



بیت کوین، حریم خصوصی، و آزادی فردی

ویراست دوم - نسخه دسکتاپ

بهار ۱۴۰۲

پیش‌نیازِ آزادی، حریم خصوصی است. این یعنی آزادی بدون حریم خصوصی امکان‌پذیر نیست. بدون حریم خصوصی افراد با دسترسی و سوءاستفاده از اطلاعات خصوصی شما قادر به کنترل شما می‌شوند و آزادی شما را به خطر می‌اندازند.

پیش‌نیاز مالکیت، آزادی است. بدون آزادی شما صاحب واقعی پول و دارایی خود نیستید چون حق مالکیت آن‌ها بدون آزادی به راحتی قابل سلب‌شدن است. وقتی از بیت‌کوین به‌عنوان یک پول مقاوم در برابر سانسور^۱ صحبت می‌کنیم منظورمان پولی است که سانسور و مصادره آن دشوار است و می‌توان به راحتی و بدون نیاز به کسب اجازه از هیچ شخص، نهاد، یا شرکتی از آن استفاده کرد.

امروز خطر بزرگی شبکهٔ بیت‌کوین را تهدید نمی‌کند. تاب‌آوری و پایداری این شبکه در گذر زمان به اثبات رسیده و ایجاد اختلال در آن کار بسیار دشواری است. برای تعطیل کردن شبکهٔ بیت‌کوین همهٔ کشورهای جهان باید با هم همکاری کنند و این موضوع با شرایطی که در دنیای امروز شاهد آن هستیم غیرممکن به نظر می‌رسد.

بزرگترین آسیب‌پذیری بیت‌کوین از جانب کاربران آن است و این موضوع با مقولهٔ حریم خصوصی ارتباط مستقیم دارد. استفاده از بیت‌کوین با توجه به عمومی بودن شبکه و شفاف بودن مقادیر انتقال یافته در تراکنش‌های آن اساساً خصوصی نیست. از طرف دیگر،

1 Censorship-resistant money

اغلب افراد بیت کوین‌هایشان را از طریق صرافی‌های رسمی خریداری می‌کنند و برای دریافت خدمات ناچار به ارائه اطلاعات هویتی خود هستند.

کاربران باید برای تکمیل مراحل احراز هویت خود، مدارک مهم و خصوصی مثل تصویر کارت ملی، یک عکس سلفی، شماره تلفن و آدرس محل سکونت‌شان را در سامانه صرافی‌های آنلاین آپلود کنند. این اطلاعات خصوصی به صورت مستقیم به سابقه خرید و فروش‌های آنان متصل و با گذشت زمان اطلاعات مالی افراد بیشتری در سامانه‌های این شرکت‌ها نگهداری خواهد شد.

ممکن است این اطلاعات در سطوح بین‌المللی میان نهادهای دولتی و قانونی به اشتراک گذاشته شوند یا به دلیل وجود داشتن حفره‌های امنیتی نرم‌افزاری در سامانه‌های صرافی‌های دیجیتال به بیرون نشت پیدا کنند یا حتی برای مقاصد تجاری به شرکت‌های ثالث فروخته شوند.

تصور قرار گرفتن اطلاعات خصوصی از قبیل عکس، شماره ملی، آدرس و تلفن محل سکونت شما در کنار سابقه خرید و فروش بیت کوین شما باعث می‌شود هرچه جدی‌تر به اهمیت این مسأله توجه کنید.

قوانین احراز هویت برای پیش‌گیری از پول‌شویی وضع شده‌اند. اما ضررهای این قوانین برای افراد عادی که قانون را رعایت می‌کنند بیشتر از منفعت آن‌ها است. زیرا حریم خصوصی این افراد با تجمع اطلاعات خصوصی و ذخیره آن به صورت دیجیتال نقض و در معرض خطر قرار می‌گیرد.

شرایط هر روز وخیم‌تر می‌شود و تعداد کاربرانی که بیت‌کوین‌های خود را از این روش به دست آورده‌اند بیشتر می‌شود. در حال حاضر نگرانی از مصادره یا سانسور شدن تراکنش

کاربران بیت کوین از جانب نهادها و صرافی‌های رسمی، بیشتر از امکان سانسور شدن تراکنش‌ها در سطح شبکه بیت کوین است.

