کوین ایران

امنیت و حریم خصوصی در بلاکچین

فهرست مطالب

نویسنده: تورج اکبری

turaj.akbati68@yahoo.com

امنیت و حریم خصوصی در بلاک‌چین

بلاک‌چین رویکردهای نوآورانه‌ای را برای ذخیره‌سازی اطلاعات، اجرای تراکنش‌ها، عملکردها و ایجاد اعتماد در یک محیط باز پیشنهاد می‌کند. بسیاری افراد بلاک‌چین را با توجه به موارد استفاده متعدد آن از سیستم‌های رمز ارزی جهانی مانند بیت کوین تا قراردادهای هوشمند، شبکه‌های هوشمند ایجاد شده برای اینترنت اشیاء و موارد دیگر به عنوان یک پیشرفت شگرف فناوری در رمزنگاری و امنیت سایبری می‌دانند. با وجود اینکه بلاک‌چین در سال‌های اخیر توجه بخش‌های دانشگاهی و صنعتی را به خود جلب کرده و فعالیت‌های متعددی برای پیشرفت آن انجام شده است، امنیت و حریم خصوصی بلاک‌چین در زمان توسعه کاربردهای مختلف این فناوری در مرکز مباحث قرار می‌گیرد.

فناوری بلاک‌چین یک موفقیت جدید در محاسبات امن در شبکه‌های باز است که به هیچ مرجع مرکزی نیاز ندارد. بلاک‌چین از منظر مدیریت داده بیانگر یک پایگاه داده توزیع‌شده می‌باشد که لیست تغییرات تراکنش‌ها در یک زنجیره سلسله مراتبی از بلاک‌ها ذخیره می‌شود. از منظر امنیتی، زنجیره بلوک با استفاده از یک شبکه هم‌پوشان همتا به همتا ایجاد و نگهداری می‌شود و امنیت آن نیز از طریق به کارگیری هوشمندانه و غیرمتمرکز رمزنگاری و محاسبات جمعی تأمین می‌شود.

الزامات امنیت و حریم خصوصی در تراکنش‌های آنلاین

بررسی هرچه دقیق‌تر امنیت و حریم خصوصی در بلاک‌چین نیازمند آشنایی با ویژگی‌های امنیتی و حریم خصوصی تعریف شده در محیط‌های آنلاین است. از این‌رو، در گام نخست به بررسی الزامات امنیتی تراکنش‌های آنلاین پرداخته می‌شود. الزامات امنیت و حریم خصوصی تراکنش‌های آنلاین در هفت دسته قرار می‌گیرند [۱].

۱. سازگاری و ثبات دفتر کل در میان مؤسسات

فرآیند مصالحه، تسویه و فسخ مابین مؤسسات مالی به دلیل تفاوت معماری و فرآیندهای کسب‌وکار در این مؤسسات و به کارگیری فرآیندهای دستی نه تنها منجر به هزینه‌های بالای تراکنش‌های ایجاد شده از سمت مشتری و کسب‌وکارهای پس زمینه مؤسسات مالی می‌شود بلکه به ناسازگاری[۱] دفتر کل موجود در بین مؤسسات مالی منجر شده و احتمال خطا را به شدت بالا می‌برد.

۲. یکپارچگی تراکنش‌ها

سهام، اوراق قرضه، اسکناس، اسناد درآمدی، رسید انبار و سایر دارایی‌ها در زمان استفاده از تراکنش‌های آنلاین برای سرمایه‌گذاری و مدیریت دارایی توسط واسطه‌های مختلف مدیریت می‌شوند. این موضوع نه تنها هزینه تراکنش را افزایش می‌دهد بلکه خطر جعل عمدی یا جعل گواهی‌های کاربران را نیز به همراه دارد. بنابراین سیستم باید یکپارچگی تراکنش‌ها را تضمین نموده و از تغییر تراکنش‌ها جلوگیری نماید.

۳. دسترس‌پذیری سیستم و داده‌ها

کاربران سیستم‌های آنلاین باید بتوانند در هر لحظه و از هر جایی به داده‌های تراکنش‌های خود دسترسی داشته باشند. دسترس‌پذیری، هم سطح سیستم و هم سطح تراکنش‌ها را پوشش می‌دهد. در سطح سیستمی حتی در صورت حمله شبکه، سیستم باید با اطمینان قابل اجرا باشد. در سطح تراکنش، داده‌های تراکنش می‌توانند بدون تناقض و ناسازگاری در دسترس کاربران مجاز قرار گیرند.

