امنیت کاربر در بلاک‌چین عمومی بیت‌کوین (قسمت اول)

User privacy in the public Bitcoin Blockchain

سلمان صادقی

۱۳۹۸/۵/۱۴

کوشش حاضر یک مجموعه دوقسمتی و مربوط به مطالعاتی‌ست که در باب امنیت کاربر در شبکه بیت‌کوین صورت گرفته است. در بخش اول از این مجموعه، ابتدا به یکی از جدی‌ترین مشکلات بلاک‌چین عمومی بیت‌کوین پرداخته‌شده است.

فهرست مطالب

کوشش حاضر یک مجموعه دوقسمتی و مربوط به مطالعاتی‌ست که در باب امنیت کاربر در شبکه بیت‌کوین صورت گرفته است. در بخش اول از این مجموعه، ابتدا به یکی از جدی‌ترین مشکلات بلاک‌چین عمومی بیت‌کوین پرداخته‌شده است. هرروزه خبرهای بسیاری از نفوذ مهاجمان به دارایی‌های کاربران منتشر می‌شود. در کنار این، حفظ محرمانگی می‌بایست یکی از اصلی‌ترین دغدغه‌های شبکه‌های پرداخت باشد. بعد از بررسی انواع بسته‌های مدیریت تراکنش (کیف پول‌ها) برای بیت‌کوین، به مشکل حفظ محرمانگی و مکانیسم عملکردی این بسته‌ها پرداخته‌شده است.

در قسمت دوم این مجموعه، متدهای موجود برای حفظ محرمانگی شبکه بیت‌کوین باهم مقایسه می‌شوند و فناوری کوین‌جوین و کیف پول مبتنی بر آن به‌عنوان یک راه حل مورد بررسی دقیق‌تر قرار می‌گیرد.

مقدمه‌ای برای بیت‌کوین

بیت‌کوین یک شبکه پرداخت فردبه‌فرد است که از آن در یک دفترکل توزیع‌شده نگهداری می‌شود. همه‌ی تراکنش‌ها می‌بایست در یک شبکه فردبه‌فرد که امنیت اطلاعات را تضمین کند، انجام شوند. تمامی گره‌های این شبکه و تمامی تاریخچه پرداخت‌های شبکه در یک پایگاه داده ذخیره می‌شود. این پایگاه داده را اصطلاحا بلاک‌چین می‌نامند (Barcelo 2007).

در سیستم‌های پرداخت سنتی، سابقه تراکنش‌های کاربران بانک‌ها عمومی نیست. یک سیستم پرداختی جدید باید محرمانگی و امنیت کاربران را تضمین کند. انتشار عمومی سابقه تراکنش‌ها در شبکه بیت‌کوین می‌تواند مسئله‌ای مهم و جدی قلمداد شود. برای دریافت بیت‌کوین، گیرنده باید یک آدرس به فرستنده بدهد؛ بر اساس تحقیقات پیشین و نظرات جامعه بیت‌کوین، استفاده مجدد از آدرس از منظر فنی کار مناسبی نیست. پیشنهاد می‌شود که برای هر تراکنش یک آدرس جدید استفاده شود[1]. ویژگی مهم دیگر بیت‌کوین رمزنگاری غیرمتقارن[2] آن است. آدرس‌ها توسط توابعی رندم به‌صورت زنجیره‌هایی از اعداد و حروف ساخته می‌شوند. به عبارت دیگر، خروجی هر تراکنش به یک آدرس ارسال می‌شود و این همان کلید عمومی است. برای هزینه کردن هر ورودی باید مالکیت فرد بر آن موجودی احراز شود. کلید خصوصی سندی بر مالکیت فرد بر خروجی هر تراکنش است.

[1] Disposable Address
[2] Asymmetric cryptographic

از منظر فنی از هر آدرس می‌توان برای دریافت و ارسال بی‌نهایت تراکنش استفاده کرد. هر آدرس ۱۶۰ بیت طول دارد و امکان تولید بی‌شمار آدرس فراهم است. پیشنهاد می‌شود که برای انجام هر تراکنش یک آدرس استفاده شود. در هر تراکنش که خود از برآیند ورودی و خروجی‌های بی‌شمار دیگری تشکیل‌شده، اگر خروجی از ورودی کمتر باشد، دو تراکنش توسط فرستنده صورت می‌گیرد؛ یکی به مقصد آدرس عمومی فرد دریافت‌کننده و دیگری که باقی‌مانده موجودی اوست (این مقدار را در این مقاله "خروجی تغییریافته" می‌نامیم)، به خودش ارسال می‌شود.

این خروجی تغییریافته می‌تواند به شناسایی فرستنده توسط مهاجم کمک کند. روش‌های متفاوتی برای فهمیدن این‌که کدام تراکنش، خروجی تغییریافته است، وجود دارد.

