مثلث بلاکچین چیست؟

استفاده از فناوری بلاکچین در سال‌های اخیر رشد قابل توجهی را تجربه کرده است و همین مسئله سبب شده تا مشکلات شبکه‌های بلاکچینی بیش از پیش خود را نشان دهند. هر کدام از پروژه‌های کریپتویی با هدف معینی وارد چنین دنیای غیرمتمرکزی شده‌اند، به عنوان مثال برخی با هدف رفع مشکلات بلاکچین‌های مشهور قبلی نظیر بیت کوین و اتریوم، برخی دیگر همچون تزوس با هدف ارائه راه‌حل‌های جدیدی نظیر مکانیزم Self-Amendment که شبکه بلاکچینی را از هاردفورک بی‌نیاز می‌سازد، پا به چنین عرصه‌ای نهاده‌اند. به طور کلی شبکه‌های بلاکچینی تلاش می‌کنند تا به سه هدف امنیت (Security)، مقیاس‌پذیری (Scalability) و تمرکززدایی (Decentralization) برسند؛ به مجموعه این اهداف، **مثلث بلاکچین** یا همان **Blockchain Trilemma** گفته می‌شود. این اصطلاح برای نخستین بار به وسیله ویتالیک بوترین، یکی از بنیان‌گذاران اتریوم، در سال 2017 به کار گرفته شد که به سه شاخصه اصلی شبکه‌های بلاک چینی اشاره دارد. از آن جایی که درک بهتر فناوری بلاکچین می‌تواند کمک خوبی برای شناخت دقیق‌تر این دنیای غیرمتمرکز نوظهور داشته باشد، ما این مقاله از بلاگ **کیف پول من** را به بررسی مثلث بلاکچین اختصاص داده‌ایم؛ بنابراین اگر شما هم در این زمینه کنجکاو هستید، تا انتهای این مطلب با ما همراه باشید.

مفهوم مثلث بلاکچین (Blockchain Trilemma)

مفهوم مثلث بلاکچین به زبان ساده در واقع به بررسی سه معضل بزرگ و اصلی پروژه‌های بلاکچینی اشاره دارد که این سه‌گانه از ضلع‌هایی به نام‌های امنیت، تمرکززدایی و مقیاس‌پذیری شکل گرفته است. جالب است بدانید که برخورداری همزمان بلاکچین‌ها از این سه عامل گفته شده، همواره برای آن‌ها چالش بزرگی محسوب می‌شود. به عنوان مثال تصور کنید که یک شبکه بلاکچینی به نام X کار خود را آغاز کرده است و تاکنون توانسته هزار کاربر فعال را به سمت خود جذب نماید. در شرایط فعلی، وضعیت این شبکه بلاکچینی به لحاظ هزینه و امنیت در سطح خوبی قرار دارد ولی سوال اصلی این است که آیا با رسیدن تعداد کاربران این شبکه به 20 هزار نفر نیز این شبکه قادر خواهد بود که تراکنش‌ها را با همان سرعت و هزینه قبلی پردازش نماید؟!

مثال عملی چنین مسئله‌ای شبکه اتریوم بود که همواره به لحاظ امنیت و تمرکززدایی در سطح خوبی قرار داشت؛ اما بسیاری از کاربران آن از هزینه بالای کارمزدها و همچنین سرعت پایین آن گلایه داشتند و این بدان معنا بود که شبکه اتریوم عملکرد خوبی در ضلع سوم **مثلث بلاکچین** که همان مقیاس‌پذیری است، نداشته است. اصولا هماهنگ کردن سه ضلع مثلث بلاکچین، کار چندان راحتی نبوده و غالبا یکی از این ضلع‌ها قربانی اضلاع دیگر می‌گردد که این دقیقا همان چیزی است که ما از آن تحت عنوان معضل و مشکل بلاکچین یاد می‌کنیم. در ادامه به بررسی دقیق‌تر ضلع‌های این مثلث می‌پردازیم:

امنیت در مثلث بلاک چین

این یک امر مسلم و کلیدی است که اگر می‌خواهیم کاربران بیشتری را به سمت تکنولوژی جدید خود جذب کنیم باید یک اطمینان خاطر خوبی را در آن‌ها ایجاد نماییم و طبیعتا چنین اطمینان خاطری در مسئله امنیت بلاکچین و انتقال سرمایه به آن زمانی رخ می‌دهد که این کاربران مطمئن شوند که هیچ تهدیدی نسبت به سرمایه آن‌ها وجود ندارد و این دقیقا همان عاملی است که از آن تحت عنوان عامل امنیت یاد می‌شود. شاید بتوان چنین گفت که عامل امنیت تنها عامل مشترکی است که چه در شبکه‌های متمرکز و چه در شبکه‌های غیرمتمرکز باید در اولویت قرار بگیرد.

