روش اثبات دانش صفرZK-SNARKs

حفظ حریم خصوصی در عین این که شبکه با مشکل مقیاس‌پذیری مواجه نشود یکی از چالش‌هایی بوده که اخیراً در توسعه شبکه‌های بلاکچینی بسیار به چشم می‌خورد. در حال حاضر پروژه‌های فعال در حوزه کریپتوکارنسی با چنگ زدن به دامن راه‌حل‌های مختلف تلاش نموده‌اند تا مشکل مقیاس‌پذیری را به حداقل رسانده و بدین شکل روند کاهشی را برای کارمزدهای دریافتی شبکه‌های بلاکچینی ترسیم کنند؛ چراکه با افزایش سرعت تائید تراکنش‌ها، ترافیک موجود در شبکه کاهش پیدا می‌کند و عملاً مهم‌ترین عامل در افزایش هزینه‌های تراکنشی از بین می‌رود. اثبات دانش صفر (Zero Knowledge Proof) یکی از این روش‌ها بوده که نقش کلیدی را در مقیاس‌پذیری و همچنین حفظ حریم خصوصی کاربران ایفا می‌نماید. لازم به ذکر است که اثبات دانش صفر خود دارای انواعی بوده که یکی از مهم‌ترین آن‌ها، روش اثبات دانش صفر ZK-SNARKs نام دارد و ما در این مقاله از بلاگ کیف پول من تلاش نمودیم تا به معرفی جامع این نوع خاص بپردازیم؛ اگر شما هم در این زمینه کنجکاو هستید، تا انتهای این مطلب با ما همراه باشید.

مروری بر مفهوم اثبات دانش صفر (ZK Proof)

پیش از آن که روش اثبات دانش صفر ZK-SNARKs را مورد بررسی قرار دهیم، ضرورت دارد نگاهی به خود مفهوم اثبات دانش صفر داشته باشیم؛ طبیعتاً موفقیت در مارکت رمزارز و کسب سود از طریق خرید ارز دیجیتال در دنیای امروز نیازمند آگاهی کامل و تسلط بر اطلاحات و روش‌های موجود در دنیای کریپتوکارنسی است. در یک تعریف کوتاه و ساده از اثبات دانش صفر می‌توان آن را یکی از رایج‌ترین روش‌های حفظ حریم خصوصی در شبکه‌های بلاک‌چین عمومی معرفی نمود که در آن کاربر قادر است با کمک شیوه‌های رمزنگاری و بدون نیاز به افشای اطلاعات حقیقی به کاربری دیگر ثابت نماید که به محتوای چنین اطلاعاتی دسترسی دارد. برای درک بهتر مفهوم اثبات دانش صفر، مثال غار علی بابا بهترین حکایتی است که می‌توانیم از آن کمک بگیریم:

فرض کنید با دوست خود در مسیر جنگل با یک غاری مواجه شده‌اید که دارای دو دهانه بوده و در وسط آن یک درب رمزدار وجود دارد. دوست شما ادعا می‌کند که این رمز را می‌داند و برای اثبات آن وارد غار شده و سپس از طرف دیگر غار خارج می‌شود و چند بار این عمل را انجام می‌دهد تا شما اطمینان پیدا کنید که وی به رمز این در دسترسی دارد. این اطمینان چگونه در ذهن شما ایجاد می‌شود؟ آیا دوست شما رمز این درب را به شما گفت؟! خیر ولی با ورود و خروج مکرر از دهانه‌های مختلف غار این موضوع را به شما ثابت کرد که به چنین اطلاعاتی دسترسی دارد و روش اثبات دانش صفر نیز دارای چنین رویکردی است. به طور خلاصه در روش اثبات دانش صفر به فردی که یک ادعا را اثبات کند، اثبات کننده (Provider) و به کسی که مسئول تائید این ادعا است، تائید کننده (Verifier) گفته می‌شود.

