که ترکیبی از تعهد پدرسن به پروتکل دانش صفر عضویت Interval برای ارائه حریم خصوصی برای ویژگی‌های خاصی از هویت کاربر	هزینه اقتصادی برای اجرای در مقیاس بزرگ	پروتکل تعهد و دانش صفر، ناشناس ماندن انتخابی ویژگی های کاربر در بلاک چین
Faber et al. (Faber et al., ۲۰۱۹)	طرح	سیستم مدیریت داده‌های شخصی و هویت مبتنی بر بلاک چین (BPDIMS) یک سیستم مدیریت هویت و داده‌های شخصی مبتنی بر GDPR و انسان محور است.	هیچ مشخصات دقیقی وجود ندارد که تعاملات مختلف بین ذینفعان مختلف سیستم را به طور واضح توصیف کند.	شفافیت و کنترل استفاده از داده های شخصی کاربران را فراهم می کند
Kikitamara et al. (Kikitamara et al.,)	طرح	سیستمی برای هویت خودمختار با استفاده از هویت دیجیتال ترکیبی	امکان آن بخش ها با مقیاس بزرگ باید مورد بحث قرار گیرد، محدودیت ها و عدم قطعیت ها در مکانیزم احراز هویت پیشرفته	ترکیبی از هویت های فدرال و کاربر محور، توسعه پذیری، فناوری اطلاعات ترکیبی و قابلیت همکاری
Ren et al. (Ren et al., ۲۰۱۹)	شبیه سازی	یک مکانیسم کنترل دسترسی پورتفولیوی مدیریت هویت مبتنی بر بلاک چین و محاسبات لبه با خودمختاری	پروتکل توافق نامه کلیدی وجود ندارد، عملکرد باید بهینه شود	گواهی ضمنی تولید شده را به هویت متصل کنید، ارتباطات ایمن در لبه دستگاه های محدود به منابع
Mell et al. (Mell et al., ۱۹۰۶)	طرح	یک سیستم مدیریت هویت فدرال که کاربران را قادر می سازد تا احراز	محدوده در دسترس باریک (مناسب برای یک سازمان بزرگ)	احراز هویت فقط از طریق ارتباط RP توسط کاربر بدون اشخاص ثالث

		هویت RP و انتقال اموال را مستقیماً بدون دخالت اشخاص ثالث انجام دهند.		است، بدون نیاز به حفظ زیرساخت کلید عمومی
Li et al. (Li et al., ۲۰۱۸b)	شبیه سازی	طرح احراز هویت عضو رمزگذاری شده برای پشتیبانی از سیستم مدیریت هویت مبتنی بر بلاک چین	درخواست کنندگان ممکن است برای فریب سایر کاربران با دریافت چندین گواهی از یک گره مورد استفاده قرار گیرند	موثرتر در توانایی افزودن یا حذف پویا گره ها و لبه ها، نشان دادن امنیت TCUGA پیشنهادی در مدل استاندارد و ارزیابی عملکرد آن برای نشان دادن امکان سنجی آن در برابر BIMS

۷- چالش های مرتبط با هویت

این خطر بالقوه وجود دارد که اطلاعات هویتی که در کنار کاربر نگهداری می شود در معرض خطر و بهره برداری قرار گیرد. به عنوان مثال می توان به موارد زیر اشاره کرد:

- هویت "کیف پول" نشت. اگر «کیف پول» هویت با موفقیت به خطر بیفتد، ممکن است اطلاعات به بیرون درز کند یا اطلاعات مفیدی در مورد کاربر به دست آید. در نتیجه، چنین اطلاعات لو رفته می تواند برای تسهیل سایر فعالیت های شرور استفاده شود.

- تغییر هویت. در واقع هویت کاربر دائمی نیست و قابل تغییر است. ارائه‌دهندگان هویت سنتی و متمرکز می‌توانند وضعیت هویت را به موقع لغو یا تمدید کنند، برای مثال در هنگام تبلیغات یا تعلیق گواهینامه رانندگی. با این حال، در سیستم هویت مبتنی بر بلاک چین، به دلیل تداوم بلاک چین و SSI، هرگونه تغییر در اطلاعات هویت کاربر مستلزم مشارکت کاربر است. از این رو، انجام تغییر هویت می تواند چالش برانگیز باشد(۴).

۸- پیامدهای هزینه

همچنین پیامدهای هزینه ای مرتبط با راه حل های مبتنی بر بلاک چین وجود دارد.

