پنجشنبه ۸ شهریور ۱۴۰۳
شماره ۴۲۱۹
FARHIKHTEGANDAILY.COM
FARHIKHTEGANONLINE

نه کلیدهای شما، نه نام شما

دنیای نامگذاری غیر متمرکز!

هومن جعفری
مترجم

چرا ما به یک راه‌حل غیرمتمرکز برای نام‌های دامنه و فضاهای نام برای یافتن محتوا در اینترنت نیاز داریم، که خارج از کنترل اشخاص ثالث متمرکز است.

پول خنثی مانند بیت‌کوین آزادی اقتصادی را حفظ می‌کند. به آزادی فردی احترام می‌گذارد. بی‌سروصدا از حقوق مالکیت دفاع می‌کند. چه یک فرد یا یک کسب‌وکار باشید، بدون تهدید سانسور، مصادره یا تحقیر، در تصمیم‌گیری‌های خود در مورد تولید، سرمایه‌گذاری و مصرف به شما قدرت کامل می‌دهد. بدون دخالت دولت‌ها، این امر خوداتکایی را تشویق می‌کند و به هماهنگی اجتماعی کمک می‌کند. به عبارت دیگر، بیت‌کوین برای حفظ یک جامعه آزاد، مرفه و عادلانه ضروری است. درمورد نامگذاری هم همین‌طور است. اگر چیزی به اندازه پول برای جامعه مهم است، نامگذاری است. نام‌ها تقریبا برای همه‌چیز مورد نیاز است و افراد و مشاغل باید بتوانند نام خود را بدون اینکه تحت کنترل یک شخص ثالث متمرکز باشد، داشته باشند. نام‌ها و پول هر دو از لحاظ تاریخی برای کارایی خود به اعتماد متکی بوده‌اند، اما درست مانند بیت‌کوین به‌عنوان پول که عصر بی‌اعتمادی را آغاز کرد، همین امر باید برای نام‌ها انجام شود.

ارائه‌دهندگان نامگذاری متمرکز به تاریخ پیوسته‌اند!

اگر هنوز متوجه نشده‌اند، مردم باید بدانند که مالک نام کاربری خود در شبکه‌های اجتماعی نیستند و همیشه با یک کلیک تا مصادره اموال یا دارایی‌هایشان فاصله دارند. خطر امنیتی تکیه بر سیستم‌های نامگذاری متمرکز به‌ویژه برای افراد و مشاغلی که در بیت‌کوین ایجاد می‌کنند صادق است. اگر به سرویس‌های نام‌گذاری متمرکز متکی هستید، تا زمانی که در معرض خطر قرار نگیرید، فقط مساله زمان است، درست مانند آنچه درمورد ربودن دی‌ان‌اس (دومین نیم سرویس) وب سایت اسکوایراسپیس در ماه گذشته مشاهده کردیم.

دولت‌ها اغلب مخالفان سیاسی را با مصادره نام آنها ساکت می‌کنند. به‌عنوان مثال، PuntCAT، یک بنیاد غیرانتفاعی خصوصی کاتالونیایی را در نظر بگیرید که مأموریت آن ترویج انواع فعالیت‌های مربوط به ایجاد، مدیریت و کنترل و به‌طور کلی ترویج زبان کاتالانی است. آنها توسط پلیس اسپانیا در یک زمان سیاسی پر فراز و نشیب مورد حمله قرار گرفتند و به دلیل فشار قانونی مادرید مجبور شدند چندین وب سایت منتقد دولت اسپانیا را مسدود کنند. رئیس بخش آی‌تی شرکت نیز به اتهام فتنه دستگیر شد.

علاوه‌بر این، شرکت اینترنتی برای نام‌ها و شماره‌های اختصاص‌یافته (ICANN)، که مسئولیت مدیریت سیستم جهانی نام‌های دامنه را برعهده دارد، در طول سال‌ها با مناقشات متعددی در ارتباط با کنترل متمرکز، شفافیت و مسئولیت‌پذیری مواجه بوده است. رویه‌ها و سیاست‌های ICANN مبهم هستند، افرادی مانند رالف نادر (سیاستمدار و متفکر مستقل آمریکایی) به دلیل نقض حقوق مصرف‌کننده آنها را مورد انتقاد قرار داده‌اند و همان‌طور که بنیاد مرز الکترونیکی می‌گوید، تمایل آشکاری برای تسخیر در احترام بیش از حد به منافع علامت تجاری اصلی وجود دارد. نکته این است که اگر در نامگذاری غیرمتمرکز موفق نباشیم، خطر سانسور، مصادره اموال و سایر حقوق همیشه مورد حمله قرار خواهد گرفت.

