مکانیسم Proof of Personhood چیست؟

مکانیسم Proof of Personhood به زبان ساده به معنای ایجاد یک سری قوانین و پروتکل‌ها در شبکه‌های بلاکچینی مالی است که به ما کمک می‌کند هویت‌های جعلی را از هویت‌های واقعی انسانی تمایز دهیم. وقتی تمرکززدایی و تقسیم حق تصمیم بین کاربران معیار اعتماد در یک فضای اینترنتی می‌شود، این مسئله اهمیت بیشتری پیدا می‌کند که تشخیص دهیم پشت هر کاربر تصمیم گیرنده که با استفاده از یک دستگاه هوشمند به شبکه متصل است واقعا چه کسی نشسته؟ آیا رای‌های صادر شده از سوی این کاربر واقعا تصمیمات یک انسان واقعی است و یا عملیاتی است که توسط ربات برنامه نویسی شده به منظور انجام یک هدف خاص به شبکه ارسال شده است؟

تشخیص چنین مسئله‌ای در شبکه‌های مالی اهمیت بسیار بالایی دارد؛ به این ترتیب مکانیسم **Proof of Personhood** به کمک توسعه دهندگان آمده است. این مکانیسم در پروژه‌های زیادی به روش‌های گوناگون پیاده سازی شده است. همین مسئله سبب شده کاربران به اجبار برای عضویت هرچه بهتر در شبکه‌های مالی، از یکی از پروتکل‌های مکانیسم Proof of Personhood رد شوند. پس اگر قصد دارید فعالیت‌های بیشتری در بلاکچین‌های مختلف مخصوصا بلاکچین اتریوم انجام دهید خوب است با هم بر مفهوم مکانیسم Proof of Personhood و همچنین مزایا و معایب و پروژه‌های پشتیبان این طرح مروری داشته باشیم.

مکانیسم Proof of Personhood چیست؟

مکانیسم Proof of Personhood که در زبان فارسی به نام **مکانسیم اثبات شخصیت** شناخته می‌شود، یکی از فناوری‌هایی است که در بستر شبکه‌های بلاکچینی راه اندازی شده تا مشخص شود آیا حساب‌های ساخته شده کاربر واقعی و انسانی دارند یا نه؟ فرآیند احراز هویت واقعی کاربران حوزه بازارهای مالی و هر زمینه‌ای که در آن از بلاکچین استفاده می‌شود بسیار دشوار است؛ چرا که هر سازمان یا فردی که کمی از نفوذ برخوردار باشد با تجهیز دستگاه‌های هوشمند در بازار عضو می‌شود و به واسطه این دستگاه‌ها، رای‌هایی را صادر می‌کند که شاید تنها به نفع خود اوست و به شبکه آسیب می‌زند.
به همین ترتیب توسعه دهندگان این فضای آنلاین درصدد این بودند که با استفاده از ایجاد یک سری پروتکل‌ها و قوانین در فناوری این شبکه‌ها، هویت کاربران را مشخص کنند و به انسانی و واقعی بودن آن‌ها پی ببرند. در این صورت هر تصمیمی که در شبکه اتخاذ شود نظر حقیقی عموم کاربران است. با چنین پروتکل‌ها و قوانینی کلاهبرداران برای اینکه بخواهند بر شبکه مسلط شوند نیاز دارند اشخاص حقیقی را برای ورود به شبکه استخدام کنند و یا از هدف خود برگردند! **PoP** یا پروتکل اثبات شخصیت برای شبکه‌های همتا به همتا که بر اساس بلوک‌های رای دهی بزرگ و سیاست‌های دموکراتیک کار می‌کنند بسیار مناسب است و هم اکنون هم رده دیگر الگوریتم‌های اجماع مانند اثبات کار، اثبات سهام و غیره فعالیت می‌کند.

