بیت کوین، حریم خصوصی، و آزادی فردی

ویراست دوم – نسخهٔ 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[1] صحبت می‌کنیم منظورمان پولی‌ست که سانسور و مصادرهٔ آن دشوار است و می‌توان به‌راحتی 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

1 Censorship-resistant money

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 انتقال‌یافته دَر تراکنش‌های آن اسَاساً خصوصی نیست. ازطرف دیگر، اغلب افراد بیت‌کوین‌هایشان 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، شمارهٔ تلفن و آدرس محل سکونت‌شان را در سامانهٔ صرافی‌های آنلاین آپلود کنند. این اطلاعات خصوصی به‌صورت مستقیم به سابقهٔ 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 قرارگرفتن اطلاعات خصوصی از قبیل عکس، شمارهٔ ملی، آدرس و تلفن محل سکونت شما در کنار سابقهٔ خرید و فروش بیت‌کوین 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

تجمیع اطلاعات خصوصی و ذخیرهٔ آن به‌صورت دیجیتال نقض و در معرض خطر قرار می‌گیرد.

شرایط هر روز وخیم‌تر می‌شود و تعداد کاربرانی که بیت‌کوین‌های خود را از این روش به‌دست آورده‌اند بیشتر می‌شود. در حال حاضر نگرانی از مصادره یا سانسورشدن تراکنش کاربران بیت‌کوین از جانب نهادها و صرافی‌های رسمی، بیشتر از امکان سانسور شدنِ تراکنش‌ها در سطح شبکهٔ بیت‌کوین است.

اولین مسأله‌ای که باید به آن آگاه باشیم این است که همهٔ اطلاعات خرید و فروش ما در سرورهای این شرکت‌ها

ثبت می‌شود و برای همیشه باقی می‌ماند. قوانین در برخی از کشورهای پیشرفته‌ای که سابقهٔ دغدغهٔ حفظ حریم خصوصی شهروندان در آن‌ها به قبل از پدیدآمدن بیت‌کوین 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 بیت‌کوین به‌عنوان وسیله‌ای برای پرداخت استفاده می‌کنیم وجود دارد. در ادامه به راه‌های به‌دست آوردن بیت‌کوین به‌صورت خصوصی و ابزارهایی که برای قطع کردن رابطه بین اطلاعات هویتی و بیت‌کوین‌های خریداری شده از نهادهای رسمی بکار می‌روند، اشاره می‌کنیم.

امروزه ابزارها و روش‌های زیادی برای به‌دست آوردن و استفادهٔ خصوصی از بیت‌کوین در اختیار کاربران ساکنان برخی از کشورهای دنیا است. اما

متأسفانه این روش‌ها به دلایلی که پرداختن به آن‌ها خارج از حوصلهٔ این مطلب است در کشور ما مورد استقبال قرار نگرفته‌اند. از جملهٔ این ابزارها می‌توان به بازار غیرمتمرکز Bisq و سایت‌های HodlHodl و Robosats اشاره کرد. سایت Robosats از سال ۲۰۲۲ شروع به کارکرده و کاربران می‌توانند با استفاده از کیف پولی که از شبکهٔ لایتنینگ[1] بیت‌کوین پشتیبانی می‌کند اقدام به خرید و فروش بدون واسطهٔ بیت‌کوین کنند.

(برای کسب اطلاعات بیشتر در مورد شبکهٔ لایتنینگ، مقالهٔ «راهنمای مقدماتی

1 Lightning Network

شبکهٔ لایتنینگ» را در سایت منابع فارسی بیت‌کوین مطالعه کنید.)

از روش‌های خصوصی به‌دست آوردن بیت‌کوین همچنین می‌توان به استخراج[1]، 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

1 Bitcoin Mining

درآمد انجام کار، پروژه، یا فروش محصولات و خدماتی که ارائه می‌کنید را با درنظرگرفتن درصدی تخفیف به بیت‌کوین دریافت کنید.

موضوع مهم بعدی، مسأله نگهداری از بیت‌کوین است. هرکس 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، مالِ شما نیست[1]» یا به عبارت دیگر بیتَ‌کوین‌هایی که روی صرافی از آن‌ها نگهداری می‌کنید را جزو بیت‌کوین‌های خود به‌حساب نیاورید.

1 Not your keys, Not your bitcoin

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 تهدید می‌کند قوانین، خصوصاً قوانین مالیاتی است. دولت می‌تواند با تغییرِ قانونِ 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 سامانهٔ الکترونیکی دیگری قابل هَک‌شدن هستند. صرافی‌های بزرگ و معروفی در دنیا وجود داشته‌اند که همه یا بخش قابل‌توجهی از دارایی مشتریان خود را از

دست داده‌اند و مشتریان پس از گذشت سال‌ها همچنان برای بازپس‌گیری دارایی خود درگیر پروسه‌های قانونی و قضایی هستند.

هَک‌شدنِ یک صرافیِ دیجیتال همواره منجر به اَز بین رفتنِ دارایی مشتریان آن نمی‌شود. در برخی مواقع هکرها به دنبال اطلاعات هویتی، آدرس ایمیل، و محل سکونت مشتریان صرافی‌ها هستند و برای اجرای روش‌های پیچیدهٔ 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 پیداکردنِ 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 جملهٔ آن‌ها می‌توان به از دست رفتنِ

کلیدها در نتیجهٔ غفلت و همچنین مسألهٔ 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 بیت‌کوین‌های خریداری شدهٔ آنان برقرار می‌شود، صحبت کنیم. همانطور که پیشتر اشاره شد زنجیرهٔ بلاکِ بیت‌کوین عمومی و

غیرقابل تغییر است. هر کس قادر است با راه‌اندازی یک نود[1] به شبکهٔ بیت‌کوین بپیوندد و به سابقه و اطلاعات دقیق همهٔ تراکنش‌های صورت‌گرفته در این شبکه دسترسی پیدا کند.