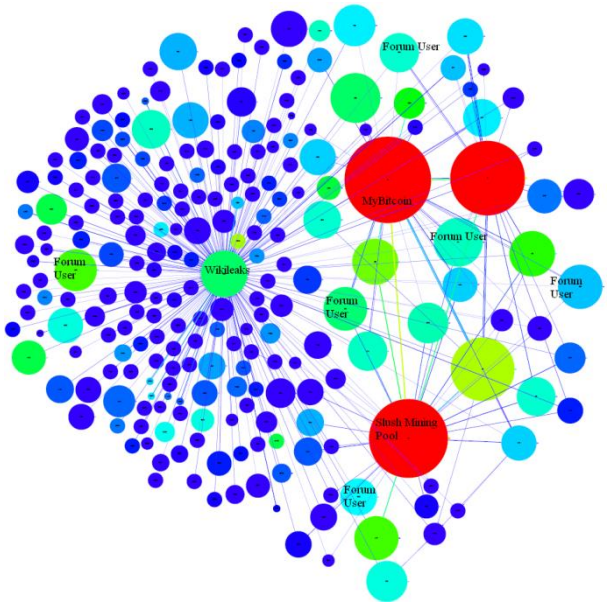
- معمولا بسیاری از تراکنش‌ها رند هستند (مثلا ۱ بیت‌کوین یا ۰,۰۰۱ بیت‌کوین) و خروجی‌های تغییریافته معمولا اعداد رندی نیستند (مثلا ۰,۰۰۱۵۷بیت‌کوین).
- یکی دیگر از این روش‌ها افزایش پاداش شبکه استخراج است. کاربری که تراکنشش منتظر تأیید در شبکه است، ممکن است با افزایش پاداش شبکه، به سریع‌تر شدن فرآیند تأیید در شبکه اقدام کند و درنتیجه فرد مهاجم می‌تواند مشاهده کند که خروجی تغییریافته در حال کاهش است.
- رد پای کیف پول نیز برای یک آنالیزور حرفه‌ای قابل ردیابی است. او می‌داند که هر کیف پول چطور تراکنش‌ها را می‌سازد. او می‌تواند از همین روش رد پای خروجی تغییریافته را پیدا کند.

یکی دیگر از این روش‌ها استفاده مجدد از آدرس است. در ادامه این مقاله به بررسی دقیق‌تر این باگ امنیتی پرداخته‌شده است(Blockchain attacks on privacy).

استفاده مجدد از آدرس

شاید در ابتدا این جالب به نظر برسد که از آدرس عمومی شبیه به کارت‌های بانکی استفاده شود. این اما یک مشکل اساسی دارد. برخلاف بانک‌ها که در آن سابقه تراکنش‌ها مخفی است، در بلاک‌چین بیت‌کوین برای هر فردی که متصل به اینترنت باشد در دسترس است. بیت‌کوین همواره به‌عنوان یک ابزار برای حفظ حریم خصوصی مالی ترویج شده است، اما تنها ابزار حریم خصوصی بیت‌کوین از آدرس مستعار آن می‌آید که آن‌هم شکننده است. درست است که هویت فرستنده و گیرنده مخفی است اما راه‌هایی وجود دارد که می‌تواند هویت پشت فرستنده و گیرنده هر تراکنش را نیز آشکار کند. استفاده مجدد، ردیابی پرداخت‌ها، مانیتور کردن آی پی سیستم‌ها و بسیاری مکانیسم‌های دیگر ازجمله روش‌هایی است که با استفاده از آن‌ها

می‌توان هویت افراد شرکت‌کننده در یک پرداخت در شبکه بیت‌کوین را آشکار ساخت. در پروسه اهدای کمک‌های نقدی به موسسه wikileaks ازآنجایی‌که هویت برخی از اهداکنندگان آشکار بود، هویت بقیه افراد شرکت‌کننده در این کمک‌رسانی مالی نیز آشکار گردید.



بارسلو در سال ۲۰۱۴ تاریخچه تمام تراکنش‌های بیت‌کوین را مورد مطالعه قرار داد. مطابق با نتایج پژوهش او که در جدول زیر نمایش داده‌شده است، تا آن تاریخ از نزدیک به ۱۳ میلیون آدرس عمومی ساخته‌شده، یک‌میلیون و چهارصد هزار آدرس بیش از یک‌بار تراکنش انجام داده‌اند. سایت‌های جست‌وجو کننده‌ی بلاک‌چین نظیر Blockchain.info برای دریافت تمامی جزییات تراکنش‌ها در دسترس‌اند.

