



درس فارغ فقه استاد حاج سید مجتبی نورمفیدی

موضوع کلی: فقه رمز ارزشها

تاریخ: ۳ آبان ۱۴۰۱

موضوع جزئی: موضوع شناسی - تفاوت‌های بلاک چین (زنجیره بلوکی) با پایگاه داده

مصادف با: ۲۸ ربیع الاول ۱۴۴۴

جلسه: ۶

«الحمد لله رب العالمین و صلی الله علی محمد وآله الطاهیرین و اللعن علی اعدائهم اجمعین»

خلاصه جلسه گذشته

در موضوع شناسی بحث رمز ارزشها عرض کردیم اموری باید تبیین شوند؛ تا اینجا چند امر و چند مفهوم و اصطلاح از امور مربوط به این موضوع مورد اشاره قرار گرفت. جلسه گذشته درباره فناوری مورد استفاده در موضوع رمز ارزشها مطالبی بیان کردیم. عرض کردیم بلاک چین یا زنجیره بلوکی یکی از مهم‌ترین زیرساخت‌های رمز ارزشهاست. محصل بیان ما این شد که زنجیره بلوکی یک پایگاه اطلاعات یا داده به نحو توزیع شده از اسناد یا یک دفتر کل عمومی از همه تبادلات مربوط به این حوزه و تراکنش‌هایی است که در آن صورت می‌گیرد. این یک دفتر کلی است متشکل از بلوک‌های متعدد که دائماً در حال افزوده شدن است و هر کسی که وارد این عرصه می‌شود یا مجموعه‌ای که به آن اضافه می‌شود، حجم این دفتر توسعه پیدا می‌کند؛ بلوک‌های جدید مثل حلقه‌های زنجیر براساس تاریخ تشکیل آنها، به آن زنجیره اضافه می‌شوند. این زنجیره شامل تمام اطلاعات مربوط به حساب‌ها، محتویات آنها، از ابتدا تا زمان حاضر است؛ و در مرئی و منظر همگان قرار دارد. یعنی هر آدرسی که در این شبکه ایجاد می‌شود، از همان نقطه صفر در معرض دید همگان قرار دارد و تمام تراکنش‌ها و رویدادهای دیجیتال در آن زنجیره از ابتدا تا آن موقع قابل دیدن و ردیابی است، ضمن اینکه هویت افراد کاملاً محرمانه است و کسی نمی‌تواند بفهمد که این کاربر یا این شخص کیست. فعل دیده می‌شود اما فاعل معلوم نیست.

تفاوت پایگاه داده با بلاک چین

عرض کردیم این صنعت یا فناوری ضمن اینکه از جنس پایگاه‌های داده یا اطلاعات محسوب می‌شود و یک تشابه‌هایی با آن دارد، اما در عین حال تفاوت‌هایی هم بین اینها وجود دارد. عرصه‌هایی که می‌توانیم پایگاه‌های داده را با بلاک چین یا زنجیره بلوکی مقایسه کنیم، چند عرصه است که این خودش می‌تواند به فهم بهتر این فناوری کمک کند. بعداً درباره چگونگی عملکرد این فناوری در حوزه رمز ارزشها و نحوه تولید و استخراج رمز ارزشها در این بستر، ان شاء الله توضیح خواهیم داد. احتمالاً دو سه دیگر باید پیرامون موضوع شناسی بحث را ادامه دهیم.

تفاوت اول

علی‌أیحال یکی از مهم‌ترین تفاوت‌های پایگاه‌های داده سنتی و فناوری بلاک چین مربوط به تمرکز و عدم تمرکز اینهاست؛ این نکته چندین بار تا به حال بیان شده و اجمالاً با آن آشنا هستید. اساس طراحی بلاک چین بر مبنای یک کار غیرمتمرکز است، در حالی که پایگاه‌های داده سنتی همیشه به نحو متمرکز عمل می‌کنند. این تمرکز و عدم تمرکز یک آثاری دارد؛ اگر گفتیم تمرکز وجود دارد چنانچه در پایگاه‌های داده معمولی مشاهده می‌شود، این حتماً نیاز به مدیریت اطلاعات دارد؛ اصلاً بدون مدیریت