۴. جلوگیری از خرج کردن دوباره

چگونگی جلوگیری از خرج کردن دوباره یکی از چالش‌های مهم در تجارت ارزهای دیجیتال در شبکه‌های غیرمتمرکز است. در محیط‌های متمرکز، یک نهاد ثالث مورد اعتماد مانند بانک مرکزی، مسئولیت تأیید تراکنش و جلوگیری از خرج کردن دوباره را برعهده دارد. برای تراکنش‌های انجام شده در محیط‌های غیرمتمرکز، باید از یک مکانیسم امنیتی قوی و اقدامات پیشگیرانه برای مقابله با خرج کردن دوباره استفاده شود.

۵. محرمانگی تراکنش‌ها

کاربران در اکثر تراکنش‌های مالی آنلاین تلاش می‌کنند تا حداقل اطلاعات تراکنش و حساب بانکی خود را در اختیار سیستم‌های مبادله آنلاین قرار دهند. حداقل بودن افشای اطلاعات شامل موارد زیر می‌باشد:

الف) اطلاعات تراکنش کاربران نباید توسط کاربران غیرمجاز قابل دسترسی باشد.

---

[۱] Inconsistency

ب) راهبر سیستم یا هرکدام از اعضای شبکه نمی‌توانند اطلاعات کاربر را بدون اجازه او در اختیار دیگران قرار دهند.

ج) تمام داده‌های کاربر حتی در زمان اتفاقات و شکست‌های غیرمنتظره یا حملات سایبری مخرب باید به صورت امن و سازگار، ذخیره‌سازی شده و قابل دسترسی باشند.

این سطح از محرمانگی درمورد بسیاری از سناریوهای مربوط به تراکنش‌های غیرمالی نیز صادق است.

۶. ناشناس بودن هویت کاربر

دشواری اشتراک مؤثر و امن داده‌های کاربر در میان مؤسسات مالی مختلف ممکن است به افزایش هزینه‌ها و تکرار احراز هویت کاربر منجر شود. اشتراک اطلاعات می‌تواند به صورت غیرمستقیم موجب افزایش ریسک افشای هویت کاربران توسط برخی از واسطه‌ها شود. علاوه بر این، در بعضی موارد یک یا هر دو طرف تراکنش شاید تمایلی نداشته باشند که طرف مقابل هویت واقعی آن‌ها را بشناسد.

۷. غیرقابل اتصال بودن تراکنش‌ها

کاربران علاوه بر ناشناسی انتظار دارند که ایجاد اتصال بین تراکنش‌های مختلف آن‌ها امکان‌پذیر نباشد؛ چراکه با اتصال تراکنش‌های یک کاربر می‌توان علاوه بر داده‌های هویتی او، به اطلاعاتی مانند موجودی حساب، نوع و تکرار تراکنش‌ها دست یافت. استفاده از چنین داده‌های آماری درمورد تراکنش‌ها و حساب‌های کاربری در کنار برخی از اطلاعات ضمنی پس زمینه درمورد کاربر می‌تواند با دقت بالایی به شناسایی هویت او منجر شود.

ویژگی‌های اصلی امنیتی بلاک‌چین

ویژگی‌های اصلی امنیتی بلاک‌چین، از پیشرفت‌های رمزنگاری و نیز از طراحی و اجرای بیت‌کوین نشأت می‌گیرد. از نظر تئوری، اولین زنجیره امن بلوکی که از رمزنگاری استفاده کرد در سال ۱۹۹۱ شکل گرفت و در سال ۱۹۹۳ با اضافه کردن ساختار درخت مرکل[۱] تغییرات قابل توجهی در آن ایجاد گردید. بلاک‌چین برای تضمین تعدادی از خصیصه‌های ذاتی امنیت مانند سازگاری، مقاومت در برابر تغییر، مقاومت در برابر حمله انکار سرویس توزیع شده[۲] (DDoS)، نام مستعار و مقاومت در برابر حمله خرج کردن دوباره ایجاد شده است. با این وجود، برای استفاده از بلاک‌چین برای تأمین امنیت فضاهای ذخیره‌سازی توزیع شده، به ویژگی‌های امنیتی و حافظ حریم خصوصی بیشتری نیاز است. در جدول زیر خلاصه‌ای از ویژگی‌های امنیتی و حریم خصوصی پایه و دیگر ویژگی‌های مورد نیاز آورده شده است [۲,۳].