آشنایی با روش اثبات دانش صفر غیرتعاملی

هرچند که ابداع روش اثبات دانش صفر تعاملی را می‌توان انقلابی در تائید اطلاعات بدون دسترسی به آن به شمار آورد؛ اما واقعیت ماجرا از این قرار است که مزایای استفاده از آن به دلیل لزوم تعامل مستقیم دو طرف اثبات و تائید کننده بسیار محدود بود و عملاً در طول آن باید پرسش و پاسخ‌هایی میان این دو طرف رد و بدل می‌شد که چنین امری علاوه بر آن که به زمان و انرژی بسیار زیادی نیاز دارد، بلکه هیچ تناسبی با سیستم‌های غیرمتمرکز نیز نخواهد داشت. در کش و قوس‌های رخ داده در حوزه رمزنگاری، در نهایت سه دانشمند به نام‌ها سیلویو میکالی (Silvio Micali)، مانوئل بلوم (Manuel Blum) و پل فلدمن (Paul Feldman) توانستند ایده اثبات دانش صفر غیرتعاملی را ارائه نمایند که در آن شخص اثبات کننده و تائید کننده از یک کلید اشتراکی (Shared Key) بهره می‌برند.

در این روش اثبات دانش صفر، اثبات کننده و تائید کننده صرفا به یک دور ارتباط نیاز دارند و در

آن اثبات کننده داده را به یک الگوریتم خاص ارسال می‌نماید تا الگوریتم دانش صفر (Zero Knowledge (Proof ایجاد گردد. این اثبات پس از ایجاد به فرد تائید کننده ارسال می‌گردد و وی می‌تواند پس از بررسی تائید نماید که اثبات کننده به اطلاعات مخفی مورد نظر دسترسی دارد. مسلماً با کاهش ارتباط موجود میان تائید و اثبات کننده، این روش به کارایی بالاتری دست پیدا خواهد کرد.

روش اثبات دانش صفر ZK-SNARKs چیست؟

حال که با مفهوم اثبات دانش صفر بهتر آشنا شدید، می‌توانیم راحت‌تر در ارتباط با مهم‌ترین نوع این اثبات یعنی اثبات دانش صفر ZK-SNARKs صحبت کنیم. این واژه در اصل مخفف عبارت لاتینی «Argument of Knowledge Zero-Knowledge Succinct Non-Interactive» بوده و به معنای اثبات دانش صفر غیرتعاملی و مختصر است. این روش در سال 2012 و در مقاله‌ای که بوسیله Nir Bitansky، Canetti Ran، Eran Tromer و Alessandro Chiesa منتشر شد، معرفی گردید. پروژه Zcash اولین کاربرد گسترده روش اثبات دانش صفر ZK-SNARKs در دنیای کریپتو به شمار می‌رود که این پروژه با استفاده از چنین نوعی از اثبات دانش صفر توانست تراکنش‌های محرمانه و محافظت شده‌ای را ایجاد نماید که در آن اطلاعات فرستنده، گیرنده و همچنین مبلغ ارسالی، کاملاً خصوصی و محرمانه نگه داشته می‌شوند.

نحوه کار روش اثبات دانش صفر ZK-SNARKs

در واقع روش اثبات دانش صفر ZK-SNARKs نوعی روش غیرتعاملی بوده که در آن از کلید مشترک به منظور اثبات کمک گرفته می‌شود و منظور از این کلید مشترک، متغیرهای عمومی بوده که Provider و Verifier با همدیگر در استفاده از آن‌ها به منظور تولید و اثبات به توافق رسیده‌اند. توجه داشته باشید تولید این متغیرهای عمومی که به آن‌ها رشته مرجع عمومی (CRSl Common Reference String) نیز گفته می‌شود، یک عملیات بسیار حساس است؛ چراکه نقش کلیدی را در امنیت پروتکا ایفا می‌نمایند. به طوری که اگر آنتروپی و ویژگی تصادفی بودن مورد استفاده در تولید CRS به دست یک Verifier افتد؛ در چنین حالتی آن‌ها به راحتی قادر خواهند بود اثبات‌های نادرست ایجاد کنند.

یک روش متداول در کاهش این قبیل از خطرات در تولید پارامترهای عمومی روش اثبات دانش صفر ZK-SNARKs، استفاده از محاسبات چند جانبه (Multi-party computation | MPC) است. در این روش، چندین شخص در یک مراسم تنظیم متغیر عمومی قابل اعتماد شرکت می‌نمایند و هر یک از آن‌ها مقادیری تصادفی به منظور تولید CRS ایجاد می‌کنند و تا زمانی که یک طرف قابل اعتماد، بخش آنتروپی خویش را از بین نبرده است، پروتکل روش اثبات دانش صفر ZK-SNARKs همچنان سلامت خویش را حفظ می‌نماید.

