



مقدمه‌ای بر حریم خصوصی بیت کوین
و سؤال و جواب درباره ویرل پول سامورایی

مقدمه

بلاک چینی که در شبکه بیت کوین به کار گرفته شده است از نوع بلاک چین عمومی است. یعنی هر کس می‌تواند با اجرا کردن نرم‌افزار بیت کوین به سابقه همه تراکنش‌های شبکه، از روز اول تا آخرین بلاک دسترسی داشته باشد.

تاکنون حتماً این سؤال برای شما پیش آمده است که دلیل انتخاب بلاک چین عمومی توسط خالق بیت کوین چه بوده است؟ ما در اینجا به دو دلیل بسیار مهم و اثرشان بر روی بیت کوین به عنوان یک «پول» اشاره می‌کنیم.

نامتمرکز بودن

یکی از مهم‌ترین ویژگی‌های بیت کوین نامتمرکز بودن آن است. بلاک چین عمومی به کاربران شبکه بیت کوین این امکان را می‌دهد بدون نیاز به اعتماد کردن به یک مرجع مرکزی، به سابقه تراکنش‌ها دسترسی داشته، و از آن مهم‌تر قادر به بازبینی و اعتبارسنجی آن‌ها باشند.

حسابداری شفاف برای بازبینی تعداد بیت کوین‌هایی که خلق می‌شوند

تعداد همه بیت کوین‌هایی که توسط ماینرهای شبکه و به‌عنوان پاداش ساختن بلاک خلق می‌شوند در نهایت ۲۱ میلیون کوین خواهد بود. بلاک چین عمومی بیت کوین به کاربران این تضمین را می‌دهد که سقف تولید آن هیچ‌گاه از عددی که در قانون اساسی آن (یعنی سورس کد بیت کوین) تعریف شده است، یعنی ۲۱ میلیون کوین بیشتر نخواهد شد.

شبکه بیت کوین برای تضمین دو ویژگی که در بالا به آن اشاره کردیم ملزم به استفاده از مدل بلاک چین عمومی است. در بلاک چین عمومی بیت کوین، هریک از تراکنش‌ها به صورت علنی ورودی و خروجی‌های خود و مقادیری که به آن وارد شده و از آن خارج شده است را به همه نمایش می‌دهد. پروژه‌های بلاک چینی دیگری هم وجود دارند که با استفاده از علم رمزنگاری مقادیر و حتی گراف ورودی و خروجی‌های تراکنش‌ها را از دید عموم پنهان می‌کنند و بالتبع ویژگی شماره ۲ یعنی «حسابداری شفاف» را از دست خواهند داد. در این پروژه‌ها شما چاره‌ای ندارید جز اینکه به گردانندگان آن‌ها اعتماد کنید که هیچ‌گاه بیشتر از سقف تعیین شده، کوین خلق نمی‌کنند.

این شفافیت در اعلام و نشان دادن مقادیر و گراف ورودی و خروجی یک تراکنش بیت کوین یک اثر جانبی بر روی آن می‌گذارد و آن این است که بیت کوین قابلیت «تعویض پذیری» یا اصطلاحاً «فانجیلیتی» خود را از دست می‌دهد.

از نظر علم اقتصاد یک پول خوب باید ویژگی‌های مختلفی داشته باشد که توضیح آن‌ها از موضوع این بحث خارج است ولی یک ویژگی مهم پول قابلیت «تعویض پذیری» یا اصطلاحاً «فانجیلیتی» آن است. یعنی واحدهای مختلف پول باید بدون هیچ مشکلی با یکدیگر معاوضه شوند.

ساده‌ترین مثال برای درک ویژگی تعویض پذیری، اسکناس‌هایی است که تا چند سال پیش همه از آن‌ها استفاده می‌کردند. شما اگر به مغازه می‌رفتید و یک اسکناس ۱۰۰۰ تومانی به مغازه‌دار می‌دادید و تقاضای پول خرد می‌کردید، او بدون هیچ مشکلی ۲ اسکناس ۵۰۰ تومانی به شما می‌داد و امکان نداشت از شما بپرسد این اسکناس را از کجا آورده‌ای. این یعنی اسکناسی که شما از آن به عنوان پول استفاده می‌کنید قابلیت تعویض پذیری دارد. در مورد طلا هم به همین شکل است، شما اگر یک تکه طلای ۵ گرمی داشته باشید و به مغازه طلافروشی بروید، می‌توانید برای همسرتان یک دستبند طلای

۵ گرمی بخرید و طلافروش فقط باید از اصالت طلای شما اطمینان حاصل کند و گرنه طلای شما با طلایی که او در مغازه‌اش می‌فروشد هیچ فرقی ندارد.

تراکنش‌های بیت کوین هم شبیه به همین مثال تکه‌های طلا هستند. در هر تراکنش ورودی‌های مختلفی از کوین‌های خرج‌نشده یا UTXO وارد، و از صاحب قدیمی به صاحب جدید دست به دست می‌شوند. تنها فرق در اینجا این است که بیت کوین‌ها یک شناسه دیجیتالی دارند که تا وقتی شبکه بیت کوین روشن باشد این شناسه هم از بین نخواهد رفت.

میکس کردن یا به عبارت دیگر کوین‌جوین، ویژگی تعویض‌پذیری از دست رفته را دوباره به بیت کوین بازمی‌گرداند و آن‌ها را به اصطلاح فاندجیل می‌کند.

کوپین جوین چیست؟

کوپین جوین که بعضی مواقع به آن میکس هم می‌گویند در واقع راه حل تأمین حریم خصوصی و اضافه شدن قابلیت تعویض پذیری بیت کوین بر روی لایه اول بلاک چین است که برای اولین بار توسط «گرگوری مکسول» در سال ۲۰۱۳ پیشنهاد شد. این روش طوری طراحی شده است تا یکی از پیش فرض‌های مهم سیستم‌های آنالیز بلاک چین، که فرض را بر این می‌گذارد همه ورودی‌های یک تراکنش مال یک نفر است از بین برود. آدرس‌های بیت کوین به هویت افراد ارتباط ندارند ولی هر کس با صرف زمان و فراهم کردن منابع لازم می‌تواند با تحت نظر قرار دادن بلاک چین عمومی بیت کوین ارتباط بین آدرس‌ها و افراد را عملاً به خاطر احراز هویتی که در صرافی‌ها انجام می‌شود پیدا کند. به این شرکت‌ها، شرکت‌های آنالیز بلاک چین بیت کوین می‌گویند.

چرا ما به کوپین جوین کردن نیاز داریم؟

همان‌طور که پیشتر اشاره کردیم بلاک چین بیت کوین عمومی است، بنابراین اگر هویت شما به بیت کوین شما گره خورده باشد (مثلاً به خاطر احراز هویت در صرافی یا اعلام آدرس دونیشن)، هر کس با صرف زمان و فراهم کردن منابع لازم برای تحت نظر قرار دادن و آنالیز بلاک چین بیت کوین می‌تواند شما را روی بلاک چین تعقیب کند. اگر سهل‌انگاری کنید و کوپین‌های خود را لیبل نزنید و بیت کوین‌هایی که از جاهای مختلف خریده‌اید یا به شما هدیه داده‌اند را با هم قاطی کنید اوضاع از این هم بدتر خواهد شد. ممکن است بگویید مشکلی نیست، من که چیزی برای از دست دادن ندارم. ولی دقت کنید که شما صورت حساب بانکی‌تان را به یک غریبه نشان نخواهید داد پس چرا می‌خواهید صورت حساب بیت کوین‌تان عمومی باشد؟

کوین جوین چگونه کار می کند؟

کوین جوین به شکل های متنوعی پیاده سازی شده است که هر کدام برداشتی از ایده اصلی داشته اند؛ دو یا چند نفر با هم برای ساختن تراکنشی که به طرزی خاص و با تعامل بین آنها ساخته می شود، UTXOهایشان را با همدیگر ادغام می کنند. این تراکنش به شکلی ساخته می شود که به دست آوردن رابطه قطعی بین خروجی ها و ورودی های این تراکنش برای شرکت های آنالیز کننده بلاک چین بسیار دشوار می شود. هر کس با بررسی این تراکنش در بهترین حالت می تواند تعداد حالت هایی که احتمال دارد ورودی ها و خروجی ها به هم مربوط باشند را محاسبه کند و هرگز نخواهد توانست رابطه قطعی بین آنها را بدست آورد. تعداد حالت های محتمل در یک تراکنش با ۵ ورودی و ۵ خروجی، عدد ۱۴۹۶ است.

