اشتراک‌گذاری اطلاعات هویتی مشتریان بین بانک‌ها مبتنی بر دفتر کل توزیع‌شده

محمدجواد صمدی، مدیرعامل شرکت زنجیره بلوک پارس، m.samadi@parsblockchain.com
محمد طهرانی*، عضو هیئت‌علمی دانشگاه خاتم، m.tehrani@khatam.ac.ir
زهرا حمیدی‌فر، دانشجوی کارشناسی ارشد دانشگاه خاتم، z.hamidifar@khatam.ac.ir

چکیده

با ظهور مفهوم فناوری دفتر کل توزیع‌شده، بسیاری از بانک‌ها و سازمان‌های خدمت‌محور در حال برنامه‌ریزی جهت استفاده یا پیاده‌سازی عملی این فناوری در فرآیندهای مرتبط با کسب‌وکار خود هستند. در این فناوری هر کاربر حداقل دارای یک زوج کلید (عمومی/ خصوصی) است که از طریق کلید عمومی شناخته می‌شود و صرفاً با کمک کلید خصوصی می‌تواند به دارایی‌های خود دسترسی پیدا کند. بانک‌ها به دلیل الزامات قانونی موظف‌اند پیش از ارائه‌ی برخی از خدمات (مانند افتتاح حساب، صدور کارت، اعتبارات و ...)، هویت مشتری نهایی را احراز نمایند که در حال حاضر این فرآیند فقط به‌صورت حضوری و از طریق شعب هر بانک به‌طور مستقل از دیگر بانک‌ها انجام می‌پذیرد. با ایجاد و گسترش شبکه‌های تبادل دارایی مبتنی بر فناوری دفتر کل توزیع‌شده بین بانک‌ها، این نهادهای مالی به فرآیندهایی نیاز دارند تا بتوانند ارتباط میان کلیدهای عمومی/ خصوصی و هویت مشتری را برقرار کنند تا ضمن رعایت مقررات و الزامات قانونی، خدمات بهتر و متنوع‌تری به مشتریان خود ارائه دهند.

در این مقاله مدل جدیدی برای به اشتراک‌گذاری فرآیند شناسایی مشتریان بین بانک‌ها ارائه گردیده است که به مشتریان کمک می‌کند پس از مراجعه حضوری و شناسایی هویت (KYC[1]) یا سایر مشخصات توسط یک بانک، از مراجعه به سایر بانک‌ها به‌منظور انجام فرآیند شناسایی مشتری بی‌نیاز گردند. در این فرآیند یک بانک صادرکننده، تعدادی توکن KYC در اختیار مشتری قرار می‌دهد و مشتری می‌تواند با ارائه این توکن‌ها به هر بانک پذیرنده، احراز هویت یا سایر مشخصات خود را به اثبات رساند. از دیگر سو، اعلام و افشای هرگونه اطلاعات مشتری صرفاً در اختیار خود مشتری و با استفاده از کلید خصوصی وی انجام می‌شود که این امر نگرانی‌های مربوط به نقض حریم خصوصی مشتری را مرتفع می‌نماید. مدل پیشنهادی به‌صورت کلی برای هر شبکه مبتنی بر دفتر کل توزیع‌شده قابل انجام است، لیکن در اینجا به‌صورت اختصاصی برای دفتر کل توزیع‌شده استلار طراحی و پیاده‌سازی شده است.

کلیدواژه‌ها: دفتر کل توزیع‌شده، زنجیره بلوک، استلار، توکنیزه کردن، شناسایی مشتری

[1] Know Your Customer (KYC)

مقدمه

در دهه اخیر و به‌ویژه پس از پیدایش بیت‌کوین، فناوری دفتر کل توزیع‌شده[۲] ابتدا در میان پژوهشگران و علاقه‌مندان به فناوری‌های غیرمتمرکز، سپس در میان سازمان‌های ارائه‌دهنده خدمات مالی و پس‌ازآن در بین سایر فعالان بازار موردتوجه قرار گرفت. این فناوری که به‌عنوان یکی از فناوری‌های بن‌افکن[۳] به شمار می‌رود، نه‌تنها روش‌های مربوط به پردازش و ذخیره اطلاعات، بلکه حتی ارزش پیشنهادی و مدل کسب‌وکار سازمان‌ها را نیز تحت‌الشعاع قرار می‌دهد و به دلیل ویژگی‌های ذاتی که در آن نهفته است، بسیاری از نهادهای مالی بزرگ جهان در حال استفاده و یا برنامه‌ریزی برای استفاده از آن هستند. این فناوری قادر است با افزایش امنیت، پایداری و شفافیت داده‌ها موجب بهبود فضای کسب‌وکار میان بازیگران مختلف یک صنعت گردد، ازاین‌رو بسیار مشاهده می‌شود که رقبای یک بازار به‌منظور بهبود کیفیت خدمات خود، نسبت به راه‌اندازی شبکه‌ای مبتنی بر فناوری دفتر کل توزیع‌شده در میان خود اقدام می‌نمایند. [۱]

