Deloitte.

گروه حصین

راه‌پرداخت

بلاکچین و امنیت سایبری

بیایید بحث کنیم

مقدمه

این روزها فناوری بلاکچین با قابلیت‌های فراوان خود در دنیا یکه‌تازی می‌کند. اما منتقدان آن، مقیاس‌پذیری، امنیت و پایداری این فناوری را زیر س,ال می‌برند. شرکت‌های عضو دیلویت (Deloitte) در سراسر جهان، در حال همکاری برای ایجاد و بهبود قابلیت‌های بلاکچینی و توسعه راه‌حل‌ها و خدمات مربوطه هستند.

در این مقاله، تشـــریح و ارزیابی‌های کارشناسان بلاکچینی و امنیت سایبری دیلویت از نقاط مختلف جهان در یک‌جا جمع شـــده‌اند. به‌طور خاص در این مقاله این دیدگاه‌های مشترک جهانی مورد بررسی قرار خواهند گرفت:

- سطح کنونی امنیت فناوری بلاکچین از دیدگاه سیستم و داده برای دفترکل‌های عمومی و خصوصی؛
- مدل امنیتی سه‌گانه CIA شامل ۱. محرمانگی، ۲. یکپارچگی و ۳. میزان در دســـترس بودن؛ برای بررســـی و ارزیابی سطح تکامل فناوری بلاکچین؛
- بررسی جوانب احراز هویت، صدور مجوز و حسابرسی (AAA)، ویژگی انکارناپذیری، جنبه‌های بنیادی امنیتی برای حفاظت از اطلاعات و طراحی/مدیریت سیستم‌های جدید و شبکه‌ها.

بلاکچین عمومی، همان بلاکچین‌های بدون مجوز هســـتند. در این نـــوع از بلاکچین‌هـــا، داده‌ها به‌صـــورت عمومی برای هرکسی که در شبکه حضور داشـــته باشد، در دسترس خواهد بود. بلاکچین‌های خصوصی یا مجوزمحور نیز معمولا توســـط گروهی از شرکت‌ها مورد استفاده قرار می‌گیرند. در این موارد نیز شـــرکت‌ها و بخش‌های خصوصی داخل یک ســـازمان که هویت افراد آنها مورد تایید قرار گرفته است، می‌توانند به داده‌ها دسترسی پیدا کنند.

مفهوم بلاکچین

انقلاب بلاکچین (یا همان فناوری دفترکل توزیع‌شده) با رشد سریع اینترنت مقایسه می‌شـــود. این فناوری از پتانسیل‌های بالایی برای اســـتفاده در صنایع مختلفی همچون بهداشت و درمان، بخش عمومی، صنایع تولیدی و مخصوصا خدمات مالی

برخوردار است؛ به‌اندازه‌ای که پیش‌بینی می‌شود این فناوری بتواند به‌طور کامل خدمات مالی و اقتصادی را متحول کرده و در نهایت یک صنعت جدید را از دل این اقتصاد سنتی بیرون آورد. به عقیده دیوید شاتسکی (David Schatsky) مدیرعامل دیلویت ایالات متحده آمریکا؛ «این فناوری روشی امن، شفاف، بسیار مقاوم در برابر اختلال، حسابرسی‌شده و کارآمد را برای ثبت معاملات یا هر تراکنش دیجیتالی دیگری ارائه می‌دهد.»
علاقه به فناوری بلاکچین باعث شده که ارائه‌کنندگان خدمات مالی و شرکت‌های فناوری در سراسر جهان، تنها در سال ۲۰۱۶ بیش از یک میلیارد دلار روی آن سرمایه‌گذاری کنند. پیش‌بینی می‌شود که این سرمایه‌گذاری تا پنج سال آینده نیز همچنان روبه‌رشد باشد. بر اساس گزارش‌های ارائه‌شده توسط گارتنر (Gartner) در سال ۲۰۱۶، فناوری بلاکچین در اوج چرخه هایپ (hype cycle) قرار گرفته است. در حال حاضر این فناوری برای رهبران صنایع، تبدیل به یک اولویت شده و همه آنها به‌دنبال این هستند که برای کسب مزیت رقابتی و باقی‌ماندن در بازار، تغییرات مدل‌های کسب‌وکار و زنجیره ارزش را مورد مطالعه قرار دهند. با این حال امروزه این فناوری با انتظارات بسیار بالایی مواجه شده و همین موضوع باعث شروع حرکت آن به سمت شیب سرخوردگی شده است.
میلان سالابا (Milan Sallaba)، رهبر بخش فناوری دیلویت آلمان به این موضوع اشاره می‌کند که «برخی از موارد استفاده‌ای که از ابتدای کار برای بلاکچین در نظر گرفته شدند،

بر ویژگی‌های اصلی آن تمرکز کافی را نداشتند. در اصل فناوری بلاکچین، پتانسیل این را دارد که اثربخشی صنایع مختلف را افزایش داده و به احتمال زیاد مدل‌های کسب‌وکار کاملا جدیدی را برای آنها به ارمغان آورد.»
صنعت بلاکچین، در حال حاضر، به سمتی فراتر از اثبات مفهومی و تولید پایلوت در حال حرکت است و کم‌کم همه افراد با مزایای آن آشنا می‌شوند. یکی از مهم‌ترین بخش‌هایی که باید در پیاده‌سازی بلاکچین مورد بررسی قرار بگیرد، بخش امنیتی و حریم خصوصی است. در صورتی که فناوری بلاکچین قصد جای‌گیری در صنایع اجتماعی و ایجاد تغییراتی در آنها را داشته باشد، تست و آزمایش جنبه حفاظتی و حریم خصوصی آن بسیار مهم و حیاتی خواهد بود.