چند پیاده‌سازی از کوین‌جوین وجود دارد؟

در حال حاضر سه پیاده‌سازی مختلف از کوین‌جوین وجود دارد.

۱. «جوین مارکت» که بر پایه مدل تأمین کننده/پذیرنده کار می‌کند. در این مدل، تأمین کننده کسی است که حاضر است بیت کوین‌هایش را در ازای دریافت مبلغی کارمزد از پذیرنده با UTXOهای او ادغام کند.
۲. «کیف پول واسابی» که از یک اپلیکیشن دسکتاپ استفاده می‌کند و تراکنش‌های بزرگی از نظر تعداد ورودی و خروجی برای کوین‌جوین می‌سازد. کیفیت کوین‌جوین واسابی تحت بررسی‌های دقیق قرار گرفته و اشکالاتی در آن مشاهده شده است.
۳. «ویرل پول از تیم سامورایی» تراکنش‌هایی با ورودی و خروجی کم (در حال حاضر ۵ ورودی و ۵ خروجی) می‌سازد و در عین حال بسیار مؤثر است. همچنین ویرل پول سامورایی بر روی اپلیکیشن موبایل کیف پول سامورایی هم امکان میکس به کاربران می‌دهد. در حال حاضر پیشنهاد می‌کنیم کاربران از این سرویس برای کوین‌جوین استفاده کنند.

آیا میکسرها هم همان کوین جوین هستند؟

خیر، یک میکسر عموماً یک سرویس متمرکز است که شما بیت کوین به آن ارسال می‌کنید و این سرویس در پشت صحنه در ازای دریافت کارمزد این UTXO شما را با دیگران مخلوط می‌کند و دوباره به شما باز می‌گرداند. در کل استفاده کردن از این سرویس‌ها پیشنهاد نمی‌شود چون وقتی شما بیت کوین برای آن‌ها ارسال می‌کنید در واقع به آن‌ها اعتماد کرده‌اید که بیت کوین را به شما باز می‌گرداند. به علاوه اینکه شما نمی‌دانید برای میکس کردن UTXO شما از چه روشی استفاده می‌کنند. همیشه این را به یاد داشته باشید که نباید تحت هیچ شرایطی کنترل بیت کوین را به فرد دیگری بسپارید.

آیا برای کوین جوین باید کارمزد پرداخت کنم؟

بله همه سرویس‌های کوین جوین موجود از کاربران کارمزد دریافت می‌کنند. هر کدام از آن‌ها روش متفاوتی برای محاسبه کارمزد طراحی کرده‌اند. بنابراین شما باید قبل از استفاده از هر کدام از آن‌ها درباره کارمزدی که می‌گیرند تحقیق کنید.

آیا ممکن است در حین کوین جوین بیت کوینم را از دست بدهم؟

ساختار سرویس‌های کوین جوینی که پیشتر معرفی شدند طوری است که کنترل کلید خصوصی بیت کوین همچنان در اختیار شما است. تاکنون هیچ موردی از سرقت یا ازدست رفتن بیت کوین بر اثر اشتباه برای کسانی که از این سرویس‌ها استفاده می‌کنند، گزارش نشده است. با وجود این شما باید همه جوانب را در نظر بگیرید و اگر به آن‌ها اطمینان ندارید ابتدا با بیت کوین‌های تستی از آن‌ها استفاده کنید. یک مورد شایان یادآوری است که این نرم‌افزارها به صورت اپن-سورس بر روی اینترنت قرار دارند و هر فرد علاقمندی می‌تواند کُد آن‌ها را بازبینی کند.

استفاده کردن از سرویس کوین جوین ممکن است چه مشکلاتی برای من به وجود بیاورد؟

تاکنون چند مورد اتفاق افتاده است که یک صرافی، به UTXO کاربری که از سرویس کوین جوین استفاده کرده است اشکال گرفته و از آن کاربر درخواست کرده است مدارکی برای احراز هویت مجدد به صرافی ارسال کند. یا در مواردی پیش آمده است که صرافی حساب کاربر را مسدود کرده و آن UTXO را به لیست سیاه افزوده است. این نکته را برای شفافیت باید گوشزد کنیم که این اتفاق تاکنون فقط برای کاربران سرویس کوین جوین واسابی افتاده است و کاربران کوین جوین ویرل پول سامورایی و جوین مارکت تاکنون چنین موردی را تجربه نکرده‌اند.

آیا استفاده از سرویس کوین جوین اثری بر روی سبک ارسال یا خرج کردن بیت کوین من می گذارد؟

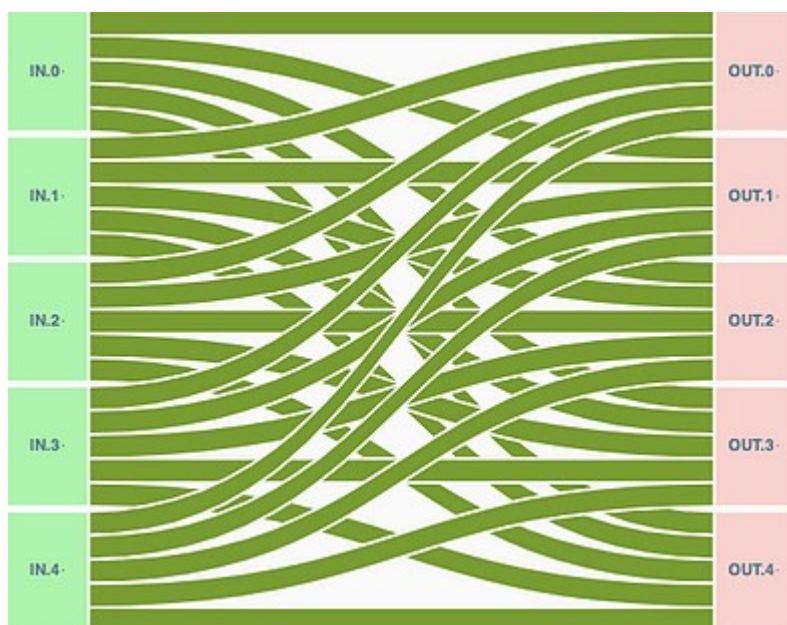
بله. این یکی از مواردی است که توجه کافی به آن نشده است. بعد از کوین جوین اگر شما در روش ارسال یا خرج کردن بیت کوین درست عمل نکنید، در واقع انگار همه زحمتهایی که کشیده‌اید و کارمزدی که بابت کوین جوین پرداخت کرده‌اید را بی‌ارزش کرده‌اید. در این صورت حریم خصوصی که به دست آورده بودید هم کاملاً از بین می‌رود. درک روش‌های ارسال بیت کوین بعد از کوین جوین کردن ممکن است در اوایل کار برای شما کمی دشوار باشد ولی خوشبختانه ابزارهای بعد از میکس کیف پول سامورایی با نام‌های Stonewall، Stonewallx2، و Stowaway این کار را تا حدودی برای کاربران آسان کرده است.