در برخی از شبکه‌های مبتنی بر دفتر کل توزیع‌شده، یک رمزارز به‌عنوان دارایی پایه‌ی شبکه تعریف‌شده است که هر یک از کاربران می‌توانند مقداری از آن را در حساب خود ذخیره کنند. لیکن در برخی دیگر از این شبکه‌ها، امکان ثبت و ذخیره‌ی هر گواهی یا توکن دارایی در شبکه وجود دارد. بدین‌صورت، دفتر کل توزیع‌شده کاربردی فراتر از تبادل یک رمزارز پیدا می‌کند و از آن می‌توان به‌عنوان بستری برای ثبت مالکیت و یا تبادل هر نوع توکن دارایی استفاده کرد. به‌عنوان‌مثال می‌توان دارایی‌های ریالی، دارایی‌های ارزی، گواهی اوراق بهادار، سند املاک، مستقلات، خودرو و یا هر دارایی دیگر یک فرد را در این دفتر ثبت نمود. [۲]

یکی از الزامات قانونی که همه‌ی بانک‌ها و نهادهای مالی به شکل سخت‌گیرانه‌ای خود را مکلف به انطباق با آن می‌دانند، الزامات مربوط به فرآیند شناسایی مشتری است که از سوی رگولاتور جهت جلوگیری از تقلب، پول‌شویی و سایر اقدامات غیرقانونی به بانک‌ها ابلاغ گردیده است. شناسایی مشتری در ساده‌ترین شکل خود ممکن است در سطح احراز هویت مشتری قلمداد گردد و به‌تدریج برحسب ضرورت با تکمیل اطلاعات مربوط به شغل، درآمد و یا دارایی‌های هر مشتری این شناسایی تکمیل گردد. [۳]

دغدغه اصلی این مقاله ارائه روشی نوین به‌منظور ثبت و ذخیره‌ی هویت و مشخصات یک مشتری به‌مثابه‌ی دارایی او در دفتر کل توزیع‌شده است، به‌نحوی‌که مشتری بتواند در هر زمان دلخواه با استفاده از کلید خصوصی خود به آن رکورد دسترسی پیداکرده و به خواست خود آن را به دیگران ارائه دهد. این فرآیند دارای دو سمت صادرکننده و پذیرنده است که منافع هر یک از آن‌ها در این فرآیند دیده‌شده و ریسک‌های احتمالی مدنظر قرارگرفته است. بعلاوه، ازآنجاکه اطلاعات مشتری صرفاً با کلید خصوصی وی قابل‌دسترسی است، تهدیدی برای حریم خصوصی او ایجاد نخواهد شد و هیچ‌یک از بانک‌های صادرکننده و پذیرنده‌ی توکن KYC نخواهند توانست مستقلاً درون این شبکه، اطلاعات مشتری را با دیگران به اشتراک گذارند.

---

[۲] Distributed Ledger Technology

[۳] Disruptive

در ادامه‌ی این مقاله ابتدا توضیحاتی در خصوص الزامات مربوط به شناسایی مشتری آورده شده و سپس دفتر کل توزیع‌شده استلار به‌عنوان بستر پیاده‌سازی این فرآیند معرفی گردیده است. در بخش بعدی مروری بر کارهای مشابه انجام‌شده در خصوص به اشتراک‌گذاری فرآیند شناسایی مشتری آورده شده و پس‌ازآن مدل پیشنهادی به ارائه روشی نوین برای به اشتراک‌گذاری این فرآیند میان بانک‌ها و نهادهای مالی پرداخته است. نهایتاً بحث در خصوص فرصت‌ها و چالش‌های پیش روی پیاده‌سازی مدل پیشنهادی پایان‌بخش این مقاله خواهد بود.

فرآیند شناسایی مشتری (KYC)

یکی از مهم‌ترین سیاست‌هایی که در سازمان‌های مختلف خصوصاً نظام بانکی جهانی اجرایی شده فرآیند شناسایی مشتری (KYC) است که از بنیادی‌ترین دلایل کاهش تقلب، جرم، پول‌شویی و ریسک‌های عملیاتی و شهرت بانک‌ها است. قوانین شناسایی مشتری در سطح ملی و بین‌المللی نه‌تنها در نهادهای مالی حائز اهمیت است، بلکه خدمات عظیمی را به گروه‌ها و اصناف مختلف ارائه می‌دهد که از این جمله می‌توان به استارتاپ‌ها، صرافی‌ها، آموزشگاه‌ها، شرکت‌های خدمات مسافرتی و بسیاری دیگر از بنگاه‌های اقتصادی اشاره کرد. ازآنجاکه شناسایی مشتری اولین اقدامی است که بانک در مراجعه مشتری برای افتتاح حساب یا دریافت برخی دیگر از خدمات انجام می‌دهد، کسب اطلاعات کافی از مشتری متناسب با خدمات درخواستی وی ضروری است. از سوی دیگر، در طول مدتی که مشتری با بانک در ارتباط است، بانک می‌بایست از طریق پایش مستمر فعالیت مالی مشتری و تشکیل پروفایل رفتار هر مشتری، وظیفه‌ی خود را برای جلوگیری از سوءاستفاده از حساب مشتری انجام دهد. از سوی دیگر، با کنترل رفتارهای پرخطر مشتری، ریسک‌هایی که ممکن است از جانب وی متوجه بانک باشد را مدیریت نماید. [۳]