همان‌طور که بیت‌کوین به همراه پروتکل‌های فناوری مجاور مانند NOSTR (یک پروتکل ارتباطی ساده و متن‌باز با هدف تسهیل ارتباطات غیرمتمرکز) به تکامل خود ادامه می‌دهد، نام‌ها به تنهایی به همین دلیل اهمیت بیشتری پیدا می‌کنند. نام‌ها می‌توانند به‌عنوان شناسه‌های اجزای مختلف در این سیستم‌ها عمل کرده و ارتباط بین طرف‌های مختلف را تسهیل کنند و قابلیت استفاده، قابلیت همکاری پروتکل‌ها و آزادی بیان را بهبود بخشند.

اسم آن را بازگشت نگذارید

تلاش‌های گذشته برای غیرمتمرکز کردن نامگذاری شامل ابتکاراتی مانند جداسازی سرور ریشه دی‌ان‌اس در سال ۱۹۹۷ و دامنه‌های سطح بالای جدید (TLD) مانند .bit و .name بوده است. در فضای ارزهای دیجیتال، پروژه‌های جدید اسم‌محور و خدمات نام مبتنی‌بر بلاک‌چین‌ها و شرکت‌های بزرگ نیز به دنبال تمرکززدایی سیستم‌های نامگذاری بوده‌اند. علی‌رغم این تلاش‌ها، بسیاری از این ابتکارات به دلیل پذیرش محدود، مسائل مقیاس‌پذیری، مسائل توزیع و سایر پیچیدگی‌های فنی کوتاهی کرده‌اند و سیستم‌های نامگذاری متمرکز را هم در فضای سنتی اینترنت و هم در چشم‌انداز رمزنگاری مسلط کرده‌اند.

در اوایل سال جاری، مت کورالو BIP (بیپ‌ها پروتکل بهبود بیت‌کوین هستند) را برای هماهنگی پرداخت‌های بیت‌کوین با استفاده از دی‌ان‌اس پیشنهاد کرد. مت درست است که به بلاک‌چین دیگری (مثلا ای‌ان‌اس در اتریوم که سرویس نامگذاری در این بلاک‌چین است) اعتماد نمی‌کند اما اذعان دارد که تکیه بر دی‌ان‌اس متمرکز سنتی یک خطر است و این تنها «بهترین گزینه» است.

سازمان‌هایی بین شما و نام شما وجود دارند، و هر وب‌سایتی که از HTTPS (پروتکل امن انتقال ابرمتن) برای رمزگذاری ترافیک استفاده می‌کند، به شخص ثالثی برای ایمن کردن آن متکی است! شما به معنای واقعی کلمه کلیدهای خود را در دست ندارید. نه کلید شما، نه نام شما.

آنچه مورد نیاز است، یک سیستم نامگذاری واقعا غیرمتمرکز و بدون مجوز است که روی بیت‌کوین ساخته شده است، فارغ از مقامات گواهی شخص ثالث، که به کاربران امکان کنترل و حفظ حریم خصوصی بر هویت آنلاین خود را می‌دهد و برخلاف تلاش‌هایی که قبلا انجام شد، نام‌گذاری باید به روشی سایفرپانک محور بدون بلاک‌چین یا تغییرات جدید انجام شود. به خود بیت‌کوین و بدون نیاز به هیچ توکن یا ساختار جدید. کاربران باید بر نحوه ثبت، مدیریت و انتقال نام‌ها کاملا کنترل داشته باشند.

نامگذاری به شیوه مطلوب سایفرپانک‌ها

[توضیح: به افرادی گفته می‌شود که با استفاده از رمزنگاری قوی و فناوری‌های تقویت‌کننده حریم خصوصی، از تغییرات اجتماعی و سیاسی حمایت می‌کنند تا حریم خصوصی مردم بیشتر یا حفظ شود. در اوایل گروه‌های غیررسمی از طریق لیست پست‌سپاری با هم ارتباط برقرار می‌کردند و هدف‌شان دستیابی به حریم خصوصی و امنیت از طریق استفاده فعال از رمزنگاری بود. سایفرپانک‌ها حداقل از اواخر دهه ۱۹۸۰ فعالیت جنبشی داشته‌اند و بیت‌کوین یکی از دستاوردهای آنهاست.] اینترنت که زمانی به‌عنوان نیرویی دموکراتیک برای بیان آزاد و ارتباطات جهانی تصور می‌شد، اکنون با تهدیدات فزاینده‌ای از سانسور دولت، نفوذ شرکت‌ها و آسیب‌پذیری‌های فنی مواجه است. نامگذاری غیرمتمرکز که بر پایه قوی و ایمن بیت‌کوین ساخته شده است، آینده‌ای را ارائه می‌کند که در آن افراد و کسب‌وکارها کنترل بیشتری بر هویت، ایده‌ها و اطلاعات خود دارند. با استفاده از تغییرناپذیری، شفافیت و ماهیت مقاوم در برابر سانسور بیت‌کوین، سیستم‌های نامگذاری غیرمتمرکز می‌توانند جایگزینی انعطاف‌پذیرتر و دموکراتیک‌تر برای مدیریت هویت خود ارائه دهند. با بیت‌کوین به‌عنوان ستون فقرات، می‌توانیم اطمینان حاصل کنیم که نامگذاری غیرمتمرکز نه‌تنها اجتناب‌ناپذیر است، بلکه در ایجاد یک اینترنت جهانی، باز و رایگان نیز واقعا موفق است؛ جایی که همه در شکل‌دهی به مکالمه جهانی بدون ترس از سانسور یا کنترل، صدایی برابر داشته باشند. اینترنت که سایفرپانک است.