پی‌جوین چیست؟

یک کوین جوین است که به صورت ویژه‌ای ساخته می‌شود و به P2EP هم معروف است. این تراکنش بین دو نفر است که یکی از آن‌ها قصد دارد برای دیگری بیت کوین ارسال کند. تراکنش در این نوع کوین جوین به صورتی ساخته می‌شود که به هیچ وجه نمی‌توان رقم واقعی که بین این دو نفر جابجا شده را بدست آورد. این نوع تراکنش مزیت دیگری هم دارد؛ برای کسی که بلاک چین بیت کوین را آنالیز می‌کند، این تراکنش با تراکنش‌های دیگر هیچ فرقی ندارد و اگر در مقیاس گسترده مورد استفاده قرار بگیرد کاملاً پیش فرض «ورودی‌های یک تراکنش همه مال یک نفر هستند» باطل خواهد شد.

آنالیز بلاک چین چیست؟

روشی است که در آن یک نهاد با فراهم کردن ابزار و منابع کافی به نظارت شدید بر روی تراکنش‌های بلاک چین بیت کوین مشغول می‌شود و سعی می‌کند الگوهای مورد نظرش را در میان تراکنش‌ها برای ردزنی افراد و تحلیل عادت‌های آن‌ها در خرج کردن بیت کوین پیدا کند. شرکت‌های آنالیز بلاک چین این کارها را به بهانه مبارزه با خلاف کاران و تروریست‌ها انجام می‌دهند. ما با نیت آن‌ها برای مبارزه با کارهای غیرقانونی که ممکن است به دیگران آسیب برساند کاملاً موافقیم، ولی با اعمال روش‌های کلی و نظارت گسترده بر روی بلاک چین بیت کوین که حریم خصوصی کاربران بیت کوین را به خطر می‌اندازد مخالف هستیم.



سؤال و جواب درباره ویرل پول سامورایی

در میان پیاده‌سازی‌های موجود از کوین‌جوین، ویرل‌پول محصول تیم سامورایی روش خلاقانه‌ای برای از بین بردن ارتباط قطعی بین ورودی‌ها و خروجی‌های یک تراکنش بیت‌کوین به کار گرفته که در حال حاضر بهترین روش است. اما برتری ویرل‌پول فقط محدود به روش کوین‌جوین آن نیست؛ تیم سامورایی مجموعه‌ای از نرم‌افزارها و سرویس‌های کاربردی برای کاربرانش فراهم می‌کند که می‌توانند بعد از میکس کوین‌هایشان از آن‌ها برای محافظت از حریم خصوصی که در کوین‌جوین بدست آمده استفاده کنند. این ابزارها به «ابزارهای بعد از میکس» معروف‌اند و در کیف‌پول موبایل سامورایی قرار داده شده‌اند. در ادامه به سؤال و جواب درباره ویرل‌پول و معرفی راه‌کارهای میکس در اکوسیستم سامورایی می‌پردازیم.

ویرل پول چیست؟

ویرل پول یک پیاده‌سازی کوین جوین بر پایه استاندارد «زیرولینک» است که توسط توسعه‌دهنده‌گان تیم سامورایی تدوین شده است. (در واقع استاندارد زیرولینک توسط nopara73 خالق کیف پول واسابی، و SamouraiDev طراح و برنامه‌نویس ارشد سامورایی تدوین شد و بعد از اختلافاتی که بین این دو تیم بوجود آمد هر کدام بصورت جداگانه آن را توسعه می‌دهند. آرشیو این استاندارد را می‌توانید در گیت‌هاب و در آدرس <https://github.com/nopara73/ZeroLink> مشاهده کنید. - م)

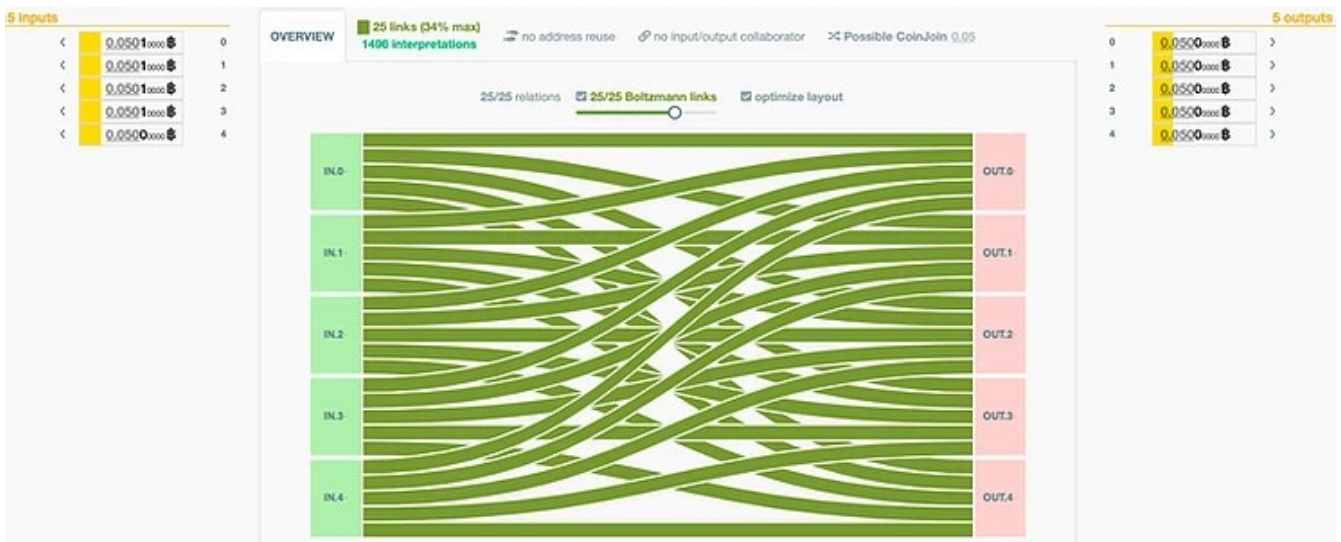
ویرل پول یکی از بهترین پیاده‌سازی‌های موجود در بازار است که هم از نظر ساختار بی‌نقص است و هم استفاده کردن از آن راحت است. ویرل پول روابط قطعی بین ورودی‌ها و خروجی‌های یک تراکنش بیت کوین را از بین می‌برد. به این کار میکس کردن بیت کوین می‌گویند. یکی از ویژگی‌های ویرل پول فراهم کردن ابزارهای پیشرفته برای خرج کردن یا منتقل کردن بیت کوین بعد از میکس آن‌ها است، بصورتی که قوانین زیرولینک همچنان پابرجا بماند.

ویرل پول چگونه کار می‌کند؟

بطور کلی اگر بخواهیم درباره آن صحبت کنیم، میکس کردن با ویرل پول اساساً تعامل ۵ نفر مشارکت‌کننده برای ساختن یک تراکنش است. رقم خروجی‌های این تراکنش‌ها همیشه با هم برابرند و این باعث می‌شود که برای تفسیر روابط ورودی و خروجی هر کدام از این تراکنش‌ها، ۱۴۹۶ تفسیر مختلف وجود داشته باشد. فردی که بلاک‌چین بیت کوین را آنالیز می‌کند وقتی به یک تراکنش ویرل پول مواجه شود نمی‌تواند با اطمینان حکم کند که کدام ورودی به کدام خروجی مربوط است. تازه این برای یک دور میکس است، فرض کنید میکس کردن را پشت سر هم ۵ یا ۱۰ یا حتی ۵۰ بار انجام دهید. (خوشبختانه دوباره میکس کردن که اصطلاحاً به ریمیکس معروف است، در ویرل پول رایگان است.)

