UniqueID

هویت دیجیتال غیرمتمرکز مبتنی بر شاخصه‌های
زیستی، هوش مصنوعی و گواهی‌های قابل اعتماد

پاییز ۱۳۹۶
uniqueid.network

۱ مقدمه

در این نوشتار روشی برای ثبت هویت واقعی افراد در بستر دیجیتال پیشنهاد می‌شود. هدف نهایی این طرح تخصیص یک هویت دیجیتال (که می‌تواند به صورت یک کلید رمزنگاری باشد) به هر فرد است به صورتی که: هیچ فردی نتواند بیش از یک هویت داشته باشد، سیستم غیرمتمرکز باشد و توسط کاربران کنترل شود و امنیت و حریم خصوصی لازم برای افراد فراهم شود. همچنین انگیزه لازم برای افراد برای شرکت در این سیستم و ثبت هویت خودشان به وجود آید. این طرح از بلاکچین به عنوان یک بستر برای انجام محاسبات، رسیدن به اجماع و برقراری ارتباط لازم میان افراد به صورت غیرمتمرکز بهره می‌برد.

۲ نیاز

وجود روشی برای ارتباط یک به یک میان هویت مجازی و هویت واقعی افراد، راه حلی برای بسیاری از چالش‌ها در دنیای دیجیتال و دنیای غیرمتمرکز است. اینترنت به عنوان یک بستر آزاد برای ارتباط میان انسان‌ها، همواره از وجود ربات‌ها ، هویت‌های تقلبی و اسپم رنج برده است. همچنین همه‌ی سیستم‌های غیرمتمرکز فعلی فاقد روشی مطمئن برای پخش کردن قدرت تصمیم گیری در فرآیند اجماع میان افراد هستند، و اکثرا از روش‌هایی مانند رای مبتنی بر قدرت محاسباتی (مانند بیتکوین) و یا رای مبتنی بر سرمایه (مانند کاردانو) هستند. بستری برای اتصال و تایید هویت مجازی افراد امکانات فراوانی از قبیل رای‌گیری غیرمتمرکز امن، تصمیم گیری و اجماع غیرمتمرکز، سیستم‌های اعتبارسنجی دیجیتال و سرویس‌های بانکی مبتنی بر بلاکچین فراهم می‌آورد.
همچنین هویت غیرمتمرکز، برخلاف همتای متمرکز خود امکان تسلط هر فرد بر داده‌های خود، هویت‌اش و نحوه تعامل وی با سایر نهادها را فراهم می‌آورد. این نگرش در مقابل جمع آوری داده‌ها توسط بنگاه‌های بزرگ اینترنتی و دولت قرار دارد و کاربر می‌تواند به انتخاب خود داده‌هایش را با دیگران به اشتراک بگذارد. مشکلاتی مانند دزدیده شدن هویت و یا گم شدن آن به راحتی توسط قراردادهای هوشمند قابل حل هستند. هم چنین در سال‌های اخیر بعضی بحث‌ها مبتنی بر تمرکز شبکه رمزارزها مطرح شده است. این تمرکز عموما به خاطر تمرکز استخراج کننده‌ها و یا تمرکز در ساختار تصمیم‌گیری این ارزها تولید می‌شود. برای شکستن تمرکز در این موارد باید از روش‌هایی مبتنی بر رای انسانی و دخالت مستقیم کاربران استفاده کرد. مشخصا در این روش‌ها نیاز به احراز هویت کاربران وجود خواهد داشت. بنابراین می‌توان گفت سیستم مطرح شده می‌تواند راهی به سوی عدم تمرکز باشد.

۳ معرفی UniqueID

کاربردها

کاربردهای بنیادین متنوعی برای سیستم تعیین هویت یکتای کاربران قابل تصور است که به بعضی از آن‌ها اشاره می‌شود. در این طرح ما سعی داریم این کاربردها را پیاده‌سازی نماییم.

