سپیدنامه[1] شناسایی مشتری (KYC) ققنوس

خلاصه

بنیاد توسعه ققنوس تلاش دارد با بهره‌گیری از مزایای فناوری زنجیره‌بلوک و دفاتر کل توزیع‌شده، فرآیند الزامات قانونی بانک‌ها را مبنی بر شناسایی و احراز نهایی مشتری تسهیل نموده و مشکلات روند سنتی آن را مرتفع نماید. شناسایی مشتری در حال حاضر 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 سند 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[2]) یا سایر مشخصات توسط یک بانک، از مراجعه به سایر بانک‌ها به‌منظور انجام فرآیند شناسایی مشتری بی‌نیاز گردند. در این فرآیند تعدادی توکن KYC در اختیار مشتری قرار می‌گیرد 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 با 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.

ویرایش اول

بهمن ماه ۱۳۹۷

wp@kuknos.org

[1] WhitePaper
[2] Know Your Customer (KYC)

مقدمه

در دهه اخیر و به‌ویژه پس از پیدایش بیت‌کوین، فناوری دفتر کل توزیع‌شده[3] 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[4] 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.

در شبکه ققنوس، 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، مستغلات، خودرو و یا هر دارایی دیگر یک فرد را در این دفتر ثبت نمود.

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. دامنه محدود نوسان قیمت، سهولت ثبت تراکنش‌ها، امنیت اطلاعات، تغییرناپذیری و جهانروایی از مهمترین خصوصیات جذاب رمزارزهای با پشتوانه دارایی هستند که محمل مناسبی برای جذب سرمایه‌های خرد در بازارهایی با بازده بالا نظیر املاک و مستغلات ایجاد نموده‌اند.

مؤسسان بنیاد ققنوس ضمن اینکه بیش از ۹۰٪ از تراکنشهای مالی ایران از طریق زیرساخت‌های مالی آنها انجام می‌شود و با دارا بودن بیش از دوسوم از مشتریان موجود در نظام بانکی کشور با هدف ایجاد بستر تبادل دارایی‌ها مبتنی بر فناوری دفاتر کل توزیع‌شده اقدام به تولید و انتشار توکن شناسایی مشتری نموده‌اند.

در ادامه‌ی این طرح ابتدا تعاریف و توضیحاتی در خصوص الزامات مربوط به شناسایی مشتری و بیان مسأله آورده شده، سپس دفتر کل توزیع‌شده ققنوس به‌عنوان بستر پیاده‌سازی این فرآیند معرفی گردیده‌است. پس‌ازآن راه حل پیشنهادی به ارائه روشی نوین برای به اشتراک‌گذاری این فرآیند میان بانک‌ها و نهادهای مالی پرداخته است. نهایتاً پس از معماری بحث در خصوص فرصت‌ها و چالش‌های پیش رو و جمع‌بندی و دعوت به اقدام پایان‌بخش این سند خواهد بود.

[3] Distributed Ledger Technology
[4] Disruptive

تعاریف

- دفتر کل توزیع‌شده[5]: اجماعی بر داده‌های دیجیتال تکثیرشده، اشتراک‌گذاری شده و همگام‌سازی شده که در مکان‌های مختلف، کشورها یا بنگاه‌ها گسترده شده است. هیچ مدیریت یا ذخیره‌سازی متمرکزی بر این داده‌ها وجود ندارد. این دفتر بر اساس سازوکار تفاهم و معماری داده مورد قبول اعضای شبکه نگهداری و به‌روزرسانی می‌شود.
- بنیاد ققنوس: بنیاد ققنوس نهادی جمعی و غیرمتمرکز متشکل از میزبان‌های شبکه ققنوس است.
- شبکه ققنوس: یک شبکه از میزبان‌ها که با کمک فناوری دفتر کل توزیع شده نسبت به نظارت، صحت‌سنجی و ثبت کلیه تراکنش ها و عملیات کاربران خود اقدام میکند. شبکه ققنوس غیرمتمرکز و خودمختار است لذا به شخص حقیقی یا حقوقی تعلق ندارد. تمام مراودات آن بر پایه حق مالکیت اعضا بر دارایی‌های خود بوده و تصمیمات مربوط به راهبری شبکه ققنوس نیز بر اساس مکانیزم رای‌دهی میزبان‌ها خواهد بود.
- شرکت ققنوس: یک شرکت سهامی خاص که با هدف توسعه و تجاری‌سازی کسب‌وکارهای سهامداران خود بر بستر شبکه ققنوس، تاسیس شده است. این شرکت از نظر حقوقی مالک و یا از نظر فنی مدیر شبکه ققنوس نیست.
- میزبان: دو نوع میزبان در شبکه ققنوس وجود دارند که هر یک از آنها وظایف زیر را بر عهده خواهند داشت:
  - میزبان‌های ناظر:

    این میزبان‌ها امکان مشاهده تراکنش‌ها در شبکه را دارند و صرفاً به عنوان ناظر عملکرد شبکه فعالیت خواهندکرد. این نوع زیرساخت میزبانی صرفاً در اختیار رگولاتورهای محلی قرار خواهد گرفت.
  - میزبان‌های پردازنده:

    این میزبان‌ها کلیه فعالیت‌های میزبان‌های ناظر را انجام داده و همچنین در تهیه بسته پیشنهادی تراکنشهای قابل ثبت در دفتر کل و همچنین ساز و کار صحت‌سنجی و اجماع ققنوس برای ثبت تراکنش‌ها همکاری خواهند داشت. علاوه بر این این میزبان‌ها می‌توانند در رای‌دهی برای راهبری شبکه ققنوس مشارکت کرده و تراکنش‌ها را در آرشیو محلی خود ثبت و ذخیره کنند.
- توکنیزه کردن[6]: فرآیندی است که توسط یک میزبان انجام می‌شود و طی آن یک گواهی مالکیت دیجیتالی برای تمام یا بخشی از یک دارایی صادر می‌شود. میزبان صادر کننده، صحت و اعتبار آن گواهی را تضمین می‌کند.
- توکن دارایی[7]: یک گواهی دیجیتال است که توسط یک میزبان صادر شده و بر مالکیت دارنده‌ی توکن بر تمام یا بخشی از یک دارایی دلالت می‌کند.
- دارایی پایه[8]: یک دارایی که نقدشوندگی آن توسط تمام میزبان‌ها تضمین شده و جهت ارزش‌گذاری و تسهیل معاملات توکن‌های دارایی در شبکه ققنوس به کار می‌رود. همچنین از این دارایی دیجیتال برای پرداخت هزینه تراکنشهای درون شبکه نیز استفاده می‌گردد.

[5] Distributed Ledger Technology (DLT)

[6] Tokenization

[7] Asset Token

- زوج‌کلید[9]: مجموعه یک کلید خصوصی و یک کلید عمومی متناظر که برای دسترسی به حساب استفاده می‌شود، در شبکه ققنوس این زوج کلید بر اساس الگوریتم رمزنگاری ED25519 ساخته خواهد شد.
- تراکنش[10]: به مجموع یک یا چند عملیات گفته می‌شود که توسط یک میزبان، جهت پردازش و ثبت، به شبکه ققنوس اعلام می‌گردد و پس از اجماع توسط میزبانها، در دفتر کل ثبت می‌شود.
- ناشر[11]: یک حساب در شبکه ققنوس است که با حمایت یک میزبان پردازنده، می‌تواند توکن‌های دارایی را صادر کند، مشخصات ناشر و جزئیات مشخصات توکنهای دارایی صادر شده توسط میزبان پردازنده مرتبط، الزاماً در اینترنت منتشر می‌گردند.
- صرافی رمزارز توزیع شده[12]: فضایی است برای تبادل انواع دارایی ها که به صورت غیرمتمرکز بر روی شبکه ققنوس قرار دارد و هر یک از کاربران می‌توانند دارایی‌های خود را در آن با یکدیگر و یا با میزبان‌ها تبادل نمایند.
- کیف پول[13]: ابزاری برای مدیریت زوج کلید حسابهای کاربران است که از طریق آن مالکان کلیدها می‌توانند نسبت به نگهداری، ارسال و دریافت توکن‌های شبکه اقدام نمایند.
- عملیات: عملی در شبکه ققنوس است، که به تنهایی قابل ثبت در دفتر کل نیست و باید به همراه یک تراکنش شبکه ققنوس ثبت شود. عملیاتهای رایج در شبکه ققنوس می‌تواند آثار مالی و غیرمالی بر حسابهای ققنوس داشته باشد.
- پیمان: دارایی پایه شبکه ققنوس را پیمان می نامیم. هر پیمان دارای پشتوانه 30 سوت طلای 24 عیار خواهد بود.
- پیناتس: واحد خرد پیمان، پیناتس (Peanuts) نام دارد و مقدار آن 10^{-7} یک پیمان خواهد بود.
- توکن KYC : یک گواهی دیجیتال است که توسط یک میزبان تأییدشده صادر شده و بر مالکیت دارنده‌ی توکن بر هویت احراز شده خود دلالت دارد. این توکن به جهت سهولت در افتتاح حساب، به اشتراک‌گذاری هویت توسط خود مشتری، عدم انکارپذیری، حفظ حریم شخصی کاربر و به مراتب رعایت قوانین مبارزه با پولشویی در شبکه تولید و استفاده می‌گردد.