در جمهوری اسلامی ایران نیز بر اساس قوانین بانک مرکزی به‌منظور مبارزه با پول‌شویی و تأمین مالی تروریست، مستندسازی اطلاعات و مدیریت ریسک‌های مختلف، دستورالعمل چگونگی شناسایی مشتری در مؤسسات اعتباری تدوین‌شده است. بر این اساس مشتریان حقیقی یا حقوقی دارنده حساب به دو دسته‌ی مشتریان گذری که بدون استمرار مراجعه نموده و تنها از خدمات غیر پایه (حواله وجوه، دریافت و پرداخت، صدور چک و ...) استفاده می‌کنند و مشتریان دائمی که از خدمات غیر پایه و پایه (افتتاح انواع حساب، اعطای تسهیلات، اعتبار اسناد، صدور انواع ضمانت‌نامه و ...) مؤسسات اعتباری به‌صورت مستمر استفاده می‌کنند تقسیم می‌شوند. مطابق با این دستورالعمل، افتتاح هر نوع حسابی منوط به حضور مشتری، تطبیق وی با تصویر اصل کارت ملی و امضای مجوز دار مشتری است. ازاین‌رو، اخذ اطلاعات مشتریان متناسب با خدمت درخواستی و میزان ریسکی که از جانب مشتری متوجه بانک است، به‌منظور شناسایی اولیه یا کامل صورت می‌پذیرد. بالطبع اطلاعات دریافتی از مشتریان حقیقی و حقوقی متفاوت بوده و ارائه خدمات به کلیه مشتریان (حتی مشاغل غیرمالی) حتماً باید حاوی تعهد پذیرش و اجرای قانون مبارزه با پول‌شویی باشد. [۴]

پس از پذیرش مشتری و اخذ اطلاعات، مؤسسات اعتباری موظف‌اند برای پیشگیری از افشاء و استفاده غیرمجاز از اطلاعات، تدابیر امنیتی لازم را بیندیشد. هم‌چنین حساب‌ها و تراکنش‌ها می‌بایست با جزئیات در یک سیستم اطلاعاتی ذخیره و

پردازش‌شده تا سوابق و فعالیت‌های مشتریان قابل‌ردیابی بوده و مدیران ارشد با نظارت کامل بر آن‌ها ریسک‌های احتمالی را مدیریت نمایند.

دفتر کل توزیع‌شده استلار

شبکه استلار[۴] یک پروتکل منبع باز و غیرمتمرکز برای تولید و تبادل هر جفت رمزارز موجود در این شبکه است و توسط نهاد غیرانتفاعی بنیاد توسعه استلار[۵] پشتیبانی می‌گردد. جد مک کالب[۶] از بنیان‌گذاران ریپل[۷] در سال ۲۰۱۴ طرح اولیه استلار را راه‌اندازی نمود و در ژانویه ۲۰۱۵ حدود سه میلیون کاربر در شبکه خود داشت سپس در ماه آوریل با ارتقاء پروتکل آن به یک الگوریتم اجماع جدید به نام پروتکل اجماع استلار[۸] شبکه استلار در نوامبر ۲۰۱۵ به‌طور رسمی شروع به کار کرد. [۵]

شبکه استلار یک شبکه غیرمتمرکز مبتنی بر دفتر کل توزیع‌شده است و شامل گره‌هایی است که می‌توانند مستقل از یکدیگر عمل کنند. قدرت انتقال اطلاعات در یک شبکه به‌جای یک منبع اصلی بین همه سرورها توزیع می‌شود. این به این معنی است که شبکه استلار به هیچ نهاد واحدی بستگی ندارد. ایده این است که تعداد زیادی سرور مستقل در شبکه استلار مشارکت داشته باشند، به‌طوری‌که حتی اگر برخی از سرورها از دسترس خارج شوند، انتقال‌ها با موفقیت اجرا خواهند شد. همه سرورها به‌طور هماهنگ بر روی یک دفتر کل و بر اساس الگوریتم اجماع با یکدیگر پیش می‌روند. [۶]

احراز هویت در هسته[۹] استلار صورت می‌گیرد و کار دشوار ارزیابی و تجمیع و توافق در وضعیت‌های مختلف هر تراکنش را بر اساس پروتکل اجماع استلار انجام می‌دهد. در استلار می‌توان برای ساخت یک شبکه قابل‌اعتماد و باثبات کنترل بیشتری روی گره‌هایی که به آن‌ها اعتماد کرده‌ایم، اعمال کنیم. بستر استلار شامل یک شبکه گسترده از میزبان‌ها[۱۰] است که تولید، توزیع، صحت سنجی و ثبت تراکنش‌ها را بر عهده دارند و نرم‌افزارهای کیف پول، صرافی یا سایر خدمات آنلاین مبتنی بر استلار از طریق API های ارائه‌شده توسط زیرساخت، هورایزون[۱۱] با این میزبان‌ها در ارتباط‌اند.