کاربرد مکانیسم Proof of Personhood چیست؟

مکانیسم Proof of Personhood برای شبکه از جهات مختلفی کاربردی تلقی شود؛ اما اصلی‌ترین کاربرد این مکانیسم جلوگیری از **حملات سیبل** یا **Sybil Attacks** است. این نوع حملات اصلی‌ترین انواع حمله‌ای هستند که شبکه‌های بلاکچینی را مورد هدف قرار می‌دهند. همه کاربران عضو شبکه‌های مالی غیرمتمرکز می‌دانند که کنترل و مسئولیت هدایت یک شبکه و بازار به عهده تمام اعضای آن است. از آنجا که هیچ ارگانی به‌عنوان ناظر بر شبکه تسلط ندارد. به این ترتیب اگر قرار است یک حرکت سودجویانه یا غیرمجاز در شبکه صورت بگیرد باید بخش زیادی از کاربران به‌صورت متفق القول بر سر آن مسئله رای دهند. همین موضوع سبب می‌شود که کلاهبرداران با ایجاد اکانت‌های فیک سعی کنند شمار رای‌های مفید و غیر مفید را به‌صورت غیر قانونی و به نفع خود عوض کنند. به این ترتیب مهم است از یک مکانیسم پیشرفته بهره بگیریم تا از ایجاد اکانت‌های فیک و ورود آن‌ها به شبکه و حتی تصمیم‌گیری جلوگیری کنیم. این فرآیند دقیقا کاربرد مکانیسم Proof of Personhood را به تصویر می‌کشد. مکانیسم Proof of Personhood

در شبکه اجرا می‌شود تا سودجویان نتوانند اجتماعاتی تحت تسلط خود در بازار تشکیل دهند و به کمک رای آن‌ها، به نفع خود شبکه را مدیریت کنند.

مزایا و معایب مکانیسم Proof of Personhood

مانند هر مکانیسم دیگری مکانیسم Proof of Personhood نیز ممکن است برای شبکه مزایا و معایبی را به همراه داشته باشد. از **مزایای** این فناوری برای اثبات شخصیت کاربران در شبکه می‌توان به موارد زیر اشاره کرد:

- مکانیسم Proof of Personhood به شبکه کمک می‌کند در مقابل حملات سیبل که بر پایه هویت جعلی اتفاق می‌افتد ایستادگی کند و شبکه را سالم نگه می‌دارد.
- این مکانیسم به کاربران کمک می‌کند در شرایط عادلانه‌تری نسبت به تصمیم گیری‌های مهم شبکه رای دهند و رای آن‌ها به سمتی خاص هدایت نشود.
- با استفاده از این مکانیسم می‌توان مطمئن بود که هر تصمیم در شبکه بر اساس تفکرات یک انسان واقعی اتخاذ شده و هیچ ارگان یا سازمانی بر آن نظارت ندارد.

در مقابل و در کنار مزایایی که مکانیسم of Personhood Proof به شبکه ارائه کرده چالش‌هایی را نیز به همراه آورده که ممکن است به مذاق برخی‌ها خوش نیاید. از **معایب** PoP می‌توان موارد زیر را نام برد:

- برای دستگاه‌ها و زیرساخت‌های فنی و سخت افزاری که عمل احراز هویت را انجام می‌دهند عموما دسترسی راحتی وجود ندارد و همه کاربران نمی‌توانند در محل مربوطه حاضر شوند.
- در روند احراز هویت کاربران مجبورند اطلاعاتی را به شبکه اعلام کنند که حریم خصوصی آن‌ها را کاهش می‌دهد.
- برای اینکه بتوان مکان‌های زیادی را با زیرساخت‌های فنی احراز هویت تجهیز کرد هزینه بسیار زیادی لازم است.

