مقالات آموزشی بنیاد سور

عنوان:

اعتماد و مسئله ژنرال های بیزانس؟

گردآورنده: بنیاد سور

نسخه: شماره دو

شبکه بلاکچین سور

www.surnet.org

مسئله ژنرال‌های بیزانس

در مقاله قبل، به‌صورت کاملاً مختصر و کوتاه اشاره‌ای به مسئله ژنرال‌های بیزانس و مسئله اعتماد شد و در این مقاله بر آنیم تا ضمن تشریح مسئله ژنرال‌های بیزانس، مفهوم اعتماد و تأثیر فناوری بلاک‌چین در بازآفرینی آن تشریح شود.

پیش از ورود به بحث اصلی، ابتدا نیاز است برخی موارد بیان شود.

- مسئله ژنرال‌های بیزانس، دشواری ایجاد اجماع و تفاهم در یک شبکه غیرمتمرکز را بیان می‌کند.
- ایجاد یک سامانه انتقال ارزش بدون نهاد واسط اعتمادساز، سال‌ها به دلیل حل نشدن مسئله ژنرال‌های بیزانس با مشکل روبرو بود.
- بیت‌کوین، راهکاری برای پاسخ به مسئله ژنرال‌های بیزانس است.
- بیت‌کوین با استفاده از سازوکار اثبات کار و فناوری بلاک‌چین، مسئله ژنرال‌های بیزانس را حل کرد.

چیستی مسئله ژنرال‌های بیزانس

مسئله ژنرال‌های بیزانس، یک مسئله مربوط به تئوری بازی‌ها است. چالش اصلی در این مسئله رسیدن بر سر یک اجماع بین چندین فرد و نهاد جدا از یکدیگر بدون وجود یک نهاد قابل‌اعتماد بین طرفین است. به‌عبارتی‌دیگر، مسئله آن است که چگونه می‌توان میان افرادی که هرکدام مستقلاً و بدون هماهنگی با دیگری تصمیم‌گیری می‌کنند و هیچ نهاد واسطی که همه به او اعتماد دارند وجود ندارد، می‌توان بر سر یک موضوع به اجماع نظر رسید. در این شبکه از افراد که هیچ‌یک نمی‌تواند هویت دیگری را بررسی و صحت‌سنجی کند، چگونه می‌توان بر سر یک موضوع و حقیقت مشخص به تفاهم رسید؟

داستان پس مسئله ژنرال‌های بیزانس این است که چندین ژنرال شهر بیزانتیوم را محاصره کرده‌اند. با اینکه آنها دورتادور شهر را در اختیار خود دارند اما برای سقوط شهر و تصرف آن، ژنرال‌ها بایستی با هماهنگی همدیگر و به‌صورت دسته‌جمعی به شهر حمله کنند. اگر همه ژنرال‌ها در یک‌زمان مشترک حمله کنند، پیروز خواهند شد، اما اگر هر ژنرال در زمان مدنظر خود حمله کند، جنگ را خواهند باخت. این ژنرال‌ها برای هماهنگی زمان حمله، کانال‌های ارتباطی امنی بین یکدیگر ندارند؛ چرا که پیام‌های ارسالی و دریافتی توسط ژنرال‌ها ممکن است توسط مدافعین بیزانتیوم دست‌کاری یا جعل شود. در این شرایط ژنرال‌ها چگونه می‌توانند در یک‌زمان مشخص همگی به بیزانتیوم حمله کنند؟

سامانه‌های متمرکز و توزیع شده

تنها سامانه‌های توزیع‌شده به دلیل نداشتن منبع اطلاعاتی قابل‌اعتماد و نداشتن روشی برای احراز درستی اطلاعاتی که از دیگر اعضای شبکه دریافت می‌کنند، با مسئله ژنرال‌های بیزانس روبرو هستند.

