دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۲، جلد ۲۱، شماره ۲ (۱۶-۲۳)
https://monadi.isc.org.ir

ارائه‌شده در بیستیمین کنفرانس بین‌المللی انجمن رمز ایران در سازمان پژوهش‌های علمی و صنعتی ایران، ۸ و ۹ شهریور ۱۴۰۲

یک طرح مخلوط کردن جدید برای بهبود حریم خصوصی در تراکنش‌های رمزارز بیت‌کوین★

هادی نوروزی چلچه* و سلمان نیک صفت

دانشگاه صنعتی امیرکبیر، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
حریم خصوصی
بیت‌کوین
زنجیره بلوکی
امضای کورجزئی

dor: 20.1001.1.24763047.1402.12.2.2.8

نوع مقاله: پژوهشی

چکیده

تراکنش‌های مالی در رمزارز بیت‌کوین در یک پایگاه داده توزیعی به نام زنجیره بلوکی ذخیره می‌شوند. کلیه تراکنش‌ها با هدف شفافیت و امکان بررسی صحت به صورت عمومی برای کلیه گره‌های شبکه در دسترس‌اند. اما این ویژگی شفافیت زنجیره بلوکی با بهره‌برداری توسط تکنیک‌های تجزیه و تحلیل تراکنش‌ها، می‌تواند منجر به نقض حریم خصوصی کاربران و فاش شدن هویت آنها شود. تکنیک‌های مختلفی مانند روش مخلوط کردن تراکنش‌ها یا مبادله عادلانه با هدف ارتقای حریم خصوصی در تراکنش‌های بیت‌کوین توسط محققین ارائه شده است. در این مقاله ما به ارائه یک طرح مخلوط کردن جدید می‌پردازیم که برخی از نقاط ضعف روش‌های پیشین را رفع کرده است. مشخصاً در طرح ارائه شده کاربران می‌توانند در هر دور از اجرای پروتکل مقادیر متفاوتی از بیت‌کوین را مخلوط کنند که منجر به دستیابی به نتیجه در زمان کوتاه‌تر و با هزینه کمتر می‌شود. همچنین این طرح مقاومت بالاتری نسبت به حملات انکار سرویس توسط کاربران بدخواه دارد.

۱ مقدمه

زنجیره بلوکی به عنوان فناوری اصلی ارزهای رمزنگاری شده، در سال ۲۰۰۸ توسط ساتوشی ناکاموتو معرفی شد. این فناوری، از نوعی پایگاه داده توزیع‌شده استفاده می‌کند که تراکنش‌ها در آن نگهداری می‌شوند. کاربر برای انتقال پول، تراکنشی ایجاد کرده و به شبکه ارسال می‌کند. این تراکنش توسط یکی از ماینرها انتخاب شده، در یک بلاک جدید قرار گرفته و فرآیند استخراج بلاک انجام می‌شود. سپس در صورت موفقیت فرآیند ماینینگ، ماینر مربوطه این بلاک را برای تمام اعضای شبکه ارسال می‌کند. تمام اعضای شبکه تراکنش‌های موجود در این بلاک را اعتبارسنجی کرده و زمانی که فرآیند اعتبارسنجی تکمیل شد، اعضای شبکه این بلوک جدید را به انتهای زنجیره بلوکی اضافه می‌کنند. در این هنگام این تراکنش توسط کاربر مقصد قابل مشاهده خواهد بود. اما این ویژگی شفافیت زنجیره بلوکی، ممکن است منجر به نقض حریم خصوصی کاربران و فاش شدن هویت آنها شود.

هرچند در زنجیره بلوکی، کاربران معمولاً از مقادیر هش کلیدهای عمومی تصادفی انتخاب شده به عنوان شناسه برای پنهان کردن هویت واقعی خود استفاده می‌کنند. با این حال، می‌توان هویت واقعی کاربران را فاش کرد یا فعالیت‌های آنها را با تجزیه و تحلیل تراکنش های آنها پیگیری کرد [۱]. به طور مثال، رِید و همکاران با ایجاد گراف پیوند پرداخت، روابط ورودی و خروجی در شبکه تراکنش‌ها را تجزیه و تحلیل کردند و سپس چندین ورودی را در یک آدرس واحد جمع‌آوری کردند تا نشان دهند که تراکنش‌های چند ورودی عموماً با امضای یک مالک آغاز شده است. کلید عمومی کاربر و اطلاعات ارائه شده توسط وب‌سایت مربوطه، تهدیدی برای حریم خصوصی هویت کاربر است [۲]. به عنوان مثال، اگر یک کاربر کالا را با استفاده از بیت‌کوین به صورت آنلاین خریداری کند، فروشگاه آنلاین می‌تواند به جزئیاتی مانند آدرس ایمیل

★از کمیته علمی بیستمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: h_norouzi@aut.ac.ir (هادی نوروزی چلچه)، niksefat@aut.ac.ir (سلمان نیک صفت)

کاربر، آدرس ارسال، آدرس IP و غیره دسترسی پیدا کند [۳]. در مرجع [۴] تجزیه و تحلیل تراکنش‌ها به این شکل است که ابتدا مهاجم با تحلیل دفترکل توزیعی بیت کوین، گرافی جهت‌دار از تراکنش‌ها ایجاد می‌کند. در این گراف هر گره یک تراکنش است و یال‌های ورودی و خروجی نیز ورودی‌های و خروجی‌های هر تراکنش را نشان می‌دهند. سپس با تحلیل گراف تراکنش‌ها، مهاجم گراف جدیدی به نام گراف آدرس‌ها ایجاد میکند که گره‌های این گراف، آدرس‌ها و یال‌های آن ارتباط بین آنها را نشان می‌دهد و در نهایت با گروه‌بندی آدرس‌هایی که به نظر می‌رسد متعلق به یک کاربر هستند می‌تواند تراکنش‌ها را ردیابی کرده و جریان پولی را به دست آورد.

جهت جلوگیری از مرتبط کردن تراکنش‌ها و فاش شدن هویت افراد در بیت کوین، روش‌های مختلفی مانند تراکنش‌های ترکیبی [۵–۸] یا مبادله عادلانه [۹–۱۱]، ارائه شده که در بخش کارهای مرتبط به بیان نقاط قوت و ضعف آنها می‌پردازیم.

در این مقاله ما طرح جدیدی بر مبنای ایده مخلوط کردن تراکنش‌ها برای مقابله با تکنیک‌های تجزیه تحلیل تراکنش‌ها ارائه می‌دهیم که برخی مشکلات و نقاط ضعف طرح‌های قبلی را را رفع می‌کند.

۱.۱ نوآوری‌های مقاله

نوآوری‌های مقاله به شرح ذیل است:

۱- امکان بینام‌سازی مقادیر متفاوت از ورودی شرکت کنندگان در اغلب طرح‌های میکسینگ فعلی، شرکت‌کنندگان می‌بایست مقادیر بیت‌کوین یکسانی به عنوان ورودی وارد طرح نمایند [۹–۱۴]. در برخی طرح‌های دیگر هر چند مقدار ورودی می‌تواند متفاوت باشد، اما مقدار پولی که میکس می‌شود بین همه افراد یکسان بوده و مابقی پول بدون حفظ حریم خصوصی به حساب شرکت‌کنندگان برمی‌گردد [۸، ۱۴]. در BCM [۱۲] هر چند مقدار ورودی می‌تواند متفاوت باشد، اما شرکت‌کنندگان نیازمند یافتن افرادی هستند که معادل بیت‌کوین خود موجودی داشته باشند. این مورد در خیلی از حالات یا سخت است یا امکان‌پذیر نیست.

ثابت بودن مقدار بینام‌شده سبب می‌شود تا برای بینام‌سازی مقادیر بیشتر، نیاز شود تا پروتکل در دورهای بیشتری اجرا شود. روش ارائه شده توسط ما امکان مشارکت کاربران با مقدار ورودی بیت‌کوین متفاوت را می‌دهد و کل مقدار بیت‌کوین ورودی هر شرکت‌کننده در هر دور می‌تواند میکس شود. این روش محدودیت‌های روش‌های قبلی را رفع می‌کند و به کاربران آزادی عمل بیشتری می‌دهد.

۲- مقاومت بهتر در برابر حملات DoS توسط کاربران بدخواه در این مقاله بحث می‌کنیم که بلک‌لیست کردن ورودی‌های کاربران بدخواه یک روش بسیار کم هزینه‌تر، سریع‌تر و موثرتر برای مقابله با حملات DoS در طرح‌های مخلوط کردن نسبت به سایر روش‌ها است. همچنین در برخی از طرح‌های مخلوط کردن موجود از ایده امضای کور آدرس‌های خروجی افراد توسط میکسر استفاده شده است. در این مقاله به این موضوع اشاره می‌کنیم که این روش می‌تواند ناامن باشد و مورد سوءاستفاده کاربران بدخواه قرار بگیرد. در این مقاله با استفاده از یک طرح امضای کور جزئی، طرحی ارائه می‌کنیم که مقاومت بالاتری در مقابل کاربران بدخواه دارد.

۲ کارهای مرتبط

در این به بخش به مرور کارهای مرتبط در حوزه افزایش حریم خصوصی تراکنش‌های بیت‌کوین پرداخته می‌شود.

سرویس‌های مخلوط کردن کلاسیک [۱۵] از اولین روش‌ها برای غیرقابل رهگیری کردن بیت‌کوین بودند که کماکان نیز فعالند. در این سرویس‌ها کاربران کوین‌های خود را برای یک میکسر مرکزی ارسال می‌کنند و میکسر طی یک یا چند تراکنش از منابع دیگر معادل بیت‌کوین ورودی (البته منهای کمیسیون میکس و هزینه ماینینگ) را برای کاربر واریز می‌نماید. در این سرویس‌ها میکسر باید صادقانه عمل کند. در غیر این صورت احتمال سرقت کوین‌ها توسط میکسر و همچنین فاش‌شدن ارتباط بین افراد وجود دارد. در برخی کارهای تحقیقاتی بعدی برای کاهش این کاستی‌ها، میکسر مسوولیت‌پذیر شده و خطای میکسر توسط کاربر قابل اثبات است [۱۳، ۱۴]. اما در این کارها کماکان امکان سرقت سکه توسط میکسر وجود دارد. ایده میکسرهای توزیعی مانند [۱۲] نیز وضعیت را بهبود داده، اما در [۱۲] باید حداقل $\frac{2}{3}$ میکسرها صادقانه عمل کنند؛ در غیر این صورت امکان تبانی، انجام حمله Sybil و سرقت سکه‌ها وجود دارد.

در یک خط تحقیقاتی دیگر، از ایده تراکنش‌های ترکیبی استفاده شده است که چندین کاربر با ورودی‌ها و خروجی‌های متعدد به طور مشترک یک تراکنش واحد را تشکیل می‌دهند. به این ترتیب، یک مهاجم نمی‌تواند به راحتی ورودی تراکنش را به خروجی تراکنش پیوند دهد [۶–۸]. ایده اولیه این کار توسط Maxwell با نام CoinJoin [۸] ارائه شده است که هم به صورت توزیعی و به هم صورت مرکزی قابل پیاده‌سازی است. چون عملیات بینام‌سازی طی یک تراکنش هماهنگ انجام می‌شود، حتی در حالت مرکزی مشکل سرقت سکه در این کارها وجود ندارد. همچنین عملیات گمنام‌سازی به سرعت (طی یک بلاک) و با هزینه پایین (یک Transaction Fee) انجام می‌شود. اما برخی از این طرح‌ها با مشکل DoS توسط کاربران بدخواه مواجه‌اند [۶] و در برخی دیگر میزان بیت‌کوینی که در هر بار اجرا بینام می‌شود بین همه افراد ثابت و معادل مقدار v است [۷، ۸].

لذا کاربری که مقدار بیت‌کوین ورودی او بیش از v است، مابقی بیت‌کوین را در یک آدرس باقی‌مانده تحویل می‌گیرد و برای بینام کردن آن باید پروتکل را در دورهای متعدد (هر بار به اندازه v) اجرا نماید. این مساله باعث صرف زمان و هزینه زیاد توسط کاربرانی می‌شود که حجم بیت کوین آنها بیشتر است.

در یک خط تحقیقاتی دیگر پروتکل‌ها و طرح‌های متعددی ارائه شده که ایده اصلی آن طرح‌های مبتنی بر مبادله عادلانه است. در این روش‌ها

دو یا تعدادی از افراد به صورت مستقیم [۵، ۹] یا با واسطه [۱۰، ۱۱] با هم، کوین‌های خود را بر مبنای یک الگوریتم مبادله عادلانه دو به دو مبادله می‌کنند [۵، ۹–۱۱]. الگوریتم مبادله عادلانه این امکان را فراهم می‌کنند که یا کل عملیات مبادله پول بین افراد انجام شود یا هیچ تراکنشی انجام شود. بدین ترتیب امکان سوءاستفاده و سرقت پول از بین می‌رود. ایده کلی این طرح‌ها مبتکرانه و جالب است، اما مشکل اصلی این طرح‌ها زمان و هزینه بالای اجرای آنهاست. در این طرح‌ها نیاز به انجام چندین تراکنش وجود دارد که این تراکنش‌ها نیز حداقل در دو بلاک مختلف می‌بایست انجام شوند. همچنین در این طرح‌ها، تراکنش‌های نهایی ثبت شده در بیت‌کوین، به صورت تراکنش‌های با ورودی و خروجی‌های متعدد نبوده و هر تراکنش بین یک فرستنده و یک گیرنده صورت می‌گیرد. این مسأله وقتی که شما یک پول کثیف را با پول خود عوض می‌کنید می‌تواند برای شما مشکل‌ساز شود، چون رد پول کثیف به آدرسی خواهد رسید که متعلق به شماست (جرم قبلی). همچنین در صورتی که شما پول خود را که ارتباط آن با شما لو رفته را توسط یکی از این پروتکل‌ها به آدرس یک فرد مجرم واریز نمایید و آن فرد با استفاده از این پول یک عمل مجرمانه انجام دهد، شما به نوعی با یک فرد مجرم مرتبط می‌شوید (جرم بعدی)، در صورتی که در کارهای مبتنی بر Coinjoin به علت منطبق شدن، ورودی و خروجی‌های متعدد، مسئولیت بسیار کمتری متوجه افراد می‌کند. علاوه بر این مانند پروتکل‌های تراکنش ترکیبی، مقدار بیت‌کوین ورودی در اغلب این طرح‌های مقدار ثابت v است و برای بینام‌سازی مقادیر بیشتر، پروتکل می‌بایست در دورهای بیشتری اجرا شود که هزینه و زمان بینام‌سازی را دوچندان می‌کند.

در این مقاله ما با الهام گرفتن از طرح Coinjoin طرحی را بر مبنای آن ارائه می‌کنیم که برخی محدودیت‌های مطرح شده در بالا را رفع می‌نماید.

۳ مفاهیم پایه

۱.۳ امضای کور جزئی

اگر در امضای کور بخشی از پیام کور و بخش دیگر پیام کور نشود، به امضای کور جزئی [۱۶] تبدیل می‌شود. مراحل این الگوریتم به این صورت است که ابتدا فرستنده پیام را با عدد تصادفی r کور می‌کند و برای امضاکننده ارسال می‌کند، امضاکننده مقدار دریافتی را با کلید خصوصی‌اش امضا می‌کند و برای فرستنده ارسال می‌کند. فرستنده با دریافت امضای کور شده، امضای کور نشده را با استفاده از مقدار تصادفی r به دست می‌آورد.فرستنده امضای دریافتی را اعتبارسنجی می‌کند که امضا معتبر است یا خیر.

۲.۳ مدل تهدید

در این طرح هم مهاجم خارجی و هم افراد شرکت‌کننده در طرح، شامل میکسر و شرکت‌کنندگان، می‌توانند رفتار بدخواهانه داشته باشند. جهت نیازمندی عدم سرقت، یک شرکت‌کننده درستکار می‌تواند در کنار تعداد دلخواهی مشارکت‌کننده بدخواه قرار گیرد. جهت تأمین حریم خصوصی حداقل دو نفر از شرکت‌کنندگان باید درستکار باشند، در غیر این صورت مهاجمین بدخواه می‌توانند با تبانی آدرس‌های خروجی فرد درستکار را تشخیص دهند.

جدول ۱. پارامترها

نام پارامتر	علامت
پیام درخواست اولیه کاربر j به میکسر	$Request_j$
شماره دور اجرای میکس	ID
مقدار بیت‌کوین ورودی کاربر jام	$amount_j$
کلید عمومی میکسر	Pk
کلید خصوصی میکسر	sk
بزرگترین مقسوم علیه مشترک تراکنش‌های ورودی	gcd
تعداد آستانه کاربران برای شروع عملیات میکسینگ	TH
عامل کور کننده کاربر jام	R_j
تعداد خروجی‌های کاربر jام	$output_j$
آدرس‌های خروجی کاربر jام	A_j
آدرس‌های خروجی کور شده کاربر jام	BA_j
آدرس‌های خروجی امضا شده کاربر jام	SA_j
آدرس‌های خروجی کورشده و امضا شده کاربر jام	SBA_i
تراکنش مخلوط شده خام شامل تراکنش‌های ورودی و آدرس‌های تأیید شده با مقدار مساوی	$Tran_{raw}$
تراکنش مخلوط شده خام امضا شده	$Signed\_Tran_{raw}$
تراکنش ترکیبی معتبر نهایی	$Tran_{mix}$

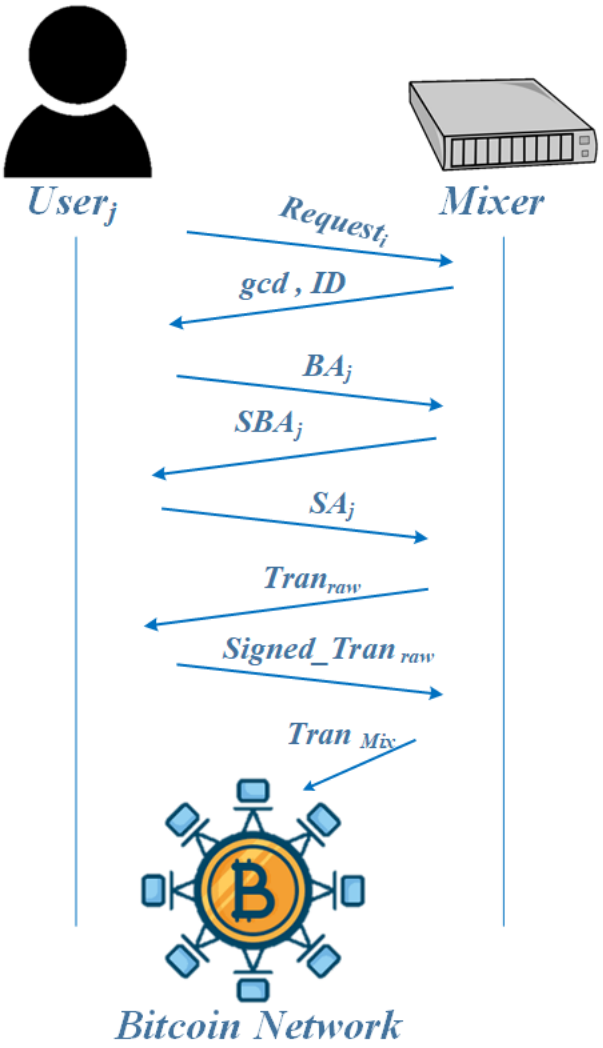
۴ طرح پیشنهادی

کل فرآیند پروتکل شامل سه مرحله اصلی است: مرحله درخواست کاربر، مرحله تولید آدرس‌های خروجی و مرحله ایجاد و انتشار تراکنش نهایی. پارامترهای استفاده شده در طرح به شرح ذیل در جدول ۱ قابل مشاهده است. شکل ۱ جریان کلی طرح پیشنهادی را نشان می دهد.ذیلاً جزئیات طرح پیشنهادی را ارائه می‌کنیم.

۱.۴ مرحله درخواست کاربر

در مرحله در خواست مراحل زیر انجام می‌شود.

۱. کاربری که می‌خواهد بیت‌کوین‌های خود را ناشناس کند، یک پیام درخواست اولیه $Request_j$ ایجاد می‌کند. در این درخواست، کاربر مقدار بیت‌کوین خود را در قالب یک پیام با کلید خصوصی متناظر با کوین خود امضا کرده و برای میکسر ارسال می‌کند. بدین ترتیب میکسر مطمئن می‌شود که یک مالک واقعی بیت‌کوین قصد مشارکت در طرح را دارد.



شکل ۱. جریان کلی طرح پیشنهادی

۲. میکسر از خرج نشده بودن تراکنش بیت‌کوین دریافتی اطمینان حاصل می‌کند و با بررسی امضا، تعلق آن به کاربر را اعتبارسنجی می‌کند. همچنین، با توجه به شرایط، میکسر می‌تواند محدودیت‌هایی در رابطه با مقدار بیت‌کوین‌های دریافتی اعمال کند. مثلا روی تعداد اعشار مبلغ یا مقدار مبلغ محدودیت‌هایی بگذارد. این محدودیت‌ها برای تامین حریم خصوصی اعمال می‌شوند و کلیه مشارکت‌کنندگان در طرح باید رعایت کنند.

در صورتی که مقدار بیت‌کوین ارسالی مجاز بود، در صف عملیات میکسینگ قرار می‌گیرد. در صورتی که صف عملیات میکسینگ به مقدار TH (حد آستانه تعداد مشارکت‌کنندگان) رسید، عملیات میکسینگ با اعلان مقدار بزرگترین مقسوم علیه مشترک مقادیر ورودی (gcd) به مشارکت‌کنندگان شروع می‌شود.

به هر دور اجرای میکس یک ID توسط میکسر اختصاص می‌یابد. در این مرحله، میکسر یک پیام پاسخ gcd معادل با بزرگ‌ترین علیه مشترک مقادیر بیت‌کوین‌های دریافتی و شناسه اجرای مخلوط کردن (ID) برای هر کاربر ارسال می‌کند.

۲.۴ مرحله تولید آدرس‌های خروجی

در این مرحله، عملیات زیر به ترتیب انجام می‌شود.

۱. هر کاربر تعداد خروجی‌های مورد نیاز خود ($output_j$) را با تقسیم مقدار پول خود به gcd محاسبه می‌کند:

$$output_j = \frac{amount_j}{gcd}.$$

سپس به تعداد خروجی‌های خود ($output_j$)، عامل کور کننده R_j و آدرس خروجی A_j برای پس گرفتن بیت‌کوین ورودی خود به صورت تصادفی تولید می‌کند. در نهایت آدرس‌های خروجی را با عوامل کورکننده، کور کرده و نتیجه را (BA_j) برای میکسر ارسال می‌کند. پیام‌های مبادله شده بین کابران و میکسر در یک کانال/صفحه عمومی که همه کاربران و میکسر به آن دسترسی دارند نوشته می‌شود. بدین ترتیب افرادی که در پروتکل شرکت می‌کنند با مانیتور کردن این کانال صبر کنند افراد دیگر هم آدرس‌های خود را ارسال کنند و بعد آدرس‌های خود را به تدریج میان آدرس‌های دیگر ارسال می‌نمایند.

۲. میکسر تعداد آدرس‌ها را با مقدار بیت‌کوین آن کاربر چک کرده و در صورت صحت، در پاسخ مقادیر آدرس‌های خروجی را به همراه ID اجرای میکس (مرحله قبل) توسط یک طرح امضای کور جزئی، امضا کرده و نتیجه را (SBA_j) به کاربر بر می‌گرداند. مقدار id بخش کور نشده پیام و آدرس‌ها بخش کور شده پیام هستند.

۳. کاربران آدرس‌های امضا شده توسط میکسر را با استفاده از عامل کور کننده از حالت کور شده خارج می‌کنند (SA_j). همچنین کاربران صحت امضای میکسر بر روی آدرس‌های خروجی خود را با کلید عمومی (pk) میکسر چک می‌کنند.

۴. کاربر آدرس‌های خروجی کور نشده خود (همراه ID) را از طریق یک شبکه Anonymous مانند TOR در کانال عمومی میکسر می‌نویسد. علت استفاده از شبکه گمنامی این است که میکسر نتواند ارتباطی بین IP کاربر و آدرس‌های ورودی و خروجی را حدس بزند. کانال عمومی این مزیت را دارد که شرکت‌کنندگان از پیشرفت پروتکل و پیام‌های سایر شرکت‌کنندگان آگاه می‌شوند و می‌توانند پیام‌های خورد را در بین سایر پیام‌ها با هدف حفظ حریم خصوصی ارسال نمایند.

۵. میکسر امضای آدرس‌ها را چک کرده و همچنین از درست بودن دور اجرا مطمئن می‌شود. بدین ترتیب یک کاربر بدخواه نمی‌تواند یک آدرس خروجی که قبلاً توسط میکسر امضا شده است را در دور جاری جا بزند.

۳.۴ مرحله ایجاد و تراکنش نهایی

۱. میکسر یک تراکنش مخلوط شده خام $Tran_{raw}$ شامل تمام تراکنش‌های ورودی و آدرس‌های تأیید شده خروجی با مقدار مساوی

ایجاد می‌کند.

۲. کاربر بررسی می‌کند که آیا تراکنش مخلوط شده $Tran_{raw}$ شامل تمام تراکنش‌های ورودی و آدرس‌های خروجی او با بیت‌کوین‌هایی که دارد مطابقت دارد یا خیر. اگر تمام اطلاعات موجود در $Tran_{raw}$ صحیح باشد، کاربر تراکنش مخلوط شده را با استفاده از کلید خصوصی مربوط به تراکنش‌های ورودی خود امضا کرده و $Tran_{raw}$ امضا شده با عنوان $Signed\_Tran_{raw}$ را با استفاده از TOR مجدداً به میکسر می‌فرستد. در صورتی که کاربری با وجود صحت تراکنش خام، از امضای آن سرباز بزند، تراکنش‌های خرج نشده فرد خاطی وارد لیست شده و در اجراهای بعدی مشارکت داده نخواهد شد.

۳. پس از دریافت تمام امضاهای معتبر تراکنش‌های ورودی، میکسر آنها را دوباره ترکیب می‌کند تا تراکنش ترکیبی معتبر $Tran_{mix}$ را تشکیل دهد و سپس آن را به عنوان تراکنش‌های عادی در شبکه بیت‌کوین پخش می‌کند.

۵ ارزیابی طرح

طرح پیشنهادی حریم خصوصی را در برابر کاربران بدخواه و میکسر و مهاجم خارجی حفظ می‌کند. که در ادامه تشریح آنها می‌پردازیم.

۱.۵ حفظ حریم خصوصی در برابر میکسر

به علت استفاده از امضای کور در مرحله تولید آدرس‌های خروجی، میکسر نمی‌تواند ارتباطی بین ورودی‌ها و خروجی‌های کاربران تشخیص دهد. همچنین استفاده از شبکه گمنامی مانع از این می‌شود که میکسر با تجزیه و تحلیل آدرس‌های IP مبدا به هویت شرکت‌کنندگان پی ببرد.

۲.۵ حفظ حریم خصوصی در برابر مهاجم خارجی

پس از انتشار تراکنش در بیت کوین، یک مهاجم خارجی ممکن است به تحلیل آدرس‌های ورودی و خروجی و ارتباط آنها با همدیگر بپردازد. توجه کنید که هر آدرس خروجی می‌تواند به هر یک از ورودی‌ها تعلق داشته باشد، اما به علت متفاوت بودن مقادیر ورودی‌ها، احتمال تعلق هر یک از آدرس‌های خروجی به هریک از ورودی‌ها متفاوت است. به طور کلی هر چه تعداد شرکت‌کنندگان بالاتر بوده و تعداد آدرس‌های خروجی به طور یکنواخت بین شرکت‌کنندگان توزیع شده باشد، به صورت میانگین حریم خصوصی بالاتری تامین می‌شود.

۳.۵ حفظ حریم خصوصی در برابر کاربر بدخواه

این طرح می‌تواند در برابر بدرفتاری کاربران ایمن باشد، زیرا کاربران مشارکت‌کننده نمی‌توانند در مرحله ارسال آدرس‌های خروجی، تعداد آدرس خروجی بیش از سهم خود برای میکسر ارسال کنند؛ چون میکسر در مرحله تولید، تنها تعداد معینی آدرس، متناسب با مقدار ورودی فرد و بزرگترین مقسوم علیه مشترک مقادیر، را برای هر کاربر امضا می‌کند. تنها حمله متصور این است که کاربر، یکی از آدرس‌های خروجی که در اجراهای موازی یا قبلی از میکسر گرفته، در طرح وارد کند. در این حالت کاربر بدخواه تلاش می‌کند جلوی ارسال یک یا چند آدرس خروجی معتبر از کاربران صادق را گرفته و آدرس‌های امضا شده قبلی خود را وارد اجرا کند تا سهم بیشتری از پول را دریافت کند یا اجرا را با اختلال مواجه کند. این حمله به علت استفاده از امضای کور جزئی و درج شماره اجرا در امضا قابل انجام نیست و میکسر تنها آدرس‌های خروجی که امضای آنها حاوی شماره دور فعلی باشد را می‌پذیرد.

همچنین در صورتی که کاربری با وجود صحت تراکنش خام، از امضای آن سرباز بزند، می تواند به نوعی طرح را با اختلال مواجه کند. در طرح پیشنهادی ما برای مقابله با این سناریو، از ایده بلک‌لیست کردن مقدار بیت‌کوین‌هایی استفاده کرد که در مرحله آخر امضا نشده‌اند. بدین ترتیب مقدار بیت‌کوین‌های فرد خاطی وارد بلک‌لیست شده و در اجراهای بعدی مشارکت داده نخواهد شد.

۴.۵ مقایسه طرح ما با دیگر طرح های مخلوط کردن

در جدول ۲ به مقایسه ویژگی‌های طرح ما با دیگر طرح‌های مخلوط کردن پرداخته می‌شود. در این جدول ویژگی تعداد بلاک مورد نیاز، تعداد بلاک مورد نیاز برای مخفی کردن تراکنش‌های شرکت کنندگان را نشان می‌دهد و ویژگی مقدار بیت کوین بی‌نام شده به ازای هر فرد، مقدار بیت‌کوینی که افراد برای شرکت در طرح استفاده می‌کنند را نشان می‌دهد که می‌تواند ثابت یا متفاوت باشد. همان‌طور که مشاهده می‌شود روش ارائه شده توسط ما امکان مشارکت کاربران با مقدار ورودی بیت‌کوین متفاوت را می‌دهد و کل مقدار بیت‌کوین ورودی هر شرکت‌کننده در هر دور می‌تواند مخلوط شود. این روش محدودیت‌های روش‌های قبلی را رفع می‌کند و به کاربران آزادی عمل بیشتری می‌دهد.

۶ نتیجه‌گیری

بیت‌کوین یک ارز دیجیتال غیرمتمرکز است که به دلیل ویژگی‌هایی که دارد به طور گسترده مورد توجه زیادی قرار گرفته است. بیت‌کوین تمام تاریخچه تراکنش‌ها را روی یک بلاک‌چین عمومی نگه می‌دارد. از آنجایی که تمام تراکنش‌های ثبت شده بیت‌کوین در بلاک‌چین برای همه عمومی است، کاربران بیت‌کوین با خطر افشای حریم خصوصی مالی روبرو هستند. روش‌های زیادی برای ناشناس کردن پیوند سوابق تراکنش‌ها به هویت‌های واقعی پیشنهاد شد اما هیچ یک از آنها تمام ویژگی‌های امنیتی مورد نیاز مشتریان را برآورده نکردند. در این مقاله یک طرح مخلوط کردن جدید ارائه داده شد که مشکلات روش‌های قبلی را نداشته باشد و حریم خصوصی تراکنش‌ها را بهبود دهد.

جدول ۲. مقایسه ویژگی طرح ما با دیگر طرح های مخلوط کردن

طرح	تکنیک مورد استفاده	حریم خصوصی در برابر میکسر	ضد سرقت توسط میکسر یا سایر کاربران	تعداد بلاک مورد نیاز (هزینه)	مقدار بیت کوین بی‌نام شده به ازای هر فرد
Coinjoin [۸]	تراکنش ترکیبی (مخلوط)	✘	✔	۱	ثابت
Coinshuffle [۷]	تراکنش ترکیبی (مخلوط)	✔	✔	۱	ثابت
Coinparty [۱۲]	چندین تراکنش یک به یک با استفاده از محاسبات چند طرفه امن	✘	اگر $\frac{2}{3}$ میکسرها صادق باشند	۲	ثابت
Xim [۹]	مبادله عادلانه دو به دو	✔	✔	۷	ثابت
Mixcoin [۱۳]	مخلوط کردن سنتی با قابلیت حسابرسی	✘	✘	۲	ثابت
Blindcoin [۱۴]	مخلوط کردن سنتی با قابلیت حسابرسی	✔	✘	۲	ثابت
Coinswap [۱۰]	مبادله عادلانه دو به دو	✘	✔	۲	ثابت
Tumblebit [۱۱]	مبادله عادلانه	✔	✔	۲	ثابت
طرح لیو [۶]	تراکنش ترکیبی (مخلوط)	✔	✔	۱	متفاوت اما با ضرایب از پیش تعیین شده
BCM [۵]	تراکنش ترکیبی (مخلوط)	✔	✔	۲	متفاوت
طرح ما	تراکنش ترکیبی (مخلوط)	✔	✔	۱	متفاوت

مراجع

[1] Peng, Li, Feng, Wei, Yan, Zheng, Li, Yafeng, Zhou, Xiaokang, and Shimizu, Shohei. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, 7(3):295–307, 2021.

[2] Reid, Fergal and Harrigan, Martin. *An analysis of anonymity in the bitcoin system*. Springer, 2013.

[3] Goldfeder, Steven, Kalodner, Harry, Reisman, Dillon, and Narayanan, Arvind. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *arXiv preprint arXiv:1708.04748*, 2017.

[4] Conti, Mauro, Kumar, E Sandeep, Lal, Chhagan, and Ruj, Sushmita. A survey on security and privacy issues of bitcoin. *IEEE communications surveys & tutorials*, 20(4):3416–3452, 2018.

[5] Tennant, Laurence. Improving the anonymity of the iota cryptocurrency. *Univ. Cambridge, Cambridge, UK, Tech. Rep*, pp. 10–09, 2017.

[6] Liu, Yi, Liu, Xingtong, Tang, Chaojing, Wang, Jian, and Zhang, Lei. Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin. *IEEE Access*, 6:23261–23270, 2018.

[7] Ruffing, Tim, Moreno-Sanchez, Pedro, and Kate, Aniket. Coinshuffle: Practical decentralized coin mixing for bitcoin. in *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19*, pp. 345–364. Springer, 2014.

[8] Maxwell, Gregory. Coinjoin: Bitcoin privacy for the real world. in *Post on Bitcoin forum*, vol. 3, p. 110, 2013.

[9] Bissias, George D, Ozisik, A Pinar, Levine, Brian N, and Liberatore, Marc D. Xim: Distributed match-and-mix for bitcoin.

[10] Maxwell, Gregory. Coinswap: Transaction graph disjoint trustless trading. *CoinSwap: Transactiongraphdisjoint-trustlesstrading (October 2013)*, 2013.

[11] Heilman, Ethan, Alshenibr, Leen, Baldimtsi, Foteini, Scafuro, Alessandra, and Goldberg, Sharon. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. in *Network and Distributed System Security Symposium*, 2017.

[12] Ziegeldorf, Jan Henrik, Grossmann, Fred, Henze, Martin, Inden, Nicolas, and Wehrle, Klaus. Coinparty: Secure multi-party mixing of bitcoins. in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 75–86, 2015.

[13] Bonneau, Joseph, Narayanan, Arvind, Miller, Andrew, Clark, Jeremy, Kroll, Joshua A, and Felten, Edward W.

Mixcoin: Anonymity for bitcoin with accountable mixes. in *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18*, pp. 486–504. Springer, 2014.

[14] Valenta, Luke and Rowan, Brendan. Blindcoin: Blinded, accountable mixes for bitcoin. in *Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*, pp. 112–126. Springer, 2015.

[15] https://www.guru99.com/best-bitcoin-mixers-tumblers.html.

[16] Abe, Masayuki and Fujisaki, Eiichiro. How to date blind signatures. in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 244–251. Springer, 1996.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2023, Volume 21, Number 2 (pp. 16–23)
https://monadi.isc.org.ir

Presented at the ISCISC 2023 in Iranian Research Organization for Science & Technology, Tehran, Iran

A New Mixing Scheme to Improve Privacy in Bitcoin Cryptocurrency Transactions★

Hadi Norouzi Cholcheh * and Salman Niksefat

Amirkabir University Of Technology, Tehran, Iran

ARTICLE INFO.

Keywords:
Privacy
Bitcoin
Blockchain
Partialy Blind Signatue

dor: 20.1001.1.24763047.1402.12.2.2.8

Type: Research paper

ABSTRACT

Financial transactions in Bitcoin are stored in a distributed database called the block chain. All transactions are publicly available for all network nodes with the aim of transparency and the possibility of verifying the correctness. But this blockchain transparency feature, exploited by transaction analysis techniques, can lead to the violation of users' privacy and the disclosure of their identities. Researchers have proposed various techniques such as transaction mixing or fair exchange with the aim of improving privacy in Bitcoin transactions. In this paper, we present a new mixing scheme that overcomes some of the weaknesses of previous schemes. Obviously, in the proposed scheme, users can mix different amounts of Bitcoin in each round of the protocol implementation, which leads to achieving the result in a shorter time and at a lower cost. Also, this scheme is more resistant to denial of service attacks by malicious users.

★ The ISCISC 2023 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: h_norouzi@aut.ac.ir (Hadi Norouzi Cholcheh), niksefat@aut.ac.ir (Salman Niksefat)