میزبان‌ها موجودیت‌هایی هستند که کاربران به آن‌ها اعتماد دارند و اقدام به تبادل توکن‌های ارائه‌شده توسط آن‌ها می‌نمایند. آن‌ها به‌عنوان یک پل بین دارایی‌های مختلف و شبکه استلار عمل می‌کنند. دارایی پایه[۱۲] شبکه استلار لومن[۱۳] نام دارد و این شبکه علاوه بر لومن، قابلیت ایجاد و انتشار هر نوع توکن[۱۴] جدید را دارد.

---

۴ Stellar
۵ Stellar Development Foundation
۶ Jed McCaleb
۷ Ripple
۸ Stellar Consensus Protocol
۹ Core
۱۰ Anchors
۱۱ Horizon
۱۲ Native Asset

در هر تراکنشی ۴ رکن اساسی: حساب فرستنده، حساب گیرنده، نوع دارایی و امضا تراکنش ، بررسی و تأیید می‌گردد. هر تراکنش یک هزینه حداقلی یک صدهزارم لومن را داراست که همین قضیه موجب جلوگیری از سربار زیاد بر روی شبکه می‌شود. در تنظیمات حساب نیز می‌توان شرط رخداد تراکنش را بر اساس چند امضاء با وزن مشخص مانند امضاء بانک و مشتری و یا حساب قابل‌اطمینان اعلام‌شده از سوی مشتری قرار داد.

یکی از ارکان اصلی تراکنش، بخش یادداشت[۱۵] است، که می‌توان داده دلخواه با اندازه محدود، را درون آن قرار داد که پس از ثبت تراکنش، غیرقابل تغییر می‌باشد. به‌منظور استناد پذیری تراکنش‌ها، اطلاعات اضافی موردنیاز هر توکن را می‌توان در بخش یادداشت تراکنش قرارداد و سپس تراکنش را با کلید خصوصی امضا و ارسال نمود. بدین ترتیب گیرنده از اصل بودن و درستی پیام مطلع گردیده و فرستنده نیز قادر به انکار ارسال آن نخواهد بود.

مرور فعالیت‌های مشابه

در زمینه شناسایی مشتری و به‌طور خاص بخش احراز هویت مشتری به‌صورت دیجیتالی طرح‌هایی مانند selfkey، KYClegal و ... انجام‌شده است. روند کار به‌صورت کلی در این‌گونه طرح‌ها به شرح ذیل است:

توکن KYClegal در سال ۲۰۱۷ و با ایده اصلی جلوگیری از جرم و پول‌شویی و لزوم تأیید شناسایی مشتری بر پایه زنجیره بلوک ارائه شد. این طرح پس از بررسی سیستم کنونی شناسایی مشتری و چالش‌های آن طرح اشتراک‌گذاری امن و نقطه‌به‌نقطه اطلاعات را بیان می‌کند. یک شبکه غیرانتفاعی، شفاف، در دسترس و پایدار را بر مبنای زنجیره بلوک ایجاد و از طریق کیف پول دیجیتالی تلاش می‌کند تا کاربران اطلاعات خود را به‌صورت رمز شده به عامل‌های شناسایی ارائه نمایند و این عامل‌ها پس از بررسی، اطلاعات را به‌صورت هش[۱۶] در زنجیره بلوک قرار داده و گواهی احراز آن‌ها را صادر نموده تا سایرین در شبکه مشاهده و به آن‌ها اعتماد نمایند. [۷]

توکن selfkey در سال ۲۰۱۷ و با ایده اصلی مدیریت و به اشتراک‌گذاری شناسایی و هویت توسط خود مشتری ارائه شد. در این طرح پس از مطرح کردن معایب و ریسک‌های امنیتی سیستم شناسایی متمرکز به ارائه راه‌حل می‌پردازد. در مدل توکن selfkey سه بازیگر اصلی ازجمله صاحبان هویت (IO)[۱۷] (که افراد، شرکت‌ها و .... را در بر می‌گیرند)، صادرکننده تأیید هویت برای مدعیان (CI)[۱۸] (مانند دادگاه، دفتر اسناد رسمی و مکان‌هایی که برای انجام این کار بر اساس اجماع نظرات سازمان‌های

---

[۱۳] Lumen(XLM)
[۱۴] Token
[۱۵] Memo
[۱۶] Hash
[17] Identity Owner
[18] Claim Issuer

ناظر و عضو تأیید و معرفی می‌شوند) و مراکز و سازمان‌های اعتماد کننده و متکی (RP)[19] (مانند بانک‌ها و ...) ایفای نقش می‌کنند.

به‌طور مثال " اسم من باب است من ۳۱ سال دارم. " این ادعا توسط یک درخواست‌کننده برای تصاحب هویت IO ارائه می‌شود سپس توسط یک منبع معتبر CI تأیید و پس‌ازآن IO صاحب هویت می‌تواند ادعای تأییدشده را با یک طرف RP متکی به سیستم به‌منظور دسترسی وی به اشتراک بگذارد. این طرح در قالب کیف پول دیجیتالی مراکز احراز، معرفی شده و افراد می‌توانند مدارک خود را به هریک از آن‌ها ارائه داده و تقاضای دریافت توکن شناسایی selfkey نمایند.