در سامانه‌های متمرکز، یک نهاد معتمد وجود دارند که همه اعضای شبکه قبول دارند این نهاد اطلاعات صحیح منتشر می‌کند و از انتشار اطلاعات غلط و مخرب در شبکه جلوگیری می‌کند.

برای مثال، در سامانه‌های مالی سنتی، بانک‌ها نهادهای معتمدی هستند که مسئولیت نمایش موجودی مشتریان و سابقه تراکنش‌های آنان را به شکل صحیح و درست را بر عهده دارند. اگر بانکی در ارائه خدمات خود صداقت نداشته باشد و یا سعی در کلاهبرداری از مشتریان خود داشته باشد، در این صورت نهاد معتمد دیگری به نام بانک مرکزی یا دولت وارد عمل شده و نسبت به احقاق حقوق افراد اقدام می‌کند.

سامانه‌های متمرکز به‌جای حل مسئله ژنرال‌های بیزانس که همان انتشار بدون نیاز به اعتماد اطلاعات درست است، صورت مسئله را پاک کردند و بی نیازی به عنصر اعتماد را قربانی کارآمدی و سرعت سامانه‌های خود کردند. به عبارتی دیگر، اعتماد به سامانه‌های متمرکز، کلید دریافت خدماتی سریع و کارآمد است.

پول و مسئله ژنرال‌های بیزانس

پول اولین نمونه از مسئله ژنرال‌های بیزانس است. چگونه بایستی یک جامعه از مردم پولی را منتشر کنند که تمامی اعضای جامعه به آن اعتماد داشته و آن را قبول کنند؟ برای مدت‌های طولانی، جوامع از فلزات گران‌بها یا سایر کالاهای کمیاب همانند صدف و مهره‌های شیشه‌ای به‌عنوان پول استفاده می‌کردند. تا حدودی، طلا توانست مسئله ژنرال‌های بیزانس را حل کند. بااین‌حال سنجش دقیق وزن و خلوص طلا از همان زمان‌های قدیم تا کنون همیشه همراه با شک و غیرقابل‌اعتماد باقی ماند. عدم توفیق طلا در حل کامل مسئله ژنرال‌های بیزانس باعث تسلط نهادهای معتمد مرکزی، معمولاً دولت‌ها، بر صدور و عرضه پول شد. دولت‌ها برای ایجاد اعتماد در وزن و خلوص پول، ضرب سکه را به انحصار خود در آوردند. سامانه‌های متمرکز به‌وضوح نتوانستند مسئله ژنرال‌های بیزانس را حل کنند. دولت‌ها یا همان نهادهای معتمد مرکزی صدور پول، با تصرف، بی‌ارزش کردن و تغییر پول، به‌صورت مستمر اعتماد را خدشه‌دار نمودند.

حجم زیادی از اعتماد، پیش‌نیاز استفاده از ارزهای رایج است و این همان مشکل و ایراد اصلی و ریشه‌ای است. بایستی به بانک‌های مرکزی اعتماد کرد که ارز رایج را بی‌ارزش نمی‌کند، اما تاریخ پر از بدعهدی‌ها و نقض اعتمادها است. - ساتوشی ناکاموتا

برای آنکه یک پول بتواند مسئله ژنرال‌های بیزانس را حل کند، بایستی قابل‌بررسی و تأیید، مقاوم در برابر جعل و تقلب و بی‌نیاز به اعتماد به یک نهاد ثالث باشد و تمامی این موارد تا پیش از معرفی بیت‌کوین هیچگاه به‌صورت کامل پاسخ داده نشد.

چگونه بیت‌کوین مسئله ژنرال‌های بیزانس را حل کرد

بیت‌کوین اولین راهکار واقعی از دید پولی برای حل مسئله ژنرال‌های بیزانس بود. پیش از بیت‌کوین پیشنهادها و پروژه‌های زیادی تلاش کردند پولی مستقل از دولت‌ها ایجاد کنند، اما همگی شکست خوردند.