---

[۱] Merkle

[۲] Distributed Denial-of-Service (DDoS)

۱- سازگاری

مفهوم سازگاری[۱] در زمینه بلاک‌چین به عنوان یک دفتر کل توزیع شده عمومی به ویژگی‌ای اشاره دارد که بر اساس آن تمامی گره‌های شبکه باید دفتر کل یکسانی در زمان یکسان داشته باشند. مفهوم سازگاری منجر به ایجاد موضوعات بحث برانگیزی شده است. برخی معتقدند که سیستم بیت کوین تنها سازگاری نهایی[۲] را فراهم می‌کند که سازگاری ضعیفی به شمار می‌رود. برخی دیگر معتقدند که شبکه بیت کوین سازگاری قوی[۳] را ارائه می‌نماید [۴].

سازگاری نهایی نوعی مدل سازگاری پیشنهاد شده برای سیستم‌های محاسباتی توزیع شده است که به دنبال ایجاد تعادلی مابین دسترس‌پذیری و سازگاری است. این مدل تضمین می‌کند که تمامی به‌روزرسانی‌ها به روش Lazy در بین تمامی نسخه‌های موجود پخش می‌شود. به عبارت دیگر، سازگاری نهایی تضمین می‌کند که داده ورودی به هر گره سیستم در نهایت در اختیار تمامی گره‌ها قرار می‌گیرد. این نوع سازگاری، به دسترس‌پذیری بالا و تأخیر کم در بازگردانی داده‌های موجود منجر خواهد شد. در این روش ممکن است مدت زمان مورد نیاز برای دستیابی گره‌ها

---

[۱] Consistency

[۲] Eventual Consistency

[۳] Strong Consistency

به داده‌های سازگار قابل تعریف نباشد. بنابراین به دلیل زمان‌بر بودن فرآیند انتشار داده‌های به‌روزرسانی شده ممکن است برخی از گره‌ها که به داده‌های جدید دسترسی نداشته‌اند داده‌های قدیمی را در پاسخ کاربران بازگردانند.

	الزامات امنیت و حریم خصوصی	ویژگی‌های امنیتی و حریم خصوصی	تکنیک‌های مورد استفاده برای تأمین امنیت و حریم خصوصی
پشتیبانی شده در بیت کوین	سازگاری	سازگاری	الگوریتم‌های اجماع
	یکپارچگی	مقاومت در برابر تغییر	مخازن متصل شده با زنجیره هش
	دسترس‌پذیری	مقاومت در برابر حمله انکار سرویس توزیع شده	الگوریتم‌های اجماع با روش‌هایی مانند تحمل خطای بیزانس
	جلوگیری از خرج کردن دوباره	مقاومت در برابر حمله خرج کردن دوباره	امضاء و تأیید [تراکنش]
	ناشناسی (گم‌نامی)	نام مستعار	کلید عمومی به عنوان مستعار
ویژگی‌های تکمیلی	غیرقابل اتصال بودن	غیرقابل اتصال بودن	ترکیب کردن[1]، امضاهای ناشناس
	محرمانگی	محرمانگی	ABE، HE، SMPC، NIZK، راه‌حل‌های مبتنی بر TEE، راه‌حل‌های مبتنی بر بازی
		مقاومت در برابر حمله ۵۱ درصد	الگوریتم‌های اجماع مستقل از قدرت محاسباتی

مدل سازگاری قوی در سیستم شبکه بلاک‌چین به این معنی است که گره‌های منتخب در زمان یکسان، دفتر کل یکسانی در اختیار دارند. هرگونه درخواست به‌روزرسانی در دفتر کل توزیع شده منوط به تأیید شبکه است. این مدل در تضاد با سازگاری نهایی قرار دارد؛ چراکه در سازگاری نهایی ممکن است به‌روزرسانی برخی گره‌ها با تأخیر انجام شود. سازگاری قوی با چالش هزینه کارایی روبه‌رو است و نمی‌تواند در تمامی موارد استفاده شود. چگونگی مدیریت به‌روزرسانی تمامی گره‌ها نیز چالش کلیدی سازگاری نهایی به شمار می‌رود.