اولین مسأله‌ای که باید به آن آگاه باشیم این است که همه اطلاعات خرید و فروش ما در سرورهای این شرکت‌ها ثبت می‌شود و برای همیشه باقی می‌ماند. قوانین در برخی از کشورهای پیشرفته‌ای که سابقه دغدغه حفظ حریم خصوصی شهروندان در آن‌ها به قبل از پدید آمدن بیت کوین بازمی‌گردد طوری تنظیم شده‌اند که اطلاعات الکترونیکی شهروندان می‌بایست بعد از گذشت زمان مشخص یا طبق درخواست کاربر کاملاً از سیستم آن‌ها حذف شود. اما متأسفانه در کشور ما چنین قانونی وجود ندارد و اطلاعات شما بعد از ایجاد یک حساب کاربری در یک صرافی آنلاین تا ابد در سرورهای آن‌ها نگهداری خواهد شد و تلاش شما برای حذف آن بی‌نتیجه خواهد ماند.

این مشکل چگونه حل می‌شود؟ راه‌های مختلفی برای حفظ حریم خصوصی در زمان خرید و همچنین در مواقعی که از بیت کوین به عنوان وسیله‌ای برای پرداخت استفاده می‌کنیم وجود دارد. در ادامه به راه‌های به دست آوردن بیت کوین به صورت خصوصی و ابزارهایی که برای قطع کردن رابطه بین اطلاعات هویتی و بیت کوین‌های خریداری شده از نهادهای رسمی بکار می‌روند، اشاره می‌کنیم.

امروزه ابزارها و روش‌های زیادی برای به دست آوردن و استفاده خصوصی از بیت کوین در اختیار کاربران ساکنان برخی از کشورهای دنیا است. اما متأسفانه این روش‌ها به دلایلی که پرداختن به آن‌ها خارج از حوصله این مطلب است در کشور ما مورد استقبال قرار نگرفته‌اند. از جمله این ابزارها می‌توان به بازار غیرمتمرکز Bisq و سایت‌های HodlHodl و Robosats اشاره کرد. سایت Robosats از سال ۲۰۲۲ شروع به کار کرده

و کاربران می‌توانند با استفاده از کیف پولی که از شبکه لایت‌نینگ^۱ بیت‌کوین پشتیبانی می‌کند اقدام به خرید و فروش بدون واسطه بیت‌کوین کنند.

(برای کسب اطلاعات بیشتر در مورد شبکه لایت‌نینگ، مقاله «راهنمای مقدماتی شبکه لایت‌نینگ» را در سایت منابع فارسی بیت‌کوین مطالعه کنید.)

از روش‌های خصوصی به دست آوردن بیت‌کوین همچنین می‌توان به استخراج^۱، و دریافت بیت‌کوین در ازای دستمزد اشاره کرد. استخراج بیت‌کوین نیاز به دستگاه‌های گرانی دارد که مصرف برق آن‌ها بسیار بالا است و در هنگام کار گرما و صدای زیادی تولید می‌کنند. شاید بتوان گفت با توجه به کمبود برق و ممنوعیت استخراج خانگی در کشور ما این روش برای عموم مردم مناسب نیست. اما دریافت بیت‌کوین در ازای خدمات یا فروش محصولات همیشه و همه جا امکان‌پذیر است. شما می‌توانید درآمد انجام کار، پروژه، یا فروش محصولات و خدماتی که ارائه می‌کنید را با در نظر گرفتن درصدی تخفیف به بیت‌کوین دریافت کنید.

موضوع مهم بعدی، مسأله نگهداری از بیت‌کوین است. هر کس باید اختیار کلیدهای خصوصی بیت‌کوین خود را شخصاً بر عهده بگیرد. این موضوع تا جایی برای فعالان بیت‌کوین مهم است که اغلب می‌گویند «بیت‌کوینی که کلید خصوصی‌اش در اختیار شخص شما نباشد، مال شما نیست»^۲ یا به عبارت دیگر بیت‌کوین‌هایی که روی صرافی از آن‌ها نگهداری می‌کنید را جزو بیت‌کوین‌های خود به حساب نیاورید.

