امنیت کاربر در بلاک‌چین عمومی بیت‌کوین (قسمت دوم)

An easy introduction to Wasabi wallet

سلمان صادقی

۱۳۹۸/۵/۱۶

در این مقاله به بررسی کیف پول واسابی و فناوری موجود در آن یا همان کوین‌جوین پرداخته شده و با مقایسه با روش‌های افزایش محرمانگی دیگر، مزایا و معایب این کیف پول موردبررسی قرارگرفته است.

فهرست مطالب

مقدمه ۲
کیف پول Wasabi ۲
فناوری Coinjoin چیست؟ ۳
جمع‌بندی و نتیجه‌گیری ۶
منابع ۷

مقدمه

همانطور که در قسمت اول این مجموعه ذکر شد، انجام تراکنش در شبکه بیت‌کوین می‌تواند موجبات از دست رفتن محرمانگی فرستنده و گیرنده را فراهم نماید. استفاده مجدد از آدرس به عنوان یکی از راه‌های نفوذ افراد مهاجم به امنیت تراکنش‌ها مطرح گردید. همچنین کیف پول‌هایی معرفی شدند که برای هر تراکنش از یک آدرس متمایز استفاده می‌کردند. حملات و مشکلات امنیتی ذکرشده در مقاله اول این مجموعه، مزیت‌های استفاده از کیف پول‌های نرم‌افزاری مرسوم بیت‌کوین را از بین می‌برند. در این کیف پول‌ها همه مقادیر ورودی یک تراکنش متعلق به یک کاربر می‌باشند. همان‌طور که پیش‌تر ذکر شد، خطر این حملات می‌تواند با تمرکز بر نقاط حساسی که حمله‌ها صورت می‌گیرد، کاهش یابد.

گر کاربران مختلف در ایجاد یک تراکنش مشارکت نمایند و کوین‌های موجود در ورودی یک تراکنش متعلق به جمعی از کاربران باشد، حملات امنیتی ذکرشده در مقاله پیشین اعتباری نخواهند داشت. این تراکنش‌ها با ایجاد یک لایه گمراه‌کننده، امنیت تراکنش را افزایش می‌دهند.

ترکیب ورودی‌های مختلف توسط عده‌ای از کاربران برای ایجاد یک تراکنش، کوین‌جوین[۱] نامیده می‌شود و می‌تواند پاسخی به مشکلات امنیتی ذکرشده باشد. در این مقاله به بررسی کیف پول Wasabi و فناوری موجود در آن یا همان کوین‌جوین پرداخته شده و در ادامه با مقایسه با روش‌های افزایش امنیتی دیگر، مزایا و معایب این کیف پول موردبررسی قرارگرفته است.

کیف پول Wasabi

کیف پول Wasabi یک کیف پول دیجیتالی برای بیت‌کوین است که برای کاربران خود امکان ذخیره، مدیریت و استعلام موجودی بیت‌کوین خود را تحت ویندوز، لینوکس و مک فراهم آورده است.

این کیف پول از روش کوین‌جوین برای دریافت و پرداخت‌های خود استفاده می‌کند. این کیف پول منبع باز، در زبان برنامه‌نویسی سی شارپ[۲] نوشته شده و از قابلیت‌های پلتفرم NET Core استفاده نموده است. این بسته کاربردی شامل شبکه اصطلاحا پیازی[۳] Tor است و همه ترافیک‌های موجود بین مشتری‌ها و سرور، به‌منظور سری ماندن در این شبکه صورت می‌گیرد. استفاده از شبکه پیازی Tor باعث می‌شود آدرس IP

[۱] Coinjoin
[۲] C#
[۳] Onion Router

کاربران مخفی بماند؛ نصب و استفاده از آن نیز ساده است. در این کیف پول کلید خصوصی شخصی است؛ به این معنی که دارنده کلید خصوصی مالک کیف پول است.