بلاک‌چین شبکه بیت‌کوین به منظور دستیابی به Partition Tolerance (P) و سازگاری (C) با دسترسی معوق از مدل سازگاری بهتری برای ایجاد تعادل مابین مدل سازگاری قوی و مدل سازگاری نهایی استفاده کرده است. تراکنش‌های بیت‌کوین در بلوک‌ها تجمیع می‌شوند. زمانی که گره فرستنده، تراکنشی را به شبکه بلاک‌چین ارسال می‌کند ماینرها آن را به بلوکی با تراکنش‌های تأیید نشده اضافه می‌کنند و با چالش گواه اثبات کار آن را تأیید کرده و به شبکه اضافه می‌نمایند.

۲- مقاومت در برابر تغییر

مقاومت در برابر تغییر، مقاومت در برابر هرگونه تغییر عمدی در یک موجودیت توسط کاربر یا مخالفان با دسترسی به آن موجودیت است. یک موجودیت می‌تواند یک سیستم، یک محصول، یک شیء فیزیکی و یا منطقی باشد. مقاومت

[1] Minxing

در برابر تغییر بلاک‌چین به معنی عدم امکان تغییر اطلاعات تراکنشی قرار داده شده در بلوک در مدت زمان تولید آن یا پس از تولید بلوک است. در سیستم بیت‌کوین، بلوک‌های جدید از طریق ماینینگ تولید می‌شوند. در فرآیند ماینینگ ممکن است ماینرها یا مخالفین شبکه برای تغییر محتوای تراکنش تلاش کنند. این تلاش‌ها به دلیل استفاده از توابع هش، الگوریتم‌های امضای امن، روش‌های رمزنگاری و ارسال تراکنش به کل شبکه با شکست مواجه می‌شوند.

به طور خلاصه، از آنجایی که هر تراکنش بیت کوین، امضا شده و به واسطه بلاک‌چین در بین تمامی گره‌های شبکه توزیع می‌شود؛ دستکاری اطلاعات تراکنش بدون اینکه شبکه از آن آگاهی داشته باشد عملاً غیرممکن است. این موضوع نشان‌دهنده قدرت جمعی مورد استفاده برای ذخیره‌سازی و توزیع در بلاک‌چین است.

۳- مقاومت در برابر حمله انکار سرویس توزیع شده

حمله انکار سرویس، به نوعی از حمله سایبری به سرور اشاره دارد که از طریق ایجاد اختلال در دسترسی به منابع سرویس‌دهنده موجب بروز وقفه در ارائه خدمات می‌شود. این نوع حملات با ایجاد درخواست‌های زائد موجب ایجاد بار اضافی بر روی سیستم میزبان یا منابع شبکه می‌شوند و در ارائه خدمات مورد انتظار، اختلال ایجاد می‌کنند.

درخواست‌ها در حمله انکار سرویس توزیع شده[۱] (DDOS) از منابع متعددی ایجاد می‌شود که در سراسر اینترنت پخش شده‌اند. در این نوع حملات ممکن است از منابع موجود در شبکه برای حمله به سرویس‌دهنده مشخصی سوء استفاده شود. دفع این نوع حملات به دلیل استفاده‌ی حمله‌کنندگان از منابع متعدد، بسیار مشکل است [۵].

حمله انکار سرویس توزیع شده موجب ایجاد نگرانی در زمینه دسترس‌پذیری بلاک‌چین شده است؛ ولی ساختار کاملاً غیرمتمرکز، روش نگهداری توزیع شده بلاک‌چین و به کارگیری مکانیسم اجماع در تولید بلوک جدید، از بروز این نوع حملات در بلاک‌چین جلوگیری می‌کند و حتی درصورت عدم سرویس‌دهی برخی از گره‌ها، شبکه به کار خود ادامه خواهد داد. مهاجم برای موفقیت در شبکه بلاک‌چین باید بتواند قدرت محاسباتی قابل توجهی را جمع‌آوری نماید و تعداد زیادی از گره‌های شبکه را در اختیار بگیرد. افزایش هرچه بیشتر تعداد گره‌های شبکه بلاک‌چین احتمال موفقیت حمله انکار سرویس توزیع شده را کاهش خواهد داد.