- **رای گیری همگانی امن** سیستم‌های رای گیری (الکترونیکی و غیر آن) همواره دارای چالش‌هایی مانند احتمال تقلب، امنیت و تضمین گمنامی رای دهندگان بوده‌اند. با در دست داشتن یک بستر غیرمتمرکز حاوی هویت افراد، می‌توان یک رای گیری کاملا امن با الگوریتم‌های شناخته شده که امنیت و گمنامی تضمین شده خواهند داشت راه اندازی کرد. به این صورت امکان رای‌گیری‌های آنی توسط تک تک اعضا، یا نظرسنجی‌های قابل اعتماد و امضای نامه‌ها، بیانیه‌ها و سایر موارد به صورت دسته جمعی به وجود خواهد آمد.

- **درآمد پایه همگانی** درآمد پایه همگانی [۱] نوعی طرح اقتصادی برای تامین اجتماعی است که در سال‌های اخیر مورد توجه قرار گرفته است. این سیستم وجود نوعی از حداقل دستمزد برای همه‌ی اعضای جامعه را مطرح می‌کند که در آن هزینه کافی برای برخی از نیازهای پایه انسانی برای هر فرد تامین شود. با این وجود هیچ روش جهانی برای انجام این کار (به صورت بدون مرز) قابل تصور نیست و یا بسیار مشکل است. در بستر ما این کار به آسانی با تخصیص سکه‌های جدید به کاربران احراز هویت شده انجام می‌پذیرد.

- **اثبات انسان بودن [۲] برای سیستم‌های استخراج رمزارز**

بیشتر رمزارزهای کنونی مبتنی بر اثبات کار [۳] و یا اثبات سهم [۴] هستند که مشکلات خاص خود مانند مصرف انرژی بیش از حد، از دست رفتن عدم تمرکز و عدم مقیاس‌پذیری را دارا هستند. اثبات انسان یکتا روشی جدید برای به اجماع رسیدن برای پروتکل‌های بلاکچینی است. در این سیستم هرکس دارای یک رای برای انتخاب بلوک جدید خواهد بود که می‌تواند آن را به دیگران نیز انتقال دهد. به این ترتیب بلوک با بیشترین تعداد رای به عنوان بلوک جدید انتخاب خواهد شد.

- **سیستم نظارت و اختیارداری [۵] غیرمتمرکز**

یکی از مشکلات اصلی رمزارزها نحوه اداره آن‌ها و به روزرسانی نسخه‌های جدید آن‌ها هستند. به صورتی که یکی از داغ ترین ترندهای دنیای رمزارز در این چندسال بحث در مورد افزایش اندازه بلوک و یا سایر روش‌های مقیاس‌پذیری بوده است. راه اندازی یک سیستم نظارت و واگذاری تصمیم‌گیری در این موارد به کاربران می‌تواند تا حد زیادی به غیرمتمرکزسازی شبکه و حل و فصل این مباحث کمک نماید. همچنین امکان انتخاب نماینده‌هایی از طرف کاربران برای انجام کارهای مختلف قابل تصور است.

- **اعتبارسنجی مالی و اجتماعی** سیستم‌های اعتبارسنجی مالی و اجتماعی امروزه به طور گسترده‌ای مورد استفاده قرار می‌گیرند، اما اطلاعات آن‌ها فوق‌العاده انحصاری است و امکان سواستفاده ازین اطلاعات نیز وجود دارد. وجود یک سیستم اعتبارسنجی مالی برای دنیای رمزارزها ضروری به نظر می‌رسد. با توجه به هویت‌های یکتای کاربران و عدم امکان امحای آن‌ها امکان ایجاد چنین سیستمی وجود دارد. همچنین سیستم‌های اعتبارسنجی اجتماعی برای کاربردهایی مانند خبرنگاری، شبکه‌های اجتماعی، فروشنده‌ها و ... قابل استفاده هستند.