مفهوم امنیت سایبری

وابستگی شدید به فناوری‌های مدرن و علی‌الخصوص اینترنت، باعث ایجاد مدل‌های کسب‌وکار و جریان‌های درآمد جدیدی برای سازمان‌ها شده است، اما همین موضوع نیمه دیگر تاریکی نیز دارد؛ چراکه این روند، فرصت بیشتری را برای مهاجمان سایبری ایجاد می‌کند. خرابکاران سایبری می‌توانند از این فرصت‌ها برای سوءاستفاده از مدل‌ها و جریان‌های جدید درآمدی استفاده کنند. با ظهور ویروس‌های جدید، حملات سایبری بسیار هدفمندتر و پیچیده‌تر شده‌اند و این موضوع به‌نوبه خود تهدید بزرگی برای سازمان‌ها به‌شمار می‌آید. مجرمان سایبری در تلاش‌اند تا داده‌های باارزشی از جمله مالکیت معنوی (IP)، اطلاعات قابل شناسایی شخصی (PII)، اطلاعات و پرونده‌های پزشکی و همچنین داده‌های مالی سازمان‌ها را سرقت کنند. این مهاجمان با استفاده از روش‌هایی چون دسترسی به داده‌ها و استفاده از تکنیک‌های باج‌گیری پیشرفته یا با ایجاد اختلال در عملکرد کلی یک کسب‌وکار از طریق حملات توزیع‌شده محروم‌سازی از سرویس (DDoS)، تجارت پرسودی را برای خود ایجاد می‌کنند.
در اکتبر ۲۰۱۶ یکی از بزرگ‌ترین ارائه‌دهنده‌های خدمات نام دامنه (DNS) دچار یک حمله بزرگ (DDoS) شد. این حمله باعث شد عملکرد وب‌سایت‌های نام‌آشنا و پرترافیکی از جمله توئیتر، نت‌فلیکس و اسپاتی‌فای با اختلال مواجه شود. متخصصان خطرات سایبری دیلویت پیشنهاد می‌کنند که سازمان‌ها در هنگام مواجهه با موارد سایبری، رویکردی امن، هوشیارانه و انعطاف‌پذیر را برای خود اتخاذ کنند.
حال سوال اینجاست که در مورد فناوری بلاکچین چطور؟ آیا این فناوری در برابر تهدیدات سایبری از امنیت کامل برخوردار خواهد بود؟ یا به یک هدف آسان و محبوب برای چنین حملاتی تبدیل خواهد شد؟ با توجه به گفته‌های اد پاورز (Ed Powers)، رهبر بخش خطرات سایبری دیلویت آمریکا؛ «با وجود جدید و نوظهور بودن فناوری بلاکچین، می‌توان به آن در جهت کمک به شرکت‌ها برای مقابله با چالش‌های سایبری خطرناکی، از جمله تایید هویت دیجیتال و یکپارچگی داده‌ها امیدوار بود.» فناوری بلاکچین، این پتانسیل را دارد که به شکل پلتفرمی امن، مورد استفاده قرار بگیرد. جلوگیری از فعالیت‌های فریبکارانه از طریق مکانیسم‌های اجماعی و تایید جمعی، شناسایی دستکاری داده‌ها از طریق ارائه سیستم شفاف، غیرقابل تغییر، قابل اطمینان، با انعطاف‌پذیری عملیاتی و با رمزنگاری داده‌ها (بدون وجود هیچ‌گونه نقطه ضعفی)، از مزایای این پلتفرم امن هستند.
با این حال سیلیان لئونوویچ، مدیر ارشد دیلویت ایرلند چنین می‌گوید: «فناوری بلاکچین یک سد غیرقابل نفوذ را برای تمامی حملات سایبری ارائه نمی‌کند. پس به نظرم به نفع شماست که در کنار استفاده از فناوری‌های مبتنی بر بلاکچین، از سیستم‌های امنیتی رایج و شبکه‌های کنترلی امنیتی نیز استفاده کنید.»

محرمانگی

طبق تعریف موسسه جهانی استانداردها و فناوری (NIST)، لغت محرمانگی به «دارایی‌هایی شامل اطلاعات حساس که نباید در اختیار افراد غیرمجاز، نهادها یا فرایندها قرار بگیرند»، اطلاق می‌شود.

این روزها اطمینان یافتن از اینکه تنها افراد ذی‌صلاح و شناخته‌شده به داده‌های صحیح و مناسب دسترسی داشته باشند، به یک چالش برای شرکت‌هایی تبدیل شده که از فناوری بلاکچین استفاده می‌کنند. محافظت از دسترسی به شبکه‌های بلاکچین به‌صورت اساسی در حفاظت از داده‌ها نهفته است (به‌خصوص این موضوع در بلاکچین‌های خصوصی بیشتر قابل لمس است). در صورتی که یک مهاجم بتواند به یک شبکه بلاکچین دسترسی پیدا کند، شانس او برای دسترسی به داده‌ها بسیار افزایش خواهد یافت. در نتیجه همانند دیگر فناوری‌ها، در اینجا نیز باید روند احراز هویت و کنترل مجوز دسترسی اجرا شود. هرچند این فناوری در ابتدا (با توجه به ماهیت خود) بدون وجود گزینه‌ای برای کنترل دسترسی‌های خاص ایجاد شده بود، ولی در برخی از موارد کاربردی بلاکچین باید به محرمانگی داده‌ها و چالش‌های کنترل دسترسی پرداخته شود. این امر با ایجاد بلوک‌های داده رمزنگاری‌شده‌ای که به قابلیت‌های AAA مجهز شده‌اند، امکان‌پذیر می‌شود. رمزنگاری کامل داده‌های بلاکچین این اطمینان را فراهم می‌کند که این داده‌ها به هیچ‌وجه در دسترس افراد غیرمجاز قرار نخواهند گرفت، حتی در صورتی که شخصی به‌صورت غیرمجاز موفق به ورود به این شبکه شود، باز هم نمی‌تواند به داده‌ها دسترسی پیدا کند. به‌ویژه هنگامی که داده‌ها از طریق شبکه‌های غیرقابل اطمینان در جریان باشند، رمزنگاری آنها بسیار حیاتی است.

دسترسی به شبکه

در بلاکچین‌های عمومی هیچ‌گونه ضرورتی برای کنترل دسترسی به شبکه‌ها وجود ندارد؛ چراکه پروتکل‌های این شبکه‌ها به هر کسی اجازه ورود به شبکه و دسترسی و مشارکت در آن را می‌دهند. در مقابل، بلاکچین‌های خصوصی نیازمند کنترل‌های امنیتی مناسب برای حفاظت از دسترسی به شبکه هستند. یک فرض آرمانی این است که شبکه‌های محلی و سیستم‌ها، به‌دلیل ماهیت خصوصی که دارند، در پس لایه‌های امنیتی همچون فایروال‌ها، شبکه‌های خصوصی مجازی، VLANها، سیستم‌های تشخیص نفوذ و پیشگیری و از طریق یک استراتژی که به دفاع در عمق مشهور است، محافظت می‌شوند. با این حال سناریوهای مربوط به امنیت در دنیای آرمانی، بسیار رویایی هستند و در دنیای واقعی، تکیه بر این روش‌های کنترلی امنیتی، اثربخشی لازم را نخواهد داشت.

در بهترین عملیات امنیتی، کنترل‌های امنیتی (مانند کنترل‌های دسترسی) در سطح کاربردی اجرا می‌شوند. این لایه اولین و مهم‌ترین خط دفاعی است. به‌ویژه در سناریوهایی که در آنها یک مهاجم به یک شبکه محلی دسترسی داشته یا در جاهایی که یک عامل مخرب حضور دارد، این موضوع بسیار صادق است. همچنین سازمان‌ها با توجه به معماری شبکه بلاکچین خود باید راه‌حل‌هایی را برای گره‌های غیرفعال و کم‌فعالیت خود در نظر بگیرند؛ چراکه در صورت وجود چنین گره‌هایی، شبکه بلاکچین نه‌تنها باید قابلیت فعالیت در غیاب آنها را داشته باشد، بلکه باید توانایی بازگرداندن آنها و انجام سریع عملکرد اصلی خود را نیز کسب کند.

در این رابطه اندرس گیل (Andres Gil)، رهبر بخش امنیت سایبری LATCO دیلویت چنین می‌گوید: «هر سازمان باید به ارتباط ذاتی بین عملکرد، نوآوری و خطرات سایبری توجه کند. همچنین سازمان‌ها باید به این نکته توجه کنند که حفاظت کامل از همه‌چیز از لحاظ اقتصادی غیرعملی است و به احتمال زیاد مانع از اجرای برخی از مهم‌ترین برنامه‌های استراتژیک آنها می‌شود.»

سازمان‌ها باید پروفایل خطر تغییرات خود را شناسایی کرده و تعیین کنند که چه سطحی از خطرات سایبری برایشان قابل قبول است. این امر باید با توجه به اولویت‌های هر سازمان و میزان سرمایه‌گذاری آنها روی حفاظت از مهم‌ترین دارایی‌هایشان انجام گیرد. سازمان‌ها و دست‌اندرکاران شبکه بلاکچین، باید بدانند که ممکن است کارمندان داخلی، تامین‌کنندگان و شرکای مورد اعتماد، باعث ایجاد خطا شوند یا اقداماتی را انجام دهند که زمینه برای انجام خرابکاری، فراهم شود؛ بنابراین، توجه به نقاط ضعف فرایندهای کاربربه‌کاربر (end-to-end) بسیار ضروری به نظر می‌رسد.

حل‌وفصل چنین چالش‌هایی، مستلزم این است که سازمان‌های مربوطه، یک برنامه امنیتی سایبری جامع و کلی را اجرا کنند. این برنامه جامع باید شامل چارچوب مدیریتی و حاکمیتی با مشخص کردن نقش‌ها، فرایندها، معیارهای پاسخگویی، معیارهای عملکرد خوب و مطلوب و مهم‌تر از همه، یک تغییر سازمانی در ذهنیت افراد باشد.

کنترل‌های پیشرفته امنیتی، به کمک بلاکچین قابل انجام هستند. برای مثال استفاده از زیرساخت کلید عمومی (PKI) موجود در شبکه بلاکچین، امکان احراز هویت شخصی و گروهی و رمزنگاری ارتباطات را فراهم می‌کند. (PKI شامل مجموعه‌ای از نقش‌ها، سیاست‌ها و رویه‌های مورد نیاز برای ایجاد، مدیریت، استفاده، ذخیره‌سازی و لغو گواهی دیجیتالی و مدیریت رمزنگاری کلید عمومی است.)

شبکه‌های عمومی بلاکچین این پتانسیل را دارند که با اینترنت مقایسه شوند؛ چراکه در چنین شبکه‌هایی سازمان‌ها قادرند تا اطلاعات خود را با هر شخصی که به سرویس و ارائه‌دهنده خدمات دسترسی دارد، به اشتراک گذاشته و از طریق آنها بازیابی کنند.

در مقابل شبکه‌های خصوصی بلاکچین را می‌توان با صفحات اینترنت مقایسه کرد؛ زیرا اطلاعاتی که در این شبکه‌ها به اشتراک گذاشته می‌شوند، تنها در دسترس کسانی قرار خواهد گرفت که با تایید و احراز هویت خود قادر به ورود به وب‌سایت باشند. چنانچه فناوری بلاکچین به‌صورت گسترده مورد پذیرش و استفاده قرار گرفته شود، شرکت‌ها باید از مواردی همچون کنترل‌های امنیتی، روش‌های احراز هویت، رمزنگاری و همچنین امنیت کامل در مسیر دسترسی به داده‌ها اطمینان کامل حاصل کنند. اوا یی انگار کووک (Eva Yee Ngar Kwok)، مشاور بخش خطرات مربوط به فناوری دیلویت چین در این‌باره چنین می‌گوید:

«مهاجمان همواره از سایتی به سایت دیگر به‌دنبال اهداف آسان‌تر می‌گردند. در نتیجه اگر کنترل‌ها و اقدامات امنیتی سازمان‌ها ناکافی باشد، اطلاعات محرمانه ذخیره‌شده در شبکه‌های بلاکچین، به یک اولویت بالا و طعمه عالی برای این افراد تبدیل خواهند شد.»

دسترسی به داده‌ها و افشای اطلاعات

امروزه چنانچه یک مهاجم به داده‌ها و شبکه بلاکچین دسترسی داشته باشد، لزوما به این معنا نیست که بتواند اطلاعات را خوانده یا بازیابی کند. آخرین استانداردهای حوزه رمزنگاری این امکان را فراهم کرده‌اند که بلاک‌های داده به‌صورت کامل رمزنگاری شده و از محرمانگی آنها اطمینان حاصل شود. رمزنگاری‌های کاربربه‌کاربر که در سال‌های اخیر به یک موضوع مهم و قابل بحث تبدیل شده‌اند، این امکان را فراهم می‌کنند که اطلاعات تنها برای کسانی قابل خواندن و استفاده باشند که به‌وسیله کلید خصوصی خود داده‌های دریافتی را رمزگشایی می‌کنند.

استفاده از کلیدهای رمزنگاری در کنار PKI می‌تواند سطح بالاتری از امنیت را برای سازمان‌ها به ارمغان آورد.

رمزنگاری داده در بلاکچین یک سطح بالای حفاظتی را برای محرمانگی اطلاعات سازمان‌ها ایجاد می‌کند و یک ابزار برای کنترل دسترسی به داده‌ها است. به‌عنوان مثال، اجرای پروتکل‌های ارتباط امن در بلاکچین (با در نظر گرفتن آخرین استانداردهای امنیتی و راهنمای پیاده‌سازی آنها) باعث ایجاد تضمینی در برابر حملاتی چون حمله مرد میانی می‌شود.

با اجرای چنین پروتکل‌هایی، در صورتی که یک مهاجم قصد حمله خرابکارانه را داشته باشد، باز هم قادر نخواهد بود تا هویت مخاطبان را جعل کرده یا اطلاعاتی که در حال تراکنش و انتقال هستند را فاش کند. حتی با فرض یک سناریوی بحرانی که در آن کلیدهای خصوصی بلندمدت نیز در معرض خطر قرار گرفته‌اند، به‌واسطه خاصیت انعطاف‌پذیری پروتکل‌های امنیتی، نشست (یا همان session)های قبلی به‌صورت محرمانه باقی خواهند ماند.

درست است که کاربران بلاکچین یک نسخه پشتیبان از کلید خصوصی خود را در فضاهایی مانند فضای ذخیره‌سازی سرد (cold storage) نگهداری می‌کنند؛ اما همچنان سرقت کلیدهای خصوصی یک خطر و تهدید بزرگ است. باید به این نکته توجه داشت که کلیدها برای اهداف مختلفی در اکوسیستم بلاکچین مورد استفاده قرار می‌گیرند.

حفاظت از اطلاعات کاربر، حفظ محرمانگی داده‌ها، احراز هویت شخصی و احراز هویت جهت دسترسی و ورود به شبکه تنها چند مورد از مهم‌ترین کاربردهای کلیدهای خصوصی هستند. لیور کلو (Lior Kalev)، مدیر ارشد بخش خدمات خطرات امنیتی دیلویت اسرائیل در این‌باره می‌گوید: «مردم دوست دارند و می‌خواهند تا از طریق هر دستگاه و در هر زمان و مکانی به داده‌های خود دسترسی داشته باشند. این موضوع باعث ایجاد خطرات سایبری جدیدی می‌شود که به‌طور ذاتی مدیریت دسترسی به شبکه‌ها در شرکت‌ها و سازمان‌های جهانی را با چالش روبه‌رو می‌کند.»

سازمان‌ها باید از این موضوع اطلاع داشته باشند که دسترسی به حساب بلاکچین از طریق چندین دستگاه مختلف، آنها را با خطرات بزرگی در رابطه با از دست دادن کلیدهای خصوصی مواجه می‌کند.

با توجه به این موضوع، مهم است که تمامی بخش‌های آنها از روش‌های مدیریت کلید مناسب (مانند دستورالعمل‌های مدیریت کلیدهای رمزنگاری‌شده IETF یا RFC 4107) استفاده کنند.

علاوه بر این سازمان‌ها به توسعه قوانینی داخلی در رابطه با ایمنی کلیدهای خود نیز نیاز دارند؛ زیرا این موضوع برای ایجاد یک شبکه امن بلاکچین بسیار ضروری است.

آرتور دسامپسائو (Artur D'Assumpção)، رئیس بخش خطرات و امنیت سایبری دیلویت پرتغال چنین می‌گوید: «در یک محیط سازمانی، حفظ ایمنی کلیدهای امنیتی برای دستیابی به محرمانگی یک موضوع بنیادی و اساسی است. استفاده از کلیدها برای هدف‌های خاص یک نمونه از حفاظت مناسب است که در آن از فناوری‌هایی نظیر ماژول‌های سخت‌افزاری برای حفاظت از امنیت و فراهم کردن یک محیط ایمن و محرمانه استفاده می‌شود.»

الگوریتم‌های رمزنگاری امروزی که برای تولید کلیدهای عمومی و خصوصی مورد استفاده قرار می‌گیرند، بر روش تجزیه اعداد صحیح تکیه دارند. در نتیجه شکستن این گونه کلیدها با کامپیوترهای امروزی بسیار دشوار است. جکی فاکس (Jacky Fox)، مدیر ارشد سایبری دیلویت ایرلند در این‌باره می‌گوید: «پیشرفت در زمینه محاسبات کوانتومی برای حوزه بلاکچین بسیار قابل توجه خواهد بود، چراکه روی امنیت و درجه اطمینان رمزنگاری تراکنش‌ها تاثیر می‌گذارد.

برای مثال بیت‌کوین از الگوریتم‌های رمزنگاری برای تولید یک جفت کلید عمومی و خصوصی استفاده کرده و در آدرس‌دهی کلید عمومی، عملیات هش و مجموع مقابله‌ای (checksum) را به کار می‌گیرد. افشای آدرس به‌خودی‌خود نمی‌تواند خطر بزرگی محسوب شود، ولی پیشرفت‌های حاصل در حوزه محاسبات کوانتومی، احتمال آشکار شدن کلید عمومی مورد نیاز برای تعامل را افزایش می‌دهد؛ افشای آدرس و کلید عمومی، می‌تواند در نهایت به کلید خصوصی منجر شود.

جکی فاکس در ادامه می‌گوید: «در حال حاضر، محاسبات کوانتومی در مقیاس‌های بزرگ و تجاری در دسترس نیستند، اما حرکت به سمت رمزنگاری‌های مقاوم در برابر محاسبات کوانتومی یک پیشگیری کاملا منطقی است. NIST در حال حاضر در حال توسعه استانداردهای رمزنگاری مقاوم در برابر محاسبات کوانتومی است. همچنین NSA به تامین کنندگان خود پیشنهاد کرده که طرح اجرای SHA-384 به جای SHA-256 را در برنامه‌های خود داشته باشند.»

یکپارچگی

یکپارچگی (Integrity) از جانب NIST به‌عنوان «حفاظت در برابر تخریب یا تحریف نابجای اطلاعات و اطمینان از صحت اطلاعات و عدم‌انکار آنها» تعریف شده است.

حفظ یکپارچگی داده‌ها و تضمین صحت آنها در تمام طول چرخه سیستم‌های اطلاعاتی بسیار مهم است. رمزنگاری داده‌ها، مقایسه هش (یا به اصطلاح هضم داده‌ها) و همچنین استفاده از امضای دیجیتالی نمونه‌هایی از روش‌هایی هستند که صاحبان سیستم‌ها را صرف‌نظر از مرحله‌ای که سیستم در آن قرار دارد (در حال جریان، در حال استراحت یا در حال ذخیره‌سازی)، از اعتبار داده‌هایشان مطمئن می‌کند.

فناوری بلاکچین که بر اساس ثبات و تغییرناپذیری بنا شده است، ابزار مناسبی را برای اطمینان یافتن از صحت و یکپارچگی داده‌ها ارائه می‌کند.

غیر قابل تغییر بودن

فناوری بلاکچین از این جهت که کاربران آن می‌توانند از صحت داده‌های مربوط به تراکنش‌ها اطمینان حاصل کنند، می‌تواند به‌عنوان یک فناوری امن در نظر گرفته شود.

به‌کارگیری ترکیبی از رمز هش و رمزنگاری پیوندی در کنار ساختار غیرمتمرکز بلاکچین، باعث شده تا افرادی که قصد مداخله در پایگاه داده‌های این تکنولوژی را دارند، با چالشی جدی مواجه شوند.

این موضوع باعث شده سازمان‌هایی که از فناوری بلاکچین استفاده می‌کنند، از صحت داده‌های خود اطمینان کافی داشته باشند. علاوه بر این پروتکل‌های مبتنی بر مدل اجماع این فناوری سطح امنیت بالاتری را برای داده‌های سازمان‌ها ارائه می‌دهد. به‌طور کلی برای ثبت و تغییر هر رکوردی، گرفتن تاییدیه ۵۱ درصد از کاربران حاضر در بلاکچین‌های عمومی و خصوصی مورد نیاز خواهد بود.

سازمان‌ها همچنین می‌توانند مکانیسم‌های بیشتری را برای کنترل سایبری و ممانعت از ایجاد شکاف در شبکه، اجرا کنند. نمونه‌هایی از این مکانیسم‌ها عبارتند از: کنترل و نظارت روی گره‌ها، بررسی قدرت پردازش گره‌ها و شناسایی تغییرات چشم‌گیر در تعداد تراکنش‌های آنها.

حق فراموش‌شدن

با توجه به اینکه داده‌ها تغییرناپذیر هستند، بررسی چگونگی انطباق با قوانین حفظ حریم خصوصی حائز اهمیت خواهد بود. چگونگی اجرای حق فراموش‌شدن در فناوری بلاکچین که تضمین می‌کند هیچ چیزی در آن پاک نخواهد شد، یک چالش جالب است و خوشبختانه راه‌حل‌های متعددی برای آن وجود دارد. یکی از این راه‌حل‌ها، رمزنگاری اطلاعات شخصی نوشته‌شده در سیستم است. راه‌حل گفته‌شده، این اطمینان را ایجاد می‌کند که با فراموش کردن کلیدها، جلوی دسترسی به اطلاعات حساس نیز گرفته خواهد شد. یک رویکرد دیگر، تولید اسناد غیرقابل تغییر از طریق نوشتن هش تراکنش‌هایی است که در خارج از سیستم ثبت شده‌اند. در این روش یکپارچگی و صداقت داده‌ها حفظ شده و در عین حال امکان پاک کردن تراکنش‌ها نیز فراهم می‌شود. در این صورت تنها امکان ردیابی اطلاعات فراموش‌شده در بلاکچین وجود خواهد داشت.

قابلیت ردیابی

هر تراکنشی که به یک بلاکچین عمومی یا خصوصی افزوده می‌شود، به‌صورت دیجیتالی امضا و تاریخ‌نگاری می‌شود. به این معنا که سازمان‌ها در هنگام نیاز می‌توانند برای ردیابی هر تراکنش به یک دوره زمانی خاص مراجعه کرده و طرفین مشارکت‌کننده در آن را شناسایی کنند (از طریق آدرس عمومی بلاکچین). این ویژگی به یکی از مهم‌ترین خاصیت‌های امنیت اطلاعات، یعنی عدم انکار مربوط می‌شود. ویژگی عدم انکار تضمین می‌کند که هیچ کسی قادر نخواهد بود تا تایید امضای خود را از روی یک فایل یا معامله‌ای که در آن شرکت داشته، کپی

کند. این ویژگی خارق‌العاده بلاکچین قابلیت اطمینان سیستم را (به‌واسطه تشخیص تلاش‌های تهاجمی و معاملات جعلی) بسیار افزایش می‌دهد؛ چراکه هر تراکنش به‌صورت رمزنگاری‌شده به یک کاربر خاص مرتبط است.

هر تراکنش جدیدی که به بلاکچین افزوده شود، به یک تغییر جهانی و سراسری در دفترکل منجر خواهد شد. این بدان معناست که با هر تکرار جدید، وضعیت قبلی سیستم ذخیره‌سازی خواهد شد و در نتیجه تاریخچه logهای هر تراکنش به‌صورت مرحله‌به‌مرحله قابل پیگیری و ردیابی است. قابل بازرسی‌بودن فناوری بلاکچین برای تراکنش‌های سازمان‌ها، یک بستر شفاف و ایمن را فراهم می‌کند. از دیدگاه امنیت سایبری، قابلیت ردیابی این اطمینان را به وجود می‌آورد که داده‌ها معتبر بوده و هیچ‌گونه دستکاری در آنها صورت نگرفته است.

قراردادهای هوشمند

امروزه قراردادهای هوشمند، برنامه‌های کامپیوتری که روی دفاتر کل در حال اجرا هستند، به یکی از ویژگی‌های اصلی بلاکچین تبدیل شده‌اند. این نوع برنامه‌ها را می‌توان به منظور تسهیل، تایید و اجرای قوانین بین طرفین به کار برد. قراردادهای هوشمند این توانایی را دارند که فرایند پردازش مستقیم را انجام دهند و با دیگر قراردادهای هوشمند در تعامل باشند.

چنین نرم‌افزارهایی فرصت بسیار بزرگی را برای حمله فراهم می‌کنند. انجام یک حمله خرابکارانه، می‌تواند تاثیر دومینوگونه‌ای را روی دیگر قسمت‌های پلتفرم داشته باشد. طی رویداد DevCon 2 که در شهر شانگهای برگزار شد، یک حمله DDoS با هدف قراردادن قراردادهای هوشمند مشتریان اتریوم مبتنی بر Go، در روند استخراج بلاک‌های بیشتر توسط ماینرها اختلال ایجاد کرده و مانع کار آنها شد.

بلاکچین یک پارادایم جدید برای توسعه نرم‌افزار به ارمغان می‌آورد. از همین رو استانداردهای توسعه ایمن (مانند اجرای کدگذاری ایمن و تست‌های امنیتی) باید در چرخه عمر قراردادهای هوشمند (که شامل مراحل ایجاد، آزمایش، استقرار و مدیریت است) اجرا (و به‌روزرسانی) شوند. دیه‌گو رودریگز رولان (Diego Rodriguez Roldan)، مدیر بخش مشاور دیلویت اسپانیا در این‌باره می‌گوید: «برای کاهش و به حداقل رساندن تهدیدات و مشکلات فنی بحرانی در طول قراردادهای هوشمند، باید روش‌هایی مانند چرخه عمر توسعه نرم‌افزارهای ایمن (یا همان S-SDLC) مورد اجرا قرار گیرد.»

حمله به DAO که یک سازمان غیرمتمرکز و بناشده بر اساس اتریوم است، نمونه‌ای دیگر از حملات انجام‌شده بر قراردادهای هوشمند است. مهاجم این حمله با سوءاستفاده از یک مشکل فنی موجود در یک قرارداد هوشمند، موفق به سرقت ۶۰ میلیون اتر شد.

کیفیت داده‌ها

فناوری بلاکچین کیفیت داده‌ها را تضمین نکرده و بهبود نمی‌بخشد. بلاکچین‌های عمومی و خصوصی تنها می‌توانند مسئولیت دقت و کیفیت داده‌هایی را به عهده بگیرند که قبلا در آنها قرار داده شده است. این بدان معناست که در تکنولوژی بلاکچین نیز همانند تکنولوژی‌های دیگر، باید به کیفیت داده‌های منتج از سیستم‌های مرجع سازمانی، اعتماد کرد.

پرکاش سانسانا (Prakash Santhana)، مشاور مدیریت در دیلویت آمریکا چنین می‌گوید: «اوراکل‌های مورد اعتماد خارج از بلاکچین، بزرگ‌ترین منبع آسیب‌پذیری چارچوب بلاکچین هستند. یک اوراکل معیوب به‌طور بالقوه می‌تواند تاثیری زنجیره‌ای و دومینویی بر کل شبکه داشته باشد. عوامل شخص ثالث متصل به اوراکل، این توانایی را دارند که به‌صورت مستقیم یا غیرمستقیم، یک حمله امنیتی را انجام دهند.»

اوراکل‌ها باعث می‌شوند تا داده‌های غیرقابل اعتماد وارد یک محیط قابل اعتماد شوند. از همین رو ممکن است سازمان‌ها برای افزایش اعتماد به درستی داده‌هایی که از طریق اوراکل‌ها وارد بلاکچین شده‌اند، نیاز به استفاده از چندین اوراکل داشته باشند.»

فراهم ساختن بستری برای وارد کردن دقیق داده‌ها باعث می‌شود که قابلیت‌های آنی و لحظه‌ای فناوری بلاکچین تقویت شود. در نتیجه این امر، سازمان‌ها قادر خواهند بود تا تاییدیه داده‌های تراکنش‌های خود را سریع‌تر از هر سیستم دیگری کنترل کرده و اقدامات پیشگیرانه بیشتری را انجام دهند. از آنجایی که این داده‌ها از سیستم‌های مرجع سازمانی به بلاکچین منتقل می‌شوند، نهادها و افراد، باید از ایمن‌بودن کانال‌های تبادلی اطمینان حاصل کنند؛ چراکه بدون شک این کانال‌های یکی از اصلی‌ترین اهداف برای حمله مهاجمان به‌شمار می‌آیند.

دسترس‌پذیری

NIST دسترس‌پذیری را به‌صورت «تضمین دسترسی به‌موقع و قابل اعتماد به اطلاعات و استفاده از آنها» تعریف می‌کند.

آمار آن دسته از حملات سایبری که فاکتور دسترس‌پذیری خدمات را هدف قرار داده‌اند، رو به افزایش است. DdoSها یکی از رایج‌ترین نوع حملات هستند که می‌توانند بیشترین اختلال را در خدمات اینترنتی و روش‌های بلاکچین‌محور ایجاد کنند. این گونه حملات می‌توانند باعث مختل‌شدن عملکرد وب‌سایت‌ها و اپلیکیشن‌های تلفن‌های همراه شوند که هر یک از این موارد می‌تواند هزینه‌های بسیاری را برای یک کسب‌وکار ایجاد کند.

با توجه به پلتفرم توزیع‌شده بلاکچین، حملات DDoS که روی آن انجام می‌گیرند، متفاوت‌تر از دیگر حملات رایج هستند. در این نوع حملات بلاکچینی تلاش می‌شود تا بر شبکه‌هایی که حجم بالایی از تراکنش‌ها را در خود جای داده، نفوذ شده و دستکاری‌هایی صورت گیرد.

ویژگی غیرمتمرکز و همتابه‌همتا بودن این فناوری باعث شده تا نسبت به معماری‌های توزیع‌شده معمولی (برای مثال client-serverها)، استقامت بیشتری داشته باشند. با این حال این فناوری نیز می‌تواند مورد هدف حملات DDoS قرار گیرد و از همین رو انجام اقدامات حفاظتی کامل و مناسب در هر دو سطح شبکه و کاربردی بلاکچین، امری لازم و ضروری است. در سال ۲۰۱۴ شبکه بیت‌کوین در برابر یک حمله DDoS به‌خوبی مقاومت کرد. مهاجمان از طریق این حمله سعی داشتند تا شبکه را با درخواست‌های کوچک سرریز کنند.

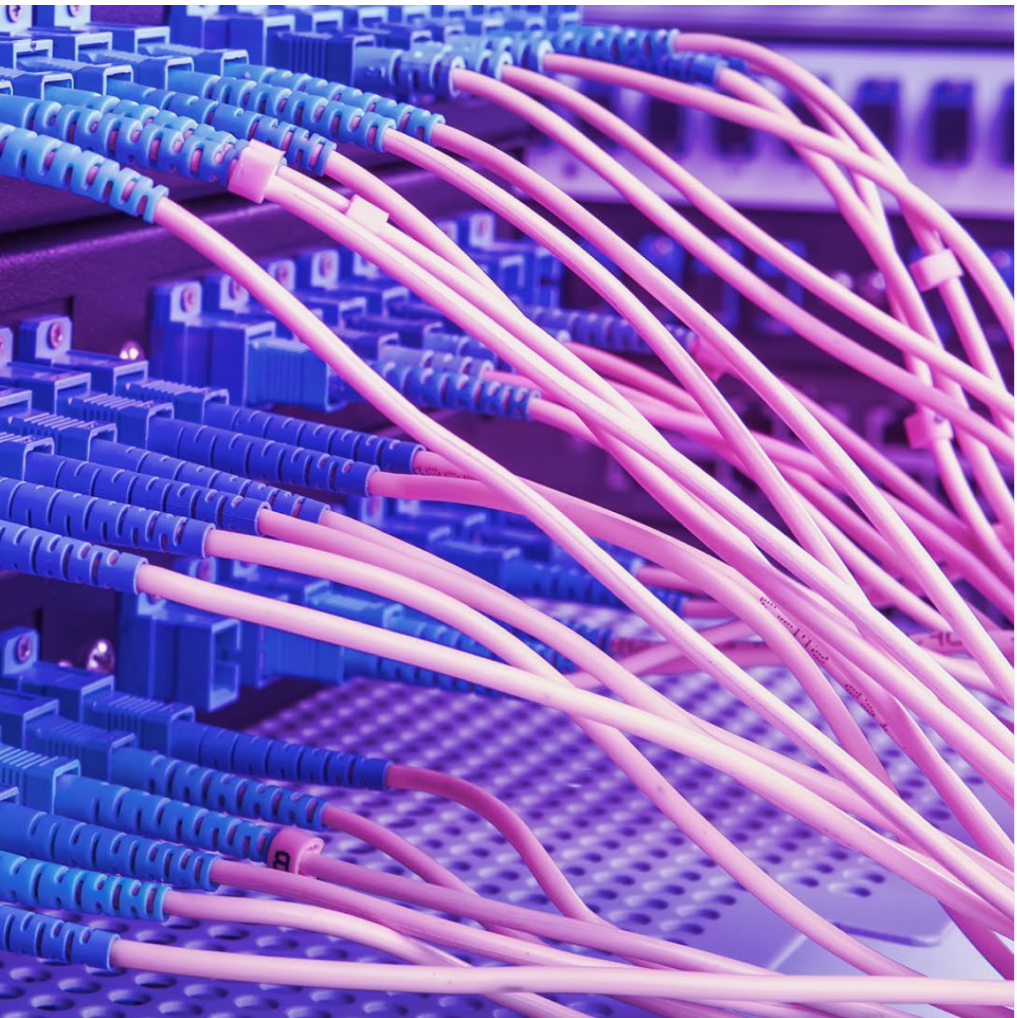
پیتر گوچ (Peter Gooch)، یکی از شرکای بخش مشاوره ریسک دیلویت بریتانیا، در این مورد می‌گوید: «احتمال تکرار مجدد این اتفاق وجود دارد. تخمین زده می‌شود که این بار حملات DDoS از لحاظ اندازه و مقیاس بسیار بزرگ‌تر بوده و همراه با حملات منظم Terabit / second برای تضعیف زیربنای اینترنت به‌صورت منطقه‌ای و حتی جهانی باشند.» یکی از دلایل افزایش حجم این نوع از حملات، رشد روزافزون نصب دستگاه‌های مرتبط با اینترنت اشیاست.

این دستگاه‌ها فرصت بیشتری برای دسترس‌پذیری آنلاین نرم‌افزارهای مخرب DDoS را فراهم کرده و حتی سرعت پهنای باند بالاتری را نیز برای آنها به ارمغان می‌آورند. انعطاف‌پذیری و غیرمتمرکز بودن فناوری بلاکچین تا حدودی وابسته به دسترس‌پذیری آن است. از همین رو حملات DDoS همچنان به‌عنوان یک تهدید مستمر باقی خواهند ماند.