تأیید هویت و ارائه گواهینامه‌ها محدود به افراد نبوده و شرکت‌ها نیز می‌توانند اسناد مدیریتی استارتاپ خود را از یک کیف پول هویتی مدیریت کنند. زمانی که یک طرف متکی و معتمد به شبکه، یک شرکت جدید را راه‌اندازی می‌کند، روند شناخت مشتری نیاز به بررسی دارد به‌گونه‌ای که همه سهام‌داران با توجه به سطحشان در ارتباط با پروژه در هرزمانی قادر به کنترل و آگاهی از وضعیت موجود باشند. [۸]

مدل پیشنهادی

روند فعلی شناسایی مشتری برای افراد و بانک‌ها بسیار پیچیده، وقت‌گیر و پرهزینه است. در این سیستم که در آن شناسایی به‌صورت متمرکز انجام می‌گیرد، مشتری با احساس عدم حفظ حریم خصوصی‌اش ناچار به مراجعه حضوری و احراز جداگانه در هر بانک یا سازمان بوده، هم‌چنین ذخیره متمرکز اطلاعات موجب افزایش حجم آن‌ها و ریسک‌های امنیتی مانند نقص، سرقت و حمله هکرها می‌گردد.

به دلیل تغییرناپذیر بودن اطلاعات واردشده در دفتر کل توزیع‌شده، با ذخیره KYC در آن، یک منبع کاملاً درست و قابل‌اعتماد ایجاد می‌شود تا بدین‌وسیله خطر تکراری بودن یا نادرست بودن اطلاعات به حداقل برسد. اطلاعات در بلوک‌هایی که به‌طور منحصربه‌فرد بر اساس شماره سری ایجادشده از زمان تراکنش، و کلید عمومی افراد ساخته‌شده، به‌صورت هش ذخیره می‌گردد. بدین ترتیب تولید، استفاده و جابجایی توکن KYC روی بستر اینترنت به‌صورت امن، فردبه‌فرد و غیرقابل تغییر صورت گرفته و پس‌ازاین مرحله، تراکنش کاربر در شبکه قابل‌شناسایی، پیگیری و کنترل است.

مشتری پس از ورود به سیستم یک حساب کاربری برای خود ایجاد کرده و یک زوج کلید عمومی/خصوصی در اختیار وی قرار می‌گیرد که به‌صورت محلی روی دستگاه کاربر ذخیره می‌شود تا در مواقع نیاز مشتری تراکنش‌های خود را با کلید خصوصی‌اش امضا نماید. این فرآیند منجر به مدیریت فضای ذخیره، افزایش امنیت حریم شخصی و انکارناپذیری عملکرد مشتری در شبکه و درعین‌حال، مدیریت و کنترل مستقیم وی می‌گردد. برای مشتری این مزیت وجود دارد که فقط یک‌بار مدارک KYC را به‌صورت حضوری ارائه دهد (تا زمانی که نیازمند به‌روزرسانی نباشد). بنابراین علاوه بر کاهش هزینه‌های اداری

[19] Relying Party

و اجرایی و ذخیره زمان، مشتری و سازمان‌های دارای مجوز از سوی مشتری در هر زمان و مکانی قادر به دسترسی به اطلاعات خواهند بود.

در این شبکه برای ذخیره فایل‌های حاوی مدارک از یک سیستم ذخیره‌سازی غیرمتمرکز فایل[۲۰] به نام IPFS استفاده‌شده است که در آن هر فایل به‌جای ذخیره و شناسایی با یک آدرس متعارف، با یک هش منحصربه‌فرد شناسایی می‌گردد. به دلیل اینکه آدرس‌دهی در این شبکه صرفاً بر اساس هش آن فایل صورت می‌گیرد، فایل‌های تکراری در سطح شبکه حذف می‌گردند.

فرآیند صدور

با مراجعه مشتری به شعبه بانک و درخواست صدور توکن KYC یک فرم ثبت‌نام و قرارداد به وی داده می‌شود تا مشخصات خود را در آن وارد نموده و تعهدات مطابق با قوانین را امضا نماید. پس‌ازآن فرم تکمیلی امضاشده به همراه مدارک موردنیاز، آدرس کلید عمومی و حداقل هزینه افتتاح حساب و شناسایی را در اختیار شعبه قرار می‌دهد. بانک اصالت مدارک و هویت کاربر را بررسی نموده و پس از تأیید، هویت کاربر را از سامانه ساها[۲۱] استعلام می‌نماید. در صورت اخذ تأییدیه از ساها، اطلاعات کاربر در قالبی که در شکل ۲ نمایش داده شده است، ثبت‌شده و سپس با کلید خصوصی بانک امضا می‌گردد. پس‌ازآن، فایل امضاشده بر روی IPFS قرار می‌گیرد و هش منحصربه‌فرد محتوای آن دریافت می‌گردد که در اینجا به‌صورت قراردادی "هش مستقیم"[۲۲] نامیده شده است.