وقتی یک تراکنش خرید یا فروشِ بیت‌کوین به شناسهٔ کاربری شما در سامانهٔ صرافی مرتبط شود، این تراکنش و تراکنش‌های بعدیِ مرتبط با آن تا روزی که شبکهٔ بیت‌کَوین روشن باشد به شما نسبت داده خواهد شد.

با توجه به شفافیت مقادیر جابجا شده در تراکنش‌های ذخیره شده در زنجیرهٔ

1 Node

بلاک بیت‌کوین ارتباط میان ورودی و خروجی‌های موجود در تراکنش‌های این زنجیره یک گراف درهم‌تنیده و مرتبط تشکیل می‌دهد که ورودی‌ها و خروجی‌های هریک 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 ثبت‌شده از مشتریان صرافی‌های دیجیتال و تحلیل و آنالیز این گراف، تراکنش‌های کاربران شبکهٔ بیت‌کوین را ردگیری و هویت صاحبان آها را شناسایی کنند. برای مقابله با این مشکل و استفاده خصوصی از بیت‌کوین

باید با روش‌های آنالیز و تحلیل این شرکت‌ها مقابله و آن‌ها را بی‌اثر کنیم. اینجاست که موضوع تراکنش‌های اشتراکی[1] یا کوین‌جوین[2] 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 شبکهٔ بیت‌کوین می‌شود. یک تراکنش اشتراکی ویژگی‌هایی دارد که به موجب آن‌ها تحلیل و محاسبهٔ احتمال ارتباط میان ورودی‌ها و خروجی‌های یک تراکنش برای ناظر بیرونی بسیار دشوار می‌شود. در حال

---

1 Collaborative transactions
2 CoinJoin

حاضر کاربران بیت‌کوین برای ایجاد تراکنش‌های اشتراکی سه ابزار جوین‌مارکت[1]، ویرل‌پول[2]، و واسابی[3] را در اختیار دارند. هر کدام از این ابزارها توسط تیم‌های جداگانه‌ای توسعه داده شده‌اند و نقاط ضعف و قوت خود را دارند.

استفادهٔ 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

1 JoinMarket
2 Whirlpool
3 Wasabi

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 شبکهٔ عموم و شفاف است و هرکس می‌تواند با استفاده از ابزارهای عمومی و در دسترس به سابقهٔ همهٔ تراکنش‌های این شبکه دسترسی پیدا کند.

فرض کنید قصد دارید با بخشی از بیت‌کوین‌هایی 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 بیت‌کوین ذخیره شده در کیف پول موبایل شما پی ببرد، به خطر نمی‌افتد؟

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

حریم خصوصی یک حق انسانی است و همهٔ ما صرف‌نظر از سن، شغل، و جایگاه

اجتماعی خود به آن نیاز داریم و باید از آن محافظت کنیم. حریم خصوصی پیش‌نیازِ آزادی است.

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

منابع فارسی مرتبط

«کتاب کوچک بیت‌کوین»

این کتاب توضیح می‌دهد که پول در دنیای امروز ما چه اشکالاتی دارد و چرا بیت‌کوین به‌وجود آمده تا جایگزینی برای آن باشد.

این کتاب در دو نسخهٔ PDF و صوتی در دسترس علاقه‌مندان به بیت‌کوین قرار دارد.

نسخهٔ صوتی – نسخهٔ PDF – نسخهٔ موبایل

مقالهٔ «آیا دولت‌ها می‌توانند بیت‌کوین را متوقف کنند؟»

آیا دولت‌ها می‌توانند
بیت‌کوین را متوقف کنند؟

نویسندهٔ این مقاله وضعیت کنونی شبکهٔ بیت‌کوین را تشریح، و روش‌هایی که تاکنون توسط دولت‌ها برای متوقف ساختن بیت‌کوین به‌کار گرفته شده را بررسی می‌کند.

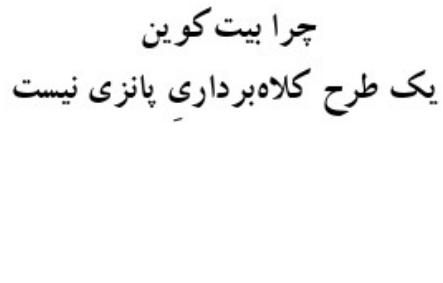
نسخهٔ صوتی – نسخهٔ PDF

کتاب «اختراع بیت‌کوین»

نویسندهٔ این کتاب تلاش می‌کند تا به‌صورت قدم به قدم به تشریح زیرساخت‌های بیت‌کوین بپردازد. این کتاب برای فهم نحوهٔ کارکرد بیت‌کوین بسیار مفید است و برای درک مطالب مطرح شده هیچ‌گونه پیش‌نیازی لازم ندارد.

نسخهٔ PDF – نسخهٔ موبایل

مقالهٔ «چرا بیت‌کوین یک طرح کلاه‌برداری پانزی نیست»



نویسندهٔ این مقاله تلاش می‌کند تا یکی از نگرانی‌های مطرح در مورد بیت‌کوین که ادعای پانزی بودن آن است را بررسی، و سیستم‌هایی که ویژگی‌های مشابهی با طرح پانزی دارند را با بیت‌کوین مقایسه می‌کند.

نسخهٔ صوتی – نسخهٔ PDF

برای دسترسی به منابع بیشتر به کتابخانهٔ سایت منابع فارسی بیت‌کوین مراجعه کنید

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

منابع فارسی بیت‌کوین

بهار ۱۴۰۲