سیستم خدمات آرشیو شخصی با استفاده از تکنولوژی بلاک چین: مطالعه موردی، نوید بخش و چالش برانگیز

چکیده

این مقاله برای کاوش کاربردهای تکنولوژی بلاک‌چین تا مفهوم «اثبات X»، همانند اثبات هویت، اثبات مالکیت اموال، اثبات معامله خاص، اثبات درجه علمی، اثبات رکوردهای پزشکی، اثبات موفقیت‌های دانشگاهی و غیره می-باشد. این مقاله رویکرد نوین ایجاد یک سیستم خدمات و مدیریت آرشیو شخصی تغییرناپذیر، شفاف، غیرمتمرکز و ایمن را توصیف می‌کند. آرشیو شخصی به عنوان کلکسیونی از مصنوعات متعدد تعریف شده است که نمونه‌کارهای شخصی و نیز هویتهای منحصر به فرد شخصی را منعکس می‌کند. نمونه‌کارهای شخصی فراتر بیان موفقیت شخصی می‌باشد. این (نمونه‌کارها) یک سند مستند طراحی شده برای ارائه اسناد و مثالهای کیفی و کمی می‌باشد. موضوعات می‌توانند اطلاعات خود را با اثبات تگ کنند به طوری که توسط نهادها یا سازمانهای مورد اعتماد همانند دانشگاهها مورد تائید قرار گیرند. چنین اثباتهایی همراه با سطوح محرمانگی می‌باشند که در حوزه‌های عمومی به نمایش در آمدند. هویتهای شخصی شامل بیومتریکها و نیز دیگر چند فاکتوریها همانند چیزی که فاعل «دارای» آن می‌باشد، فاعل آن را «می‌داند» یا فاعل به آن «عمل» می‌کند. ذینغعان در یک کنسرسیوم با رویکرد شبکه بلاک‌چین به عنوان تصدیق کنندگان و یا ماینرهایی عمل می‌کنند که به خدمات مورد اعتماد آنها اجماع توزیع شده ارائه می‌کنند. چنین سیستم مبتنی بر آرشیو شخصی می‌تواند تا اپلیکیشنهای متعدد از جمله شبکه‌های حرفه‌ای همانند لینکدین، تائید اعتبار آنی همانند alipay یا انسان زنده از باتهای اجتماعی همانند رسانه اجتماعی اینترنت بسط داده شود. شبیه-

سازی نمونه الگو (پروتوتایپ) نشان می‌دهد که مدیریت چنین نمونه‌کارهای شخصی و سیستم خدمات ممکن بوده و در برابر حملات ID بسیاری مصون می‌باشد.

واژگان کلیدی: سیستم خدمات آرشیو شخصی، نمونه‌کارهای دیجیتال، شناسایی (هویت)، بلاک‌چین، کنسرسیوم بلاک‌چین، کلید عمومی و خصوصی، ناشناسی، شفاف، غیرمتمرکز.

1-مقدمه

سیستم خدمات آرشیو شخصی (PASS) به عنوان کلکسیونی از مصنوعات دیجیتالی و نیز کلکسیونی از ابزارهای خدماتی تعریف شده است. مصنوعات دیجیتالی شخصی (PDA) یک شکل دیجیتال از دستاوردهای شخصی با اسناد مستند (PAE) یا هویتهای شخصی (PID) می‌باشد می‌تواند برای شناسایی منحصر به فرد یک شخص استفاده شود. مثالهایی از PAE عبارتند از آموزش شخصی، تجربیات، درجه (مدرک)، آموزش و یادگیری، دیپلم، نسخه‌های دانشگاهی (آکادمیک) و گواهی‌های متعدد. ثروت شخصی همانند ارزش دارایی، موجودی بانکی و سرمایه-گذاریها نیز می‌توانند مثالهای یاز PAE باشند. مثالهای معمول PID عبارتند از سنجشهای بیومتریک از شخص (فرد) همانند اثرات انگشت، عنبیه و رگ. اطلاعات دیگری که تنها شخص از آنها آگاه می‌باشد، اشیاء فیزیکی که شخص مالک آنها می‌باشد، می‌توانند مثالهایی از PID باشند. الگوهای رفتاری، بازتاب شخصی و خصوصیات نیز به عنوان مثالهایی از PID در نظر گرفته شدند.

کلکسیونی از PAEها مشابه با نمونه‌کارهای شخصی (PP) می‌باشند. این همراه با جدول زمانی می‌باشد که خصوصیات مخصوص یک شخص را شکل می‌دهند. PP یک شکل متمایزی از رزومه می‌باشد که بسیار انحصاری و جامع‌تر نسبت یک بیانات در رزومه است.

برای اینکه مفید و مورد اعتماد باشند، PDAها نیاز دارند تا توسط یک شخص ثالث مورد تائید قرار گیرند کسی که باید دانش این مصنوعات ادعا شده را راهنمایی کند. برای مثال، دانشگاه می‌تواند نسخه‌های (متون) رسمی به فارغ-التحصیلان خود ارائه کند. مالک یک زمین قادر به ارائه یک نامه مرجع به مستاجرین خود ارائه کند. هیچ نهاد دیگری نمی‌تواند این را انجام دهد.

نقش‌های متعددی را در این فرآیند تعریف کردیم. از عبارت «فاعل» به عنوان شخص یا کاربری استفاده می‌کنیم که در حال ایجاد کلکسیون PDAهای خود می‌باشد، «گواهی دهنده» یا «مرجع صدور گواهی» موسسه یا نهادی که گواهی ارائه می‌کند، «مفتش » آژانس یا سازمانی می‌باشد که خدمات بررسی و جمع‌آوری ادله‌های مرتبط با هرگونه موضوعات خاص را عهده‌دار می‌باشد و «کلاینت» یا «مشتری» شخص یا سازمانی می‌باشد که از خدمات حرفه‌ای ارائه شده توسط «مفتش » استفاده می‌کند. برای مثال، برای استخدام یک کاندید بالقوه توسط یک کمپانی، کاندید فاعل می‌باشد، کمپانی مشتری می‌باشد که نیازمند استخدام یک شخص ثالث برای اعتبارسنجی تمام اطلاعات ارائه شده توسط فاعل است. این شخص ثالث مفتش بوده و کمپانی مشتری مفتش می‌باشد. مفتش نیاز دارد تا با مراجع صدور گواهی متعدد همانند دانشگاهها تماس حاصل کند کسی که آموزش را ارتقاء می‌دهد، کمپانی‌هایی که برای کار استفاده شدند یا سازمانهایی که گواهی‌های دیگری صادر می‌کنند.