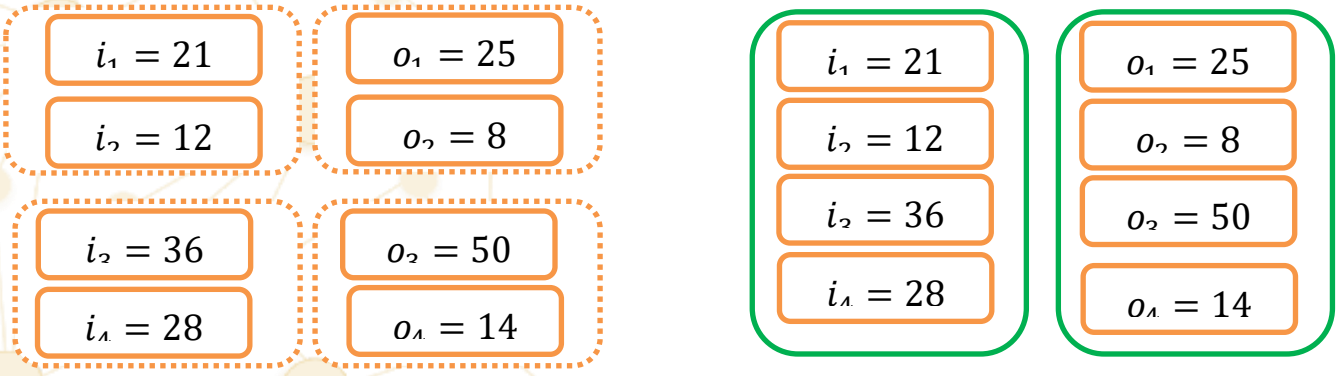
این کیف پول از تمامی استانداردهای امنیتی نظیر کیف پول قطعی[۴] و اجتناب از استفاده مجدد از آدرس[۵] و همچنین کنترل اجباری موجودی استفاده می‌کند. این کیف پول با استفاده از فیلتر کردن بلوک‌های مشتری محور، تاریخچه پرداخت‌های خود را به روشی خصوصی به دست می‌آورد. برای آشنایی با مکانیزم عملکردی این کیف پول، در ادامه مقاله به شرح فناوری استفاده‌شده توسط توسعه‌دهندگان این کیف پول پرداخته شده است.

فناوری Coinjoin چیست؟

گرگ مکسول (Greg Maxwell) توسعه‌دهنده مطرح بلاک‌چین در سال ۲۰۱۳ برای حفظ محرمانگی تراکنش‌ها روش کوین‌جوین را معرفی کرد (Maxwell 2013).

کوین‌جوین یک فناوری برای ترکیب چند تراکنش بیت‌کوین از فرستنده‌های مختلف در یک تراکنش است که امکان تشخیص اینکه کدام پرداخت‌کننده چه رسیدی پرداخت کرده را برای نهادها و یا افراد ثالث دشوار می‌کند. برخلاف روش‌های حریم خصوصی دیگر، این فناوری نیازی به همگام شدن با پروتکل بیت‌کوین را ندارد.

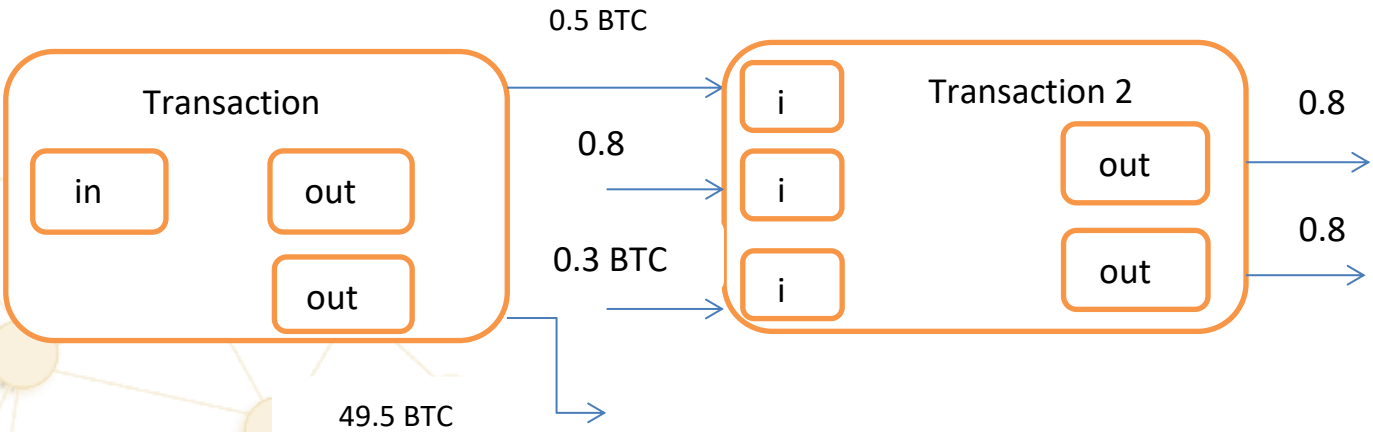
ایده اولیه این روش ساده است. در ساده‌ترین حالت ممکن دو کاربر، دو ورودی خود را برای ایجاد یک تراکنش ترکیب می‌کنند. آن‌ها دو خروجی و دو آدرس تغییریافته در انتهای تراکنش خواهند داشت (Barcelo 2007). به گراف زیر توجه کنید.



[۴] Deterministic wallet
[۵] Address reuse avoidance

در گراف بالا سارا می‌خواهد ۲۵ بیت‌کوین ارسال کند. او مالک دو تراکنش i_1 و i_2 است و خروجی او نیز o_1 و o_2 است. دارا نیز می‌خواهد ۵۰ بیت‌کوین ارسال کند و او نیز مالک i_3 و i_4 است و خروجی‌های او نیز o_3 و o_4 هستند.

برای توضیح اینکه چگونه یک تراکنش کوین‌جوینی می‌تواند یک پرداخت ناشناس را فراهم آورد باید بر مفهوم معاملات محرمانه[۶] دقت شود. معاملات محرمانه یک افزونه بر شبکه بیت‌کوین است که به کاربر امکان می‌دهد بدون مشخص شدن مقادیر ورودی و خروجی، یک تراکنش انجام دهد. برای پنهان کردن این اعداد و در پاسخ به مسئله مشهور کوله‌پشتی[۷] از الگوریتم رمزنگاری homomorphic commitments استفاده می‌شود. در این الگوریتم مقادیر ورودی تبدیل به خروجی‌هایی می‌شوند که وزن ارزشی ورودی اول را تکرار می‌کنند (Ruffing and Moreno-Sanchez n.d). در مثال فوق دارایی سارا ۳۱ بیت‌کوین و دارا ۶۴ بیت‌کوین است. با توضیحات بالا در یک تراکنش کوین‌جوینی مجموع دارایی‌های سارا و دارا به‌عنوان یک ورودی ۹۵ بیت‌کوینی و با استفاده از الگوریتم‌های معرفی‌شده بالا و با استفاده از بردارهای دوتایی خروجی‌های o_1 و o_2 و o_3 و o_4 را می‌سازند (Konstantin Maurer, Neudecker, and Florian). اجازه بدهید از مثال زیر برای هرچه بیشتر روشن شدن مفهوم تراکنش کوین‌جوینی استفاده شود.



یک تراکنش بیت‌کوین از یک یا چند ورودی تشکیل می‌شود و یک یا چند خروجی می‌سازد. هر ورودی خود خروجی یک تراکنش دیگر است. برای هر ورودی یک امضای متمایز مطابق با قوانین مشخص‌شده در

[۶] Confidential Transactions
[۷] Knapsack problem

خروجی تراکنش گذشته وجود دارد که استفاده می‌شود. سیستم بیت‌کوین زمانی فعال می‌شود که اطمینان حاصل کند امضاها معتبرند، ورودی‌ها واقعا وجود دارند و قابل خرج کردن هستند و همچنین مقدار خروجی

کمتر یا مساوی با مقدار ورودی است. هر خروجی از مجموع تمام ورودی‌ها تشکیل می‌شود. مقدار خروجی با جمع تمام ورودی‌ها برابر است. مقدار مشخص‌شده برای خروج از کیف پول خارج و مابقی به کیف پول خود فرد منتقل می‌شود. برای ورود به ادامه بحث لازم است دو مفهوم مهم در تراکنش‌های بیت‌کوین یعنی ScriptPubKey و Scriptsig تعریف شوند.

- یک سند قفل‌شده یا ScriptPubKey بر روی هر تراکنش بیت‌کوین قرار می‌گیرد و نیازمند شرایط خاصی است که دریافت‌کننده با فراهم کردن آن شرایط می‌تواند آن مقدار بیت‌کوین را خرج کند.
- امضای سند یا Scriptsig، مدرکی از مالکیت بر کلید خصوصی است که شرایط خاص تراکنش بیت‌کوین که توسط ScriptPubKey مشخص می‌شود را تأمین می‌کند و اجازه می‌دهد تا بیت‌کوین دریافت شده قابل‌خرج‌کردن شود.

هم ScriptPubKey و هم Scriptsig با زبان برنامه‌نویسی Script نوشته شده‌اند. این زبان برنامه‌نویسی فاقد توابعی است که زبان‌های توسعه‌یافته‌ی امروزی از آن استفاده می‌کنند و همین باعث امنیت بالاتر آن می‌شود (Bisola 2018).

با توجه به مطالب ذکرشده، هیچ نیازی نیست که ScriptPubKey ورودی‌هایی که خرج می‌شوند باهم یکسان باشد. در گراف بالا و در تراکنش شماره ۲، ورودی ۰٫۳ بیت‌کوین و ۰٫۸ بیت‌کوین که هرکدام ScriptPubKey مختص خود را دارند، در حال خرج شدن هستند. آیا لزومی دارد که فرستنده‌ی این دو مقدار یک فرد باشد؟ شاید حیرت‌انگیز باشد که بگوییم این فرض نادرست است و همین باعث می‌شود که Coinjoin را بتوان ممکن دانست.

امضاها (برای هر ورودی یک امضا) در یک تراکنش کاملا مستقل از یکدیگر هستند. این بدین معنی است که کاربران بیت‌کوین که برای خرج کردن مقداری بیت‌کوین ورودی و تبدیل آن به چند تراکنش خروجی موافقت کرده‌اند، به‌طور مستقل و جدا از هم تراکنش‌های خود را امضا کرده و بعدتر این امضاها را باهم ترکیب کنند. این نوع از تراکنش تا همه امضاها انجام نشوند توسط شبکه مورد تأیید قرار نمی‌گیرد و معتبر نیست و همچنین هر امضایی نیز نمی‌تواند با آن‌ها ترکیب شود.

برای انجام تراکنش به‌این‌ترتیب، تعداد مشخصی از کاربران باید بر روی یک استاندارد اندازه خروجی توافق کنند و ورودی‌هایی را صادر کنند که حداقل به آن اندازه‌ی توافق شده باشد. تراکنش به همان تعداد مشخص و به همان اندازه توافق شده خروجی خواهد داشت، همه کاربران امضا خواهند کرد و تراکنش صورت خواهد گرفت. در این مکانیزم هیچ شانسی برای دزدی در هیچ مرحله‌ای وجود ندارد.

در شکل بالا بیایید فرض کنیم ۰,۳ بیت مال فرستنده‌ای به نام سارا و ۰,۸ بیت مال فرستنده‌ای به نام دارا بوده است. آیا می‌توان گفت چه مقدار و کدام‌یک از ۰,۸ بیت‌کوین خروجی از تراکنش ۲ پول سارا و کدام‌یک پول دارا بوده است؟ این نوع تراکنش‌ها به‌مراتب غیرقابل تشخیص‌تر از تراکنش‌های مرسوم شبکه‌اند. به همین خاطر اگر این نوع تراکنش‌ها فراگیر شوند امنیت همه اعضا حتی آن‌هایی که از این مدل پرداخت استفاده نمی‌کنند را افزایش می‌دهد(Bitcoin Wiki 2017).