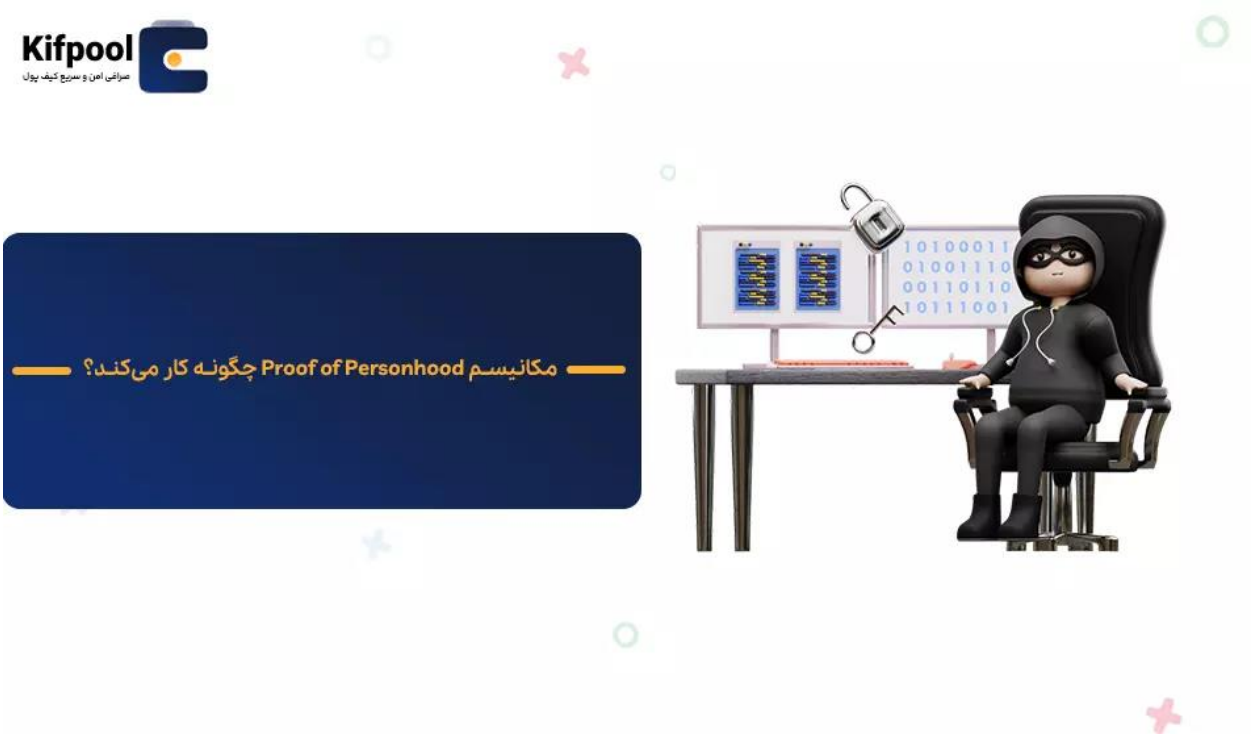
مطلب پیشنهادی: ممو آیدی تراکنشات بلاک چین چیست؟

چرا مکانیسم Proof of Personhood ایجاد شد؟

دلیل ایجاد مکانیسمی مثل مکانیسم Proof of Personhood برمی‌گردد به خطراتی که در سالیان اخیر سلامت شبکه را تهدید کرده است. حملات سیبل برای دهه‌های متمادی یک چالش اساسی برای سیستم‌های توزیع شده کامپیوتری که به‌صورت شبکه‌ای با هم در ارتباط بودند به حساب می‌آمد. برای جلوگیری از چنین حمله‌هایی تدابیر زیادی اندیشیده شد که یکی از آن‌ها **فناوری کپچا (CAPTCHA)** بود. همه ما با CAPTCHAها که امروزه به‌صورت تصویری یا ترکیبی از عدد و حروف در وبسایت ها و سیستم‌های مختلف مورد استفاده قرار می‌گیرند آشنایی داریم. حتما برای شما هم پیش آمده که سیستم بخواهد ثابت کنید ربات نیستید.
این فناوری تا مدتی پاسخگوی نیاز امنیتی شبکه‌ها بود و می‌توانست انسان‌ها را از ربات‌ها و ماشین‌هایی که درخواستی را به سیستم می‌فرستادند و عموما مخرب بودند تمایز بخشد؛ اما با پیشرفت هوش مصنوعی و فناوری‌های تشخیص تصویر CAPTCHAها نیاز ما را برطرف نمی‌کردند. همچنین علاوه بر هوش مصنوعی، کاربرانی که ضعف و اختلال بینایی داشتند و یا اختلال یادگیری داشتند نیز با این مسئله به مشکل برمی‌خوردند و نمی‌توانستند به خوبی CAPTCHAها را تشخیص دهند. از طرفی با بروز چنین موانعی این امکان وجود داشت که سیستم‌های توزیع شده از یک ارگان یا سازمان در جهت احراز هویت کاربران کمک بخواهند؛ اما در نهایت نظارت این سازمان‌ها باعث می‌شد هویت کاربران و حریم خصوصی آن‌ها در خطر باشد که این مورد نیز با اصول و اهداف شبکه‌های مالی در تناقض بود.
به این ترتیب با وجود چنین مسائلی کم کم توسعه دهندگان به فکر ایجاد مکانیسمی افتادند

که بدون به خطر انداختن هویت فرد، بتوان او را در شبکه به‌عنوان یک نود مورد اعتماد شناسایی کرد. در ابتدا رویکردی پیشنهاد شد که در آن اعتبارنامه‌های ناشناس به ازای هر نفر در سیستم توزیع شده پخش می‌شد و هر حزب یا نفر می‌توانست با اسم مستعار در رویدادهای حضوری شرکت کند و به این ترتیب کاربران می‌توانستند به‌صورت فیزیکی احراز هویت شوند. در نهایت ویتالیک بوترین در سال 2014 مسئله منحصربه‌فرد بودن کاربران شبکه‌های توزیع شده را مطرح کرد و در سال 2017 اصطلاح مکانیسم Proof of Personhood که یکی از زیرمجموعه‌هایش رویکرد رویداد حضوری مبتنی بر نام مستعار بود ایجاد شد.

مکانیسم Proof of Personhood چگونه کار می‌کند؟



مکانیسم Proof of Personhood سازوکار مشخصی ندارد و از روش‌های متعددی در جهت احراز هویت کاربران استفاده می‌کند. به عبارت دیگر این مکانیسم ممکن است نسبت به پروژه‌های مختلف و ذات عملکرد آن‌ها با روش‌های متعددی به جنگ کلاهبرداران و سود جویان برود؛ اما نکته‌ای که مشخص است این است که مکانیسم Proof of Personhood در هر روش تلاش می‌کند در مقابل قدرت هوش مصنوعی و حملات سیبل بایستد.

روش‌های گوناگونی مانند احراز هویت بیومتریک، مکانیسم اثبات دانش صفر، احراز هویت فیزیکی، پروتکل‌های هویت غیرمتمرکز و غیره در مکانیسم Proof of Personhood مورد

استفاده قرار می‌گیرند هرچند به عقیده وتالیک بوترین که **خالق رمزارز اتریوم** است، این کار فقط می‌تواند در دو روش احراز هویت بیومتریک و احراز هویت مبتنی بر گراف اجتماعی به‌صورت صحیح صورت بگیرد. در این بخش به برخی از روش های احراز هویت شخصی کاربران در مکانیسم Proof of Personhood اشاره می‌کنیم:

احراز هویت بیومتریک

انسان موجودی است که شاخص‌های زیستی او نسبت به دیگر هم نوعانش یکتا و منحصربه‌فرد است و از قدیم‌الایام این شاخص‌ها همواره معیاری برای تمایز بخشیدن او نسبت به دیگران و همچنین کلید مباحث امنیتی بوده است. یکی از روش‌های مکانیسم Proof of Personhood نیز همین است؛ یعنی ما به روش‌های مختلف از بیومتریک انسان‌ها استفاده می‌کنیم تا آن‌ها را در شبکه نسبت به دیگری تمایز بخشیم. بخشی از شاخص‌های بیومتریک شامل اثر انگشت، عنبیه چشم، چهره و غیره هستند که هر کدام با اسکن شدن می‌توانند داده‌های منحصربه‌فردی را برای ما تولید کنند. این روش چندان عجیب نیست و همه انسان‌ها حداقل در یک مورد از این ویژگی‌های زیستی به‌عنوان کلید عبور استفاده می‌کنند؛ مانند زمانی که گوشی موبایل را برای اسکن چهره و باز شدن قفل جلوی صورت خود می‌گیرید.

مکانیسم اثبات دانش صفر

اثبات دانش صفر (Zero-knowledge proof) یکی دیگر از روش‌های مکانیسم Proof of Personhood است که به نظر می‌رسد منطقی‌تر از روش‌های دیگر باشد! در این روش از احراز هویت نیاز نیست کاربر کلیه اطلاعات شخصی خود را به شبکه معرفی کند؛ بلکه می‌تواند تنها برخی خصوصیات شخصی مانند سن، ملیت و غیره را آشکار سازد. هدف از این کار این است که کاربر در عین اینکه حریم خصوصی خود را حفظ می‌کند، در شبکه به‌عنوان یک کاربر منحصربه‌فرد و واقعی شناخته شود. این روش به نام روش اثبات هیچ آگاهی نیز شناخته می‌شود.

احراز هویت فیزیکی

احراز هویت فیزیکی اولین روشی بود که به ذهن توسعه‌دهندگان رسید. در این روش از احراز هویت مکانیسمProof of Personhood قرار شد که احزاب و افراد با نام مستعار در مکانی که به‌صورت تصادفی انتخاب می‌شد حضور پیدا کنند. این عمل به‌صورت دوره‌ای انجام می‌شد و نیاز نداشت که حضار در این مسئله احراز هویت کامل شوند و با استفاده از نام‌های مستعار برای شناسایی آن‌ها در شبکه یک توکن یک نفره خاص یا حتی NFT ایجاد می‌شد. یکی از پروژه‌هایی که از این روش استفاده می‌کرد پروژه **Encointer** نام داشت که می‌خواست این حضور فیزیکی را به‌صورت گروه‌های کوچک ولی همزمان در مکان‌های مختلف راه اندازی کند. از معایبی که این

روش نسبت به روش‌های دیگر مکانیسم Proof of Personhood دارد، ناراحتی کاربرانی بود که مجبور بودند در زمان و مکانی خاص حضور پیدا کنند؛ حال آنکه ممکن بود برخی از آن‌ها بر سر مسئولیت‌های روزمره بسیار مهم‌تر باشند. از دیگر اشکالات این روش این است که ایجاد یک گروه و مجموعه برای سازماندهی تمام این مهمانی‌ها به‌صورت همزمان کار سختی است؛ مخصوصا وقتی به هر گروه اجازه می‌دهد درباره گروه‌های دیگر تاییدیه صادر کنند.

مکانیسم مبتنی بر گراف اجتماعی

گراف اجتماعی Social Graph اشاره به یک سیستم ضمانت دارد. در این نوع سیستم اگر یک نود بخواهد به‌عنوان کاربر واقعی و انسانی شناخته شود باید نودهای دیگری که قبلا شخصیت واقعی آن‌ها اثبات شده برای این نود ضمانت ارائه دهند؛ برای مثال فرض کنید شخص A، B و C در شبکه به‌عنوان یک کاربر واقعی شناخته می‌شوند. اگر کاربر D نیز بخواهد به شبکه به‌عنوان نود اضافه شود، سه کاربر قبلی باید او را تایید کنند. به این ترتیب این روند به‌صورت سلسله وار ادامه می‌یابد تا اعضای شبکه بیشتر شود. همچنین در این نوع مکانیسم که زیر مجموعه مکانیسم Personhood Proof of است، تشویق و تنبیه‌هایی برای فعالیت صحیح و غیر صحیح در نظر گرفته می‌شود. به این صورت که اگر شما به‌عنوان کاربر یک کاربر دیگر را تایید کردید، اما کاربر تایید شده به هر نحوی یک نود غیرواقعی از آب دربیاید، شما هم به همراه تمام کسانی که این نود را تایید کرده‌اند جریمه خواهید شد.

مطلب پیشنهادی: کریپتوگرافی (Cryptography) چیست؟

کدام پروژه ها از مکانیسم اثبات شخصیت استفاده می‌کنند؟

به نظر می‌رسد به مرور زمان مکانیسم Proof of Personhood در حال تبدیل شدن به یکی از روش‌های اصلی ورود به دنیای سیستم‌های توزیع شده مخصوصا شبکه‌های مالی غیرمتمرکز است. از آنجایی که هرروزه تعداد بیشتری از پروژه‌های ایجاد شده تلاش می‌کنند به نحوی پروتکل‌های اثبات شخصیت را در بستر خود پیاده سازی کنند. در این بخش به چند مورد از مهم‌ترین پروژه‌های دنیای مجازی که در زمینه رمزارزها فعال هستند و از مکانیسم Proof of Personhood استفاده می‌کنند اشاره می‌کنیم:

ورلد کوین (Worldcoin)