این فرآیند اعتبارسنجی PDAها از سوی مفتش (یا بازپرس) اغلب زمانبر می‌باشد. همچنین این فرآیند هر بار که مشتری درخواست ارائه می‌کند، تکرار می‌شود. در برخی موارد، این فرآیند اطلاعات فراتر از رضایت ارائه شده توسط فاعل فراهم می‌کند. بنابراین، حاوی تهدید حریم خصوصی می‌باشد. به علاوه، این فرآیند اساسا یک مدلی از سیستم متمرکز می‌باشد که می‌تواند به طور بالقوه مسبب یک نقطه شکست، یک نقطه تنگنا، یک نقطه سردرگمی و نقطه سوء استفاده شود. برای مثال، اجازه آموزش در هنگام استخدام یک یار کمکی (وردست) توسط شخص ثالث زمان‌بر می‌باشد. در برخی موارد حدی، تجربه کردیم که ترم شروع شده است در حالیکه این اجازه هنوز در حالت تعلیق می‌باشد. مثال دیگر درباره نام تغییر داده شده توسط فاعل می‌باشد. بدون آشکارسازی نام قبلی آن، تائید فاعل سخت می‌باشد. موردی را می‌بینیم که فاعل از یک موسسه می‌خواهد تا دیپلم جدید به دلیل تغییرنام صادر کند. این معمولا یک ماموریت غیرمحتمل می‌باشد اگرچه در این مورد فاعل تمام دیگر IDها را دارا می‌باشد که به همان شکل باقی می‌مانند و تنها نام متفاوت می‌باشد.

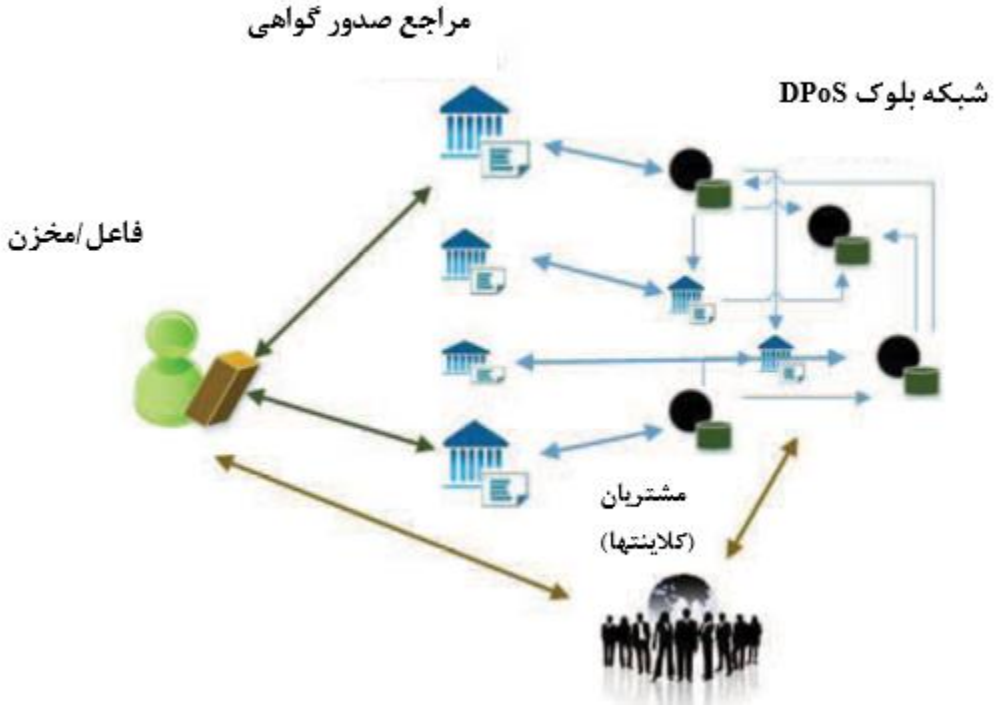
اما، فرآیند اعتبارسنجی (تائید) بسیار ضروری می‌باشد و باید انجام شود. مشاهده می‌کنیم که پدینگ رزومه بسیار فراگیر شده است [1]. پدینگ رزومه افزودن اطلاعات غلط یا اغراق‌شده به رزومه جهت ارتقاء شانس برای یک شغل

می‌باشد. بیش از 40 درصد رزومه‌ها حقوق خود را افزایش می‌دهند، 33 درصد توصیف ناصحیح از شغل دارند، 29 درصد تاریخ‌های اشتغال را تغییر می‌دهند، 27 درصد رفرنسها را جعل می‌کنند و 21 درصد مدارک را جعل می‌کنند. از این رو، می‌توانیم تصور کنیم که مسئولیت الزام تائید اعتبار بسیار سنگین می‌باشد.

اخیرا، تکنولوژی بلاک‌چین که در ابتدا در بیت کوین [20] به عنوان یک شبکه پرداخت نوآورانه و نوع جدید از پول معرفی شد، در صنایع مرتبط با امور مالی مورد استفاده قرار گرفته است. زمینه‌های دیگر بسیاری همانند زنجیره تامین، تولید و اینترنت اشیاء نیز در حال استفاده از آن می‌باشند. [برای مثال مراجع 21 و 22]. خصوصیات کلیدی از استفاده از تکنولوژی بلاک‌چین عبارتند از غیرمتمرکز بودن، سرفصل مشترک مبتنی بر اجماع، قرارداد هوشمند، شفافیت بالا و حریم خصوصی قوی. ایده ذخیره و انتقال ایمن اسناد امضاء شده به صورت دیجیتال با یک دنباله ممیزی فوق‌العاده در شبکه های تبادل سند تغییرناپذیر در تجارت مالی، حمل و نقل و بیمه در حال ظهور می‌باشد جایی که هرکس دارای تقاضای مشابه برای اعتبارسنجی هویت افراد و دارایی‌ها می‌باشد. این نیازمند شخص ثالث به عنوان یک میانجی (واسطه) یا نهاد برای اعتبارسنجی، تمیز کردن خانه یا هر هدف دیگر نمی‌باشد. این در ایجاد یک سرویس ID تغییرناپذیر ناشناس ایمن و هنوز شفاف مورد استفاده قرار می‌گیرد [33].

سیستم خدمات آرشیو شخصی (PASS) پیشنهادی در این مقاله برای استفاده از تکنولوژی بلاک‌چین جهت بکارگیری خصوصیات مطلوب آن همانند تغییرناپذیری، شفافیت، ناشناسی و اجماع عمومی می‌باشد. فاعل PDAهای خود را کنترل می‌کند و تصمیم می‌گیرد که این PDAها در اختیار چه کسی قرار دهد. شکل1 زیرساختار عمومی (کلی) و نمای معماری یک PASS تحت بلاک‌چین را نشان می‌دهد. فاعل، که به وسیله یک آیکون نشان داده شده است، مخزن خود را دارد که تمام PDAهای مربوطه خود جمع‌آوری می‌کند. گواهی دهنده‌ها گواهی‌ها را به صاحبان آنها و نیز به شبکه مورد اعتماد صادر می‌کنند. چنین گواهی‌هایی فقط یکبار برای تمام افراد درگیر صادر می‌شوند و دیگر نباید صادر شوند. هیچ نیازی برای حضور شخص ثالث یا مفتش وجود ندارد. آنها (مراجع صدور گواهی) همچنین گواهی‌ها را به شبکه بلاک چین با گرایش کنسرسیوم ارائه می‌کنند که اعتماد در آن

به صورت اجماع نظر حاصل شده است. مشتری از فاعل درخواست می‌کند و به PDAهای اعطا شده دسترسی پیدا می‌کند.