[8] Native Asset

[9] Key Pair

[10] Transaction

[11] Distributer

[12] Exchange

[13] Wallet

بیان مسأله و راه حل

مهمترین مسائل و چالش هایی که ققنوس در پی رفع آنهاست به شرح زیر است:

اجرای قوانین KYC و مبارزه با پولشویی

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.

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.

پایش رفتار مشتری و مدیریت ریسک

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.

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.

مالکیت مشتری بر هویت خود و دسترسی مستمر به آن

دغدغه اصلی این طرح 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.

تسهیل روند شناسایی مشتری با حفظ حداکثر امنیت

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.

حفظ حریم شخصی کاربر، به اشتراک‌گذاری هویت و انکارناپذیری

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 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[14] 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.

جزئیات راه حل

دفتر کل توزیع‌شده ققنوس

شبکه ققنوس[15] یک پروتکل منبع باز و غیرمتمرکز برای تولید و تبادل هر جفت رمزارز موجود در این شبکه است و بنیاد توسعه ققنوس[16] پشتیبانی می‌گردد.

شبکه ققنوس 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 ققنوس به هیچ نهاد واحدی بستگی ندارد. ایده این است که تعداد زیادی سرور در شبکه ققنوس مشارکت داشته باشند، به‌طوری‌که حتی اگر برخی از سرورها از دسترس خارج شوند، انتقال‌ها با موفقیت اجرا شود. همه سرورها به‌طور هماهنگ بر روی یک دفتر کل و بر اساس الگوریتم اجماع ققنوس[17] با یکدیگر پیش می‌روند.

احراز هویت در هسته[18] ققنوس صورت می‌گیرد و کار دشوار ارزیابی و تجمیع و توافق در وضعیت‌های مختلف هر تراکنش را بر اساس پروتکل اجماع ققنوس انجام می‌دهد. در ققنوس می‌توان برای ساخت یک شبکه قابل‌اعتماد و باثبات کنترل بیشتری روی گره‌هایی که به آن‌ها اعتماد کرده‌ایم، اعمال کنیم. بستر ققنوس شامل یک شبکه گسترده از میزبان‌ها[19] است که تولید، توزیع، صحت سنجی و ثبت تراکنش‌ها را بر عهده دارند و نرم‌افزارهای کیف پول، صرافی یا سایر خدمات آنلاین مبتنی بر ققنوس از طریق API های ارائه‌شده توسط زیرساخت، هورایزون[20] 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 ققنوس عمل می‌کنند. دارایی پایه[21] شبکه ققنوس پیمان[22] نام دارد و این شبکه علاوه بر پیمان، قابلیت ایجاد و انتشار هر نوع توکن[23] جدید را دارد.