جدول ۱ نتایج تحقیق بارسلو

تعداد آدرس‌های ساخته‌شده	۱۲,۹۶۳,۱۹۹
میانگین استفاده از هر آدرس	۳,۱۸
کمترین استفاده از هر آدرس	۱
بیشترین استفاده از هر آدرس	۱,۲۳۸,۹۳۱
تعداد آدرس‌های یک‌بار استفاده‌شده	۱۰,۴۷۶,۸۹۹
تعداد آدرس‌های دو بار استفاده‌شده	۱,۳۹۷,۳۷۳
آدرس‌های با استفاده بیش از ۱۰۰ بار	۲۵,۰۰۴

استفاده مجدد از آدرس نه‌تنها برای خود فرد خطرناک است بلکه برای فرستنده و حتی کسانی که ارتباطی به آن تراکنش ندارند نیز خطرآفرین است و به‌نوعی می‌تواند نقض حقوق معقول مصرف‌کننده قلمداد شود. با شناسایی شما توسط افراد مهاجم در اثر استفاده چندباره از یک آدرس، شرکا و همکاران تجاری شما نیز شناسایی می‌شوند و پیدا کردن آدرس‌ها و تراکنش‌های آنان نیز کار سختی به نظر نمی‌رسد(Address reuse - Bitcoin Wiki).

کیف پول‌های بیت‌کوین

قبل از ورود به معرفی انواع کیف پول‌های بیت‌کوین، ابتدا لازم به ذکر است که به‌طورکلی کیف پول‌ها به دو دسته تقسیم‌بندی می‌شوند. کیف پول‌های داغ[۱] و کیف پول‌های سرد[۲]. کیف پول‌های داغ متصل به اینترنت هستند و کیف پول‌های سرد متصل به اینترنت نیستند. کیف پول‌های داغ ازآنجایی‌که متصل به اینترنت هستند دسترسی راحت‌تری به موجودی را برای کاربران فراهم می‌کنند و برای دادوستدهای روزانه و پرداخت‌های مستمر گزینه مناسب‌تری به نظر می‌رسند. کیف پول‌های سرد به دلیل عدم اتصال به اینترنت در موارد حمله هکرها به‌راحتی قابل‌دسترسی نخواهند بود و برای نگهداری بلندمدت و ذخیره ارزش انتخاب مناسبی هستند (KHATWANI 2019).

با توجه به مطالب ذکرشده، استفاده مجدد از آدرس از منظر فنی امر مناسبی قلمداد نمی‌شود. راه‌حل ساده برای آن استفاده از آدرس‌های یک‌بار مصرف است. بسته‌های نرم‌افزاری بسیاری مدیریت استفاده از آدرس‌های یک‌بار مصرف را انجام می‌دهند که به آن‌ها کیف پول قطعی[۳] می‌گویند. این کیف پول‌ها در صورت خواست کاربر، هراندازه آدرس که موردنیاز هست را می‌سازند و از آن‌ها برای دریافت و پرداخت استفاده می‌کنند. آن‌ها همچنین مجموع ورودی و خروجی هر آدرس را محاسبه می‌کنند تا موجودی واقعی کیف پول را نشان دهند. مدیریت کلید خصوصی‌های هر آدرس نیز بر عهده کیف پول است. کیف پول‌های قطعی را می‌توان پاسخی به مشکل امنیتی استفاده مجدد از آدرس دانست. کیف پول قطعی (Deterministic Wallets) یک سیستم، استخراج کلید از یک نقطه مشخص به سید[۴] است. سید (seed) این امکان را برای کاربر فراهم می‌کند که به‌سادگی یک پشتیبان از کیف پول خود تهیه کند. این سید (seed) ها به کلمات قابل‌خواندن برای انسان‌ها تبدیل می‌شوند. سه نوع کیف پول قطعی

[۱] Hot wallet
[۲] Cold wallet
[۳] Deterministic Wallets
[۴] Seed

(Deterministic Wallets) وجود دارد. کیف پول قطعی معمولی که از یک رشته‌های شناخته‌شده برای ساخت آدرس استفاده می‌کند. کیف پول‌های قطعی نوع دوم[۱] از استاندارد BIP 0032 برای تولید عبارات سید (seed) استفاده می‌کنند. کیف پول‌های قطعی نوع سوم[۲] مبتنی بر کلید ریشه[۳] و کد زنجیره‌ای[۴] هستند (Bitcoin Wiki).