شکل1: معماری PASS

اهداف اصلی ما پیشنهاد یک چارچوب استفاده از تکنولوژی بلاک چین برای ایجاد یک آرشیو شخصی می‌باشد که همراه با گواهی است. این آرشیو هویت، دقت و شفافیت را حفظ می‌کند در حالیکه از حریم خصوصی محافظت می‌کند. مفتشان دیگر موردنیاز نیستند. فاعل می‌تواند تصمیم بگیرد که چه چیزی را در اختیار چه کسانی و در چه هنگامی براساس ماهست درخواست قرار دهد. وقتی که یک درخواست بیشتر از یک دستاورد دانشگاهی می‌باشد، هرگونه PDAهای همراه با چنین تگ (برچسب)، می‌توانند قفل‌شکنی شده و در دسترس قرار گیرند. وقتی که یک درخواست در ارتباط شناسایی هویت باشد، فاعل میتواند PDAهایی همانند بیومتریکها را قفل‌شکنی کند. مشتری میتواند به PDAها سریعا دسترسی پیدا کند و بر این اساس تصمیم‌گیری نماید. به علاوه، ابزارها و خدمات ارائه شده توسط PASS می‌توانند هرگونه پروژه مرتبط با رشد شخصی و جدول زمانی را بسیار آسانتر سازند.

بخش زیر آخرین توسعه مفهوم «اثبات X» را با استفاده تکنولوژی بلاک‌چین مرور می‌کند جایی که X می‌تواند هر چیزی همانند هویت، مالکیت دارایی، معامله خاص، درجه دانشگاهی، اطلاعات پزشکی و دستاوردهای آکادمیک باشد. بخش بعد PASS را بحث خواهد کرد، یک سیستم خدمات آرشیو شخصی که بر اساس آن فاعل می‌تواند آرشیوهای شخصی به طور زمان‌مند و دقیق ایجاد کند. آنها به گونه‌ای گواهی داده شدند که نیازمند اعتبارسنجی در هر بار استفاده نمی‌باشند. PASS فراگیر می‌باشد در حالیکه حریم خصوصی را حفظ می‌کند. آخرین بخش به بحث درباره شانس، چالشها و کاربردهای آینده اختصاص داده شده است.

2- مرور منابع و مراجع

مسائل اصلی ایجاد مصنوعات دیجیتال شخصی (PDAها) عبارتند از فرآیند اعتبارسنجی و قابلیت اعتماد. همانطور به لحاظ آماری در بخش1 نشان داده شد، بیش از 30 درصد کارجویان اطلاعات دیپلم خود را تغییر می‌دهند. 70 درصد در دستاورد خود اغراق می‌کنند [1].

تلاشهای متعدد برای ایجاد اعتبار و گواهی در کنار موفقیت دانشگاهی انجام شدند. ایده Open Badge یکی از آنها می‌باشد. گروه کاری استاندارد برای Open Badgeها همانطور که در وبسایت آن عنوان شده است [2]، مهارتها و دستاوردها را به وسیله ارائه نمادهای بصری همراه با داده‌های قابل تائید و شواهدی که می‌توانند در وب به اشتراک گذاشته شوند، مبادله می‌کنند. Open Badgeها فاعل را برای مدیریت دستاوردهای یادگیری آنها توانمند می‌سازد. هدف این گروه کاری استانداردسازی بیشتر ملاحظات می‌باشد که انطباق با آنها، حفاظت از آنها و ایجاد آنها بسیار واضح‌تر و آسانتر می‌باشد. آکلیم[1] [3] پلتفرم نشان‌گذاری دیجیتال براساس استاندارد Open Badge بوده و توسط پیرسون[2] ارائه شده است. آکلیم میلیونها امضاء از سازمانهای مشهور همانند IBM برای دستاوردهای پیشرفت شغلی صادر کرده است که به حرفه‌ای شدن افراد کمک می‌کند. یک امضاء صادر شده از طریق آکلیم یک بازنمایی دیجیتال از نتیجه یادگیریف تجربه یا رقابت می‌باشد. این امضاها میتوانند به صورت آنلاین در یک شیوه‌ای که آسان و ایمن می‌باشد، به اشتراک گذاشته شده و تائید شوند. آنها محتوی اطلاعات دقیق می‌باشند که متون مرتبط درباره چیزی

[1] Acclaim
[2] Pearson

دقیقا حاصل شده است، فراهم می‌کنند که کدام سازمان دستاورد را شناسایی می‌کند و چه فردی این شناسایی را به دست اورده است. خدمات ارائه شده شایستگی‌های مربوط به خود را دارا می‌باشندو نقص اصلی مدل متمرکز آن می-باشد.

آموزش جهانی سونی اعلام می‌کند که تکنولوژی را با استفاده از بلاک‌چین برای اشتراک آزاد مهارت دانشگاهی و رکوردهای پیشرفته در سال 2016 توسعه خواهد داد [4]. آنها هدف استفاده از خصوصیات ایمن بلاک چین برای تحقق انتقال رمزگذاری شده داده‌ها همانند اطلاعات مهارتی دانشگاهی فرد و سنجشهای پیشرفت بین دو نهاد معین دارند. جریان کار حقیقی هنوز در حال مشاهده می‌باشد و نیازمند آزمایش است.

سیستم ID یک مسئله طولانی مدت می‌باشد. W3 هفت الزام عمومی برای خدمات مدیریت هویت جهانی شناسایی می‌کند [9]: قابلیت حمل و قابلیت همکاری، قابلیت بسط و توسعه، حریم خصوصی و امنیت مذاکره شده، مسئولیت-پذیری، قدرت ثبت توزیع شده، قدرت گواهی توزیع شده و قدرت مدیریت مستقل. چنین سرویسی باید از شناساگرهای منحصر به فرد جهانی در یک فرمت تبادل مشترک استفاده کنند، نگاشت قابل بسط برای این شناساگرها از دیگر شناساگرهای استفاده شده معمول و از یک پروتکل مشترک برای اثبات و احراز هویت یک هویت جهانی استفاده کنند. این باید تعریف واژگان جهانی و نیز تعریف واژگان محلی توزیع شده را پشتیبانی کند. این نیازمند پشتیبانی ناشناسی و نام مستعار برای حفاظت حریم خصوصی می باشد. بنابراین، ناشناسی و ناشناسی دروغین (نام مستعار) برای حفاظت حریم خصوصی تحت صلاحیت حریم خصوصی و امنیت می‌باشد.

