فصل

۱۱

امنیت بیت‌کوین

امن کردن بیت‌کوین چالشی بزرگ است، چون بیت‌کوین یک ارزش انتزاعی (مثل تراز یک حساب بانکی) نیست. بیت‌کوین در واقع بسیار شبیه پول یا طلای دیجیتال است. در دنیای بیت‌کوین، همه چیز به مالکیت مربوط می‌شود؛ یعنی اگر مقداری بیت‌کوین در دست شما باشد، آن بیت‌کوین قطعاً مال شماست. در مورد پول نقد (اسکناس و سکه) مالکیت ۹۰ درصد قضیه است، و گاهی اوقات همچنان باید ثابت کنید مالک واقعی آن پول یا فلز گرانبها هستید. داشتن کلیدهایی که بتوانند قفل بیت‌کوین را باز کنند، معادل مالکیت مقداری پول یا فلزات گرانبها است. وقتی مقداری بیت‌کوین دارید، ممکن است آن را گم کنید، از شما بدزدند، یا اشتباهاً به کسی بدهید. و درست مثل وقتی پول نقد خود را گم می‌کنید، در اینجا هم هیچ راه برگشتی وجود ندارد.

با این حال، بیت‌کوین ویژگی‌هایی دارد که پول نقد، طلا و حساب‌های بانکی ندارند. از یک کیف‌پول بیت‌کوین، که حاوی کلیدها است، می‌توان مثل یک فایل نسخه‌ی پشتیبان گرفت، می‌توان آن را در چند نسخه تکثیر کرد، و یا حتی روی کاغذ چاپ کرد. از پول نقد، طلا یا حساب‌های بانکی نمی‌توان «نسخه‌ی پشتیبان» گرفت. بیت‌کوین چنان با همه‌ی آنچه تاکنون دیده‌ایم، فرق دارد که برای امنیت آن باید چاره‌ای تازه اندیشید.

اصول امنیت

اصل بنیادی بیت‌کوین غیرمتمرکز بودن آن است، و این عدم‌تمرکز پیامدهای مهمی برای امنیت آن در بر دارد. مدل‌های متمرکز، مانند بانک‌های سنتی یا شبکه‌های پرداخت، برای دور نگه داشتن افراد ناباب و خبیث بر مبنای شناسایی و کنترل دسترسی مشتریان خود عمل می‌کنند. در مقایسه، یک سیستم غیرمتمرکز مانند بیت‌کوین مسئولیت و کنترل را به کاربران می‌سپارد. از آنجا که امنیت این مدل بر اساس اثبات-کار قرار داده شده، نه کنترل دسترسی، شبکه‌ی بیت‌کوین می‌تواند باز باشد و نیازی به رمزگذاری ترافیک آن نیست.

پرداخت در یک شبکه‌ی پرداخت سنتی، مثل سیستم‌های کارت اعتباری، کاملاً باز است چون هویت خصوصی کاربر (شماره‌ی کارت اعتباری) روی آن درج شده است. وقتی یک کارت اعتباری صادر شد، هر کسی می‌تواند با داشتن این کارت از آن «برداشت» یا قبوض آن را «پرداخت» کند. بنابراین، این شبکه‌ی پرداخت باید در تمام طول مسیر (از مشتری تا سیستم) کاملاً امن باشد و هیچ نوع استراق‌سمع یا دخالتی در ترافیک بین این دو نقطه‌ی انتهایی (در هیچ یک از مراحل انتقال داده یا ذخیره‌سازی آن) ممکن نباشد. اگر یک فرد خبیث به این سیستم دسترسی پیدا کند، می‌تواند اطلاعات

تراکُنش‌ها و پرداخت‌ها را ببیند و با اطلاعاتی که به دست می‌آورد، تراکُنش‌های دروغین انجام دهد. از آن بدتر، وقتی اطلاعات مشتری لو برود، در معرض خطر جعل هویت قرار می‌گیرد، و باید اقدامی برای جلوگیری از سوءاستفاده از اطلاعات حساب‌های لو رفته صورت گیرد.

سیستم بیت‌کوین به کلی متفاوت است. یک تراکُنش بیت‌کوین فقط اجازه‌ی پرداخت یک مبلغ مشخص به یک گیرنده‌ی خاص را صادر می‌کند و هیچ اطلاعات دیگری در آن وجود ندارد که بتوان برای جعل یا تحریف از آن سوءاستفاده کرد. در یک تراکُنش بیت‌کوین هیچ گونه اطلاعات شخصی، مثل نام و هویت طرفین پرداخت، وجود ندارد و امکان استفاده از آن برای پرداخت‌های دیگر وجود نخواهد داشت. بنابراین، رمزگذاری و حفاظت ترافیک شبکه‌ی بیت‌کوین در مقابل استراق‌سمع ضرورتی ندارد. در حقیقت، یک تراکُنش بیت‌کوین را می‌توان بدون نگرانی امنیتی روی کانال‌های باز و عمومی، مثل شبکه‌های بلوتوث یا وای-فای، منتشر کرد.

مدل امنیتی غیرمتمرکز بیت‌کوین بخش اعظم قدرت را به کاربران می‌سپارد؛ قدرت با خود مسئولیت می‌آورد، مسئولیت حفظ امنیت کلیدها. برای اکثر کاربران تأمین این امنیت کار ساده‌ای نیست، به خصوص روی دستگاه‌های همه-منظوره که تقریباً همیشه به اینترنت متصل هستند، مثل کامپیوترهای شخصی و تلفن‌های هوشمند. هر چند مدل غیرمتمرکز بیت‌کوین از لو رفتن‌های دستجمعی مانند آنچه در کارت‌های اعتباری دیده شده است، جلوگیری می‌کند، ولی بسیاری از کاربران قادر به تأمین امنیت کافی برای کلیدهای خود نیستند، و یک به یک شکار می‌شوند.

توسعه‌ی اَمن سیستم‌های بیت‌کوین

مهمترین اصل برای برنامه‌نویسان بیت‌کوین غیرمتمرکز بودن آن است. اکثر برنامه‌نویسان با مدل‌های امنیت متمرکز آشنایی دارند و ممکن است وسوسه شوند آن مدل‌ها را در برنامه‌های کاربردی که برای بیت‌کوین می‌نویسند، اِعمال کنند، اقدامی که نتایج آن فاجعه‌بار خواهد بود.

این مدل امنیت به کنترل غیرمتمرکز بر کلیدها و اعتبارسنجی مستقل تراکُنش توسط معدنچیان متکی است. اگر می‌خواهید امنیت بیت‌کوین را بالا ببرید، باید چارچوب مدل امنیتی بیت‌کوین را ترک نکنید. به بیان ساده: *کنترل کلیدها را از کاربر نگیرید و تراکُنش‌ها را از بلاک‌چین خارج نکنید.*

برای مثال، بسیاری از صرافی‌های اولیه‌ی بیت‌کوین تمام سرمایه‌ی کاربر را در یک کیف‌پول «داغ» (آنلاین) قرار می‌دادند و همه‌ی کلیدها را روی یک سرویس‌دهنده‌ی واحد ذخیره می‌کردند. این طراحی کنترل را از کاربر می‌گیرد و آن را در یک سیستم واحد (که کلیدها در آن قرار دارند) متمرکز می‌کند. وقتی این سیستم هَک شود (اتفاقی که به دفعات افتاده)، پیامدهای فاجعه‌باری برای مشتریان آن خواهد داشت.

یک اشتباه رایج دیگر خارج کردن تراکُنش‌ها از بلاک‌چین، به طمع کاهش کارمزد تراکُنش و سرعت دادن به پردازش آن، است. سیستمی که «خارج-بلاک‌چین» است، باید تراکُنش‌ها را در داخل خود ذخیره کند، یک دفتر کل متمرکز داشته باشد، و فقط هر از چند گاهی بلاک‌چین مستقل خود را با بلاک‌چین بیت‌کوین همسان‌سازی کند. این روش هم امنیت غیرمتمرکز بیت‌کوین را با رویکردی تکروانه و متمرکز جایگزین می‌کند. وقتی تراکُنش‌ها خارج از بلاک‌چین اصلی بیت‌کوین هستند، امکان دستکاری خرابکارانه در دفتر کل محلی (به خصوص آنهایی که به خوبی حفاظت نمی‌شوند) وجود دارد که خطر سرقت بیت‌کوین را برای کاربران به همراه خواهد داشت.

اگر می‌خواهید سرمایه‌ی خود را از زیر چتر حمایت امنیت غیرمتمرکز بیت‌کوین خارج کنید، باید آماده‌ی پرداخت هزینه‌ی سنگین امنیت عملیاتی، لایه‌های متعدد کنترل دسترسی، و حسابرسی دقیق (مثل کاری که بانک‌های سنتی می‌کنند) باشید. حتی اگر سرمایه و انضباط کافی برای پیاده‌سازی یک مدل امنیتی مستحکم داشته باشید، این مدل امنیتی

چیزی بیش از یک کپی ناقص و شکننده از شبکه‌های مالی سنتی نخواهد بود، شبکه‌هایی که هرگز از جعل هویت، رشوه و اختلاس رهایی نداشته‌اند. برای بهره‌گیری از مدل منحصر به فرد امنیت غیرمتمرکز بیت‌کوین، در مقابل وسوسه‌ی به‌کارگیری معماری‌های متمرکز (که ممکن است با آنها خو گرفته باشید ولی در نهایت امنیت بیت‌کوین را از درون تضعیف می‌کنند) مقاومت کنید.

بنیان اعتماد

معماری امنیت سنتی بر مفهومی موسوم به **بنیان اعتماد** (root of trust) استوار است. «بنیان اعتماد» یک هسته‌ی امن و قابل‌اعتماد است که اساس امنیت کل سیستم یا برنامه‌ی کاربردی را تشکیل می‌دهد. معماری امنیت به صورت دایره‌های هم‌مرکز (مثل لایه‌های پیاز) که از داخل به بیرون گسترش می‌یابند، حول این بنیان اعتماد توسعه داده می‌شود. هر لایه با استفاده از کنترل دسترسی، امضای دیجیتال، رمزگذاری، و دیگر عملکردهای امنیتی، روی لایه‌ی داخلی که قابل‌اعتمادتر است، ساخته می‌شود. با پیچیده‌تر شدن سیستم نرم‌افزاری، احتمال بروز باگ نیز بیشتر خواهد شد، که آن را در مقابل حمله‌های امنیتی آسیب‌پذیرتر می‌کند. در نتیجه، هر قدر یک سیستم نرم‌افزاری پیچیده‌تر شود، امن کردن آن سخت‌تر خواهد شد. مفهوم «بنیان اعتماد» تضمین می‌کند که بخش اعظم اعتماد بر بخش‌هایی از سیستم که کمترین پیچیدگی (و درنتیجه کمترین آسیب‌پذیرتری) را دارند، گذاشته می‌شود، و بخش‌های پیچیده‌تر به صورت لایه حول این مرکز شکل خواهد گرفت. این معماری امنیت در مقیاس‌های مختلف تکرار می‌شود، از بنیان اعتماد که معمولاً در سخت‌افزار یک سیستم واحد پیاده‌سازی می‌شود، تا لایه‌های بعدی که این بنیان اعتماد را ابتدا به سیستم‌عامل، و از آنجا به سرویس‌های سیستمی سطح-بالا، و سرانجام به تعداد زیادی سرویس‌دهنده (که به صورت حلقه‌های هم‌مرکز با اعتماد فروکاهنده سازماندهی شده‌اند) گسترش می‌دهند.

معماری امنیت بیت‌کوین متفاوت است. در بیت‌کوین، سیستم اجماع یک دفتر کل قابل‌اعتماد به وجود می‌آورد که کاملاً غیرمتمرکز است. یک بلاک‌چین معتبر از بلاک زاینده به عنوان بنیان اعتماد استفاده می‌کند و زنجیره‌ی اعتماد را تا بلاک فعلی می‌سازد. سیستم‌های بیت‌کوین می‌توانند و *باید* از این بلاک‌چین به عنوان بنیان اعتماد خود استفاده کنند. در طراحی‌های برنامه‌های کاربردی پیچیده‌ی بیت‌کوین که از تعداد زیادی سرویس روی سیستم‌های مختلف تشکیل شده‌اند، برای اطمینان از بجا بودن اعتماد باید دقت زیادی صرف بررسی این معماری امنیت شود. در نهایت، آن چیزی که باید به صراحت به آن اعتماد کنید، یک بلاک‌چین کاملاً معتبر و اعتبارسنجی‌شده است. اگر یک برنامه‌ی کاربردی بیت‌کوین اعتماد (صریح یا ضمنی) خود را روی چیزی غیر از این بلاک‌چین بنا کند، باید با شک و تردید به آن نگاه کرد، چون همین اعتماد بیجا عامل ایجاد آسیب‌پذیری سیستم خواهد بود. یک روش خوب برای ارزیابی معماری امنیت یک برنامه‌ی کاربردی بیت‌کوین در نظر گرفتن اجزای مختلف برنامه و ارزیابی سناریوهای فرضی است که در آنها این بخش از سیستم کاملاً آسیب دیده و تحت کنترل یک فرد خبیث (نفوذگر) است. اجزای مختلف برنامه باید یک به یک ارزیابی شده و تأثیر اختلال در آنها بر امنیت کل سیستم سنجیده شود. اگر با به خطر افتادن یک بخش از برنامه کل سیستم دیگر امن نیست، یعنی این بخش مبنای اعتماد بیجا قرار گرفته است. یک برنامه‌ی کاربردی بیت‌کوین که بخواهد مبری از این گونه آسیب‌پذیری‌ها باشد، باید بنیان اعتماد خود را فقط بر قویترین بخش از معماری امنیت بیت‌کوین قرار دهد. چنین برنامه‌ای فقط در برابر خطراتی آسیب‌پذیر است که کل سیستم بیت‌کوین را هدف قرار می‌دهند.

بررسی نمونه‌های متعدد هَک شدن صرافی‌های بیت‌کوین نشان می‌دهد که در طراحی این برنامه‌ها تا چه حد به اصول و معماری امنیت بیت‌کوین بی‌توجهی شده است، موارد پیش‌پاافتاده‌ای که حتی با یک بررسی ساده قابل مشاهده هستند. در اکثر موارد، این برنامه‌های متمرکز بنیان اعتماد خود را بر عامل متعدد خارج از بلاک‌چین بیت‌کوین، از قبیل کیف‌پول آنلاین، پایگاه داده‌ی دفتر کل متمرکز، روش‌های رمزگذاری پُرخطر و مانند اینها، قرار داده بوده‌اند.

بهترین شیوه‌های امنیت کاربر

هزاران سال است که انسان از کنترل‌های امنیت فیزیکی استفاده می‌کند. در مقایسه با آن، امنیت دیجیتال فقط ۵۰ سال قدمت دارد. سیستم‌عامل‌های همه-منظوره‌ی امروزی چندان اَمن نبوده و به خصوص برای ذخیره کردن پول دیجیتال مناسب نیستند. کامپیوترهای ما تقریباً همیشه به اینترنت متصل بوده و پیوسته در معرض تهدیدات خارجی قرار دارند. هزاران قطعه‌ی نرم‌افزاری از صدها برنامه‌نویس مختلف روی این سیستم‌ها در حال اجرا هستند که در اغلب موارد دسترسی کامل و بدون محدودیت به فایل‌های کاربر دارند. اگر از میان این هزاران برنامه فقط یکی از آنها نفوذی باشد، می‌تواند امنیت فایل‌ها و صفحه کلید شما را به خطر انداخته و بیت‌کوین‌های ذخیره‌شده در برنامه‌های کیف‌پول را به سرقت ببرد. فقط بخش بسیار کوچکی از کاربران از مهارت و تخصص کافی برای دور نگه داشتن یک کامپیوتر از هر گونه ویروس و اسب تروا [برنامه‌های به ظاهر بی‌خطر و حتی مفیدی که مترصد سرقت اطلاعات کاربر هستند] برخوردار هستند.

با وجود چندین دهه پژوهش و پیشرفت در زمینه‌ی امنیت اطلاعات، دارایی‌های دیجیتال به گونه‌ای تأسف‌بار در معرض خطر نفوذگران مصمم قرار دارند. حتی حفاظت‌شده‌ترین و کنترل‌شده‌ترین سیستم‌ها (در شرکت‌های خدمات مالی، سازمان‌های جاسوسی، و پیمانکاران نظامی)، اغلب مورد حمله قرار گرفته و به آنها نفوذ می‌شود. بیت‌کوین یک دارایی دیجیتال با ارزش ذاتی است که می‌توان آن را سرقت کرد؛ وقتی مالکیت یک سکه‌ی بیت‌کوین عوض شود، دیگر قابل‌برگشت نیست. این ویژگی انگیزه‌ی زیادی برای سرقت بیت‌کوین به نفوذگران می‌دهد. تا به امروز، نفوذگران بعد از سرقت مجبور به تغییر اطلاعات هویتی یا اطلاعات حساب (مانند شماره‌ی حساب بانکی و کارت اعتباری) هستند، ولی با وجود دشوار بودن جعل اطلاعات مالی و پول‌شویی، میزان این قبیل سرقت‌ها همواره رو به افزایش بوده است. بیت‌کوین این معضل را وخیم‌تر کرده است، چون حتی نیازی به جعل اطلاعات یا پول‌شویی ندارد؛ ارزش بیت‌کوین در خود دارایی دیجیتال نهفته است.

خوشبختانه، همین ویژگی باعث شده تا انگیزه‌ها برای بهبود امنیت سیستم‌های کامپیوتری نیز افزایش یابد. اگر در گذشته خطر هَک شدن کامپیوتر مبهم و غیر مستقیم بود، اکنون این خطر واضح و آشکار شده است. وقتی بیت‌کوین‌های خود را روی یک کامپیوتر نگه می‌دارید، باید به فکر ارتقای امنیت آن نیز باشید. به عنوان یکی از پیامدهای مستقیم گسترش محبوبیت و کاربرد بیت‌کوین و دیگر ارزهای دیجیتال، تکنیک‌های نفوذ و روش‌های مقابله با آنها هر دو به سطحی بی سابقه ارتقا یافته‌اند. به بیان ساده، نفوذگران اکنون هدفی چرب و شیرین پیش رو می‌بینند و کاربران انگیزه‌ای آشکار برای حفاظت از دارایی خود دارند.

در چند سال گذشته، در نتیجه‌ی پذیرش جهانی بیت‌کوین، شاهد ابتکارات شگرفی در حوزه‌ی امنیت اطلاعات، از رمزگذاری سخت‌افزاری گرفته تا کیف‌پول‌های سخت‌افزاری، فناوری چندامضایی، و ضمانت‌نامه‌های دیجیتال بوده‌ایم. در چند قسمت آینده تعدادی از بهترین شیوه‌های عملی برای تأمین امنیت کاربران را بررسی خواهیم کرد.

ذخیره‌سازی فیزیکی بیت‌کوین

از آنجا که اکثر کاربران با امنیت فیزیکی بسیار راحت‌تر از امنیت اطلاعات هستند، یکی از مؤثرترین روش‌های حفاظت از سکه‌های بیت‌کوین تبدیل آنها به اشیاء فیزیکی است. کلیدهای بیت‌کوین چیزی جز اعداد بسیار طولانی نیستند، یعنی می‌توان آنها را با رمزگذاری BIP-38 روی کاغذ چاپ کرده یا روی سکه‌های فلزی ضرب کرد. در این حالت حفاظت از بیت‌کوین مانند حفاظت از چند ورق کاغذ یا مقداری سکه‌ی معمولی خواهد بود. وقتی بیت‌کوین را روی کاغذ چاپ می‌کنید، چیزی خواهید داشت که به آن کیف‌پول کاغذی (paper wallet) می‌گویند؛ ابزارها و سایت‌هایی زیادی هستند که این کار را مجانی برای شما انجام می‌دهند. خوبی کیف‌پول کاغذی این است که می‌توانید از آن چندین کپی بگیرید و آنها را در محل‌های مختلف نگه دارید. اغلب افراد بخش اعظم سکه‌های بیت‌کوین خود را به همین روش نگهداری می‌کنند.

یک روش بسیار خوب دیگر برای حفاظت از بیت‌کوین نگهداری آن به صورت آفلاین (دستگاه یا وسیله‌ای که به اینترنت متصل نیست) است که به آن انباره‌ی سرد (cold storage) نیز گفته می‌شود. دیسک‌های CD و DVD، یا حافظه‌های USB فلَش از بهترین و پُرکاربردترین انباره‌های سرد محسوب می‌شوند.

کیف‌پول سخت‌افزاری

در بلندمدت، امنیت بیت‌کوین هر روز بیش از قبل به کیف‌پول‌های سخت‌افزاری غیرقابل‌نفوذ سپرده خواهد شد. کیف‌پول سخت‌افزاری (hardware wallet)، بر خلاف تلفن هوشمند یا کامپیوتر شخصی، فقط یک هدف دارد: نگهداری اَمن بیت‌کوین. بدون نرم‌افزارهای گوناگونی که با رفتارهای غیرقابل‌کنترل خود امنیت بیت‌کوین را به خطر می‌اندازند، یک کیف‌پول سخت‌افزاری، مانند تریزور (Trezor)، امنیتی تقریباً خلل‌ناپذیر برای کاربران غیرحرفه‌ای به همراه می‌آورد. پیش‌بینی‌ها حکایت از آن دارند که کیف‌پول سخت‌افزاری به روش غالب ذخیره‌سازی و نگهداری بیت‌کوین تبدیل خواهد شد.

متعادل‌سازی خطر: ترس برادر مرگ است

هر چند اکثر کاربران به درستی نگران سرقت بیت‌کوین‌های خود هستند، اما خطر بزرگتری نیز وجود دارد: فایل‌های کامپیوتری همیشه می‌توانند خراب، حذف یا گم شوند. در تلاش برای اَمن کردن کیف‌پول بیت‌کوین نباید تا جایی پیش بروید که خودتان هم دیگر نتوانید به آن دسترسی داشته باشید. در ژوئیه ۲۰۱۱، یک پروژه‌ی تبلیغی و آموزشی بیت‌کوین چیزی حدود ۷۰۰۰ بیت‌کوین از دست داد. صاحبان این پروژه، در تلاش برای جلوگیری از سرقت سکه‌های بیت‌کوین، یک سری نسخه‌های پشتیبان رمزگذاری‌شده‌ی پیچیده از آنها گرفتند، اما در آخر پروژه کلیدهای رمزگشایی را گم کردند و امکان گشودن نسخه‌های رمزگذاری‌شده برای همیشه از دست رفت. درست مثل مخفی کردن گنج در بیابان، اگر سکه‌های بیت‌کوین خود را خیلی ماهرانه پنهان کنید، شاید خودتان هم دیگر نتوانید دوباره آنها را پیدا کنید!