در مرحله‌ی بعد، به تعدادی که کاربر تقاضا کرده باشد، رشته‌هایی شامل هش مستقیم دریافت شده از IPFS، تاریخ، ساعت، یک عدد تصادفی و امضای بانک احراز کننده، تولیدشده و با کلید عمومی مشتری رمزگذاری می‌گردد. این رشته‌ها به‌صورت جداگانه داخل IPFS بارگذاری شده و برای هر یک به‌طور مستقل یک هش دریافت می‌شود که در اینجا "هش غیرمستقیم"[۲۳] نامیده شده است. بانک پس از دریافت هش‌های غیرمستقیم، تراکنش‌هایی به‌عنوان انتقال توکن KYC ایجاد کرده و هریک از هش‌های غیرمستقیم را در بخش یادداشت یکی از تراکنش‌ها قرار می‌دهد و به مشتری ارسال می‌کند. شبکه پس از پردازش تراکنش‌ها آن توکن‌ها را به‌حساب داخل دفتر کل توزیع‌شده مشتری انتقال می‌دهد. با هر توکن می‌توان به نام و هویت سازمان صادرکننده[۲۴] توکن، کلید عمومی کاربر، برچسب زمان، نوع توکن و هش غیرمستقیم اطلاعات اصلی مشتری دست پیدا کرد که به‌هیچ‌وجه حریم خصوصی مشتری را دچار مخاطره نخواهد ساخت.