زیر ساخت. SSI نسبتا جدید است و ممکن است به راحتی توسط سیستم های IDM موجود و زیرساخت های پشتیبانی کننده آنها پشتیبانی نشود. از این رو، پیامدهای هزینه ای مرتبط با ارتقاء زیرساخت وجود خواهد داشت. به عنوان مثال، رمزهای عبور کاربر باید با گواهی ها جایگزین شوند و وابستگی های مکانیزم احراز هویت در ارائه دهنده خدمات باید بهبود یابد. واضح است که ارتقاء تجهیزات و روش ها تنها بخشی از هزینه است. سایر هزینه ها شامل آموزش کارکنان و نگهداری تجهیزات می باشد. برای به حداقل رساندن هزینه ها، ارتقاء زیرساخت ها می تواند تدریجی باشد(۱۵).

مدیریت کلیدی. در سیستم مبتنی بر بیت کوین، از دست دادن کلید خصوصی منجر به از دست رفتن دارایی مرتبط (به عنوان مثال بیت کوین) می شود. بر خلاف یک سیستم مبتنی بر رمز عبور، مکانیزمی برای بازنشانی رمز عبور فراموش شده وجود ندارد. از این رو، یک رویکرد قابل دوام، ادغام چنین ویژگی بازنشانی یا برون سپاری مدیریت کلید به یک شخص ثالث

است. با این حال، مدیریت انتقال کلید خصوصی با مفهوم SSI در تضاد است. برای پشتیبانی از SSI، پیامدهای هزینه نگهداری قابل توجهی وجود دارد (۱۵).

ما همچنین می‌توانیم از مدیریت کلید چند حزبی، مانند مدیریت کلید (۶) استفاده کنیم.

جدول کلمات مخفف

کلمه	معادل فارسی
SSI	هویت خودمختار
IDM	مدیریت هویت
IAM	مدیریت هویت و دسترسی
IMA	مدیریت هویت مستقل
P۲P	فناوری همتا به همتا
uPort	سیستم هویت خودمختار

۹- نتیجه گیری

در این مقاله، بررسی عمیقی از سیستم‌های مدیریت هویت مبتنی بر بلاک چین ارائه کردیم. به عنوان بخشی از بررسی، تعدادی از چالش‌ها را شناسایی کردیم، مانند چالش‌های مربوط به ذخیره‌سازی داده‌های بلوک. به عنوان مثال، نیاز کاربر به فضای ذخیره سازی با افزایش تعداد کاربران و خدمات مشترک افزایش می یابد.

از این رو، چگونه یک مکانیسم مقیاس پذیر طراحی کنیم که قابلیت ذخیره سازی متفاوت کاربران مختلف را نیز در نظر بگیرد؟ چالش دیگر مربوط به طبقه بندی عدم مجوز در بلاک چین است. برخی از گره ها می توانند در حسابداری شرکت کنند در حالی که برخی دیگر فقط می توانند داده های بلوک را مشاهده کنند. به دلیل وجود هویت گره، این به طور بالقوه می تواند منجر به تقسیم مرزی زنجیره شود. سیستم های IDM مبتنی بر بلاک چین بر تعدادی از محدودیت های ذاتی سیستم های IDM معمولی غلبه می کنند. چنین سیستم های مبتنی بر بلاک چین را می توان به عنوان یک انقلاب هویت توصیف کرد. به عنوان مثال، کاربر مالک هویت می شود و نیازی نیست که کاربران ایمنی را فدای راحتی کنند. علاوه بر این، یکی از توسعه‌های بالقوه آینده، اتخاذ برخی از عوامل منحصربه‌فرد در واقعیت به‌عنوان شواهدی برای بازنشانی حساب است.

منابع

۱. "Aggarwal, S., Chaudhary, R., Aujla, G.S., Kumar, N., Choo, K.-K.R., Zomaya, A.Y., ۲۰۱۹. Blockchain for smart communities: applications, challenges and opportunities. J. Netw. Comput. Appl. ۱۴۴, ۱۳–۴۸.".

۲. "Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H,.Pervez, Z., Dahal, K., Dns-idm, ۲۰۱۹. A blockchain identity management system to secure personal data sharing in a network. Appl. Sci. ۹ (۱۵), ۲۹۵۳.".

۳. "Baars, D., ۲۰۱۶. Towards Self-Sovereign Identity Using Blockchain Technology, Master's Thesis. University of Twente.".

٤. "Dhamija, R., Dusseault, L., ۲۰۱۸. The seven flaws of identity management: usability and security challenges. IEEE Secur. Priv. ۶ (۲), ۲۴–۲۹.".