توزیع خطر: همه‌ی تخم‌مرغ‌های خود را در یک سبد نگذارید

آیا همیشه تمام دارایی نقدی خود را توی جیبتان می‌گذارید و این طرف و آن طرف می‌برید؟ از نظر اکثر افراد، این یک بی‌احتیاطی محض محسوب می‌شود؛ با این حال، وقتی پای بیت‌کوین در میان است، اغلب کاربران تمام سکه‌های بیت‌کوین خود را در یک کیف‌پول واحد نگه می‌دارند. با پخش کردن و نگهداری سکه‌های بیت‌کوین در چند کیف‌پول مختلف، خطر از دست رفتن یکباره‌ی آنها را کاهش دهید. افراد محتاط معمولاً فقط مقداری کمی بیت‌کوین (موسوم به «پول توجیبی») در کیف‌پول موبایل حمل می‌کنند یا آن را به صورت آنلاین نگه می‌دارند، و بخش اعظم دارایی بیت‌کوین خود را در یک انباره‌ی سرد یا کیف‌پول کاغذی حفظ می‌کنند.

چندامضایی و مدیریت مخارج

شرکت‌هایی که به صورت روزمره با مقادیر زیاد بیت‌کوین سر و کار دارند، عاقلانه‌تر است از *آدرس بیت‌کوین چندامضایی* استفاده کنند. آدرس‌های چندامضایی امنیت بسیار بالاتری دارند، چون برای خرج کردن آنها به بیش از یک امضا نیاز است. این روش تضمین می‌کند که یک فرد واحد نتواند کل سرمایه‌ی شرکت را به خطر بیندازد. افراد مختلفی که حق امضای سندهای پرداخت بیت‌کوین را دارند (مانند مدیران اجرایی شرکت)، باید کلیدهای خود را به صورت مستقل و در مکان‌های مختلف نگهداری کنند. آدرس‌های چندامضایی برای کاربران منفرد نیز کاربرد دارند، جایی که فرد برای پرداخت یک تراکُنش مجبور است از چندین کلید که در مکان‌های مختلف نگهداری می‌شوند، استفاده کند.

بقا و پایستگی

یکی از جنبه‌های مهم امنیت که اغلب نادیده گرفته می‌شود، دسترس‌پذیری است، به خصوص در مواردی که مالک از نظر جسمی ناتوان می‌شود یا فوت می‌کند. به کاربران بیت‌کوین توصیه می‌شود برای محفوظ نگه داشتن کلیدهای خود از گذرواژه‌های طولانی و پیچیده استفاده کنند و آنها را در اختیار دیگران نگذارند. متأسفانه، این رویه باعث می‌شود تا در صورت فوت یا ناتوانی یا عدم حضور مالک اصلی برای باز کردن کیف‌پول، دسترسی به موجودی آن برای خانواده‌ی وی نیز تقریباً غیرممکن باشد. در حقیقت، در اکثر موارد، ممکن است افراد خانواده حتی از وجود این دارایی‌های بیت‌کوین نیز کاملاً بی‌خبر باشند.

اگر مقدار زیادی بیت‌کوین دارید، عاقلانه این است که جزئیات دسترسی به آن را با افراد معتمد یا وکیل خود در میان بگذارید. امروزه وکلایی نیز هستند که به عنوان «مجری دارایی دیجیتال» شناخته می‌شوند و می‌توانند با ارائه‌ی طرح‌های چندامضایی پیچیده، شما را از انتقال صحیح و قانونی بیت‌کوین به خانواده یا شرکا مطمئن کنند.

نتیجه‌گیری

بیت‌کوین یک فناوری کاملاً جدید، بی‌سابقه و پیچیده است. بدون تردید، در آینده ابزارها و شیوه‌های امنیتی بهتری برای کاربران غیرحرفه‌ای توسعه داده خواهند شد. ولی، در حال حاضر، کاربران بیت‌کوین می‌توانند با به کار بستن هر چه بیشتر توصیه‌هایی که در این فصل کردیم، تجربه‌ای امن و بدون دردسر با بیت‌کوین داشته باشند.