۴- مقاومت در برابر حمله خرج کردن دوباره

حمله خرج کردن دوباره در مفهوم بلاک‌چین بیت‌کوین به مشکل خاصی اشاره دارد که مختص تراکنش‌های ارز دیجیتال است. ممکن است حمله خرج کردن دوباره با توجه به سادگی بازتولید اطلاعات دیجیتال، به عنوان یک نگرانی امنیتی عمومی در نظر گرفته شود. به طور مشخص، تراکنش‌هایی که توکن‌های دیجیتال را مبادله می‌کنند با مشکل بازتولید توکن دیجیتال از طرف فرستنده و ارسال چند باره آن مواجه هستند. اگر در فرآیند تراکنش توکن‌های بازتولیدشده ناسازگاری بین گره‌ها نیز رخ دهد مشکل خرج کردن دوباره به یک تهدید امنیتی جدی بدل خواهد شد.

[۱] Distributed Denial of Service (DDoS)

بیت کوین برای جلوگیری از خرج کردن دوباره، صحت هر تراکنش را با استفاده از سابقه موجود از تراکنش در بلاک‌چین، ارزیابی و تأیید می‌کند. بیت‌کوین با بهره‌گیری از پروتکل اجماع خود تضمین می‌کند که تمامی تراکنش‌های اضافه شده به بلاک‌چین معتبر بوده و ارسال‌کننده‌ی هر تراکنش قوانین مربوط به استفاده از شبکه را رعایت کرده است. علاوه بر این، تمامی تراکنش‌ها با استفاده از الگوریتم امضای دیجیتال امن توسط فرستنده امضاء می‌شوند. تأییدکننده با استفاده از امضای دیجیتال به راحتی می‌تواند جاعل را شناسایی نماید. ترکیب تراکنش امضا شده با امضای دیجیتال و تأیید عمومی تراکنش با اجماع اکثریت، تضمین می‌کند که بلاک‌چین بیت‌کوین می‌تواند در برابر حمله خرج کردن دوباره مقاومت نماید.

۵- مقاومت در برابر حمله اجماع اکثریت (۵۱ درصد)

این حمله به تقلب در پروتکل اجماع اکثریت اشاره دارد. حمله ۵۱ درصد یکی از مهم‌ترین انواع این حمله به ویژه در زمینه خرج کردن دوباره به شمار می‌رود. به عنوان مثال، حمله ۵۱ درصد می‌تواند در حضور ماینرهای مخرب اتفاق بیفتد. اگر ماینری بتواند بیش از ۵۰ درصد قدرت محاسباتی شبکه بلاک‌چین را در اختیار بگیرد کنترل کل تراکنش‌های شبکه را دراختیار خواهد داشت. اگر یک کاربر یا گروهی از کاربران هم‌دست، کنترل بلاک‌چین را در اختیار بگیرند مشکلات امنیتی و حریم خصوصی متعددی مانند انتقال رمز ارزها به آدرس‌های مشخص و معکوس کردن تراکنش‌ها برای شبکه ایجاد می‌شود.

۶- نام مستعار

نام مستعار[۱] به حالتی اشاره دارد که هویت واقعی فرد پنهان است. در شبکه بیت کوین، آدرس‌های موجود در شبکه بلاک‌چین نشان‌دهنده هش کلید عمومی یک کاربر (گره) در شبکه است. کاربران می‌توانند با استفاده از هش کلید عمومی خود به عنوان یک هویت مستعار با شبکه تعامل کنند بدون اینکه مجبور باشند هویت واقعی خود را آشکار نمایند. نام مستعار را می‌توان به عنوان ویژگی حریم خصوصی شبکه در نظر گرفت که برای محافظت از نام واقعی آن‌ها مورد استفاده قرار می‌گیرد. اگرچه نام مستعار با استفاده از کلیدهای عمومی می‌تواند به شکل ضعیفی از ناشناس بودن منجر شود همچنان ریسک‌های مربوط به افشای اطلاعات هویتی کاربران در شبکه‌های بلاک‌چین عمومی به قوت خود باقی‌ست.