مثال عملی در ارتباط با **ضلع امنیت در مثلث بلاکچین**، شبکه بیت کوین است که برای تامین امنیت و تمرکززدایی از فناوری رمزنگاری و مکانیزم اجماع اثبات کار (PoW) کمک گرفت. به کمک توابع هش و الگوریتم Proof-of-Work، منحصرا افرادی قادر هستند در اعتبارسنجی بلاک‌ها فعالیت نمایند که توان محاسباتی خویش را به حل معادلات پیچیده بلاکچین اختصاص داده‌اند. هرچند که به نظر برخی از افراد سازوکار الگوریتم PoW در تامین ضلع امنیت و تمرکززدایی عملکرد خوبی دارد؛ اما مسلما چنین الگوریتمی چندان عملکرد خوبی در تامین ضلع مقیاس‌پذیری نداشته است.

مطلب پیشنهادی : آیا بلاک چین به اندازه کافی امنیت دارد؟

تمرکززدایی در مثلث بلاکچین

یکی از دلایل اصلی محبوبیت یافتن استفاده از فناوری بلاکچین، غیرمتمرکز بودن آن است که سبب شده تا برخلاف تمامی سیستم‌های سنتی هیچ نهاد و موسسه خاصی بر آن نظارت نداشته و از شفافیت بیشتری برای عموم کاربران برخوردار باشد. وجود چنین شفافیتی می‌تواند موانعی قابل توجه را در برابر تخلفات و فسادهای مالی ایجاد نماید؛ چراکه کلیه فعالیت‌های مالی در رصد عموم کاربران قرار داشته و دسترسی کلیه کاربران به اطلاعات در سطح یکسانی قرار دارد.

اگر به وایت پیپر بسیاری از پروژه‌های بلاکچینی نظیر بیت کوین نگاهی بیاندازید متوجه می‌شوید که در آن از اصطلاح سیستم مالی همتابه‌همتا (Peer-to-Peer) استفاده شده که بر ویژگی **تمرکززدایی** چنین شبکه‌هایی دلالت دارد. هرچند که تمرکززدایی یکی از عوامل اصلی و کمک کننده به امنیت شبکه است؛ اما باید دانست که چنین عاملی به تنهایی کافی نبوده و ممکن است با افزایش میزان فعالیت شبکه و همچنین ترافیک بیشتر، تراکنش‌ها و داده‌ها با افت سرعت پردازش مواجه شوند. در نتیجه ما به ضلع دیگری به نام مقیاس‌پذیری نیاز پیدا می‌کنیم.

مقیاس‌پذیری در مثلث بلاکچین

اگر بخواهیم به تعریف ساده‌ای از ضلع **مقیاس‌پذیری** برسیم، باید بگوییم که این ضلع در واقع به این معناست که تکنولوژی مورد نظر ما آیا می‌تواند فعالیت خویش را در ابعاد بزرگتر نیز ادامه دهد و تمامی نیازهای کاربران خویش را برطرف نماید یا خیر؟! مثلا شبکه بیت کوین به طور میانگین در هر ثانیه حدودا 7 تراکنش را مورد بررسی و تائید قرار می‌دهد که چنین مسئله‌ای می‌تواند یکی از موانعی باشد که همواره بیت کوین را از این که در مقیاس جهانی به عنوان ابزاری برای انجام ریز تراکنش‌ها شناخته شود، دور نگه داشته است.

با توجه به نقش کلیدی ضلع **Scablibility** در کارامدی بلاکچین‌ها، غالب شبکه‌های بلاکچینی به دنبال این هستند که به این هدف بنیادین دست پیدا کنند؛ چراکه مقیاس‌پذیری به معنای پردازش تعداد تراکنش بیشتر در زمان کمتر است. اگر شبکه‌های بلاکچینی راه‌حلی برای مقیاس‌پذیری خود نیابند، این مسئله می‌تواند منجر به افزایش هزینه‌ها و همچنین کندی قابل توجه در تراکنش‌ها گردد. برخی از پلتفرم‌های مشهور نظیر Visa، که در هر ثانیه تا 24 هزار تراکنش را مورد پردازش قرار می‌دهند توانسته است اضلاع امنیت و مقیاس‌پذیری را به سطح قابل قبولی برسانند؛ اما رویکرد متمرکز آن‌ها سبب شده تا ضلع تمرکززدایی قربانی گردد. این یک مثال کاربردی که نشان می‌دهد حتی کمپانی‌های بزرگ نیز در برقراری چنین مثلثی با چالش‌های اساسی مواجه هستند.