در هر تراکنشی 4 رکن اساسی: حساب فرستنده، حساب گیرنده، نوع دارایی و امضا تراکنش ، بررسی و تأیید می‌گردد. هر تراکنش یک هزینه حداقلی یک صدهزارم پیمان را داراست که همین قضیه موجب جلوگیری از سربار زیاد بر روی شبکه

[14] Inter Planetary File System
[15] Kuknos
[16] Kuknos Development Foundation
[17] Kuknos Consensus Protocol
[18] Core
[19] Anchors
[20] Horizon
[21] Native Asset
[22] Paymon(PMN)
[23] Token

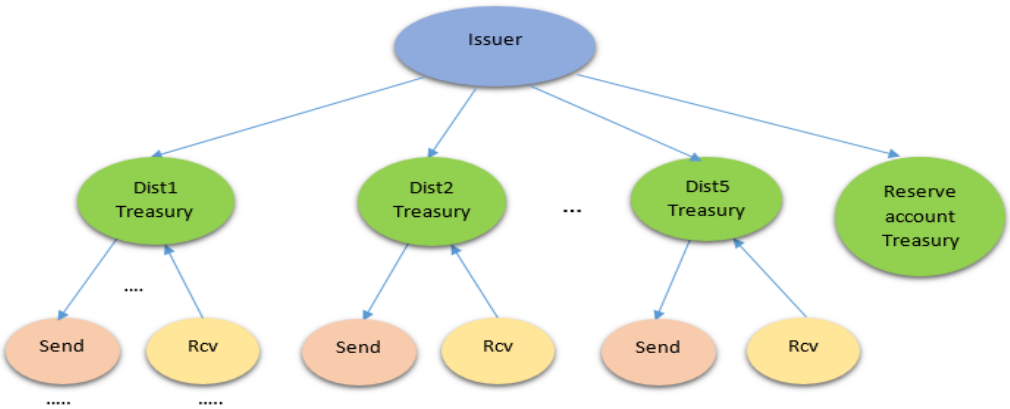
می‌شود. در تنظیمات حساب نیز می‌توان شرط رخداد تراکنش را بر اساس چند امضاء با وزن مشخص مانند امضاء بانک و مشتری و یا حساب قابل‌اطمینان اعلام‌شده از سوی مشتری قرار داد.

یکی از ارکان اصلی تراکنش، بخش یادداشت[24] 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.

معماری شبکه

نقش های فنی اعضای شبکه ققنوس

- میزبان ناشر: در شبکه ققنوس توکن‌های KYC ققنوس توسط این بنیاد به عنوان ناشر در حدود 100 میلیارد تولید و به مخازن میزبان‌های توزیع‌کننده و پذیرنده انتقال داده می‌شود.
- میزبان توزیع کننده و پذیرنده: هر میزبان توزیع کننده دارای دو حساب در شبکه ققنوس، یکی برای توزیع توکن KYC و یکی برای پذیرش آن ایجاد می نمایند. بدین ترتیب برای درخواست صدور توکن KYC کلید عمومی حساب توزیع‌کننده و برای پذیرش توکنKYC کلید عمومی حساب پذیرنده میزبان‌ها در اختیار مشتری قرار می‌گیرد.
- مخزن رزرو: سپس باقی مانده توکن‌ها در یک حساب به عنوان مخزن رزرو نگهداری شده تا به حساب میزبان‌هایی که در آینده به شبکه ققنوس می‌پیوندند واریز گردد. میزبان‌های آتی با رأی بیش از نیمی از اعضای بنیاد ققنوس برای مثال سه پنجم اعضا قادر به پیوستن به شبکه به عنوان میزبان خواهند بود.



[24] Memo

کاربران ققنوس

کاربران ققنوس می‌توانند از طریق هر یک از میزبان‌های شبکه ققنوس، به این شبکه متصل شده و بر اساس امکانات فراهم شده توسط آنها، اقدام به فعالیت نمایند. بدیهی است کاربران در هسته شبکه ققنوس بر اساس شماره حساب و امضاهای تعریف‌شده در آن حساب شناسایی می‌گردند و لذا صیانت از کلیدهای خصوصی کاربران توسط ایشان بسیار حائز اهمیت است. کاربران ققنوس به روش‌های زیر شناسایی می‌شوند که این امر خود سطوح KYC را برای کاربران آن به وجود می آورد. این روشها عبارتند از:

- آدرس ققنوسی معادل یک کلید عمومی که توسط یکی از میزبان‌ها فراهم می‌گردد.
- آدرس ایمیل تأیید شده برای یک کلید عمومی ققنوسی
- شماره تلفن همراه تأیید شده برای یک کلید عمومی ققنوسی
- احراز هویت حضوری در بانک برای یک کلید عمومی ققنوسی

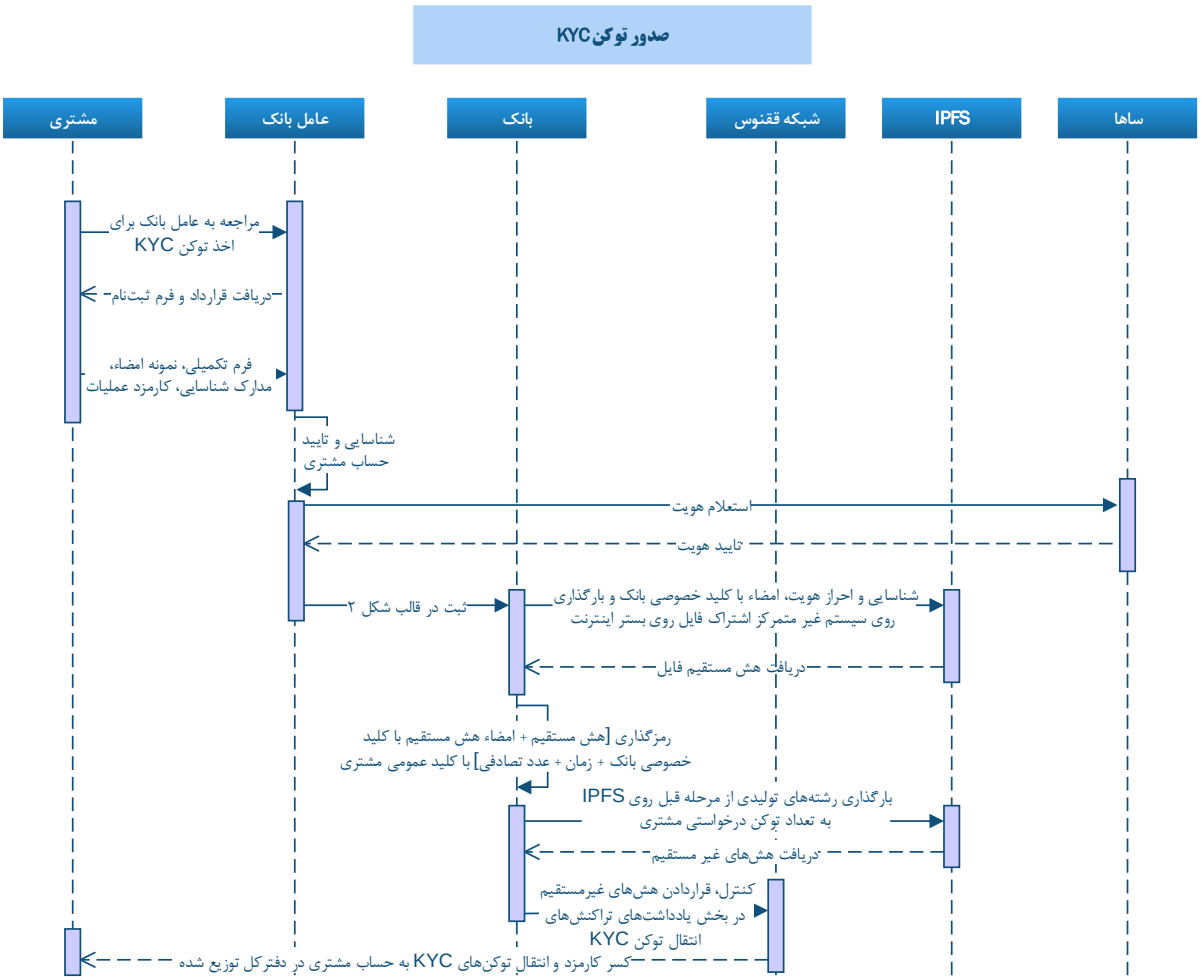
فرآیند صدور

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[25] استعلام می‌نماید. در صورت اخذ تأییدیه از ساها، اطلاعات کاربر در قالب ققنوس که در شکل 2 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"[26] 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"[27] 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[28] 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.