نگهداری از بیت‌کوین روی صرافی یا سیستم‌های مالی دیجیتال چه مخاطراتی برای صاحبان آن به همراه دارد؟ کمترین خطری که بیت‌کوین‌های موجود در صرافی‌ها را

1 Lightning Network

1 Bitcoin Mining

2 Not your keys, Not your bitcoin

تهدید می‌کند قوانین، خصوصاً قوانین مالیاتی است. دولت می‌تواند با تغییر قانون مالیات، حساب شما در صرافی‌های دیجیتال را مسدود یا درصدی از دارایی‌تان را به‌عنوان مالیات اخذ کند. همچنین توجه به این نکته ضروری است که سامانه‌های صرافی‌های دیجیتال مثل هر سامانه الکترونیکی دیگری قابل هک شدن هستند. صرافی‌های بزرگ و معروفی در دنیا وجود داشته‌اند که همه یا بخش قابل توجهی از دارایی مشتریان خود را از دست داده‌اند و مشتریان پس از گذشت سال‌ها همچنان برای بازپس‌گیری دارایی خود درگیر پرونده‌های قانونی و قضایی هستند.

هک شدن یک صرافی دیجیتال همواره منجر به از بین رفتن دارایی مشتریان آن نمی‌شود. در برخی مواقع هکرها به دنبال اطلاعات هویتی، آدرس ایمیل، و محل سکونت مشتریان صرافی‌ها هستند و برای اجرای روش‌های پیچیده کلاهبرداری خود از این اطلاعات استفاده می‌کنند. به این موضوع دقت کنید:

در کشور ما صرافی‌های دیجیتال ملزم به اطلاع‌رسانی در مورد حمله‌های هکری و نشت پیدا کردن اطلاعات مشتریان خود نیستند. تصور اینکه علاوه بر کارمندان صرافی هکرها نیز به اطلاعات خصوصی شما از قبیل محل زندگی و مقدار دارایی شما دسترسی داشته باشند برای افرادی که به حریم خصوصی مالی خود بها می‌دهند یک کابوس وحشتناک است.

این بزرگترین خطری است که کاربران صرافی‌های دیجیتال را تهدید می‌کند. باید به این نکته اشاره کرد که پذیرش مسئولیت نگهداری از کلیدهای خصوصی بیت‌کوین موضوعی حساس و مهم است. این کار مخاطرات خاص خود را دارد که از جمله آن‌ها می‌توان به از دست رفتن کلیدها در نتیجه غفلت و همچنین مسأله مهم وراثت اشاره کرد.

نگهداری از کلیدهای بیت کوین موضوعی است که به کسب دانش و تمرین نیاز دارد.
برای کسب اطلاعات بیشتر به سایت منابع فارسی بیت کوین مراجعه کنید.

حال زمان آن فرا رسیده است که در مورد مشکل بعدی یعنی ارتباط همیشگی که میان اطلاعات هویتی مشتریان صرافی‌های قانونی با بیت کوین‌های خریداری شده آنان برقرار می‌شود، صحبت کنیم. همانطور که پیشتر اشاره شد زنجیره بلاک بیت کوین عمومی و غیرقابل تغییر است. هرکس قادر است با راه‌اندازی یک نود^۱ به شبکه بیت کوین بپیوندد و به سابقه و اطلاعات دقیق همه تراکنش‌های صورت گرفته در این شبکه دسترسی پیدا کند.

وقتی یک تراکنش خرید یا فروش بیت کوین به شناسه کاربری شما در سامانه صرافی مرتبط شود، این تراکنش و تراکنش‌های بعدی مرتبط با آن تا روزی که شبکه بیت کوین روشن باشد به شما نسبت داده خواهد شد.

با توجه به شفافیت مقادیر جابجا شده در تراکنش‌های ذخیره شده در زنجیره بلاک بیت کوین ارتباط میان ورودی و خروجی‌های موجود در تراکنش‌های این زنجیره یک گراف درهم‌تنیده و مرتبط تشکیل می‌دهد که ورودی‌ها و خروجی‌های هر یک از تراکنش‌های آن با درجه‌ای از احتمال با یکدیگر مرتبط هستند.