جمع‌بندی و نتیجه‌گیری

تاکنون روش‌های متعددی برای افزایش محرمانگی تراکنش‌ها در شبکه بیت‌کوین مطرح شده‌اند. پروژه‌هایی چون Zerocoin و CoinWitness با فناوری‌هایی جدید و حیرت‌انگیز خود و با همکاری با دانشگاه‌های معتبری چون MIT و The Technion برای افزایش حریم خصوصی کاربران شبکه بیت‌کوین تلاش می‌کنند. به عقیده نگارنده اما فناوری کوین‌جوین می‌تواند بهترین راه‌حل موجود برای افزایش این محرمانگی باشد. در پروژه Zerocoin، فارغ از اینکه اندازه امضاها بسیار بزرگ است (20kbyte) و این خود منجر به متورم شدن بلاک‌چین می‌شود، کاربران نیازمند یک نهاد سوم مورد اعتماد هستند که اگر متقلب باشد می‌تواند ارزها را به سرقت ببرد. در این پروژه که هنوز درحال‌توسعه است، تراکنش‌ها بزرگ و کند و درنتیجه گران هستند.

کوین‌جوین اما از روز اول تولد بیت‌کوین وجود داشته است. تاکنون چندین نوبت تراکنش‌هایی از نوع کوین‌جوین صورت گرفته است. به‌تازگی ۱۰۰ نفر از کاربران Wasabi با همکاری یکدیگر، یک تراکنش کوین‌جوین را به انجام رسانده‌اند. شواهد حاکی از آن است که تراکنش صورت‌گرفته از سوی کاربران Wasabi بزرگ‌ترین نمونه این نوع از تراکنش‌ها می‌باشد. هیچ محدودیتی برای تعداد مشارکت‌کنندگان در یک تراکنش کوین‌جوینی وجود ندارد. به‌واقع هرچه تعداد شرکت‌کننده‌ها بیشتر باشد، شکست محرمانگی تراکنش سخت‌تر خواهد بود. تنها محدودیت این فناوری این است که باید برای ایجاد تراکنش افراد دیگری نیز نیازمند انجام تراکنش باشند و این افراد به همدیگر متصل شوند که این محدودیت نیز توسط کیف پول Wasabi مرتفع گردیده است (Barcelo 2007).

جدای بحث افزایش محرمانگی، افزایش هزینه انتقال بیت‌کوین در آینده نیز می‌تواند ایده‌ی یک تراکنش همگانی را قوت بخشد.

منابع

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

Bisola, A., 2018. scriptPubKey & scriptSig Explained - Mycryptopedia. *Mycryptopedia*. Available at: https://www.mycryptopedia.com/scriptpubkey-scriptsig/ [Accessed July 18, 2019].

Bitcoin Wiki, 2017. CoinJoin - Bitcoin Wiki. Available at: https://en.bitcoin.it/wiki/CoinJoin [Accessed July 18, 2019].

Konstantin Maurer, F., Neudecker, T. & Florian, M., *Anonymous CoinJoin Transactions with Arbitrary Values*, Available at: https://www.comsys.rwth-aachen.de/fileadmin/papers/2017/2017-maurer-trustcom-coinjoin.pdf [Accessed July 25, 2019].

Maxwell, G., 2013. I taint rich! (Raw txn fun and disrupting “taint” analysis; >51kBTC linked!). *Bitcointalk*. Available at: https://bitcointalk.org/?topic=139581 [Accessed July 18, 2019].

Ruffing, T. & Moreno-Sanchez, P., *Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin*, Available at: https://allquantor.at/blockchainbib/pdf/ruffing2017mixing.pdf [Accessed July 25, 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