[25] سامانه احراز هویت الکترونیکی

[26] Direct Hash
[27] Indirect Hash
[28] Issuer



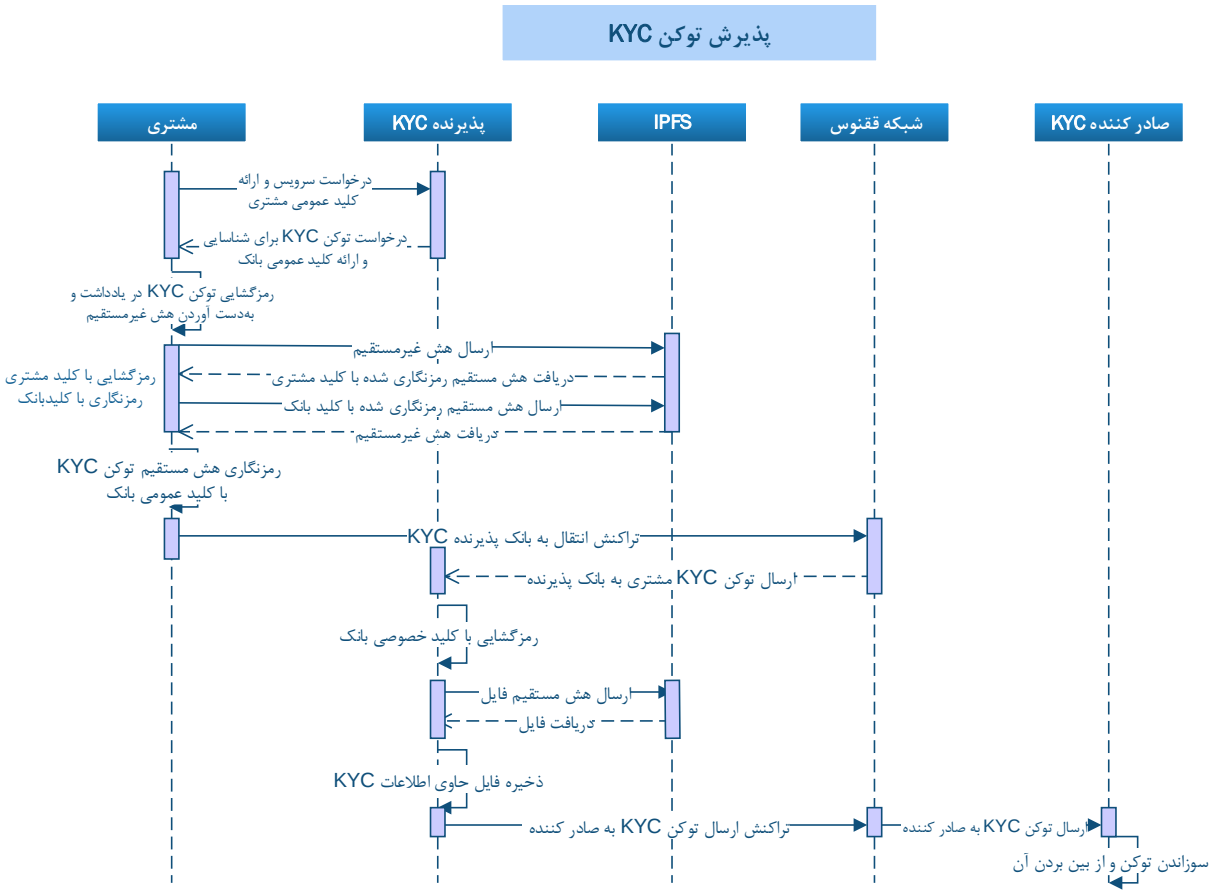
شکل 1 – فرآیند صدور توکن شناسایی مشتری

شکل2 – قالب ذخیره مدارک شناسایی مشتری ققنوس

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[29] 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.

[29] Acquire



شکل 3- فرآیند پذیرش توکن شناسایی مشتری

جمع‌بندی و دعوت به اقدام

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.