هریک از شرکت کنندگان میکس در ویرل پول یک ورودی به این تراکنش اضافه می کنند. برای اینکه یک دور جدید از میکس شروع شود حداقل ۲ تا از این ورودی ها باید از طرف شرکت کنندگان جدید باشد. این ورودی های جدید به Premixers معروف اند و جزء مهمی از ساختار ویرل پول هستند. الزام برای وجود داشتن ۲ ورودی از نوع Premixers این اطمینان را بوجود می آورد که به هر یک از تراکنش ها در هر دور میکس UTXO جدید وارد می شود و هر دور میکس فقط شامل UTXO هایی نیست که قبلاً میکس شده اند. اگر UTXO جدید به هر دور میکس وارد نشود به این کار «بُر زدن کوین ها» می گویند که کیفیت میکس را پایین می آورد.

اگر می خواهید کاملاً یک تراکنش ویرل پول را متوجه شوید، به [این مقاله](#) عالی از «استودیو بیت کوین» نگاهی بندازید.

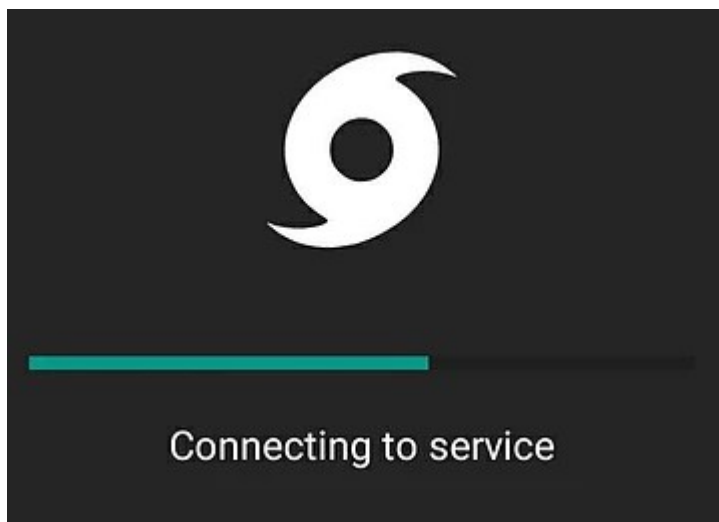


یک تراکنش میکس ویرل پول

چطور از ویرل پول استفاده کنم؟

از ۳ راه مختلف می‌توانید با ویرل پول میکس کنید. ولی برای هر کدام از آنها باید اول کیف پول سامورایی را بر روی تلفن اندرویدی خود نصب کنید.

روش اول - میکس با کیف پول سامورایی



راحت‌ترین راهی که شما می‌توانید اولین میکس ویرل پول‌تان را انجام دهید استفاده از اپلیکیشن آن روی تلفن است. برای راهنمای قدم به قدم میکس روی موبایل می‌توانید [این مقاله](#) را بخوانید. ابزار میکس موبایل سریع‌ترین روش برای شروع است ولی لزوماً بهترین روش برای حجم‌های بالای بیت کوین نیست.

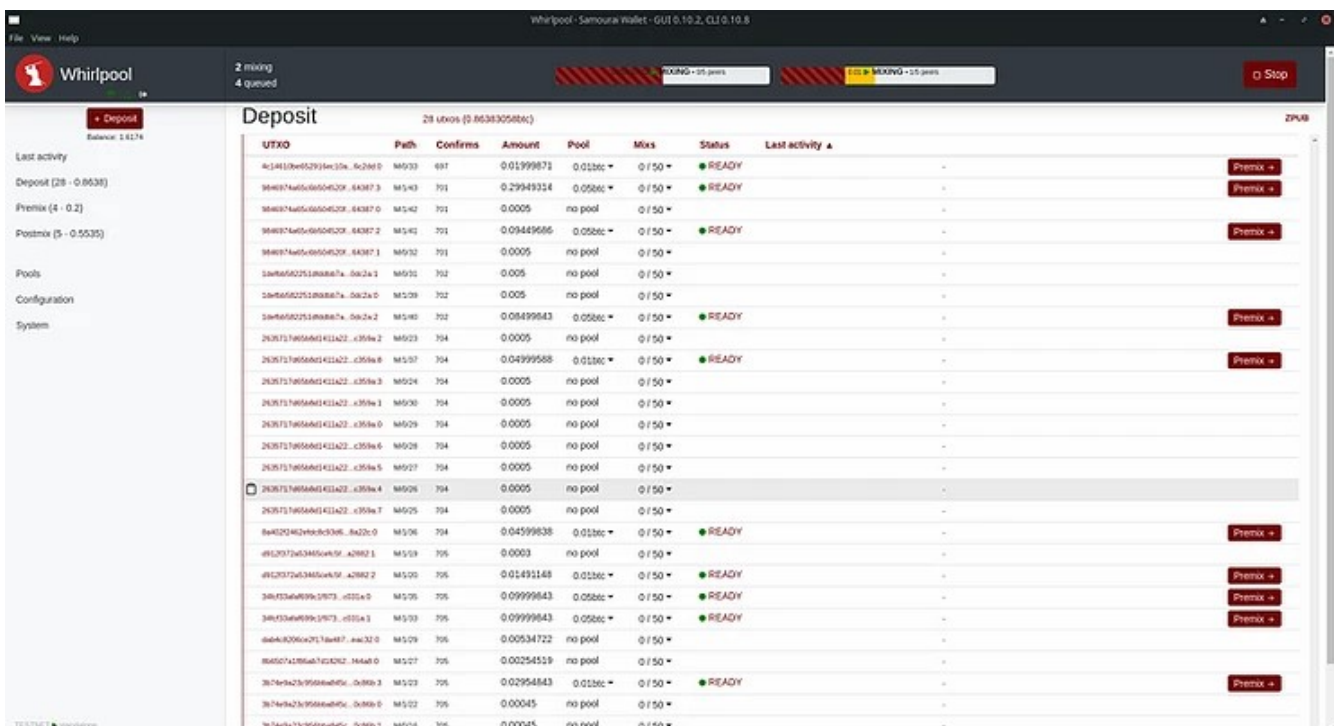
متأسفانه سیستم عامل اندروید گاهی اوقات برنامه‌هایی که در پشت‌صحنه اجرا می‌شوند را بصورت خودسرانه می‌بندد. این موضوع می‌تواند تجربه میکس شما را خراب کند. می‌توانید این نکته‌ها را که توسط DammKewl تهیه شده برای بهتر شدن تجربه میکس بر روی موبایل انجام دهید:

- تلفن‌تان را طوری تنظیم کنید که اپلیکیشن سامورایی را نبندد. سایت dontkillmyapp.com را ببینید
- هرگونه حالت eco را بر روی گوشی‌تان خاموش کنید
- هرگونه حالت performance را بر روی گوشی‌تان فعال کنید
- اگر امکان‌ش هست از یک ویجت برای روشن نگه داشتن صفحه گوشی‌تان استفاده کنید
- تلفن‌تان را به شارژ وصل کنید
- صفحه میکس ویرل‌پول را روی تلفن‌تان باز کنید و بگذارید بالا بماند
- بطور متناوب به صفحه اصلی والت سامورایی برگردید، دکمه Close را بر روی نوتیف ویرل‌پول بزنید و دوباره به صفحه اصلی ویرل‌پول برگردید

روش دوم - نسخه دسکتاپ ویرل پول

[اپلیکیشن](#) دسکتاپ به والت سامورایی شما وصل می‌شود و به شما این اجازه را می‌دهد فرآیند میکس را بر روی کامپیوترتان مدیریت کنید. با استفاده از این نرم‌افزار شما می‌توانید به آدرسی که برای شما ساخته می‌شود بیت کوین ارسال کنید، معین کنید حداقل چند بار می‌خواهید بعد از میکس اول دوباره ریمیکس کنید، شناسه TxID تراکنش‌های میکس شده را برای دیدن آن‌ها روی سایت [OXT.me](#) ببینید.