---

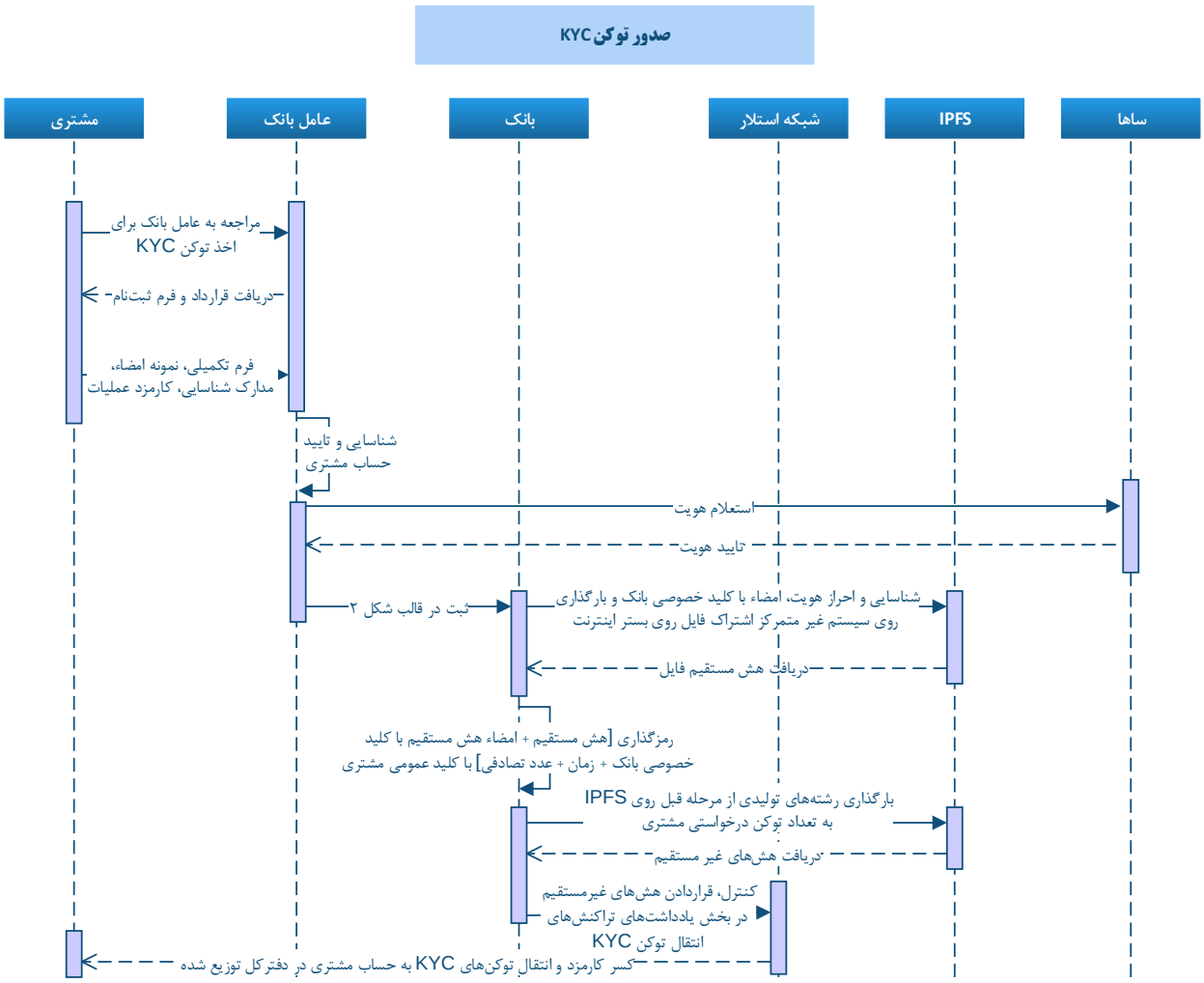
[۲۰] InterPlanetary File System

[۲۱] سامانه احراز هویت الکترونیکی

[۲۲] Direct Hash

[۲۳] Indirect Hash

[۲۴] Issuer



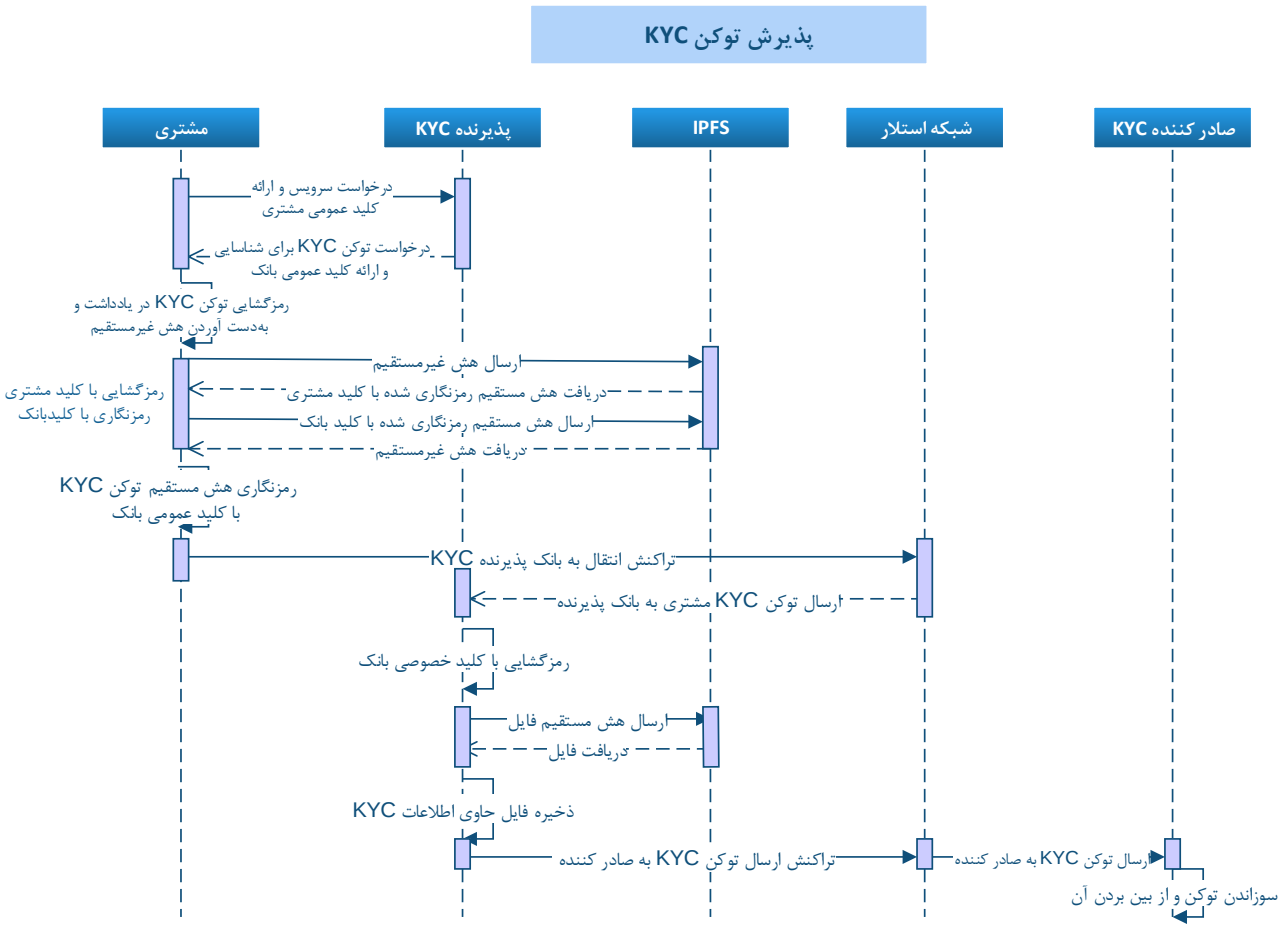
شکل ۱ – فرآیند صدور توکن شناسایی مشتری

شکل۲ – قالب ذخیره مدارک شناسایی مشتری

فرآیند پذیرش

مشتری با ارائه کلید عمومی خود به بانک‌ها و سازمان‌ها از آن‌ها درخواست خدمات می‌نماید، سپس بانک کلید عمومی خود را برای مشتری ارسال می‌کند تا مشتری بتواند توکن KYC را برای او رمزگذاری و ارسال نماید. مشتری توکن KYC موجود در یادداشت تراکنش که در حقیقت همان هش غیرمستقیم است را به IPFS ارسال کرده و هش مستقیم رمزگذاری شده با کلید خود را دریافت و رمزگشایی می‌کند. سپس آن را با کلید عمومی بانک پذیرنده، رمزگذاری نموده و در IPFS ثبت می‌کند و هش غیرمستقیم را از IPFS دریافت می‌کند و در قالب یادداشت تراکنش از طریق شبکه به بانک پذیرنده[۲۵] KYC می‌فرستد. بانک پس از دریافت توکن KYC آن را با کلید خصوصی‌اش رمزگشایی نموده و هش مستقیم فایل را به دست می‌آورد. پس‌ازآن با اخذ فایل حاوی اطلاعات KYC آن را شناسایی و در پایگاه داده خود ذخیره می‌نماید. درنهایت بانک پذیرنده طی تراکنشی توکن KYC را به صادرکننده ارسال نموده و صادرکننده آن را از بین برده یا به‌اصطلاح منجمد می‌کند. بدین ترتیب سازمان پذیرنده، مشتری را به رسمیت شناخته و خدمات موردنظر وی را در اختیارش قرار می‌دهد. در اینجا به‌منظور امنیت و جلوگیری از تخلف توسط بانک پذیرنده در قالب استفاده از هش و اطلاعات مشتری، توکن به‌گونه‌ای تعریف می‌شود تا تنها یک‌بار قابل‌مصرف بوده و پس از استفاده، منجمد و غیرقابل استفاده گردد.