به‌عنوان یک نظام پولی، بیت‌کوین نیازمند روشی برای مدیریت مالکیت‌ها و جلوگیری از خرج مجدد (که در یک مقاله مجزا به‌صورت کامل تشریح خواهد شد) بود. برای دستیابی به این مهم به روشی بی‌نیاز از اعتماد، بیت‌کوین از یک بلاک‌چین یعنی یک دفتر کل توزیع شده و عمومی که سابقه تمامی تراکنش‌ها را در خود نگهداری می‌کند، استفاده می‌کند. در مسئله ژنرال‌های بیزانس، حقیقتی که تمامی افراد بایستی بر سر آن تفاهم کنند، همان بلاک‌چین است.

اگر تمامی اعضای شبکه بیت‌کوین که به آنها نود نیز گفته می‌شود موافقت کنند که کدام تراکنش‌ها و به چه ترتیبی رخ داده‌اند و مورد تأیید هستند، آنها می‌توانند مالکیت بیت‌کوین‌ها را تأیید کنند و بدین ترتیب یک پول کارآمد و بدون نیاز به اعتماد بدون وجود یک نهاد متمرکز را ایجاد کنند.

بیت‌کوین با استفاده از سازوکاری به نام اثبات کار یا POW، توانسته یک مجموعه قوانین مشخص و شفاف برای بلاک‌چین ایجاد کند. بدین ترتیب برای اضافه‌شدن اطلاعات یا همان بلوک به بلاک‌چین، یک عضو از شبکه بایستی اثبات کند برای ایجاد آن بلوک میزان زیادی کار و تلاش یا همان Work، انجام داده است. انجام این حجم بالایی از کار نیازمند صرف هزینه بالاست، در نتیجه یک مکانیزم مشوق و انگیزه‌دهی در صورت انتشار اطلاعات صحیح، در بیت‌کوین تعبیه شده است.

به دلیل آنکه قوانین شبکه بیت‌کوین عینی و واضح است، در این شبکه در میان اعضا عدم توافق بر سر اطلاعات پیش نمی‌آید. مجموعه قوانین حاکم بر شبکه که تعیین می‌کند چه تراکنشی تأیید و چه تراکنشی رد شود نیز عینی و مشخص است. همین شرایط شفاف بر نحوه استخراج بیت‌کوین نیز حاکم است. همچنین چنانچه یک بلوک به زنجیره بلوک متصل شود، فرایند حذف و یا تغییر آن به‌شدت دشوار و تقریباً نشدنی است و به همین دلیل بلاک‌چین غیرقابل‌تغییر و مانا است.

بدین ترتیب، در همه لحظات، اعضای شبکه بیت‌کوین می‌توانند بر سر حالت شبکه، وضعیت بلاک‌چین و تمامی تراکنش‌های درون آن به توافق برسند. هر یک از گره‌های (اعضا) شبکه منفرداً بلوک‌ها را بر اساس قوانین اجماع، اثبات کار و سایر قوانین شبکه بیت‌کوین بررسی و ارزیابی می‌کند.

چنانچه هر یک از اعضای شبکه نسبت به انتشار اطلاعات غلط و نادرست اقدام کند، همه اعضای شبکه بلافاصله این امر را تشخیص می‌دهند و به اطلاعات ارسالی از سوی آن گره توجهی نمی‌کنند. ازآنجایی‌که هر گره خود به‌تنهایی می‌تواند تمامی اطلاعات موجود در شبکه را بررسی و ارزیابی کند، هیچ نیازی به اعتماد به سایر گره‌ها وجود ندارد و بدین ترتیب بیت‌کوین به یک سیستم بی‌نیاز به اعتماد تبدیل شده است.

در مقالات بعدی، زیرساخت بلاک‌چین به‌عنوان ابزاری برای حل مسئله ژنرال‌های بیزانس مورد بررسی موشکافانه قرار خواهد گرفت.