٥. "Dunphy, P., Petitcolas, F.A.P., ۲۰۱۸. A first look at identity management schemes on the blockchain. IEEE Secur. Priv. ۱۶ (۴), ۲۰–۲۹.".

٦. "Faber, B., Michelet, G.C., Weidmann, N., Mukkamala, R.R., Vatrapu, R., ۲۰۱۹. Bpdims: a blockchain-based personal data and identity management system. In: Proceedings of the ۵۲nd Hawaii International Conference on System Sciences.".

V. "Feng, Q., He, D., Zeadally, S., Khan, MK., Kumar, N., ۲۰۱۹. A survey on privacy protection in blockchain system J. Netw Comput. Appl. ۱۲۶, ۴۵–۵۸.".

۸. "Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L., Shi ,W, ۲۰۱۸. Blockchain-based identity management with mobile device. In: Proceedings of the ۱st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. ACM, pp. ۶۶–۷۰.".

۹. "Jindal, A., Aujla, G.S., Kumar, N., ۲۰۱۹. Survivor: a blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment. Comput. Network. ۱۵۳, ۳۶–۴۸.".

۱۰. "Lesavre, L., Varin, P., Mell, P., Davidson, M, Shook, J., ۲۰۱۹. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (Draft). Tech. rep.. National Institute of Standards and Technology.".

۱۱."Lim, S.Y., Fotsing, P.T., Almasri, A., Musa, O., Kiah, M.L.M., Ang, T.F., Ismail, R., ۲۰۱۸. Blockchain technology the identity management and authentication service disruptor: a survey. Int. J. Adv. Sci. Eng. Inf. Technol. ۸ (۴۲), ۱۷۳۵–۱۷۴۵.".

۱۲."Lin, C., He, D., Huang, X., Choo, K.K.R., Vasilakos, A.V., ۲۰۱۸. Bsein: a blockchain-based secure mutual authentication with fine-grained access control systemfor industry ۴,۰. J. Netw. Comput. Appl. ۱۱۶ (۱), ۴۲–۵۲.".

۱۳."Lin, C., He, D., Huang, X., Khan, M.K., Choo, K.-K.R., ۲۰۱۸. A newtransitively closed undirected graph authentication scheme for blockchain-based identity management systems. IEEE Access ۶, ۲۸".۲۸۲۱۲–۲۰۳

۱٤."Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M,(۲۰۱۷) Uport: a platformfor self-sovereign identity.".

۱۵."M Goodner, A. Nadalin, Web Services Federation Language (Ws-federation) Version ۱,۲, OASIS Web Services Federation (WSFED) TC.".

۱٦."Martinez, L.V., Ting-Toomey, S., Dorjee, T., ۲۰۱۶. Identity management and relational culture in interfaith marital communication in a United States context: a qualitative study. J. Intercult. Commun. Res. ۴۵ (۶), ۱–۲۳.".

۱۷."Mell, P., Dray ,J., Shook, J., (۲۰۲۰). Smart contract federated identity management without third party authentication services. arXiv preprint ۱۹۰٦,۱۱۰۵۷.".

۱۸."Mell, P., Dray, J., Shook, J., Smart contract federated identity management without third party authentication services. arXiv preprint ۱۹۰۶,۱۱۰۵۷.".

۱۹."Mohamad, B., Bakar, H.A., Ismail, A.R., Halim, H., Bidin, R., ۲۰۱۶. Corporate identity management (cim) in malaysian higher education sector: developing a conceptual model. Int. Rev. Manag. Market. ۶ (۷S), ۱۷۵–۱۸.".۰

۲۰."Ren, Y., Zhu, F., Qi, J., Wang, J., Sangaiah, A.K., ۲۰۱۹. Identity management and access control based on blockchain under edge computing for the industrial internet of things. Appl. Sci. ۹ (۱۰), ۲۰۵۸.".

۲۱."S. Kikitamara, M van Eekelen, D. I. J.-P. (۲۰۱۸). Doomernik, Digital Identity Management on Blockchain for Open Model Energy System, Unpublished Masters thesis Information Science.".

۲۲."S. Kikitamara, M van Eekelen, D. I. J.-P. Doomernik, Digital Identity Management on Blockchain for Open Model Energy System, Unpublished Masters thesis Information Science.".

۲۳."V. K. Madisetti, A. Bahga, Method and System for Identity and Access Management for Blockchain Interoperability, uS Patent App. ۱۵/۸۳۰,۰۹۹ (Oct. ۴ ۲۰۱۸).".