راه‌حل‌های کلیدی برای رفع مشکل مثلث بلاکچین

حل مشکل **مثلث بلاکچین** با توجه به ماهیت خاص آن شاید در عمل کمی دشوار بنظر برسد به عنوان مثال توجه به ارتقا سرعت و مقیاس‌پذیری شبکه ممکن است امنیت شبکه را به خطر انداخته و ریسک خطرات بلاکچینی را افزایش دهد و در طرف دیگر ماجرا اتخاذ تدابیر امنیتی می‌تواند موجب شود که مقیاس‌پذیری به پاشنه آشیل شبکه ما تبدیل شده و به دلیل بالا رفتن میزان کارمزد و کاهش سرعت، کاربران چندان رغبتی به استفاده از آن پیدا ننمایند. با این وجود می‌توان سه راه‌حل کلی را برای حل چنین معضلاتی متصور بود که این راه‌حل‌ها به شرح زیر هستند:

1. **استفاده از مکانیزم اجماع های متنوع:** از دلایل اصلی استفاده از مکانیزم‌های اجماع می‌توان به تضمین امنیت شبکه اشاره کرد و همان طور که در مطالب فوق مشاهده کردید، استفاده از مکانیزم PoW هرچند تاثیر خوبی بر اضلاع **امنیت** و **تمرکززدایی** داشت ولی با **ضلع مقیاس‌پذیری** چندان همسو نبوده و **مثلث بلاکچین** را با مشکلاتی مواجه می‌ساخت برای حل چنین مشکلاتی می‌توان از سایر مکانیزم‌های اجماع نظیر مکانیزم PoS کمک گرفت.

2. استفاده از راه حل های لایه دوم بلاکچین: گاها توسعه‌دهندگان به منظور حل مشکلات موجود در شبکه بلاکچینی تصمیم می‌گیرند تا پروتکل‌های لایه 2 را ایجاد نمایند. در واقع دیدگاه چنین توسعه‌دهندگانی این است که برای دستیابی به اهداف خویش باید از زنجیره‌های جانبی و کانال‌های پرداخت استفاده نمایند.

مطلب پیشنهادی :لایه های بلاکچین

3. شاردینگ (Sharding): یکی از راه‌حل‌هایی که می‌تواند به بهبود میزان مقیاس‌پذیری شبکه بلاکچینی منجر گردد،مکانیزم شاردینگ نام دارد که از این قابلیت برای مدیریت و همچنین مرتب‌سازی داده‌های دیتابیس کمک گرفته می‌شود. در سازوکار تقسیم‌بندی زنجیره‌ها، هر زنجیره به طور مستقل فعالیت کرده و در نهایت تحت یک زنجیره اصلی مدیریت می‌شود.

تامین مثلث بلاکچین؛ معضل اصلی توسعه‌دهندگان شبکه‌های بلاکچینی

همان طور که در مطالب فوق مشاهده کردید، با بررسی مفهوم **مثلث بلاکچین** متوجه می‌شویم که این سه‌گانه به یک سد و مانع محکم برای اوج‌گیری شبکه‌های بلاکچینی تبدیل شده است؛ به طوری که اگر یک شبک بلاکچینی بخواهد توجه خود را بر روی عامل مقیاس‌پذیری متمرکز نماید، ممکن است مسیر ورود باگ‌های امنیتی را به چنین شبکه‌ای باز نماید. به طور کلی سه عامل **امنیت**، **تمرکززدایی** و **مقیاس‌پذیری** که از آن‌ها تحت عنوان **مثلث بلاکچین** یاد کردیم، همواره مورد توجه توسعه‌دهندگان شبکه بلاکچینی قرار داشته و به نظر کارشناسان ما در مجموعه **کیف پول من** می‌توان با استفاده از راه‌حل‌هایی نظیر لایه دوم بلاکچین، شاردینگ و استفاده از الگوریتم‌های اجماع متنوع تا حدودی مشکلات پیش آمده در این حوزه را برطرف نمود. ناگفته نماند که اگر در ارتباط با **مثلث بلاکچین** (Blockchain Trilemma) سوالی دارید که در این مقاله از کیف پول من به آن اشاره نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.