دانشکده مهندسی کامپیوتر

تمرین کروم

امنیت سیستم‌های کامپیوتری

مدرس: دکتر ابوالفضل دیانت

محمدحسین عباسپور، فرزان رحمانی

شماره دانشجویی: ۹۹۵۲۱۴۳۳، ۹۹۵۲۱۲۷۱

نیم سال دوم
سال تحصیلی ۱۴۰۳-۱۴۰۲

یک روش اثبات دانایی صفر به صورت غیرتعاملی که در زنجیره بلوکی استفاده میشود را تشریح کنید.

۱ مقدمه

اثبات دانایی صفر (Zero-Knowledge Proofs) روش‌های رمزنگاری هستند که به یک طرف (اثبات‌کننده) اجازه می‌دهند تا به طرف دیگر (تأییدکننده) ثابت کند که مقداری را می‌داند، بدون اینکه هیچ اطلاعاتی در مورد آن مقدار فاش کند. اثبات دانایی صفر غیرتعاملی (Non-Interactive Zero-Knowledge Proofs) نوعی هستند که تعامل بین اثبات‌کننده و تأییدکننده به حداقل می‌رسد، معمولاً فقط یک پیام از اثبات‌کننده به تأییدکننده.

یکی از معروف‌ترین NIZKPs مورد استفاده در فناوری زنجیره بلوکی، zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) است.

۲ اجزای zk-SNARKs

اجزای اصلی zk-SNARKs عبارتند از:

۱. زبان بیانی: توصیف مسئله‌ای که باید اثبات شود.

۲. تنظیمات اولیه (Setup Phase): تولید پارامترهای عمومی و خصوصی.

۳. ساخت اثبات (Proof Generation): اثبات دانایی بدون افشای اطلاعات.

۴. تأیید اثبات (Proof Verification): تأیید اعتبار اثبات بدون نیاز به تعامل.

۳ توضیح فرآیند

فرآیند zk-SNARKs را می‌توان به مراحل زیر تقسیم کرد:

۱.۳ تنظیمات اولیه (Setup Phase)

- یک الگوریتم راه‌اندازی وجود دارد که دو مجموعه پارامتر تولید می‌کند: پارامترهای عمومی و پارامترهای خصوصی.
- پارامترهای عمومی به‌طور عمومی منتشر می‌شوند و برای ساخت و تأیید اثبات‌ها استفاده می‌شوند.
- پارامترهای خصوصی مخفی نگه داشته می‌شوند و تنها برای اطمینان از امنیت پروتکل ضروری هستند.

۲.۳ ساخت اثبات (Proof Generation)

- اثبات‌کننده با استفاده از پارامترهای عمومی و دانش مخفی خود، یک اثبات غیرتعاملی تولید می‌کند.
- این اثبات شامل یک رشته کوتاه از داده‌ها است که ثابت می‌کند اثبات‌کننده واقعاً دانش مخفی مورد نیاز را دارد، بدون اینکه آن دانش را فاش کند.

۳.۳ تأیید اثبات (Proof Verification)

- تأییدکننده با استفاده از پارامترهای عمومی و اثبات تولید شده، می‌تواند صحت اثبات را تأیید کند.
- تأیید اثبات بسیار سریع است و نیازی به تعامل با اثبات‌کننده ندارد.

۴ کاربرد در زنجیره بلوکی

- حفظ حریم خصوصی: در ارزهای رمزنگاری شده مانند ،Zcash از zk-SNARKs برای مخفی‌سازی جزئیات تراکنش‌ها (مانند فرستنده، گیرنده و مقدار تراکنش) استفاده می‌شود.
- کاهش بار محاسباتی: تأیید تراکنش‌ها به‌صورت غیرتعاملی و سریع انجام می‌شود، که می‌تواند بار محاسباتی را کاهش دهد و به مقیاس‌پذیری شبکه کمک کند.

۵ مثال کاربردی

فرض کنید یک فرستنده می‌خواهد اثبات کند که یک مقدار خاص از ارز رمزنگاری شده را دارد و می‌تواند آن را به گیرنده منتقل کند، بدون اینکه جزئیات تراکنش (مانند مقدار دقیق) را فاش کند. با استفاده از ،zk-SNARKs فرستنده می‌تواند اثبات کند که تراکنش معتبر است، در حالی که اطلاعات حساس مخفی باقی می‌مانند. گیرنده و سایر اعضای شبکه می‌توانند به راحتی و بدون نیاز به تعامل با فرستنده، صحت این اثبات را تأیید کنند.

۶ نتیجه‌گیری

zk-SNARKs به عنوان یک ابزار قدرتمند در زنجیره بلوکی برای ایجاد تراکنش‌های امن و خصوصی به‌کار گرفته می‌شوند، و به افزایش اعتماد و کارایی در سیستم‌های غیرمتمرکز کمک می‌کنند.