این نکته را به یاد داشته باشید که اگر فقط از نسخه دسکتاپ ویرل پول استفاده می‌کنید برای انجام شدن میکس و ریمیکس باید دستگاه شما روشن و این اپلیکیشن در حال اجرا باشد. بنابراین مراقب تنظیمات خاموش شدن خودکار سیستم خود باشید.



The screenshot displays the Whirlpool GUI interface. At the top, it shows 'Whirlpool - Samourai Wallet - GUI 0.10.2, CL1.0.10.8'. The main area is titled 'Deposit' and shows a list of 28 txos with a total value of 0.8638305886 BTC. The table columns are: TXID, Path, Confirms, Amount, Pool, Mixs, Status, and Last activity. Each row includes a 'Premix +' button. The interface also shows a sidebar with 'Deposit' and 'Balance 1.8274', and a top status bar with '2 mixing' and '4 queued'.

TXID	Path	Confirms	Amount	Pool	Mixs	Status	Last activity
4c14d10e052914c15a...628d0	M533	697	0.01999871	0.02btc	0 / 50	READY	
984897465c60504c29...643873	M543	701	0.29949334	0.05btc	0 / 50	READY	
984897465c60504c29...643870	M542	701	0.0005	no pool	0 / 50		
984897465c60504c29...643872	M541	701	0.09449686	0.05btc	0 / 50	READY	
984897465c60504c29...643871	M532	701	0.0005	no pool	0 / 50		
1a8a692251808a7a...0a2a1	M531	702	0.005	no pool	0 / 50		
1a8a692251808a7a...0a2a0	M528	702	0.005	no pool	0 / 50		
1a8a692251808a7a...0a2a2	M540	702	0.08499643	0.05btc	0 / 50	READY	
2d3f73786568d1411a22...c359a2	M523	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a6	M537	704	0.04999588	0.02btc	0 / 50	READY	
2d3f73786568d1411a22...c359a3	M524	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a1	M530	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a0	M529	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a6	M528	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a5	M527	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a4	M526	704	0.0005	no pool	0 / 50		
2d3f73786568d1411a22...c359a7	M525	704	0.0005	no pool	0 / 50		
8a482d4024b2a8c306...8a20c0	M536	704	0.04599838	0.02btc	0 / 50	READY	
4912037a034850495f...a28021	M539	705	0.0003	no pool	0 / 50		
4912037a034850495f...a28022	M535	705	0.01491148	0.02btc	0 / 50	READY	
348433a4899a3973...c010a0	M535	705	0.09999843	0.05btc	0 / 50	READY	
348433a4899a3973...c010a1	M533	705	0.09999843	0.05btc	0 / 50	READY	
46a4d206a0713a0d7...aa31c0	M539	705	0.00534722	no pool	0 / 50		
8045071186a67c2d2c...144a00	M527	705	0.00254519	no pool	0 / 50		
3874e9a23c9568e405c...0a80a0	M523	705	0.02954843	0.02btc	0 / 50	READY	
3874e9a23c9568e405c...0a80a0	M522	705	0.00045	no pool	0 / 50		
3874e9a23c9568e405c...0a80a1	M524	705	0.00045	no pool	0 / 50		

نمایی از اپلیکیشن whirlpool-gui

روش سوم - رابط کامندلاین (cli) ویرل پول

رابط کامندلاین ویرل پول نقطه اوج ابزارهای ویرل پول است. این رابط به گونه‌ای طراحی شده است که بصورت شبانه‌روزی بر روی یک دستگاه مثل رزبری پای ۴ یا راک پرو ۶۴ که همیشه روشن است اجرا شود. چون بصورت شبانه‌روزی روشن است این مدل بیشترین شانس را به شما می‌دهد تا با کمترین زحمت بیشترین تعداد ریمیکس را به دست بیاورید. همه کارهای سخت را برای شما انجام می‌دهد تا شما به زحمت نیفتید. فقط مسأله این است که راه‌اندازی آن از دو روش دیگری که پیشتر معرفی شد، دشوارتر است. هرچند با پروژه‌هایی مثل [RoninDojo](#) می‌توانید به راحتی آن را روی یک دستگاه رزبری پای ۴ نصب کنید. همچنین رابط کامندلاین ویرل پول بر روی [myNode](#) و [Nod1](#) هم اجرا می‌شوند.

حالت ایده‌آل

کاربران حرفه‌ای هر سه روشی که در بالا معرفی کردیم را با هم ادغام و از این حالت ایده‌آل به صورت زیر استفاده می‌کنند:

- مقداری بیت کوین به والت سامورایی ارسال می‌کنند
- میکس را بر روی والت سامورایی روی موبایل آغاز می‌کنند
- بر روی اپلیکیشن دسکتاپ تعداد ریمیکس را بر روی بی‌نهایت تنظیم می‌کنند
- باقی کار را به رابط کامندلاین ویرل پول می‌سپارند
- مرحله اول را تکرار می‌کنند

شکل زیر نحوه تعامل قسمت‌های مختلف را به تفصیل شرح می‌دهد



برای بزرگ‌تر شدن متن زوم کنید

یک توضیح مختصر درباره دوجو

دوجو سروری است که کیف پول سامورایی شما به آن وصل می‌شود. برای استفاده کردن از کیف پول سامورایی و ویرل پول، راه انداختن دوجو الزامی نیست ولی ایده آل‌ترین حالت از نظر حفظ حریم خصوصی این است که هر فردی دوجوی شخصی خود را راه اندازی کند و کیف پول و ویرل پول را به آن وصل کند. شما می‌توانید دوجو را از طریق یکی از راه‌هایی که پیشتر به آن‌ها اشاره شد، یا اگر کاربر حرفه‌ای هستید از طریق نصب مستقیم بر روی لینوکس یا مک‌اواس راه اندازی کنید. بعد از راه اندازی دوجو وصل کردن کیف پول سامورایی به سادگی اسکن کردن یک qr code است. به خاطر داشته باشید که اگر شما از دوجوی شخصی خود استفاده نمی‌کنید به این معنی است که به زیرساخت‌های یک نفر دیگر اعتماد کرده‌اید.

Tx0 چیست؟

تراکنشی است که والت سامورایی یا اپلیکیشن ویرل پول شما می‌سازد تا UTX0 (یعنی بیت کوینی که می‌خواهید میکس کنید) را بسته به ساینز استخر میکسی که انتخاب کرده‌اید به بخش‌های مختلف تقسیم کند. جلوتر درباره استخرها بیشتر توضیح می‌دهیم.