در چند سال اخیر شاهد پدید آمدن شرکت‌هایی هستیم که تلاش می‌کنند با استفاده از اطلاعات ثبت شده از مشتریان صرافی‌های دیجیتال و تحلیل و آنالیز این گراف، تراکنش‌های کاربران شبکه بیت کوین را ردگیری و هویت صاحبان آنها را شناسایی کنند. برای مقابله با این مشکل و استفاده خصوصی از بیت کوین باید با روش‌های آنالیز و تحلیل

این شرکت‌ها مقابله و آن‌ها را بی‌اثر کنیم. اینجاست که موضوع تراکنش‌های اشتراکی^۱ یا کوین‌جوین^۲ مطرح می‌شود.

استفاده از کوین‌جوین خطای محاسباتی این روش‌های تحلیلی را بالا می‌برد و باعث ایجاد شک و شبهه در روند تعیین هویت صاحبان ورودی و خروجی‌های تراکنش‌های شبکه بیت‌کوین می‌شود. یک تراکنش اشتراکی ویژگی‌هایی دارد که به موجب آن‌ها تحلیل و محاسبه احتمال ارتباط میان ورودی‌ها و خروجی‌های یک تراکنش برای ناظر بیرونی بسیار دشوار می‌شود. در حال حاضر کاربران بیت‌کوین برای ایجاد تراکنش‌های اشتراکی سه ابزار کوین‌مارکت^۳، ویرل‌پول^۴، و واسابی^۵ را در اختیار دارند. هر کدام از این ابزارها توسط تیم‌های جداگانه‌ای توسعه داده شده‌اند و نقاط ضعف و قوت خود را دارند.

استفاده خصوصی از بیت‌کوین نیز مانند نگهداری از کلیدهای خصوصی، امری است که به کسب دانش و تمرین نیاز دارد. برای کسب اطلاعات بیشتر در مورد ابزار ویرل‌پول که توسط تیم سامورایی توسعه داده شده به بخش کتابخانه سایت منابع فارسی بیت‌کوین مراجعه کنید.

برخلاف تصور عامه تلاش برای حفظ حریم خصوصی در بیت‌کوین هیچ‌گونه ارتباطی با انجام کارهای غیرقانونی ندارد. همانطور که قبلاً اشاره کردیم بیت‌کوین یک شبکه عموم و شفاف است و هر کس می‌تواند با استفاده از ابزارهای عمومی و در دسترس به سابقه همه تراکنش‌های این شبکه دسترسی پیدا کند.

1 Collaborative transactions
2 CoinJoin
3 JoinMarket
4 Whirlpool
5 Wasabi

فرض کنید قصد دارید با بخشی از بیت کوین‌هایی که در طول سال‌ها پس‌انداز کرده‌اید یک لپ‌تاپ بخرید. آیا امنیت شما در صورتی که مغازه‌دار قادر باشد با بررسی اجمالی تراکنش به مقدار واقعی بیت کوین ذخیره شده در کیف پول موبایل شما پی‌برد، به خطر نمی‌افتد؟

یا مثلاً فرض کنید مقدار کمی بیت کوین به عنوان هدیه برای دوست خود ارسال می‌کنید و او با بررسی تراکنش به بخشی از دارایی ذخیره شده در کیف پول موبایل شما پی‌برد. این مسأله چه اثری روی رابطه شما و دوست‌تان خواهد گذاشت؟

حریم خصوصی یک حق انسانی است و همه ما صرف‌نظر از سن، شغل، و جایگاه اجتماعی خود به آن نیاز داریم و باید از آن محافظت کنیم. حریم خصوصی پیش‌نیاز آزادی است.

اگر به مطالعه در مورد تاریخچه بیت کوین، طرز کار آن، و روش‌های استفاده از کیف پول‌های بیت کوین علاقه‌مند هستید، به سایت منابع فارسی بیت کوین مراجعه کنید.

منابع فارسی مرتبط

«کتاب کوچک بیت کوین»

کتاب کوچک بیت کوین

این کتاب توضیح می‌دهد که پول در دنیای امروز ما چه اشکالاتی دارد و چرا بیت کوین به وجود آمده تا جایگزینی برای آن باشد.