اجزای شبکه‌ی UniqueID

- **ادعا** هر کاربر جدید برای اینکه اثبات کند یک فرد جدید و یکتاست باید یک ادعا ارائه کند. ادعا می‌تواند یک شاخصه‌ی بیلوژیکی [۶] مثل اثرانگشت یا تصویر رگ‌های انگشت [۷] یا امضای صوتی فرد باشد. همچنین شاخه‌های غیر بیلوژیکی نظیر تصویر چهره یا هر اطلاعات یکتای دیگری که توسط فرد به راحتی قابل بازتولید باشد و همچنین بین همه‌ی افراد یکتا باشد می‌تواند به عنوان ادعا ارائه شود. انتخاب نوع این شاخصه یک پارامتر طراحی برای شکبه‌ی UniqueID است.

---

[۱] Universal Basic Income
[۲] Proof of unique individual
[۳] Proof of Work
[۴] Proof of Stake
[۵] Governance
[۶] Biometric
[۷] Finger vein picture

- **زیرساخت ذخیره‌سازی و محاسباتی غیرمتمرکز** شکبه‌ی UniqueID برای ذخیره اطلاعات مربوط به ادعاهای تایید شده و منتظر تایید از زیرساخت غیرمتمرکز دفتر غیرقابل تغییر [۸] (نظیر قراردادهای هوشمند در بستر Ethereum) و سرویس غیرمتمرکز ذخیره‌سازی [۹] (نظیر سرویس Storj) استفاده می‌کند. همچنین شبکه‌ی UniqueID برای اجرای موتور هوشمند تایید کننده که وظیفه‌ی اعتبار سنجی اولیه‌ی ادعاهای تایید نشده را دارد از سرویس پردازش غیرمتمرکز (نظیر سرویس Golem) استفاده می‌کند.

- **موتور هوشمند تائید کننده** موتور هوشمند تایید کننده یک سیستم خودکار غیرمتمرکز مبتی بر هوش مصنوعی است که با تحلیل ادعاهای تایید شده و ادعاهای منتظر تایید، از جدید و معتبر بودن ادعاهای جدید اطمینان حاصل می‌کند.

- **کاربر یکتای تاییدشده** [۱۰] کاربری که ادعای خود را در سیستم ثبت‌کرده‌اند و سپس توسط اعتبار سنج‌ها تایید شده‌اند، کاربر یکتای تایید شده نامیده می‌شود.

- **اعتبار سنج‌ها** وظیفه‌ی تایید ادعای کاربران جدید با اعتبار سنج‌هاست که کاربران یکتای تایید شده‌ای هستند که تمایل دارند در فرایند اعتبار سنجی همکاری کنند. هر کاربر یکتای تایید شده می‌تواند در فرایند اعتبارسنجی و تایید کاربران جدید نقش داشته باشد. برای افزایش بهره‌وری و مقیاس‌پذیری سیستم در UniqueID هر کابر می‌تواند برای تایید کاربران جدید به یک کاربر دلخواه وکالت [۱۱] بدهد. کاربرانی که در فرایند اعتبار سنجی مشارکت دارند به عنوان جایزه توکن ID می‌گیرند که توکن داخلی شبکه‌ی UniqueID است.

- **آغاز به کار قابل اعتماد** [۱۲] یک مسئله‌ی اساسی در طراحی شبکه‌ی UniqueID اطمینان به نقطه‌ی آغازین شبکه و کاربران یکتای تایید شده‌ی اولیه‌ی آن است. برای دست‌یابی به یک مجموعه‌ی اولیه از کاربران که به احتمال بسیار بالا افراد یکتا هستند، در ابتدا شبکه‌ی UniqueID به هر کابر تعداد زیادی مسئله‌ی سخت متفاوت نظیر Captcha می‌دهد، به طوری که یک نفر توان حل کردن دو مسئله را در زمان محدود نداشته باشد. کاربرانی که به همه‌ی مسئله‌ها در زمان محدود پاسخ درست داده‌اند به صورت اولیه تایید می‌شوند. سپس در مرحله‌ی بعدی کاربرانی که تایید اولیه شده‌اند باید تایید تعداد قابل قبولی از همتاهای خود را بگیرند تا به عنوان یک کاربرا یکتای تایید شده وارد سیستم شوند.