برای نمونه حالت زیر را در نظر بگیرید که 2.2550 بیت کوین به عنوان ورودی به تراکنش Tx0 وارد شده و به خروجی‌های زیر تقسیم شده است:

- ۴ خروجی 0.5000302 (این‌ها UTX0هایی هستند که آماده وارد شدن به استخر 0.5 و شرکت در کوین جوین هستند)
- ۱ خروجی 0.0250 (این کارمزد هماهنگ کننده یعنی سامورایی است)

- ۱ خروجی 0.22998418 (این باقی مانده پول صاحب UTXO است که به کیف پولش بازگردانده می شود. به آن doxxic change می گویند چون اگر بصورت درستی از این UTXO استفاده نشود می تواند حریم خصوصی بدست آمده را از بین ببرد.)

حالا چرا بجای 0.5000000 ۴ خروجی با مقدار 0.5000302 داریم؟

در مثالی که زدیم ما در حالت «پیش از میکس» هستیم و می خواهیم برای اولین بار وارد استخر شویم. پس آن مقدار اضافی 0.0000302 در واقع برای پوشش دادن کارمزد تراکنش کوین جوین (که به ماینرها پرداخت می شود) به آن اضافه شده است. شما فقط یکبار و در مرحله «پیش از میکس» این مقدار اضافی را پرداخت می کنید و در دورهای بعدی کوین جوین، افراد جدید کارمزد تراکنش شما را پرداخت خواهند کرد.



یک تراکنش Tx0

استفاده از سرویس ویرل پول چقدر هزینه دارد؟

ساختار کارمزد ویرل پول را می توان به راحتی فهمید. شما برای وارد شدن به یک استخر ویرل پول و در هنگام ساختن تراکنش Tx0 یک کارمزد ثابت پرداخت می کنید. البته که کارمزدهای تراکنشی که به ماینرها پرداخت می شود متغیر است و ما به این موضوع خواهیم پرداخت.

کارمزدهای ثابت برای وارد شدن به استخرهای ویرل پول:

0.01 pool fee = 0.0005 (50,000 sats)

0.05 pool fee = 0.0025 (250,000 sats)

0.5 pool fee = 0.025 (2,500,000 sats)

این کارمزدها ثابت هستند و ارتباطی به حجم بیت کوینی که به استخر وارد می کنید یا تعداد ریمیکسها ندارند.

برای محاسبه کارمزد تمام شده بر اساس شرایط خود می توانید از سایت whirlpoolfees.com استفاده کنید.

Whirlbot چیست؟

یک ربات تلگرامی است که آمار و اطلاعات مختلفی درباره وضعیت ویرل پول به شما می‌دهد تا تصمیم بگیرید چه زمانی و چه مقداری بیت کوین وارد استخرهای ویرل پول کنید. شما می‌توانید از دستور `/start` برای دیدن همه قابلیت‌های آن استفاده کنید.

یه یاد داشته باشید که دستور `/calculate` در حال حاضر غیرفعال است و برای محاسبه کارمزد از سایت whirlpoolfees.com استفاده کنید.

```
Welcome to Whirlbot
Type /pools to see current Whirlpool Pool status
Type /fees to see the pool entry fees for all pools
Type /minerfees to see the current miner fee rates used
Type /cycles to see the total number of cycles today.
Type /calculate to help choose the right pool with best fees.
Type /liquidity to see the current depth of each pool. 09:32
```

آیا برای هر دور میکس باید کارمزد پرداخت کنم؟

خیر. شما فقط اول کار وقتی `Tx0` را می‌سازید و وارد می‌شوید باید کارمزد پرداخت کنید. برای دوره‌های بعدی هماهنگ کننده از شما کارمزدی نمی‌گیرد و کارمزد ماینرها هم توسط افرادی که وارد استخر می‌شوند پرداخت خواهد شد.

باید در کدام استخر میکس کنم؟

هرکسی ترجیحات خود را دارد و پاسخی قطعی برای این سؤال وجود ندارد. هرچند باید ۲ موضوع را در نظر بگیرید؛ کارمزدی که قرار است برای وارد شدن به یک استخر پرداخت کنید و تعداد UTXOهایی که تراکنش اول یعنی Tx0 برای شما خواهد ساخت.

یک موضوع دیگر که باید در نظر بگیرید، نحوه خرج کردن شماست. مثلاً اگر پرداخت‌های کوچک زیادی با بیت کوین انجام می‌دهید احتمالاً استخر 0.01 برای شما انتخاب مناسب‌تری است. از سوی دیگر اگر می‌خواهید حجم بالایی از بیت کوین را میکس کنید و قصد خرج کردن آن‌ها را فعلاً ندارید و نمی‌خواهید تعداد UTXOهای زیادی را مدیریت کنید، احتمالاً استخر 0.5 انتخاب خوبی برای شما باشد. معمولاً پیشنهاد می‌شود UTXOهای میکس شده‌ای از همه سائزهای استخرهای ویرل پول در اختیار داشته باشیم تا در هنگام ارسال گزینه‌های بیشتری در اختیار داشته باشیم.

از سایت [whirlpoolfees](https://whirlpoolfees.com/) برای محاسبه کارمزد کوین‌جوین و تعداد UTXOهایی که بعد از میکس ساخته می‌شود استفاده کنید.

SCODE چیست؟

کدهای تخفیفی هستند که تیم سامورایی هرچند وقت یکبار منتشر می کند تا کاربران بتوانند از درصدی تخفیف بر روی کارمزد وارد شدن به استخر میکس استفاده کنند. این کد تخفیف را می توانید در کیف پول موبایل سامورایی یا اپلیکیشن ویرل پول وارد کنید. دقت کنید که برای اعمال تخفیف باید میکس را از همان دستگاہی که کد تخفیف بر روی آن وارد شده است شروع کنید.

How to use a SCODE in Samourai Wallet's mobile Whirlpool

1. Select menu >
2. Whirlpool >
3. Drop-down menu >
4. Whirlpool SCODE >
5. Type in code and select "OK" >
6. You'll be sent back to main menu. Repeat steps and verify code is entered, but this time press cancel.

Happy mixing!

یک میکس معمولاً چقدر طول می کشد؟

اولین میکس شما مخصوصاً در استخرهای کوچک تر، معمولاً خیلی سریع اتفاق می افتد. باید این موضوع را به خاطر بسپارید که هر دور میکس به دو شرکت کننده که در مرحله «پیش از میکس» قرار دارند، نیاز دارد. حالا اگر شما به استخری وصل شده‌اید که در آن فقط یک شرکت کننده در مرحله «پیش از میکس» حاضر است، باید منتظر باشید تا یک نفر دیگر به استخر اضافه شود تا یک دور میکس شروع شود. شما می‌توانید آمار شرکت کنندگان حاضر در استخرهای ویرل پول را با دستور liquidity / در whirlbot مشاهده کنید.

به آن‌هایی که در یک دور میکس شرکت کرده‌اند و منتظر وارد شدن به ریمیکس‌های مجانی یا به دنبال «سواری گرفتن مجانی» هستند freerider می‌گویند. این افراد بصورت کاملاً تصادفی برای شرکت در میکس‌های بعدی انتخاب می‌شوند بنابراین تعداد ریمیکس‌هایی که ممکن است نصیب شما شود خیلی متغیر است. اگر نقدیگی زیادی وارد استخری که در آن هستید شود، احتمالاً در ریمیکس‌های بیشتری شرکت خواهید کرد. اگر استخری که انتخاب کرده‌اید روز خلوتی را پشت سر می‌گذارد، ممکن است حتی یک ریمیکس هم نصیب شما نشود و مجبور باشید بیشتر صبر کنید. این یکی از ویژگی‌های ویرل پول است، نه مشکل آن. در ویرل پول کیفیت میکس از هر موضوع دیگری مهم تر است.