[۱] Anonymous

ویژگی‌های تکمیلی مربوط به امنیت و حریم خصوصی در بلاک‌چین

اگرچه بلاک‌چین بیت‌کوین سه خاصیت امنیتی اصلی یعنی سازگاری، مقاومت در برابر تغییر و مقاومت در برابر حمله انکار سرویس توزیع شده را حفظ کرده است؛ ممکن است یک سیستم بلاک‌چین عمومی به دنبال بهره‌گیری از مزایای مربوط به ویژگی‌های امنیتی و حریم خصوصی تکمیلی باشد که برای سیستم ارزهای دیجیتال و سرویس‌های دفتر کل توزیع شده جهانی، حیاتی می‌باشند. در ادامه به دو مورد از این ویژگی‌ها اشاره شده است.

۱- غیرقابل اتصال بودن

غیرقابل اتصال بودن، به عدم توانایی در ایجاد ارتباط مابین دو مشاهده یا دو موجودیت سیستم با اطمینان بالا اشاره دارد. ناشناس بودن هم به حالت گمنام بودن و تعریف نشدن برمی‌گردد. با وجود اینکه بلاک‌چین بیت کوین از طریق ارائه هویت مستعار به عنوان پشتیبانی برای ناشناسی هویت کاربر می‌تواند نام مستعار را تضمین نماید؛ ولی نمی‌تواند غیرقابل اتصال بودن تراکنش‌های کاربر را فراهم کند. به طور شهودی، اگر کاربر همیشه از حالت ناشناسی برای تعامل با سیستم استفاده کند، می‌توان با تضمین نام مستعار و غیرقابل انکار بودن از ناشناس بودن کامل یک کاربر محافظت کرد. این، به علت آن است که غیرقابل اتصال بودن، احتمال وقوع حملات Deanonymization Inference را کاهش می‌دهد. این حملات از ایجاد ارتباط مابین تراکنش‌های کاربر برای دستیابی به هویت واقعی او استفاده می‌کنند. به طور مشخص، کاربر در سیستم‌هایی مانند بیت کوین می‌تواند چندین آدرس وابسته به نام مستعار داشته باشد. هرچند به دلیل ثبت آدرس‌های ارسال و دریافت و دسترسی آزاد به اطلاعات تراکنش‌ها ممکن است بتوان به هویت واقعی کاربر پی برد.

۲- محرمانگی تراکنش‌ها و حریم خصوصی داده

حریم خصوصی داده بلاک‌چین نشان می‌دهد که بلاک‌چین مورد نظر می‌تواند محرمانگی را برای تمامی داده‌ها یا داده‌های حساس ذخیره‌شده در آن فراهم نماید. اگرچه بلاک‌چین در اصل به عنوان دفتر کل توزیع شده عمومی برای رمز ارز بیت کوین توسعه داده شده است می‌توان کاربردهای بالقوه بسیار بیشتری برای آن برشمرد. محرمانگی اطلاعات تراکنش مانند محتوا و آدرس آن از ویژگی‌های امنیتی مورد انتظار برای تمامی کاربردهای بلاک‌چین است. ولی این ویژگی به دلیل نمایش عمومی آدرس‌ها و محتوای تراکنش در بلاک‌چین بیت‌کوین پشتیبانی نمی‌شود. رعایت حریم خصوصی در دسترسی به محتوای تراکنش، می‌تواند به کاهش ایجاد ارتباط مابین تراکنش‌ها و دستیابی به هویت واقعی کاربران کمک کند.

منابع

[۱] R. Zhang, R. Xue و L. Liu, “Security and Privacy on Blockchain ”,*ACM Comput* ,۱ جلد , ,۱ شماره p. 35, 2019 .

[۲] S. Haber و W. S. Stornetta, “How to time-stamp a digital document ”,*Journal of Cryptology* ,۲ شماره ,۳ جلد ,pp. 99--111, 1991 .

[۳] D. Bayer, S. Haber و W. S. Stornetta, “Improving the Efficiency and Reliability of Digital TimeStamping ”,pp. 329--334, 1993 .

[۴] R. Wattenhofer, “The Science of the Blockchain (1st ed.),” CreateSpace Independent Publishing Platform, 2016.

[۵] M. Mindi, “Understanding Denial-of-Service Attacks,” 2013.