ورلد کوین یکی از مهم‌ترین پروژه‌هایی است که در دستور کار خود استفاده از مکانیسم Proof of Personhood را قرار داده است. در این پروژه کابران باید از **روش‌های بیومتریکی** استفاده کنند و با مراجعه به مراکز احراز هویت، توسط دستگاهی به نام دستگاه Orbe به‌صورت حضوری برررسی شوند. در این روند دستگاه عنبیه چشم کاربران را اسکن می‌کند و یک دیتای منحصر به فرد درباره آن‌ها ثبت می‌شود. سپس برای هر کاربری که با موفقیت احراز هویت می‌شود می‌توان یک World ID ثبت کرد تا در شبکه شناخته شود. ورلد کوین یک پروژه رمزنگاری شده است که توسط مدیر عامل گروه OpenAI یعنی سم آلتمن ایجاد شده و از این راه برای اثبات شخصیت

بهره می‌گیرد؛ اما بسیاری از تحلیلگران معتقدند با پیش گرفتن مکانیسم Proof of Personhood دیری نمی‌پاید که ورلدکوین شکست می‌خورد!

پروف آو هیومنیتی (Proof of Humanity)

سخت‌گیرترین پروژه‌ای که در حال حاضر مشغول راه اندازی پروتکل‌های جدی در خصوص مکانیسم Proof of Personhood است، پروژه **Proof of Humanity** نام دارد. همان طور که از نام پروژه (اثبات انسانیت) نیز مشخص است، توسعه دهندگان آن حساسیت بیشتری روی فرآیند احراز هویت دارند. در ابتدای مسیر، کاربر باید یک ویدیو از خودش در شبکه آپلود کرده و مقداری از توکن‌های پروژه را به‌صورت سپرده در شبکه قفل کند. بعد از این کار، فرد برای تکمیل احراز هویت خود باید کاربر دیگری را برای ضمانت خود معرفی کند. بعد از اینکه کاربران دیگر این نود را تایید کردند، تازه نوبت به سپری کردن یک دوره آزمایشی می‌رسد. این پروژه برای خود یک دادگاه مجازی دارد که نام آن Kleros است. در کلروس منوال بر این است که کاربران دیگر تلاش کنند شما را به چالش بکشند تا هویت شما به‌صورت قطعی اثبات شود. اگر بعد از مراحل متعدد به هر طریقی ثابت شود که ویدیو آپلود شده شما واقعی نیست، تمام سرمایه‌ای که در شبکه سپرده‌گذاری کرده بودید از شما سلب می‌شود و کاربری که شما را به چالش کشیده و غیرواقعی بودن شما را علنی کرده از شبکه پاداش دریافت می‌کند.

سیویک پس (Civic Pass)

پروژه بعدی که تلاش می‌کند اصول مکانیسم Proof of Personhood را پیاده سازی کند، **سیویک پس** نام دارد. این پروژه به نوعی یک پاسپورت برای کاربران در سطح شبکه ایجاد می‌کند که به او اجازه می‌دهد با استفاده از آن در محیط‌هایweb3 و DeFi به راحتی تراکنش انجام دهد و به‌عنوان یک نود واقعی شناخته شود. به نظر می‌رسد این پروژه در گامی جلوتر از بقیه ایستاده؛ چرا که خدمات مرتبط با احراز هویت را هم روی بلاکچین و هم خارج از زنجیره به افراد متعددی نظیر کسب‌وکارها، توسعه دهندگان پروژه‌ها و همچنین کاربران عادی ارائه می‌دهد. سیویک با این روش از رویکری نوین در شبکه بهره می‌برد.

آیدنا (Idena)

یکی دیگر از پروژه‌هایی که سعی می‌کند رسالت مکانیسم Proof of Personhood را اجرا کند، آیدنا نام دارد. این پروژه که مرتبط با یک بازی است از **سیستم کپچا** برای این احراز هویت بهره می‌برد. البته روش این پروژه بسیار متفاوت است و کاربران برای احراز هویت باید در زمانی خاص نسبت به حل برخی کپچاها آماده باشند که خود این کپچاها برای احراز هویت کاربران دیگر مورد

استفاده قرار می‌گیرند. آیدنا برای اینکه از حضور افراد تکراری با دستگاه‌ها و شناسه‌های متفاوت در شبکه جلوگیری کند از این روش بهره می‌برد.