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 39 A3 B0 FD 7A 79 12 B2 7A C7 2C 28 >
00000030 67 75 80 61 7F CE 1B C3 88 BA 51 32 3A 9F 88 AA >
00000040 48 18 58 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C >
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 40 04 FF FF 00 1D .....
00000080 01 04 65 54 68 95 20 54 69 80 85 73 20 30 33 2F ..
00000090 48 61 68 2F 32 31 30 39 20 43 88 81 88 83 85 8C ..
000000A0 6C 6F 73 20 6F 6E 20 62 72 69 6E 68 20 6F 6E 20 ..
000000B0 73 65 63 67 6E 64 20 62 61 69 6C 6F 75 74 20 66 ..
000000C0 6F 72 20 62 61 6E 68 73 FF FF FF 01 00 F2 03 ..
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 ..
000000E0 18 87 F1 A8 71 30 B7 10 5C D4 A8 28 B0 29 09 A6 ..
000000F0 79 62 80 2A 1F 61 0E B6 49 F4 3C 3F 4C FF 18 C4 ..
00000100 F3 55 04 85 1E C1 12 DE 5C 38 4D F7 DA 0B 8D 57 ..
00000110 8A 4C 70 28 68 F1 1D 5F AC 00 00 00 00 00 00 00 ..
```

این کتاب در دو نسخه PDF و صوتی در دسترس علاقه‌مندان به بیت کوین قرار دارد.

[نسخه صوتی](#) - [نسخه PDF](#) - [نسخه موبایل](#)



مقاله «آیا دولت‌ها می‌توانند بیت کوین را متوقف کنند؟»

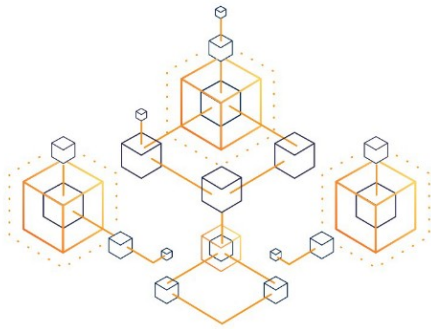
نویسنده این مقاله وضعیت کنونی شبکه بیت کوین را تشریح، و روش‌هایی که تاکنون توسط دولت‌ها برای متوقف ساختن بیت کوین به کار گرفته شده را بررسی می‌کند.

آیا دولت‌ها می‌توانند
بیت کوین را متوقف کنند؟

[نسخه صوتی](#) - [نسخه PDF](#)

کتاب «اختراع بیت کوین»

اختراع بیت کوین



نویسنده این کتاب تلاش می کند تا به صورت قدم به قدم به تشریح زیرساخت های بیت کوین پردازد. این کتاب برای فهم نحوه کارکرد بیت کوین بسیار مفید است و برای درک مطالب مطرح شده هیچ گونه پیش نیازی لازم ندارد.

[نسخه PDF](#) - [نسخه موبایل](#)

مقاله «چرا بیت کوین یک طرح کلاه برداری پانزی نیست»



نویسنده این مقاله تلاش می کند تا یکی از نگرانی های مطرح در مورد بیت کوین که ادعای پانزی بودن آن است را بررسی، و سیستم هایی که ویژگی های مشابهی با طرح پانزی دارند را با بیت کوین مقایسه می کند.

[نسخه صوتی](#) - [نسخه PDF](#)

چرا بیت کوین

یک طرح کلاه برداری پانزی نیست

برای دسترسی به منابع بیشتر به

[کتابخانه سایت منابع فارسی بیت کوین](#) مراجعه کنید

این مطلب در تابستان سال ۱۴۰۱ توسط یکی از مخاطبان سایت منابع فارسی بیت کوین تهیه و با استفاده از سیستم متن به گفتار شرکت مایکروسافت به فایل صوتی تبدیل شده است.

این راهنما با مجوز «مالکیت عمومی» منتشر می‌شود و بازنشر آن به هر شکل آزاد است.

منابع فارسی بیت کوین

بهار ۱۴۰۲