منبع

مایک کارسون/ بیت کوین مگازین

اگر برای کارت به‌کارت کردن مشکل‌داری این مطلب را نخوان!

بیت‌کوین و روش انقلابی پرداخت خاموش

بیت‌کوین با اجازه دادن به افراد برای انجام معاملات بین یکدیگر بدون شخص ثالث، به پیشرفت عظیمی در عصر دیجیتال ادامه می‌دهد. مجله بیت‌کوین بیش از دوسال پیش به پرداخت‌های خاموش پرداخت تا یکی از کاستی‌های بیت کوین را روشن کند: حریم خصوصی. این مشکل آن موقع بود و امروز هم هست... همان‌طور که گفته شد: «... یک سیستم پرداخت مبتنی‌بر فشار (هیچ نهاد ثالثی اجازه ندارد پرداخت‌ها را از شما دریافت کند، شما باید مستقیم آنها را به‌طرف خودتان پرداخت کنید)، بیت‌کوین به فرستنده نیاز دارد که اطلاعات لازم برای تعریف را داشته باشد. مقصد پولی که می‌فرستند مستلزم آن است که گیرنده آدرس بیت‌کوین خود را به هر طریقی با فرستنده درمیان بگذارد. حضور دائمی آنلاین هرکسی می‌تواند به‌سادگی یک آدرس بیت‌کوین را در جایی آنلاین ارسال کند و از آن نقطه، هرکسی که بخواهد برای آن شخص پول ارسال کند، می‌تواند این کار را انجام دهد، اما هیچ حریم خصوصی‌ای در جمع‌آوری پول از این طریق وجود ندارد. به‌سادگی آن آدرس را بگیرید و آن را در بلاک‌چین جست‌وجو کنید، و شما نمی‌توانید ببینید که آن شخص چقدر پول فرستاده شده است، بلکه می‌توانید ردپای همه افرادی را که برای آنها پول ارسال کرده‌اند، ببینید و هرکسی به آنها کمک مالی کرده، هیچ حریم خصوصی‌ای ندارد. همه چیز کاملا باز و مرتبط است تا همه دنیا ببینند.» قبل از پرداخت‌های بی‌صدا، تنها راه جایگزین استفاده مجدد از آدرس‌ها براساس هر تماس برای محافظت از حریم خصوصی شما یا اجرای سروری بود که هربار کسی درخواست ارسال پول از شما می‌کند، آدرس جدیدی ارائه می‌دهد. هیچ یک از این دو گزینه برای اکثر کاربران قابل استفاده یا مقیاس‌پذیر نیستند. حریم خصوصی برای تعداد کمی از کاربران ممتاز قابل دستیابی است که می‌دانند چگونه به آن دست یابند. خوشبختانه جامعه از آن زمان با پیشرفت‌های زیادی داشته است.

پس از بحث‌های فراوان در مورد چگونگی پیاده‌سازی این ویژگی تا حد امکان کارآمد، روش کارآمد BIP۳۵۲ اکنون یک واقعیت است. هنگامی که شخصی می‌خواهد به‌صورت خصوصی پول دریافت کند، مثلا یک سازمان فعال، می‌تواند آدرس پرداخت بی‌صدای خود را به جای آدرس بیت‌کوین سنتی در سایت خود قرار دهد. اکنون زمانی که کاربری می‌خواهد برای سازمان پول ارسال کند، از آدرس پرداخت بی‌صدا در کیف پول پشتیبانی استفاده می‌کند. این به‌طور خودکار از کلید عمومی منحصربه‌فرد متصل به آدرس پرداخت بی‌صدا، همراه با کلیدهای عمومی خروجی‌هایی که می‌خواهند ارسال کنند، استفاده می‌کند تا یک آدرس کاملا جدید و یکبار مصرف را ایجاد کند که شبیه هر آدرس بیت‌کوین دیگری است. پیچیده به‌نظر می‌رسد، اما همه اینها در پشت‌صحنه عمل می‌کنند. تنها کاری که کاربر باید انجام دهد این است که آدرس را بردارد و مانند هر آدرس دیگری به آن پول بفرستد. این روش فواید زیادی دارد:

۱ خود سازمان فقط باید یک آدرس را در سایت خود پست کند تا همچنان از مزایای ایجاد آدرس‌های جدید برای هر تراکنش برخوردار شود.