[۲۵] Acquire



شکل ۳- فرآیند پذیرش توکن شناسایی مشتری

جمع‌بندی

در این مقاله روشی جهت شناسایی و ثبت ویژگی‌های مشتری بر بستر دفتر کل توزیع‌شده پیشنهاد داده شد که نه‌تنها برای بانک‌ها، بلکه برای کلیه نهادها و سازمان‌هایی که ملزم به شناسایی و ثبت اطلاعات مشتریان خود هستند کاربرد دارد. در این مدل، امکان انکار از هر یک از سه رکن صادرکننده، پذیرنده و مشتری سلب شده و تمامی تراکنش‌ها استناد پذیر و قابل‌ردیابی است. ازآنجاکه هر یک از این ارکان در هنگام ارسال تراکنش انتقال KYC آن را امضا کرده‌اند، لذا نمی‌توانند وقوع آن تراکنش را انکار کنند.

از دیگر سو، به دلیل امنیت بالای الگوریتم‌های رمزنگاری کلید عمومی، نگرانی‌های بانک و مشتری در خصوص افشای اطلاعات شخصی و نقض حریم خصوصی به‌کلی مرتفع می‌گردد. با توجه به دغدغه‌هایی که بانک‌ها در خصوص اطلاعات مشتریان خود دارند، چنانچه تراکنش‌های KYC یک بانک در دفتر کل توزیع‌شده ردیابی شود، صرفاً اطلاعات مربوط به کلید عمومی مشتریان قابل‌دسترسی است و هیچ‌چیزی در مورد هویت و مشخصات صاحب آن کلید عمومی قابل استحصال نمی‌باشد. ازنقطه‌نظر مشتری و حساسیتی که در حفظ اطلاعات خصوصی خود دارد نیز همین مسئله صدق می‌کند. اطلاعات مشتری صرفاً با ارائه، هش مستقیم قابل‌دستیابی است که به‌هیچ‌وجه و در هیچ مرحله‌ای از صدور و تبادل توکن KYC، این هش در شبکه ثبت یا منتقل نمی‌گردد. بلکه هش غیرمستقیم که توسط کلید بانک یا مشتری رمزگذاری شده است در تراکنش‌ها تبادل می‌شود.

از دیگر سو، با توجه به اینکه در مدل پیشنهادی فرصت‌های مناسبی برای کسب‌وکارهای مربوط به صدور و پذیرش توکن KYC پیش‌بینی‌شده است، می‌توان انتظار داشت که مدل‌های کسب‌وکار برای صادرکنندگی و پذیرندگی این توکن‌ها شکل گیرد. بدین‌صورت که بانک‌هایِ با شعب و مشتریان بیشتر در نقش صادرکننده، با دریافت کارمزد صدور، حجم زیادی از مشتریان را احراز هویت و شناسایی نمایند. در طرف دیگر، بانک‌هایی که تعداد شعب و مشتریان کمتری دارند، با پذیرش توکن‌های KYC صادرشده توسط این بانک‌ها به‌صورت حضوری یا اینترنتی، کمبود شعب خود را جبران کرده و بر دامنه مشتریان خود بیفزایند. توسعه‌ی این کسب‌وکار، قادر است که بانک‌ها را از تأسیس شعب جدید بی‌نیاز کرده و از دیگر سو، کسب‌وکار مناسبی برای شعب بانک‌های بزرگ به‌ویژه در مناطقی که سایر بانک‌ها کمتر شعبه دارند ایجاد نماید.

منابع

[1] B. Patel, "How can Blockchain Help with AML KYC," Finextra, 12 February 2018.

[2] G. W. Peters and E. Panayi, "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," Spring Link, 01 September 2016.

[3] J. Parra Moyano and O. Ross, "KYC Optimization Using Distributed Ledger Technology," *Springer Link*, 15 November 2017.

[۴] دستورالعمل شناسایی مشتریان ایرانی مؤسسات اعتباری، "آیین‌نامه اجرایی قانون مبارزه با پول‌شویی،" موضوع تصویب‌نامه شماره ۱۸۱۴۳۴ /ت ۴۳۱۸۲ ک مورخ۱۴ /۱۳۸۸/۹.

[5] www.stellar.org

[6] D. MAZIERES, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus," 2018. [Online whitepaper].

[7] "KYC LEGAL Blockchain Identity Verification", https://kyc.legal, November 24, 2017. [Online whitepaper]

[8] "SelfKey, The SelfKey Foundation", https://selfkey.org, September 11th 2017. [Online whitepaper]