لازم به ذکر است که در این روش، کاربران ناگزیر به اعتماد به شرکت‌کنندگان در این مراسم تولید متغیرهای عمومی هستند. طبیعتاً چنین ویژگی برای پروتکل‌های غیرمتمرکز رمزارزی که نیاز به اعتماد به دیگران را از بین می‌برند، ویژگی چندان مثبتی محسوب نخواهد شد و به همین

علت امروزه عموما پروژه‌های رمزارزی به سراغ نوع توسعه یافته روش اثبات دانش صفر غیرتعاملی یعنی ZK-STARK رفته‌اند.

مولفه‌های اصلی روش اثبات دانش صفر ZK-SNARKs

این روش از چهار مولفه اصلی شکل گرفته است که به شرح زیر هستند:

- **دانش صفر (Zero-Knowledge):** فرد Verifier قادر است اعتبار جمله‌ای را بدون دسترسی به محتوای آن تائید نماید. در این حالت تنها دانشی که تائید کننده در ارتباط با جمله دارد این است که وضعیت آن «True» یا «False» است.
- **اختصاری (Succinct):** داده‌های روش اثبات دانش صفر ZK-SNARKs کوتاه بوده و به راحتی می‌توان آن را تائید نمود.
- **غیرتعاملی (Non-Interactive):** در این روش خاص تائید کننده و اثبات کننده صرفاً یک بار با همدیگر ارتباط می‌گیرند و همین ارتباط برای تائید نهایی کافی خواهد بود.
- **اثبات دانش (Argument of Knowledge):** اثبات ایجاد شده در روش اثبات دانش صفر ZK-SNARKs تقلب در فرآیند را بسیار دشوار می‌سازد. در واقع برای یک اثبات کننده تقریبا غیرممکن است که بتواند بدون داشتن اطلاعات و داده یک اثبات دانش صفر معتبر را ایجاد نماید.

مقایسه روش اثبات دانش صفر ZK-SNARKs با ZK-STARK

دومین نوع اثبات دانش صفر، ZK-STARK نام دارد که در اصل مخفف عبارت «Zero-Knowledge Scalable Transparent Argument of Knowledge» بوده و به معنی اثبات دانش صفر شفاف و مقیاس‌پذیر می‌باشد. در روش ZK-STARK، عموماً اثبات‌های تولید شده بسیار بزرگتر از حالتی است که در ZK-SNARKs با آن مواجه هستیم و همین مسئله موجب شده تا هزینه‌های کمی بالاتر رود؛ اما با این وجود باید توجه داشت که اثبات مجموعه اطلاعات بزرگ به شکل یکجا سبب می‌شود تا این روش جدید مقرون به صرفه‌تر باشد.
ناگفته نماند که در روش اثبات دانش صفر ZK-SNARKs به منظور ایجاد اثبات رمزنگاری شده از منحنی‌های بیضوی استفاده می‌کند که به دلیل اندازه کوچک هزینه مقرون کمتری دارند؛ در نقطه مقابل، روش ZK-STARK برای تولید اثبات به سراغ توابع هشینگ رفته که نیازمند تعامل کمتری میان شخص اثبات کننده و تائید کننده بوده و به همین علت دارای سرعت بیشتری است.

ZK-SNARKs؛ روشی برای صیانت از حریم خصوصی

اگر با خرید بیت کوین و به طور کلی سرمایه‌گذاری بر روی ارزهای دیجیتالی به دنبال کسب سود هستید، باید بدانید که چنین امری بدون کسب دانش کافی از اصطلاحات و پروتکل‌های موجود در دنیای کریپتوکارنسی امکان‌پذیر نخواهد بود و به همین علت ما این مقاله از بلاگ کیف پول من را به معرفی روش اثبات دانش صفر ZK-SNARKs اختصاص دادیم. همان طور که در مطالب فوق مشاهده کردید، اثبات دانش صفر یک روش کاربردی به منظور اثبات دسترسی به یک داده بدون نیاز به فاش کردن آن است و نوع غیرتعاملی آن به دو نوع تقسیم شده است و ZK-SNARKs یکی از این انواع است که با استفاده از آن می‌توان از هویت کاربران حفاظت نمود و تراکنش‌های خصوصی ایجاد کرد. حال که با روش اثبات دانش صفر ZK-SNARKs بهتر آشنا شدید، نظر شما درباره آن چیست؟ آیا این نوع از روش اثبات دانش صفر می‌تواند عملکرد خوبی از خود در دنیای کریپتوکارنسی نشان دهد؟ برای ما بنویسید.