سیستم ID باید هردوی مدلهای ثبت سلسله مراتبی و همتا به همتا (یا نظیر به نظیر) را پشتیبانی کند. نهاد مدریت کننده باید به صورت یک سازمان ناسودآور بین‌المللی تعیین شود بنابراین در تمام جوانب به لحاظ دولتی، صنعتی و فروش بی‌طرف می‌باشد. این سازمان باید هردوی استانداردهای فنی و عملیاتی برای خدمات را برآورده کند از آنجایی که این دو مورد به طور نزدیکی آمیخته به یکدیگر می‌باشند. این سازمان باید توسعه واژه جهانی برای ویژگیهای هویت عمومی و ساختارهای کنترل پروتکل جهانی را مدیریت کند. این سازمان باید قوانین مسئولیت‌پذیری را برای

تمام عوامل از جمله نهادهای ثبت و صدور گواهی برآورده کند. این سازمان باید به عنوان یک نهاد بنیادی غیرنسبی برای ثبت سلسله مراتبی یا مدلهای صدور گواهی عمل کند.

OpenID با اتصال OpenID [6 تا 11] برای تعریف و توسعه یک استاندارد باز و پروتکل احراز هویت غیرمتمرکز می‌باشد. این مورد نهادهای متکی (RP) برای اعتبارسنجی هویت کاربر نهایی براساس احراز هویت انجام شده توسط ارائه کننده OpenID (OP) یا سرور احراز هویت و نیز برای دستیابی به اطلاعات پروفیال بنیادین درباره کاربر نهایی در یک شیوه متقابل و همانند REST توانمند می‌سازد. با انجام احراز هویت کاربران از طریق یک سرویس شخص ثالث، این مورد نیاز برای وب‌مسترها جهت ارائه سیستم‌های ادهاک خود آنها و هویت و پسورد مجزا حذف می‌کند.

در حالیکه OAuth سرویس احراز هویت شخص ثالث را توانمند می‌سازد، هنوز از نظر ارائه کننده OpenID متمرکز می‌باشد. و کاربران باید اطلاعات خصوصی بسیاری را در دسترس قرار دهند تا احراز هویت شوند. این همچنین دارای یک نقطه شکست مجزا می‌باشد. به علاوه، این همچنین برخلاف ماهیت اینترنت می‌باشد که نهاد مرکزی مجزا می‌باشد که کنترل را انجام می‌دهد، چه کسی میتواند چه چیزی را انجام دهد.

اطلاعات خاص بیومتریک متعدد میتوانند برای شناسایی انسان با دقت بسیار بالا استفاده شوند [8، 32، 33]. این به خصوص در اپلیکیشنهای رسانه اجتماعی مفید می‌باشد که در آن کاربر میتواند ناشناس باشد اما نیاز است تا به صورت یک انسان حقیقی به جای یک دسته از باتهای اجتماعی استامپ (برچسب) شود. بنابراین، نتایج همانند احساسات یا نظرسنجی از اپلیکیشن رسانه اجتماعی میتوانند شرایط حقیقی را بیان کنند و توسط باتهای اجتماعی دچار سردرگمی نشوند.

برخی اپلیکیشنهای وب همانند taskstream (جریان مسئولیت) یک پلتفرمی را برای کاربر جهت ایجاد نمونه‌های شخصی فراهم می‌کنند. این میتواند پیشرفت در پروژه‌های خاص را ردیابی کند و بازتاب موضوعات خاص را ثبت کند. این اپلیکیشنها میتوانند به عنوان یک شیوه‌ای برای نشان دادن اثر رشد شخصی عمل کنند که میتواند منشاء مهارتهای خاص را فراهم کند.

در مرجع [35]، مولف ایده‌هایی از استفاده از بلاک چین جهت اثبات هویتها در جهان دیجیتال بدون دیتابیس متمرکز پیشنهاد می‌کند که منجر به انحصار طبیعی می‌شود که هرکسی ملزم به استفاده می‌باشد. در حالیکه یک سیستم غیرمتمرکز پیرو یک پروتکل رایج می‌باشد که به افراد اجازه می‌دهد تا نسخه‌های جدید اضافه کنند و آنها با استفاده از معماری نظیر به نظیر با دنباله حسابرسی فوق‌العاده توزیع کنند. فاعل می‌تواند استفاده کلیدی کنترل شده به مشتریان همانند بانکها، مراکز بیمه یا دولتها ارائه کند کسانی که میخواهند اسناد راب ا قراردادهای هوشمند بازرسی کنند. یک قرار داد هوشمند یک قطعه کد ثبت شده در بلوکهای مشترک می‌باشد. این قرارداد میتواند تعداد یا زمانبندی تفتیش را محدود کند و تمام آنها را برای فاعل ثبت کند.

3- ساختار PASS

A-مصنوعات، نمونه‌کارها و آرشیو

یک PDA یک قطعه‌ای از سند دیجیتال امضاء شده می‌باشد که حاوی تگها یا فیلدهای زیر می‌باشد:

- PDA-ID: شاخص ایجاد شده توسط سیستم
- PDA-Type: دستاوردهای شخصی با اسناد مستند (PAE) یا هویت‌های شخصی (PID). این پیرو تیپ (نوع) فرعی همانند دیپلم، مدرک (درجه)، مهارتها و سنجش بیومتریک می‌باشد. آنها باید در نهایت کدهای استاندارد شده باشند.
- PDA-Description: یک رشته برای توصیف ماهیت PDA.
- PDA-Subject: نام شخصی که مالک PDA می‌باشد.
- PDA-Certifier: شخص یا سازمانی که گواهی برای این PDA صادر می‌کند.
- PDA-Date-Start: تاریخ شروع PDA.
- PDA-Date-End: تاریخ تکمیل PDA.
- PDA-Date-Validation: تاریخ اختیاری که PDA معتبر می‌باشد.
- PDA-Comment: فیلد اختیاری

- PDA-Key-Cert: کلید عمومی همراه با مرجع صدور گواهی.
- PDA-Key-Sub: کلید عمومی ایجاد شده برای فاعل و این PDA خاص. کلید خصوصی توسط فاعل در اپلیکیشن خود نگهداری می‌شود.
- PDA-Unique: برای اعتبارسنجی مالکیت این PDA توسط مرجع صدور گواهی استفاده شده است. تاریخ تولد، ID دانش آموز یا ID جهانی و یا چیزی که تنها برای فاعل شناخته شده می‌باشد. این میتواند فیلدهای متعدد موردنیاز توسط مرجع صدور گواهی باشد.
- PDA-Data: داده‌های موردنیاز توسط مرجع صدور گواهی. برای تیپ PDA، این میتواند اطلاعات بیومتریک خاص باشد. برای PAE، این میتواند یک اسکن از گواهی اصلی (نسخه قابل چاپ) باشد.

نمونه‌کار شخصی (PP) یک کلکسیونی از PDAها می‌باشد که تیپ PDA آنها تحت PAE می‌باشد. هویتهای شخصی (PID) یک کلکسیونی از PDAها می‌باشد که تیپ PDA آنها تحت PID می‌باشد. بنابراین، PA یک PP و PID یکپارچه می‌باشد. به لحاظ نمادی،

$$PA = \{P_p, P_{id}\},$$

جایی که

$$P_p = \{PDA_{PAE1}, PDA_{PAE2}, \cdots, PDA_{PEAn}\}$$

و

$$P_{id} = \{PDA_{PID1}, PDA_{PID2}, \cdots, PDA_{PIDm}\}.$$

.

B- ابزارهای سرویس

ابزار سرویس قطعه‌ای از کد می‌باشد که مسئولیت خاص موردنیاز توسط PP را اجرا می‌کند. این باید شامل فیلدهای زیر باشد:

- ST-ID: شاخص ایجاد شده توسط سیستم.
- ST-Type: ماهیت سرویس همانند مفتش ، مدیر یا غیره.
- ST-Description: یک رشته برای توصیف ماهیت سرویس
- ST-Input: شرایط و پارامترهای سرویس.
- ST-Output: نتایج سرویس
- ST-Codition: تحت چه شرایط و یا امتیازی سرویس باید اجرا شود.
- ST-Creator: شخص یا سازمانی که ابزار را صادر می‌کند.
- ST-Date: تاریخ سرویس در محل
- ST-Comment: فیلد اختیاری
- ST-Language: زبان خاص که ابزار را اجرا می‌کند.

یک کلکسیونی از ابزارهای سرویس به صورت T بیان شدند. این یک تنوعی از سرویسهای موردنیاز برای کارآمدسازی PA را پوشش می‌دهد. برای مثال، درخواست برای گواهی، جمع‌آوری و همگام‌سازی PP در مخزن محلی (موضعی) از سربرگ عمومی، اعطا مجوز به یک نهاد خاص جهت بازرسی PDA. دوباره، میتوانیم از فرمول زیر برای نمایش مجموعه ابزارها استفاده کنیم.

$$T = \{ST_1, ST_2, \cdots, ST_n\}.$$

از این رو، PASS میتواند به صورت زیر نمادگذاری شود:

$$PASS = \{PA, T\}$$

C- فاعل، مفتش ، مرجع صدور گواهی، مشتری، استیک

این مقاله از عبارات زیر برای توصیف یک سیستم همتا به همتای توزیع شده مبتنی بر بلاک چین استفاده می‌کند:

- عبارت «فاعل» شخصی می‌باشد که درباره PDAهای او بحث می‌شود.

- عبارت «مرجع صدور گواهی» یک موسسه یا نهادی می‌باشد که گواهی ارائه می‌کند.
- عبارت «مفتش » آژانس یا سازمانی می‌باشد که به ادله‌های مرتبط دست پیدا می‌کند.
- عبارت «مشتری» شخص یا سازمانی می‌باشد که از سرویسهای حرفه‌ای (توسط «مفتش ») استفاده می‌کند.
- عبارت «stake node» یک گره مخصوص در یک شبکه بلاک چین با گرایش کنسیرسیوم می‌باشد. اعتماد در یک شیوه اجماع کل توسعه داده شده است. این همانند «کاوش و اعتبارسنجی» در یک شبکه بیت کوین می‌باشد.

برای مثال، برای اینکه یک کاندید بالقوه که توسط یک کمپانی استخدام شود، کاندید فاعل بوده و کمپانی نیازمند استخدام یک شخص ثالث جهت تائید تمام اطلاعات ارائه شده توسط فاعل می‌باشد. شخص ثالث مفتش بوده و کمپانی مشتری (کلاینت) مفتش می‌باشد. مفتش نیاز دارد تا با مراجع صدور گواهی متعدد همانند دانشگاهها ارتباط برقرار کند کسی که آموزش را ارتقاء می‌دهد، کمپانی‌هایی که برای کار استفاده شدند یا سازمانهایی که گواهی‌های دیگری صادر می‌کنند.

D- اعتماد اولیه و بلوک شبکه کنسرسیوم

به طور کلی، بلوک اولیه یا اولین بلوک در یک بلاکچین، ابداع شده به صورت حالت اولیه یک شبکه P2P، یک مسئولیت سخت می‌باشد. این نیازمند یک فرض قابل قبول توسط تمام همتایان می‌باشد. PASS از یک شبکه کنسرسیوم استفاده می‌کند که در آن حالتهای با اعتبار و شهرت معین گنجانده شدند و برای آنها رای داده می‌شود. بنابراین، میتوانیم فرض کنیم که چنین بلوکی شامل ساختار داده در PASS و استیکهای اولیه به طور انحصاری می‌باشد. مرجع صدور گوای میتواند یکی از استیکها باشد اما نیاز به این وجود ندارد. برای اینکه یک مرجع صدور گواهی مورد اعتماد بود، مرجع صدور گواهی نیاز دارد تا استیکهای با هویت فراهمکند.

E- Delegated Proof of Stake (DPoS) (دستیابی به اجماع توزیع شده در یک سیستم رمزنگاری شده)

اثبات کار (PoW) یک الگوریتم اجماع استفاده شده در شبکه بیت کوین می‌باشد. PoW از طریق کاوش انجام شده است که فرآیند اصلی تمیزکاری خانه غیرمتمرکز می‌باشد که به وسیله آن نسخه‌ها (معاملات) اعتبارسنجی شده و

پاکسازی می‌شوند. کاوش سیستم بیت کوین را ایمن می‌کند و ظهور اجماع در سرتاسر شبکه بدون یک نهاد مرکزی را مقدور می‌سازد. رقابت برای حل الگوریتم اثبات کار برای دستیابی به جایزه و دقیقا برای ثبت معاملات بروی بلاکچین مبنا برای مدل امنیت بیت کوین می‌باشد.

Delegated Proof of Stake (DPoS) یک الگوریتم اجماع بسیار کارآمد می‌باشد. این یک نوعی از اثبات استیک (PoS) می‌باشد. هردوی اینها به منظور کاهش هزینه و استفاده برق ناکارآمد همراه با PoW توسعه داده شدند. PoS به هر والت که محتوی کوین برای استیک می‌باشد اجازه می‌دهد تا در فرایند اعتبارسنجی معاملات و تشکیل اجماع توزیع شده و به نوبه خود دستیابی به کوین (سکه) مشارکت کند. در حالیکه در DPoS، هر والت که حاوی کوین می‌باشد، قادر به رای دادن به نمایندگان می‌باشد و این نمایندگان هستند که وظیفه اعتبارسنجی معاملات و حفظ بلاکچین را انجام می‌دهند و هزینه‌های معامله را به عنوان سود در اختیار می‌گیرند. این نسبت به PoS بسیار کارآمد می‌باشد.

PASS از DPoS استفاده می‌کند. ذینفعان منتخب سربرگ جهانی (کلی) را ایجاد می‌کنند.

F- بیومتریکها و منحصر به فردی

بیومتریکها در علم کامپیوتر زمینه استفاده از متریکهای مرتبط با مشخصات انسانی جهت شناسایی، احراز هویت و کنترل دسترسی می‌باشد. اثر انگشت، ریشه‌های کف دست، تشخیص چهره، DNA، هندسه دست، تشخیص عنبیه و شبکیه در میان آنها قرار دارند. متریکهای دیگر میتوانند مرتبط با رفتارهایی همانند صدا، ریتم تایپ و الگوهای پیاد-روی و واکنش در برابر محرک معین باشند (برای مثال مراجع 25 و 26]. با پیشرفت تکنولوژی، دقت بیومتریکها شدیدا بهبود می‌یابد. زمان موردنیاز برای دستیابی به چنین اطلاعاتی بسیار کمتر می‌باشد. شویه دستیابی به آنها آسانتر می‌باشد. قیمت آنها قابل استطاعت می‌باشد.

یک جهت اصلی در احراز هویت بیومتریک تشخیص بیومتریکهای جعلی به طور سریع می‌باشد به طوریکه چنین سیستمی میتواند برای احراز هویت همزمان استفاده شود [25 و 26]. در یک سناریو کاربرد متفاوت، که در آن بیومتریکها برای تمایز بین انسان و ربات استفاده شدند. مسئله چالش برانگیز تشخیص موثر بیومتریکهای غیرانسانی

همانند تغییر دیجیتال از میزان کثیری از بیومتریکهای انسانی می‌باشد. این به خصوص در کاربردهایی که نیازمند ناشناسی اما ماهیتهای انسانی قابل شناسایی می‌باشند، مفید می‌باشد. در حال بررسی روشهای متعدد همانند آنالیز مولفه اصلی، موجکها و همبستگی‌ها برای آزمایش چنین طبقه‌بندیهایی می‌باشیم [برای مثال 27].

همانند دیگر PDAها، بیومتریکهای حقیقی مورد استفاده قرار گرفتند اما در شبکه ذخیره نشدند. تابع یک طرفه دستیابی به بیومتریکهای اصلی را سخت می‌سازد. به علاوه، این نیازمند اطلاعات بیومتریک متعدد برای کاهش احتمال مثبت کاذب می‌باشد. بدین ترتیب، احتمال وجود دو بیومتریک مشابه برای دو فرد در طیف آستانه‌های معین صفر می‌باشد.

4- ارتباطات PASS

اکنون توالی جنس برای فاعل جهت دستیابی به یک PDA را توصیف می‌کنیم. شکل1 در بخش1 جریان کار را نشان می‌دهد. ایده اصلی استفاده از بلاکچین کنسرسیوم می‌باشد که در آن گره‌های ثبت شده با ادله منتخب میتوانند نتیجه را در یک سربرگ کلی ثبت کنند. این گره‌ها میتوانند کلکسیونی از سازمانها و کمپانی‌های مشهور باشند. مراجع صدور گواهی نیازی نیست تا به عنوان گره در شبکه باشند. وظیفه اصلی آنها ارائه یک گواهی به فاعل می‌باشد. برای مثال، یک فارغ التحصیل می‌تواند یک نسخه رسمی را درخواست که یکی از PDAهای او باشد. این فارغ التحصیل فاعل می‌باشد. دانشگاه مرجع صدور گواهی می باشد. شبکه بلاکچین میتواند به وسیله یک کلکسیونی از سازمانها تشکیل شود که مشهور و قابل اعتماد بوده و دارای انگیزش برای حفظ بلوکها می‌باشند. دانشگاهها، ناشران کتب متنی و جوامع آموزشی کاندیدهای ایده‌آل می‌باشند. کلاینتها می‌توانند هرگونه کارفرما باشند که قصد پیشنهاد کار به فاعل را دارند.

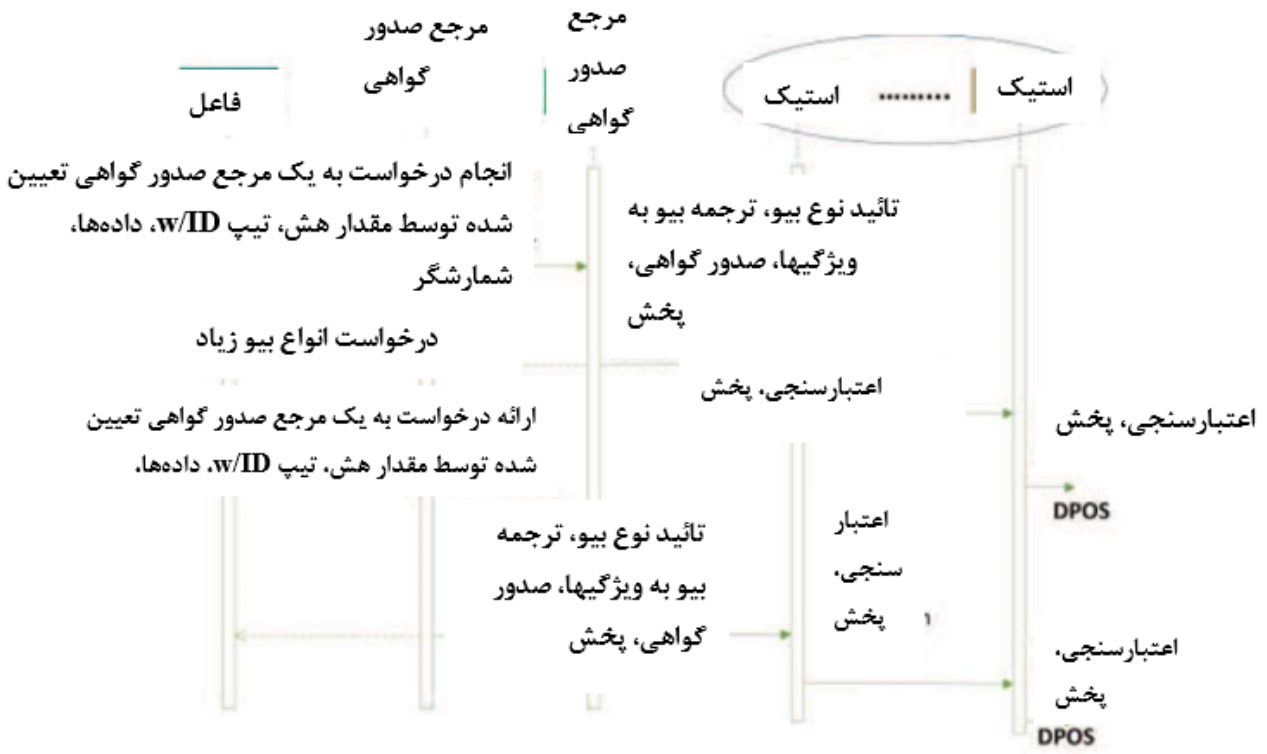
شکل2 ترتیب زمانی برای PDA-PAE را نشان می‌دهد. این برای نمایش بوده و فاقد ساختار تبادل داده دقیق می‌باشد. در اینجا، فاعل یک درخواست گواهی به دلیل یک دستاورد مخصوص به یک مرجع صدور گواهی انجام می-دهد. مرجع صدور گواهی ثبت شده و برای صادر کردن چنین گواهی صلاحیت دارد. این اطلاعات به وسیله کلید عمومی مرجع صدور گواهی رمزنگاری شدند به طوریکه هیچ کس دیگری نمیتواند PDA را مشاهده کند. وقتی که

مرجع صدور گاهی درخواست را دریافت می‌کند، اطلاعات درخواست را در اولین PDA تائید می‌کند و پاسخ رد می‌دهد یا گواهی را صادر می‌کند. در واقعیت، ارتباطات بین فاعل و مرجع صذور گواهی بسیار پیچیده‌تر از چیزی می‌باشد که نشان داده شده است. این ممکن است نیازمند شواهد و اطلاعات بیشتر مرتبط با PDA باشد. این ممکن است اثبات پرداخت را برای خدمات قبل از صدور گواهی درخواست کند. مرجع صدور گواهی همچنین گواهی را به گره‌های دیگر در شبکه بلاکچین کنسرسیوم ارسال می‌کند. گواهی شامل اطلاعاتی همانند امضاء دیجیتال مرجع صدور گواهی با تعداد منحصر به فرد، یک کلید عمومی برای PDA و غیره می‌باشد و میتواند توسط دیگر مشارکت کنندگان مشاهده شود. هر گره که گواهی را دریافت می‌کند، اعتبارسنجی را انجام خواهد داد. این گره اعتبارسنجی را به گره‌های دیگر پخش می‌کند. این گواهی در سربرگ جهانی به وسیله استیک منتخب ثبت خواهد شد.

شکل2: توالی زمانی برای PDA-PAE

شکل3 مثال دیگری از توالی زمانی را برای PDA-PID نشان می‌دهد. PID داده بیومتریک یا دیگر اطلاعات مرتبط با ID می‌باشد که فاعل مالک آن می‌باشد، از آن آگاه است و به آن عمل می‌کند. در اینجا از سنجش بیومتریک برای نمایش استفاده می‌کنیم. از آنجایی که به صورت آماری با استفاده از دو یا چند نوع اطلاعات بیومتریک نشان داده شده است، برخورد شدیدا کاهش خواهد یافت، از فاعل خواسته خواهد شد تا حداقل دونوع

مختلف سنجش بیومتریک ارائه کند. در پایان، سربرگ دارای تمام اطلاعات قابل تائید فاعل از طریق اجماع می‌باشد. بنابراین، نیازمند یک شمارشگر برای شمارش انواع مختلف اطلاعات بیومتریک می‌باشد.



شکل3: توالی زمانی PDA-PID

عملیاتهای بعد از تثبیت دقیق می‌توانند در مرجع [33] دیده شوند. به یاد بیاورید که روشهای مختلف تحقق توالی زمانی در اشکال 2 و 3 وجود دارند.

5- سیستم سرویس

یک سازمان یا نهاد (مشتری) کسی که نیازمند برخی یا تمام PDAهای فاعل در PA می‌باشند، میتوانند با فاعل به طور مستقیم به جای استخدام یک مفتش برای انجام اعتبارسنجی وارد مذاکره شوند. با یک قرارداد هوشمند بین مشتری و فاعل، مشتری قادر به بررسی اسناد امضاء شده درخواستی همانند مدرک، نسخه (رونوشت)، تجارب کاری، هویتها و غیره باشد.

شکل4 یک مثالی از استفاده از PASS [32] در مورد رسانه اجتماعی اینترنت می‌باشد. رسانه اجتماعی اینترنت فاقد لایه کنترل کیفی برای هر ارسال پست می باشد، به طور نسبی دارای اطلاعات پیشینه اندک درباره افراد در دایره رسانه یا کنترل برای افراد مجاز در این دایره می باشد. ارزیابی قابلیت اعتماد ارسال پست آنها براساس ارسال پست خود آنها می‌باشد و اطلاعات مربوطه آنها به صورت سیگنالهایی عنوان شدند. اغلب محققان بروی سیگنالهای برونزاد همانند ساختارهای هایپرلینک متمرکز می‌شوند [11 تا 18، 36]. تحقیق اخیر بروی سیگنالهای درونزاد همانند تصحیح اطلاعات واقعی درباره ارسال پستها می‌باشد [36]. چنین سیگنالهایی منجر به قرارگیری ارسال پست کیفیت بالا اغلب توسط متخصصان در یک رتبه‌بندی نسبتا بالا می‌شود در غیر اینصورت در یک دریایی از پستها گم می‌شوند. برخی فعالیتهای نوین را درباره کنترل کیفی ارسال پست استفاده شده در رسانه اجتماعی اینترنت مشاهده کردیم که همراه با حساب فردی می‌باشند. مثالها عبارتند از واکنش در برابر اشیاء (در فیسبوک)، امتیازات (در کارما [14]) و شهرت (برخی گروههای چت از شهرت برای تصمیم‌گیری اینکه چه کسی مجاز به ارسال کامنت می باشد [15]، استفاده می‌کنند)، رتبه‌بندی آنلاین شخصی براساس هویت دیجیتال جمع‌آوری شده [7]. برخی تحقیقات درباره کسانی که چیزی و در چه موقع را ارسال می‌کنند. در طول فرایند ورود، برخی اپلیکیشنها از کپچا [17]، احراز هویت اجتماعی مبتنی بر عکس (فیسبوک)، نقض بلادرنگ (توئیتر، GitHub، Redit و غیره) و خصوصیت اتصال حساب [16] استفاده می‌کنند.

با PASS، سرویس ID می‌تواند با اعتماد به نفس بالا با خصوصیات مطلوب زیر فراهم شود: 1- انسان حقیقی، 2- بدون هیچگونه حساب مستعار، 3- ناشناس و ایمن، 4- شفاف، 5- تغییرناپذیر، 6- غیرتمرکزی مبتنی بر اجماع و 7- قابل فسخ.

شکل4: سرویس PASS

مراحل به شکل زیر هستند:

1-یک اپلیکیشن همانند رسانه اجتماعی اینترنت یک درخواست برای فاعل برای اعتبارسنجی ویژگی انجام می‌دهد.

2- فاعل آن را به کلید عمومی و PDAهای مرتبط برای اپلیکیشن ارسال می‌کند.

3- اپلیکیشن کلید عمومی خود را به صورت امضاء شده به وسیله کلید عمومی فاعل برگشت می‌دهد؛

4- فاعل اسکریپت قفل شکنی امضاء شده خود، امضاء، لیست PDAها با انواع آنها و روشها برای دسترسی به بررسی PDAها ارسال می‌کند.

5- فاعل همچنین یک اسکریپت قفل‌گذار ارسال می‌کند که شامل کلید عمومی اپلیکیشن برای بررسی امضاء می-باشد. این تنها زمانی که امضاء منطبق با اپلیکیشن باشد، قفل شکنی می‌شود.

6- یک استیک در شبکه P2P کنسرسیوم بررسی می‌کند که آیا فاعل دارای چنین PDAهایی می باشد؛ در صورت وجود ادامه می‌دهد.

7- استیک بقیه استیکها را پخش می‌کند بنابراین تمام آنها می‌توانند از این اعتبارسنجی استفاده کنند.

8- اپلیکیشن اسکریپ قفل شکنی را با امضاء آن ارسال می‌کند.

9- استیک از اسکریپت قفل شکنی برای برگشت به اپلیکیشن استفاده می‌کند اگر اعتبارسنجی به طور موفق یا ناموفق انجام شده باشد.

همانطور که مشاهده می‌کنیم، چنین توالی از PASS میتواند به هر اپلیکیشن دیگری تعمیم داده شود که نیازمند اعتبارسنجی PDAها می باشد.

6- نتیجه‌گیری

در این مقاله، یک رویکرد نوین برای مدیریت سند شخصی با استفاده از تکنولوژی بلاکچین، PASS، نشان دادیم. PASS از ویژگیهای بلاکچین به خوبی استفاده می‌کند. هر زمان که فاعل مایل به ردیابی موفقیت یا مشخصه‌های جدید باشد، میتواند آن درست در آن زمان آرشیو کند به جای اینکه منتظر مفتش باشد.

شانس برای چنین اپلیکیشنی فراگیر می‌باشد. این میتواند در اپلیکیشنهای آنلاین و نیز دیگر اپلیکیشنهایی همانند استخدام و ترفیع استفاده شود. این اپلیکیشن شخص ثالث را به طور کامل حذف می‌کند و ناشناسی و مسئولیت-پذیری آن را حفظ می‌کند.

یک مسئله چالش برانگیز اصلی در اجرای یافتن یک کلکسیونی از استیکها می باشد که قابل اعتماد هستند در حالیکه دارای انگیزش در کار بروی شبکه می‌باشند. این همچنین نیازمند یک مکانیسم یا پروتکلی برای رای‌گیری یک استیک می‌باشد. نیاز است تا وزن استیک به لحاظ کمی تعریف شود.

مسئله چالش برانگیز مرتبط درخواست از سازمانهای شناخته شده می‌باشد که به عنوان مراجع صدور گواهی باشند. این است که این سازمانها نیاز دارند تا پدازش دستی خود را به پردازش الکترونیک تغییر دهند و گواهی‌ها را به صورت دیجیتال صادر کنند. طرف دیگر این مسئله چالش برانگیز آستانه برای رد درخواست گواهی یک درخواست کننده می‌باشد.

به منظور استفاده گسترده، استانداردسازی ساختار PDA و پروتکل ارتباطی (مخابراتی) ضروری می‌باشد. می‌دانیم که برخی PDAها معمول هستند و دریافت گواهی از سوی آنها آسان می‌باشد. برخی PDAهای دیگر اینگونه نیستند. برای مثال، این یک فرایند استاندارد برای رسیدن به نسخه گواهی صادر شده می‌باشد. اما، گواهی یک بازتاب از یک پروژه خاص اجرا شده توسط پرسنل مخصوص همانند پروفسورها آسان نمی‌باشد. نامه‌های مرجع معمولا در این هدف عمل می‌کنند. یک کار پروژه‌ای زمانی دقیق نیز می‌تواند به هدف عمل کند. بنابراین، تبدیل چنین مرجعی به گواهی دیجیتال ...

REFERENCES

[1] http://infographicsmania.com/resume-padding-statistics/

[2] Open badge, https://openbadges.org/

[3] Acclaim https://www.youracclaim.com

[4] Sony Global Education https://www.sonyged.com/ and https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

[5] https://www1.taskstream.com/

[6] OpenID Connect, http://openid.net/connect/

[7] A. Yasin and L. Liu, "An Online Identity and Smart Contract Management System", *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, 2016, pp. 192-198.

[8] X Luna Dong, et al., Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources, 02/2015, https://arxiv.org/abs/1502.03519,

[9] Requirements for a Global Identity Management Service, April 2001, https://www.w3.org/2001/03/WSWS-popa/paper57

[10] W Gitt, R Compton and J Fernandez, Biological Information — What is It?, http://www.worldscientific.com/doi/pdf/10.1142/9789814508728_0001

[11] L Page, The PageRank Citation Ranking: Bringing Order to the Web, 1998

[12] https://en.wikipedia.org/wiki/PageRank

[13] https://www.facebook.com/help/like

[14] http://lesswrong.com/

[15] http://www.wechat.com/en/

[16] X Yang, Q Cao, M Sirivianos, SybilRank: Aiding the Detection of Fake Accounts in Large Scale Social Online Services, https://users.cs.duke.edu/~qiangcao/sybilrank_project/index.html

[17] L v Ahn, et al, reCAPTCHA: Human-Based Character Recognition via Web Security Measures". Science, September 12, 2008. pp 1465-1468.

[18] S Yardi, N Feamster and A Bruckman, Photo-based authentication using social networks, Proceedings of the first workshop on Online social networks, WOSN'08 PP 55-60

[19] OAuth: https://kantarainitiative.org/about/principles/

[20] S Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf

[21] Hyperledger https://www.hyperledger.org/

[22] R3 CEV Financial Consortium http://www.r3cev.com/

[23] The Enterprise Ethereum Alliance (EEA) http://entethalliance.org/

[24] DAO,decentralized autonomous organization https://forum.daohub.org/

[25] Chien Le, A Survey of Biometrics Security Systems, 2011, http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf

[26] L Lai, S Wai Ho and H. Vicent Poor "Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case" IEEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011

[27] S B Nikam, S Agarwal, Ridgelet-based fake fingerprint detection, Neurocomputing, Volume 72, Issues 10–12, June 2009, Pages 2491–2506

[28] LF WU, et al, Non-Invertible Transformation Schems for Face Templete Protection, Signal Processing, Vol 28, No 7, 2012.

[29] M-d Yu and Srinvas Devadas, Pervasive, Dynamic Authentication of Physical Items, COMMUNICATIONS OF THE ACM, V60, N4, 2017, pp32-39

[30] K Gai, et al, Privacy-Preserving Adaptive Multi-channel Communications Under Timing Constraints, 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp 190-195

[31] Schneier, B. Sensible authentication. ACM Queue 1, 10(2004): 74–78

[32] Wilson, C.et al, Fingerprint vendor technology evaluation 2003: summary of results and analysis report. NIST Internal Report 7123 (2004).

[33] Yixuan Zhu and Zhixiong Chen, RealID: Building A Secure Anonmous Yet Transparent Immutable ID Service, 2017 IEEE 3rd International Conference on Big Data Security on Cloud, Beijing, China

[34] Smart Contracts: The Blockchain Technology That Will Replace Lawyers, https://blockgeeks.com/guides/smart-contracts/

[35] Michael Mainelli, Blockchain Will Help Us Prove Our Identities in a Digital World, Harvard Business Review, March, 2016, https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world

[36] Xin Luna Dong, et al, Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources, https://arxiv.org/abs/1502.03519 Submitted on 12 Feb 2015)