دانشکده مهندسی کامپیوتر

درس امنیت سیستم های کامپیوتری
تمرین کروم

ملیکا محمدی فخار - ستاره باباجانی

۹۹۵۲۱۱۰۹-۹۹۵۲۲۰۸۶

استاد درس: دکتر ابوالفضل دیانت

بهار ۱۴۰۳

توضیح یک روش غیرتعاملی اثبات دانش صفر که در بلاکچین استفاده می‌شود

مفهوم کلی zk-SNARKs

این مفهوم در واقع یک روش رمزنگاری برای اثبات دانش بدون افشای آن دانش است. در زمینه بلاکچین، zk-SNARKs به کاربران اجازه می‌دهد تا تایید کنند که آن‌ها قوانین خاصی را رعایت کرده‌اند (مثلاً تایید اینکه آن‌ها مالکیت مبلغی از ارز را دارند) بدون اینکه اطلاعات خاصی مانند مقدار دقیق ارز یا هویت‌شان را فاش کنند.

فرآیند کار zk-SNARKs

این فرآیند شامل سه بخش اصلی است: ایجاد، اثبات و تایید.

ایجاد (Setup)

قبل از اینکه هرگونه اثباتی انجام شود، باید یک ''معامله اولیه'' ایجاد شود که شامل ایجاد یک کلید عمومی و یک کلید خصوصی است. کلید عمومی در دسترس همه قرار می‌گیرد، در حالی که کلید خصوصی باید مخفی نگه داشته شود و پس از استفاده از بین برود تا امنیت سیستم حفظ شود.

اثبات (Proving)

اثبات‌کننده، که می‌خواهد دانش خود را نشان دهد بدون افشای اطلاعات، یک ''اثبات'' ایجاد می‌کند که اطلاعات مورد نظر را رمزنگاری می‌کند. این اثبات به طور خلاصه و کوچک است و حاوی مقادیر عددی است که از محاسبات ریاضی برای تایید صحت دانش بدون افشای آن استفاده می‌کنند.
مراحل اصلی در فرآیند اثبات عبارتند از:

- **تولید مدار:** اثبات‌کننده ابتدا یک مدار ریاضیاتی تولید می‌کند که بیانگر محاسباتی است که باید انجام شود. این مدار شامل ورودی‌های عمومی و خصوصی است.
- **تولید اثبات:** اثبات‌کننده با استفاده از مدار و ورودی‌ها، یک اثبات مختصر و کوچک تولید می‌کند. این اثبات به گونه‌ای است که تاییدکننده می‌تواند با استفاده از آن و بدون نیاز به دیدن ورودی‌های خصوصی، صحت ادعا را تایید کند.
- **ارسال اثبات:** اثبات‌کننده اثبات تولید شده را به تاییدکننده ارسال می‌کند.
- **تایید اثبات:** تاییدکننده اثبات را دریافت و با استفاده از کلید عمومی و الگوریتم تایید، صحت آن را بررسی می‌کند.

تایید (Verification)

تاییدکننده، که می‌خواهد اطمینان حاصل کند اثبات صحیح است، می‌تواند با استفاده از کلید عمومی، اثبات را بررسی کند. این فرآیند بسیار سریع‌تر از ایجاد اثبات است و نیازی به دسترسی به اطلاعات خصوصی اثبات‌کننده ندارد.

کاربردها در بلاکچین

در بلاکچین‌ها، این روش به خصوص در ارزهای دیجیتالی مانند Zcash به کاربران امکان می‌دهد تا تراکنش‌های خصوصی را انجام دهند. به این ترتیب، آن‌ها می‌توانند اطمینان حاصل کنند که تراکنش‌ها معتبر هستند بدون اینکه اطلاعات شخصی یا مقادیر تراکنش‌ها را فاش کنند. این امر موجب حفظ حریم خصوصی در معاملات می‌شود و در عین حال امنیت شبکه را تضمین می‌کند.