گیت کوین پاسپورت (Gitcoin Passport)

گیت کوین پاسپورت نیز از دیگر نام‌هایی است که باید آن را در گروه پروژه‌هایی که از مکانیسم Proof of Personhood استفاده می‌کنند آورد. این پروژه در اصل زحمت دریافت اطلاعات از کاربر را به خود نمی‌دهد و به اطلاعاتی که درباره هر نود در شبکه از قبل موجود است اکتفا می‌کند. این پروژه اطلاعات هر کاربر که در فضای web2 و web3 قرار دارد استخراج می‌کند و با استفاده از آن‌ها کارت شناسایی دیجیتالی تولید می‌کند که به کاربر اجازه می‌دهد در سراسر شبکه به‌عنوان یک نود واقعی و قابل اعتماد حضور پیدا کند.

سرکلز (Circles)

سرکلز از آن دسته پروژه‌هایی است که از گراف اجتماعی برای احراز هویت مکانیسم Proof of Personhood استفاده می‌کند. روش کار این پروژه بسیار ساده است و کاربران برای احراز هویت در آن تنها نیاز به تعدادی کاربر دارند که از قبل در شبکه احراز هویت شده باشند و واقعی و انسان بودن نود جدید را تایید کنند. به عبارت دیگر، لازم نیست در این شبکه توکن یا کارت شناسایی برای شما صادر شود و این قضیه با رای نودهای دیگر حل می‌شود.

برایت آی دی (BrightID)

در نهایت از میان پروژه‌هایی که از مکانیسم Proof of Personhood دفاع می‌کنند و سعی می‌کنند کاربران را به شیوه‌ای نوین احراز هویت کنند، پروژه **BrightID** است. در این پروژه منوال بر این است که کاربران با تماس‌هایی در بستر اینترنت، یکدیگر را از نظر شخصیت انسانی تایید کنند. هر کاربر می‌تواند به‌صورت گروهی یا خصوصی با تماس‌های ویدیویی هویت خود را اثبات کند. همچنین این پروژه از طریق یک سیستم به نام Bitu کاری کرده که کاربران اعتبار هویت خود را در شبکه افزایش دهند؛ به طوری که هرچه کاربران بیشتری نود مدنظر را تایید کنند، میزان اعتبار او افزایش می‌یابد. هر کاربر در سیستم Bitu ضامن کاربران دیگر شود.

مکانیسم Proof of Personhood؛ راه نجات شبکه‌های مالی از حساب‌های غیرواقعی

مکانیسم Proof of Personhood مانند دیگر الگوریتم‌های اجماع به یکی از مهم‌ترین پروتکل‌ها و فناوری‌های شبکه‌های مالی غیرمتمرکز و سیستم‌های توزیع شده تبدیل شده است. این مکانیسم به شبکه کمک می‌کند حساب‌ها و نودهای واقعی و انسانی را از نودهای غیر انسانی تشخیص دهد تا به این ترتیب اکوسیستم به دور از هر گونه خطر سوگیری نظرات یا کلاهبرداری به واسطه تسلط نودهای خرابکار در امان باشد. مکانیسم Proof of Personhood روش خاصی ندارد و مجموعه‌ای از روش‌های مختلف برای احراز هویت از جمله شاخص‌های بیومتریک، گراف اجتماعی، دیدارهای حضوری و غیره به حساب می‌آید.

این مکانیسم نیز مانند دیگر مکانیسم‌های شبکه مزایا و معایبی را برای شبکه به همراه می‌آورد؛ اما در نهایت به نظر می‌رسد کاربران سعی می‌کنند به نقاط مثبت این اتفاق توجه داشته باشند. از آنجا که تعداد پروژه‌هایی که هم اکنون از مکانیسم Personhood Proof of استفاده می‌کنند در حال افزایش است. چنانچه شما هم دوست دارید به یکی از این پروژه‌ها ورود کنید و با مکانیسم Proof of Personhood آشنا شوید پیشنهاد می‌کنیم سوال یا نظر خود را در بخش کامنت‌های این مقاله از وبسایت کیف پول من کامنت کنید یا سری به پایگاه وبلاگی ما بزنید.