بدون نقطه تکی شکست (No Single Point of Failure)

بلاکچین فاقد هرگونه تک‌نقطه خرابی است. این مساله به‌شدت احتمال شکست در برابر حملات DDoS مبتنی بر IP را کاهش می‌دهد. در این فناوری چنانچه یک گره برداشته شود، داده هنوز هم در داخل شبکه در دسترس خواهد بود؛ چراکه هر یک از گره‌ها همواره نسخه کاملی از دفترکل را به همراه دارد. ماهیت توزیع‌شده این فناوری حلالی برای مساله عمومی بیزانس در مورد اجماع نادرست است.

بیت‌کوین، در بازار به‌عنوان یک پلتفرم مستحکم و آزمون‌دیده شناخته می‌شود؛ چراکه برای بیش از هفت سال، در برابر حملات



سایبری، مقاومت کرده و پیروز شده است. زیرساخت بلاکچین، سطح دسترسی بیشتری به داده‌ها را فراهم می‌کند؛ چراکه داده‌ها از طریق هر یک از گره‌ها در شبکه در دسترس هستند و حتی در صورت وقوع حمله DDoS، تنها برخی از گره‌های شبکه مختل شده و داده‌های بقیه گره‌ها در دسترس خواهند بود. اما مساله به همین جا ختم نمی‌شود. حتی اگر یک شبکه بلاکچین فاقد هر گونه تک‌نقطه خرابی باشد، سازمان‌ها همچنان ممکن است با خطرات بیرونی و خارج از کنترل روبه‌رو شوند. برای مثال در صورت بروز یک قطعی جهانی در اینترنت، شبکه‌های عمومی و توزیع‌شده بلاکچین مانند بیت‌کوین و اتریوم نیز با اختلال مواجه خواهند شد. این مساله بدون شک عملکرد سازمان‌ها و هر فناوری دیگری را نیز مختل خواهد کرد. در شبکه‌های خصوصی بلاکچین که تعداد گره‌های کمتری وجود دارند، باید از این مساله اطمینان حاصل شود که شبکه به اندازه کافی در سطح جهانی توزیع‌شده و انعطاف‌پذیر بوده و فاقد تک‌نقطه خرابی در سطح یک سازمان یا کل پلتفرم است. در این صورت می‌توان از عملکرد صحیح پلتفرم در هنگام بروز اختلالات طبیعی و ناگهانی یا حملات هماهنگ‌شده اطمینان داشت.

انعطاف‌پذیری عملیاتی (Operational Resilience)

ترکیب ماهیت همتابه‌همتا و تعداد گره‌های موجود در شبکه که به شیوه توزیع‌شده در هر روز و ساعتی مشغول فعالیت هستند، باعث شده تا این پلتفرم از لحاظ عملیاتی انعطاف‌پذیر شود. با توجه به اینکه بلاکچین‌های عمومی و خصوصی از گره‌های متعددی تشکیل شده‌اند، در صورت بروز حمله، سازمان‌ها می‌توانند یکی از گره‌ها را در معرض حمله قرار داده و با سایر گره‌ها به‌طور عادی به کار خود ادامه دهند. بنابراین حتی در صورتی که بخش عمده‌ای از شبکه بلاکچین مورد حمله قرار بگیرد، ماهیت توزیع‌شده این فناوری باعث خواهد شد که بدون هیچ‌گونه اختلالی به کار خود ادامه دهد.

اما این مساله بدان معنا نیست که شبکه بلاکچین به‌صورت کامل ضدگلوله و بی‌هیچ عیب و نقصی است! از سال ۲۰۰۸ که بلاکچین به وجود آمد، این پلتفرم با تهدیدها و حملات بسیاری مواجه شده است. در این حملات مهاجمان تلاش کرده‌اند تا با استفاده از روش‌های مختلفی ثبات این پلتفرم را به خطر اندازند. در خلال این حملات برخی اشکالات فنی در پلتفرم بلاکچین کشف شد.

برای مثال یکی از این باگ‌ها در وضعیت در حال انتظار برای تایید رخ می‌داد. مهاجمان از طریق همین باگ در سال ۲۰۱۴ به شبکه بیت‌کوین حمله کردند که این مساله تاثیر شدیدی را بر تجربه کاربران آن گذاشت. در سال ۲۰۱۶ یک مهاجم با هدف قرار دادن قراردادهای هوشمند اتریوم و نحوه عملکرد آنها، باعث ایجاد یک سرریز در شبکه شد. این اتفاق اعتبارسنجی معاملات را به‌شدت تحت تاثیر قرار داده و باعث کاهش سرعت شبکه شد. در نتیجه این امر، یک هارد فورک (hardfork) ایجاد شد که به معنای انحراف دائمی از نسخه‌های پیشین بلاکچین است.

سوچیترا نایر (Suchitra Nair)، مدیر بخش مشاوره خطرات دیلویت بریتانیا چنین می‌گوید: «رگولاتورها، باید تمرکز ویژه‌ای بر انعطاف‌پذیری عملیاتی بلاکچین داشته باشند و شرکت‌ها باید به‌منظور کسب تضمین‌های رگولاتوری، این ویژگی بلاکچین را به‌صورت خیلی دقیق، مورد آزمایش و اثبات قرار دهند. مدیران ارشد باید قابلیت شناسایی و معرفی ریسک‌های کلیدی راهکارهای بلاکچین‌محور و چارچوب‌های قانونی و نظارتی حاکم بر آنها را داشته باشند.»

جنیفر چین (Jennifer Qin)، مدیر بخش سرمایه‌گذاری دیلویت در آسیا و اقیانوسیه، در ادامه مبحث اهمیت مشارکت تنظیم‌کنندگان برای تسهیل در توسعه و انطباق بلاکچین چنین می‌گوید: «برای ایجاد یک بلاکچین قابل اعتماد که به‌طور کامل از جانب کسب‌وکارها و دولت‌ها مورد پذیرش واقع شود، باید آن را کاملا مطابق با تنظیمات مقرراتی، آداب و محیط کسب‌وکارهای مختلف طراحی کرد.»

Deloitte.

راه پرداخت

این گزارش با حمایت شرکت حصین توسط تیم راه پرداخت، ترجمه و بازتولید شده است