چندبار باید ریمیکس کنم؟

یکبار میکس کردن هم ارتباط قطعی بین ورودی‌ها و خروجی‌های UTXOهای شما را قطع خواهد کرد ولی پیشنهاد می‌شود UTXO خود را حداقل ۳ بار میکس کنید. اما اگر از من بپرسید پیشنهاد می‌کنم تا جایی که امکان دارد UTXOها را در استخر نگه دارید و در ریمیکس‌های رایگان شرکت کنید.

بخاطر داشته باشید که شما فقط یکبار کارمزد پرداخت می‌کنید و با هر بار ریمیکس به کیفیت میکس و حریم خصوصی شما افزوده می‌شود و از همه مهم‌تر رایگان است.

چرا ریمیکس‌های کمی نصیب می‌شود؟

همانطور که پیشتر گفتیم ریمیکس‌ها کاملاً بطور تصادفی انتخاب می‌شوند. روزهایی هستند که ریمیکس‌های زیادی نصیب شما می‌شود و روزهایی هم هست که حتی یکبار هم ریمیکس نخواهید داشت. برای هرچه بیشتر کردن شانس ریمیکس UTXOهایتان پیشنهاد می‌کنیم از روش رابط کامندلاین ویرل پول (cli) استفاده کنید تا همیشه آنلاین و آماده برای ریمیکس باشید.

با مقداری که در استخر وارد نمی‌شود یا همان doxxic change چه کار کنم؟

این موضوع را به تفصیل در [این مقاله](#) بررسی کرده‌ایم.

آیا کوین جوین می تواند حریم خصوصی را به بیت کوینی که با احراز هویت خریدهام برگرداند؟

هم بله هم خیر. بعد از کوین جوین کردن UTXO هایتان هرکس که شما را بر روی بلاک چین بیت کوین دنبال کند نخواهد توانست رابطه قطعی بین ورودی ها و خروجی های تراکنش های میکس شده را بدست آورد بنابراین نمی داند کدام خروجی به شما مربوط می شود. اما با همه این تفاسیر در نظر داشته باشید که آن صرافی (و در نتیجه هر نهادی که به اطلاعات آن ها دسترسی دارد) می داند دقیقاً چقدر بیت کوین خریداری کرده اید.

بهترین راه برای حفظ حریم خصوصی مالی خریدن بیت کوین بدون احراز هویت از سایت [HodlHodl](#) یا پلتفرم [Bisq](#)، و اقدام برای میکس بعد از خرید است.

بعد از میکس باید چکار کنم؟

بهترین کار این است که بگذارید بیت کوین ها روی کیف پول سامورایی شما باقی بمانند تا بصورت رایگان ریمیکس شوند. هر وقت خواستید آن ها را خرج کنید می توانید از ابزارهای «پس از میکس» کیف پول سامورایی که باعث حفظ حریم خصوصی بدست آمده هستند و در ادامه توضیح داده شده اند، استفاده کنید.

آیا بعد از میکس امکان ارسال کوین ها به کیف پول آفلاین وجود دارد؟

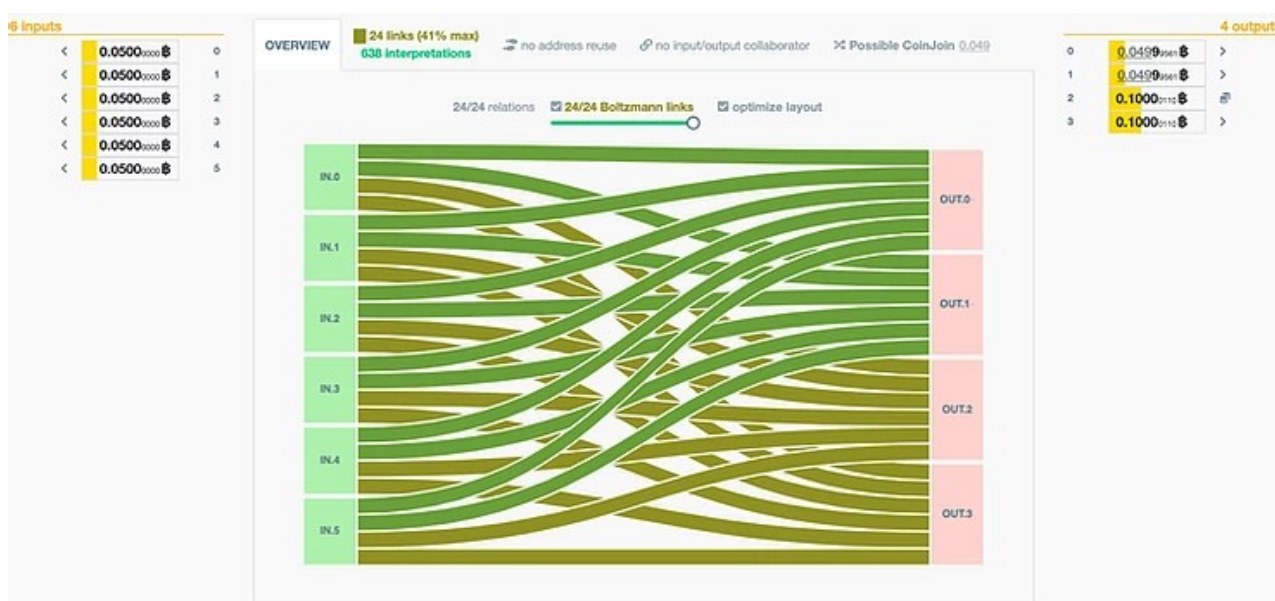
بله این امکان وجود دارد. اما برای انجام این کار باید مسائل مهمی رعایت شوند که در [این راهنما](#) به آن ها اشاره شده است.

STONEWALL چیست؟

یک ابزار در کیف پول سامورایی است که تراکنش‌های شما را به شکل ویژه‌ای درست می‌کند تا تعداد ارتباطات احتمالی بین ورودی و خروجی تراکنش هرچه بیشتر و به همین خاطر آنالیز این تراکنش دشوارتر شود. در هنگام ارسال بیت کوین اگر شرایط لازم برای ساختن این نوع تراکنش فراهم باشد، کیف پول سامورایی شما به‌طور خودکار آن را می‌سازد و آنتروپی تراکنش ساخته شده را به شما نشان می‌دهد. Stonewall در واقع یک کوین جوین مینیاتوری از UTXOهای شماست.

Stonewall می‌تواند هم از UTXOهای «بعد از میکس» شما این تراکنش را بسازد، هم از موجودی عادی که در کیف پول‌تان دارید. اما این الگوریتم هوشمند است و به‌هیچ‌وجه این دو نوع UTXO مختلف را با هم ادغام نمی‌کند. خروجی‌های یک تراکنش Stonewall همیشه ۴ عدد هستند:

- مقداری که به یک آدرس ارسال کرده‌اید
- یک خروجی برای گول زدن سیستم‌های آنالیز که به کیف پول شما برمی‌گردد
- دو خروجی برای برگشت بقیه بیت کوینی که باقی مانده به کیف پول شما



یک تراکنش Stonewall

چرا کیف پول سامورایی من قادر به ساختن یک تراکنش Stonewall نیست؟

الگوریتم Stonewall کمی پیچیده است ولی اولین قانونی که باید رعایت شود این است که مقدار بیت کوین که ارسال می کنید نباید بیشتر از نصف موجودی کیف پول شما باشد. اگر با وجود رعایت کردن این قانون همچنان کیف پول شما قادر به ساختن این نوع تراکنش نیست، به احتمال خیلی زیاد به اندازه کافی UTXOهای مناسبی برای انتخاب ساختن تراکنش با حداقل آنتروپی لازم در کیف پول شما موجود نیست. هرچقدر در کیف پول شما UTXOهای بیشتری وجود داشته باشد، کیف پول سامورایی انتخاب های بیشتری برای ساختن یک تراکنش Stonewall با آنتروپی بالا دارد.