- **ID توکن** توکن داخلی شبکه‌ی UniqueID که با ورود هرکاربر یکتای جدید تولید می‌شود و به عنوان انگیزه‌ی ورود به سیستم و همچنین مشارکت در فرایند اعتبار سنجی کاربرد دارد. همچنین پیاده‌سازی کاربردهایی مثل درآمد پایه‌ی همگانی با استفاده از توکن ID ممکن است.

- **نرم‌افزار کاربر نهایی** [۱۳] نرم‌افزار کاربر نهایی UniqueID امکاناتی نظیر مدیریت حساب توکن ID و انتقال آن و همچنین امکاناتی نظیر ثبت ادعای جدید و انجام فرایند اعتبار سنجی را فراهم می‌کند.

معماری شبکه

در این بخش نحوه ارتباط اجزای شبکه با یک دیگر و به طور خلاصه جریان تایید هویت یک کاربر از ابتدا تا هنگام در دست داشتن هویت خود توضیح داده می‌شود.

[۸] decentralised immutable ledger
[۹] Decentralised storage service
[۱۰] Certified unique individual
[۱۱] delegation
[۱۲] trustless setup
[۱۳] end user application

در ابتدا کاربر پس از نصب نرم‌افزار مورد نظر، اقدام به ایجاد مشخصه‌ی بیولوژیکی مشخصی می‌نماید، به عنوان مثال در سیستم از او خواسته می‌شود جمله مشخصی را با صدای خود ضبط نماید. این مشخصه، در سرویس حافظه مورد نظر ضبط می‌شود و سپس محاسبات لازم بر آن توسط موتور هوش مصنوعی (با استفاده از سرویس محاسبه قابل تایید) انجام می‌شود. به این صورت از جدید بودن کاربر اطمینان حاصل می‌شود.

برای اطمینان از معتبر بودن کاربر موردنظر، در این مرحله تعداد مشخصی از اعتبارسنج‌ها به وی تخصیص داده می‌شود و کاربر باید با برقراری ارتباط مستقیم با اعتبارسنج‌ها، «گواهی» های کافی کسب کند. این گواهی‌ها حاوی تایید ادعای بیولوژیکی مطرح شده توسط کاربر هستند، و در واقع اعتبارسنج‌ها تایید می‌کنند که فرد موردنظر دارای همان اطلاعات زیستی قرارداده شده بر روی بلاکچین است.

در صورت تایید شدن کاربر، او به یک کاربر یکتای تایید شده تبدیل می‌شود که می‌تواند به سرویس‌های مختلفی که در شبکه وجود دارند دسترسی پیدا کند. همچنین برای تشویق کاربران اولیه به ثبت‌نام و گسترش شبکه، تعداد مشخصی توکن به آن‌ها داده می‌شود که با ثبت‌نام کاربران بیشتر، این عدد کمتر می‌شود (و به این صورت افراد انگیزه بیشتری برای شرکت کردن اولیه در سیستم خواهند داشت).

همچنین سازوکار دقیقی برای تخصیص اعتماد و ارتباط کاربران وجود دارد که از ریسک‌ها و خطرات احتمالی مانند ثبت نام دوباره، تولید تعداد زیادی ID تقلبی و جلوگیری از ورود یک کاربرخاص جلوگیری نمود. همچنین سیستم اختیارداری پیشنهاد شده می‌تواند شامل انتخاب نماینده‌هایی توسط کاربران برای رسیدگی به اشتباهات احتمالی به صورت شفاف باشد.