۲ کاربر ارسال‌کننده پول به سازمان همیشه می‌تواند به یک آدرس ثابت ارجاع دهد و این امر ارسال مداوم پول را بدون نیاز به ردیابی چندین آدرس برای آنها آسان می‌کند.

۳ اگر همان کاربر به‌طور مداوم به همان آدرس پرداخت بی‌صدا پول بدهد، هربار یک آدرس بیت‌کوین جدید ایجاد می‌شود، بنابراین فرستنده نیازی به نگرانی در مورد گیرنده ندارد که بداند همان کاربر برای او پول ارسال می‌کند.

۴ از آنجا که کاربران نمی‌توانند به‌راحتی به وجوه کیف پول خود نگاه کنند و ببینند چه کسی برای آنها پول می‌فرستد، گیرنده مزایای زیادی در حفظ حریم خصوصی به‌دست می‌آورد.

۵ آدرس‌هایی که برای تراکنش بین هر دو کاربر ایجاد می‌شوند، مانند هر تراکنش بیت‌کوین دیگری ظاهر می‌شوند، به این معنی که استفاده از این ویژگی برای طرف‌های خارجی مبهم است.

۶ نیازی به سرور نیست. هر کیف پولی که از پرداخت بی‌صدا پشتیبانی می‌کند، تمام این فناوری را به صورت محلی در کیف پول مدیریت می‌کند.

برای خلاصه کردن مزایا: با پرداخت بی‌صدا، هر شخص یا سازمانی اکنون می‌تواند از آدرس بیت‌کوین پرداخت بی‌صدا به جای آدرس ثابت سنتی خود استفاده کند تا نه‌تنها حریم خصوصی بهتری برای خود داشته باشد، بلکه از افرادی که سعی در ارسال پول به آنها دارند نیز محافظت می‌کند. با حصول اطمینان از اینکه حتی آنها به‌عنوان گیرنده نیز نمی‌توانند اطلاعات مربوط به فرستنده‌ها را به دام بیندازند. با پرداخت‌های بی‌صدا، فرستنده و گیرنده لایه بزرگی از حریم خصوصی را به‌دست می‌آورند، درحالی‌که هنوز هم تا حد زیادی از قدرت پروتکل اصلی بیت‌کوین بهره می‌برند تا به آنها آزادی انجام معاملات را به دلخواه بدهند.

با این اوصاف اشکالاتی وجود دارد. اولین مورد نتیجه مستقیم مزیت عدم نیاز به دستگاه اختصاصی آنلاین برای تسهیل معاملات است. کاربران باید تراکنش‌های بلاک‌چین را برای شناسایی پرداخت‌های انجام‌شده به آنها اسکن کنند. این اسکن ممکن است زمان ببرد، اما مزایای زیادی برای حفظ حریم خصوصی برای هر دو کاربر دارد. با گذشت زمان، عملکرد اسکن را نیز می‌توان بهبود بخشید تا این مشکل برای کاربران کمتر شود. مساله دوم یکی از قابلیت پذیرش است، زیرا پرداخت‌های بی‌صدا جدید هستند و پشتیبانی کیف پول در زمان نوشتن تقریبا محدود است. هم فرستنده و هم گیرنده باید از کیف پولی استفاده کنند که از این ویژگی پشتیبانی کند. silentpayments.xyz وبسایتی است که از طریق آن متوجه می‌شوید کدام کیف پول‌ها از پرداخت بی‌صدا پشتیبانی می‌کنند.

اگر جامعه امیدوار است که شاهد پذیرش گسترده‌تر پرداخت‌های بی‌صدا باشد، کیف پول‌ها باید این عملکرد را ادغام کنند تا به کاربران بیشتری مزایای حفظ حریم خصوصی ارائه شده توسط پرداخت‌های بی‌صدا بیت‌کوین را ارائه دهند. به‌طورکلی ایده محافظت از حریم خصوصی کاربران از طریق پروتکل بومی بیت‌کوین، ایده مهمی است که می‌تواند حریم خصوصی کاربر را بدون به خطر انداختن آنچه بیت‌کوین را بیت‌کوین می‌سازد، ارائه دهد. درواقع مزایای حفظ حریم خصوصی روش پرداخت خاموش با ارائه آزادی به کاربران برای انجام معاملات با حریم خصوصی بهتر در صورت تمایل باورهای اساسی جامعه بیت‌کوین را تقویت می‌کند.