STONEWALL X2 چیست؟

این نوع تراکنش در واقع یک کوین جوین مینیاتوری با استفاده از UTXOهای شما و یک نفر دوم است. در این شکل از تراکنش، UTXOهای دو نفر با هم ادغام می شود تا یکی از آنها مقداری بیت کوین به شخص ثالث ارسال کند و تراکنش StonewallX2 ساخته شود. برای ساختن این تراکنش حتی لازم نیست این دو نفر در یک مکان حضور داشته باشند چون کیف پول سامورایی امکان برقراری ارتباط از طریق اینترنت را برایشان فراهم می کند. بدیهی است که شخص سوم لزوماً نباید از کیف پول سامورایی استفاده کند و فقط کافیست یک آدرس بیت کوین به فرد ارسال کننده بدهد.

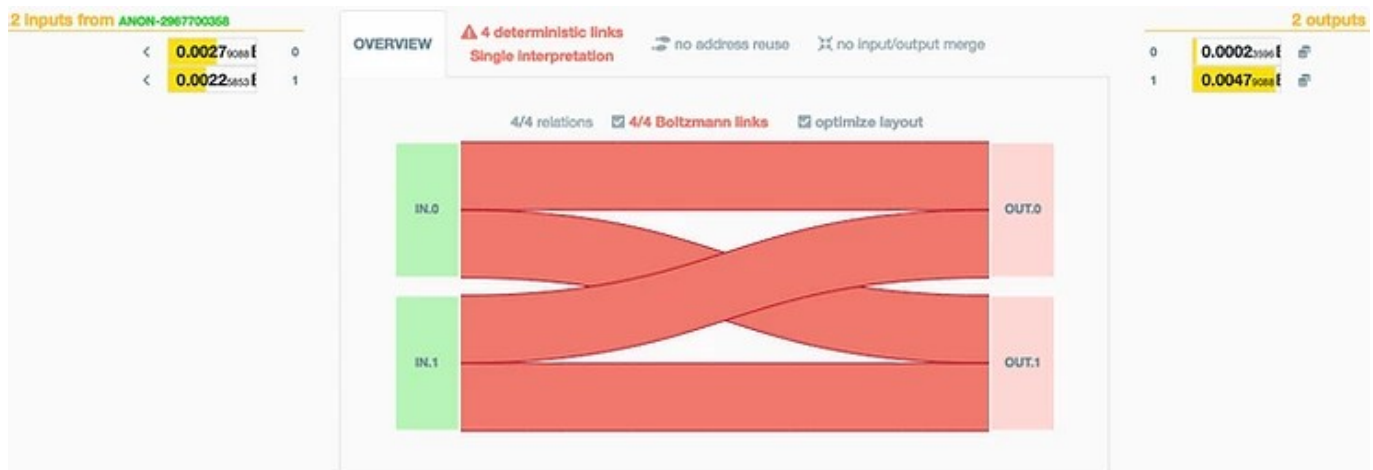
شایان یادآوری است که ادغام UTXOهای افراد یعنی آنها در این حد که از بخشی از UTXOهای همدیگر اطلاع پیدا کنند به هم اعتماد دارند. بنابراین این نکته را در انتخاب فرد شماره دو مد نظر داشته باشید.

Stowaway چیست؟

این نوع تراکنش در واقع پیاده‌سازی تیم سامورایی از مدل تراکنش P2EP یا همان پی‌جوین است. وقتی دو نفر از کیف پول سامورایی استفاده می‌کنند و یکی از آن‌ها قصد دارد برای دیگری مقداری بیت کوین ارسال کند می‌توانند از این نوع تراکنش استفاده کنند که از نظر سیستم‌های آنالیز بلاک چین شبیه به یک تراکنش معمولی است ولی در حقیقت یک کوین جوین مینیاتوری کوچک است. یکی از مؤثرترین ویژگی‌های تراکنش از نوع Stowaway این است که مقادیر بیت کوینی که در تراکنش است و بر روی بلاک چین ثبت می‌شود در اصل با مقادیر واقعی جابجا شده از کیف پول فرد اول به فرد دوم تفاوت دارد. همچنین برای ساختن تراکنش از نوع Stowaway، کیف پول سامورایی از UTXOهایی که در هر دو کیف پول فرد اول و دوم قرار دارد استفاده می‌کند و پیش فرض معروف «همه ورودی‌های یک تراکنش مال یک نفر است» را از بین می‌برد. از بین رفتن این فرض به شدت بر دقت تحلیل‌های شرکت‌های آنالیز بلاک چین اثر منفی می‌گذارد. برای ساختن این نوع تراکنش هم مثل روش StonewallX2 نیازی به حضور فیزیکی هر دو نفر در یک مکان نیست و می‌توانند از راه تعامل از راه دور این تراکنش را بسازند.

عکس زیر یک تراکنش از نوع Stowaway را نشان می‌دهد که من در این تراکنش دقیقاً 0.002 بیت کوین دریافت کرده‌ام. اگر خروجی‌های این تراکنش را بررسی کنید خواهید دید نمی‌توانید این رقم را در میان آن‌ها پیدا کنید. سایت kycp.org فرض را بر این می‌گذارد که صاحب هر دو UTXO ورودی به این تراکنش در واقع فرد ارسال کننده بیت کوین بوده است و این فرض غلط است، چون فقط یکی از آن‌ها متعلق به من بود. یک نکته حتی جالب‌تر این است که اصل وجود داشتن چنین تراکنشی می‌تواند شرکت‌های آنالیز بلاک چین بیت کوین را در تحلیل یک تراکنش معمولی که همه ورودی‌های آن مال یک نفر هستند هم دچار شک و تردید کند. ممکن است آن‌ها به خودشان بگویند «ممکن است یک تراکنش Stowaway باشد». به عبارت ساده‌تر یعنی افرادی که برای حفظ حریم خصوصی مالی تراکنش‌های ویژه‌ای مثل Stowaway می‌سازند،

به طور غیرمستقیم به حفظ حریم خصوصی افرادی که از تراکنش‌های معمولی بیت کوین استفاده می‌کنند کمک می‌کنند.



یک تراکنش Stowaway

از کجا می توانم اطلاعات بیشتری بدست بیاورم؟

- اطلاعات زیادی در گروه‌های تلگرامی «[اطلاع‌رسانی کیف پول سامورایی](#)» و «[ویرل پول](#)» وجود دارد و می‌توانید سؤالات‌تان را به صورت مستقیم از اعضای آنها پرسید
- تیم سامورایی [این مقاله](#) را درباره معیارهای حریم خصوصی تراکنش‌های ویرل پول نوشته است
- در سایت whirlpoolstats.com می‌توانید آخرین اطلاعات آماری ویرل پول را مشاهده کنید

بخش اول، مقدمه‌ای بر کوین‌جوین ترجمه bitcoinqna.com/coinjoin است.
بخش دوم، سؤال و جواب درباره ویرل‌پول ترجمه بخش ویرل‌پول همان سایت به آدرس
زیر است.

bitcoinqna.com/post/whirlpool-faq

هرگونه استفاده از این ترجمه برای همگان آزاد است.

تهیه کننده: ر.فرد

بازبینی و صفحه‌بندی: [@bitcoind_me](https://twitter.com/bitcoind_me)

پاییز ۱۳۹۹

bitcoind.me

منابع فارسی بیت‌کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند