****

**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 می­باشد. 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. شبیه­سازی 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 سرمایه­گذاریها 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 فارغ­التحصیلان 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]](#footnote-1) [3] پلتفرم نشان­گذاری دیجیتال براساس استاندارد Open Badge بوده و توسط پیرسون[[2]](#footnote-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 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 می­باشد.

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، مسئولیت­پذیری، 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،



جایی که



و

.

**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.



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



**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 پیاد­روی 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 می­دهد. 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 می­باشد. 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 مسئولیت­پذیری 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 ...









1. Acclaim [↑](#footnote-ref-1)
2. Pearson [↑](#footnote-ref-2)