پروتکل Bitcoin-QT پروتکلی برای پرداخت است. این پروتکل که هنوز اجرایی نشده است و احتمالا در آینده‌ای نزدیک عرضه خواهد شد، هدفش افزایش امنیت کاربران و بهبود تجربه کاربری آن‌هاست. در حال حاضر، تاجران آدرس کیف پول خود را در مرورگرها به مشتریان نمایش داده و مشتری‌ها با کپی کردن این آدرس‌ها پرداخت را انجام می‌دهند. اشکالات متعددی به این شیوه وارد است. اشتراک‌گذاری آدرس در اینترنت به‌صورت عمومی از دیدگاه فنی مناسب به نظر نمی‌رسد. مهاجم‌ها می‌توانند با دست‌کاری، آدرس دیگری را به مشتری نمایش دهند و استفاده از آدرس‌های الفبایی چندان کاربرپسند به نظر نمی‌رسد. طبق ادعای توسعه‌دهندگان، پروتکل Bitcoin-QT این مشکلات را حل کرده است. وقتی مشتری می‌خواهد تراکنشی انجام دهد، یک لینک دانلود برای او ظاهر می‌شود که یک درخواست تراکنش امضاشده است. با کلیک کاربر بر روی لینک، کیف پول او این درخواست را لود می‌کند. در این درخواست آدرس کیف پول تاجر، مبلغ و شرح خرید را دربر می‌گیرد. درخواست توسط سند X.509 امضا شده است که به مهاجم اجازه نمی‌دهد این سند را به‌راحتی جعل کند. گفتنی است که این پروتکل نیز برای هر تراکنش خود آدرس جدیدی می‌سازد.

مخفی کردن آدرس نیز یکی از راه‌های افزایش امنیت کاربران در شبکه پرداخت بیت‌کوین است. این پروتکل به کاربران آفلاین اجازه نمی‌دهد در تراکنش نقش داشته باشند. یک آدرس مخفی[۵] این امکان را فراهم می‌آورد که یک آدرس ثابت برای ارسال مشخص شود، اما بعد از پرداخت به آدرس‌های گمنامی تقسیم شود. این نه‌تنها مشکل استفاده مجدد از آدرس را حل می‌کند، بلکه به افراد اجازه نمی‌دهد از موجودی حساب کسی باخبر شوند(Bitcoinnotbomb)

[۱] Heuristic Wallet
[۲] Armory Deterministic Wallets
[۳] Root Key
[۴] Chain Code
[۵] stealth address

نتیجه‌گیری

با استفاده از نوآوری‌های جدید، اکنون تراکنش‌های شبکه بیت‌کوین امن‌تر و با محرمانگی بیشتری صورت می‌گیرد. ازجمله مشکلات تراکنش‌ها در این شبکه امکان مشاهده تمامی تراکنش‌های یک آدرس عمومی در بلاک‌چین است. روش‌های متعددی برای مهاجم وجود دارد که توسط آن‌ها امنیت یک تراکنش بیت‌کوین به خطر می‌افتد. در این مقاله استفاده مجدد از آدرس به‌عنوان یک عمل توصیه نشده مطرح گردید و معایب استفاده چندباره از یک آدرس عمومی به تفضیل بررسی شد. کیف پول‌های قطعی، پاسخی از طرف علاقه‌مندان و توسعه‌دهندگان شبکه به این مشکل است. این کیف پول‌ها با تمامی مزیت‌های خود، معایبی نیز دارند. استفاده از پروتکل Bitcoin-QT می‌تواند تا حد زیادی از این مشکلات بکاهد اما این پروتکل نیز تا به امروز اجرایی نشده است. مقاله بعدی از این مجموعه دوقسمتی به معرفی کیف پولی خواهد پرداخت که با استفاده از فناوری Coinjoin، مشکل امنیتی مطالعه شده در این مقاله را تا حد قابل قبولی مرتفع کرده است.

منابع

Anon, Address reuse - Bitcoin Wiki. Available at: https://en.bitcoin.it/wiki/Address_reuse [Accessed July 30, 2019a].

Anon, Blockchain attacks on privacy. *allprivatekeys*. Available at: https://allprivatekeys.com/blockchain-attacks-on-privacy [Accessed July 30, 2019b].

Barcelo, J., 2007. *User Privacy in the Public Bitcoin Blockchain*, Available at: https://github.com/jbarcelo/txfillstat [Accessed July 25, 2019].

Bitcoin Wiki, Deterministic wallet - Bitcoin Wiki. Available at: https://en.bitcoin.it/wiki/Deterministic_wallet [Accessed July 30, 2019].

Bitcoinnotbomb, Innovations that Enhance Bitcoin Anonymity » Bitcoin Not Bombs. Available at: https://www.bitcoinnotbombs.com/innovations-that-enhance-bitcoin-anonymity/ [Accessed July 30, 2019].

KHATWANI, S., 2019. 5 Different Types Of Crypto Wallets You Should Know About. *coinsutra*. Available at: https://coinsutra.com/types-of-crypto-wallets/ [Accessed July 7, 2019].

نویسنده

نام نویسنده: سلمان صادقی

ایمیل نویسنده: salli.sadeghi@gmail.com

منتشر شده توسط

کوین ایران

کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلوند و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید . هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com