متمرکز، این اطلاعات نمی‌تواند در معرض استفاده قرار گیرد. این مدیر به طور کلی ابزارهای لازم را برای کنترل آن پایگاه داده دارد؛ می‌تواند اطلاعات این پایگاه را اصلاح کند، حذف کند، اضافه کند، به‌گونه‌ای گذشته آن را پاک کند که کسی نتواند گذشته آن را ببیند. اینها همه با مدیریت متمرکز امکان انجام دارد؛ این مدیر در رأس این پایگاه داده هم این پایگاه را بروز رسانی می‌کند، اطلاعات آن را تغییر می‌دهد، بهینه‌سازی می‌کند. پس تمرکز یکی از ویژگی‌های مهم پایگاه‌های داده است. در حالی که در بلاک چین اساساً این تمرکز وجود ندارد و لذا نیازمند یک مدیریت واحد نیست؛ کنترل و نظارت از ناحیه همگان صورت می‌گیرد؛ ورود اطلاعات از ناحیه همگان است و لذا هیچ‌کسی نمی‌تواند اطلاعات موجود در این زنجیره را حذف کند یا تغییر دهد؛ افزودن اطلاعات ممکن است، اما حذف و تغییر و اصلاح در آن ممکن نیست. در حقیقت یک مدیریت جمعی است؛ همه با هم کأن این زنجیره را مدیریت می‌کنند. این یک ویژگی و تفاوت مهم این دو پایگاه محسوب می‌شود.

تفاوت دوم

تفاوت دیگر این دو صنعت یا این دو فناوری مربوط به ساختار این پایگاه‌هاست. در بلاک چین ساختار و معماری به صورت دفتر کل توزیع شده است؛ آن ساختاری که اطلاعات در آن قرار می‌گیرد، یک دفتری است که کأن در اختیار همه هست، اولین اطلاعات که در این دفتر ثبت می‌شود، کأن بقیه صفحات سفید است و در اختیار جمع‌کننده گذاشته شده و اینها اطلاعات را در این اوراق ثبت می‌کنند و به این دفتر اضافه می‌کنند. ساختار، ساختار شبکه دفتر کل توزیع شده است. گاهی از این تعبیر می‌کنند به شبکه نظیر به نظیر یا شبکه هم‌تا به هم‌تا؛ هر یک از افرادی که در این زنجیره قرار می‌گیرند می‌توانند با بهره‌برداری از پروتکل‌های رمزنگاری شده، با دیگران ارتباط برقرار پیدا کنند. همه این کاربران یا گره‌ها می‌توانند با یکدیگر به صورت هم‌تا به هم‌تا ارتباط داشته باشند و البته یک نقش جمعی هم برای این کاربران تعریف شده؛ اینها در قالب یک الگوریتمی که به نام الگوریتم اجماع شناخته می‌شود، اطلاعات مندرج در این زنجیره را تأیید می‌کنند؛ اینجا تأیید توسط یک نفر یا یک بخش صورت نمی‌گیرد. تأیید از یک مکانیزمی تبعیت می‌کند که آن مکانیزم امکان غلط و اشتباه و خطا را در آن بسیار پایین می‌آورد. از آنجا که در پایگاه داده به واسطه اینکه مدیر دارد و از یک معماری خاص دیگری که در حقیقت سرور است، بهره می‌گیرد، امکان خطا و اشتباه و غلط در آن زیاد است، اما در بلاک چین امکان خطا کمتر است.

پس ساختار این دو فناوری کاملاً با هم متفاوت است؛ معماری این شبکه‌ها گوناگون است. اگر در معماری مربوط به پایگاه داده به صورت متمرکز این اطلاعات وارد می‌شود و امکان اشتباه و خطا در آن هست و ارتباطات هم‌تا به هم‌تا فردی نیست، اینجا کاملاً ارتباطات هم‌تا به هم‌تا است و در یک محیط امن هر کسی می‌تواند با دیگری ارتباط برقرار پیدا کند. پس تفاوت دیگر مربوط به ساختار این دو فناوری است.

تفاوت سوم

معیار سوم برای تفاوت بین این دو فناوری، مربوط به انعطاف‌پذیری آنهاست. بالاخره هر دو به نوعی اطلاعات را ذخیره می‌کنند، هر دو پردازش و مدیریت می‌کنند، ولی به دو شکل متفاوت. در پایگاه داده سنتی ذخیره اطلاعات، پردازش اطلاعات و مدیریت اطلاعات به یک نحو است، در صنعت بلاک چین به نحو دیگری است. در پایگاه‌های داده سنتی انعطاف‌پذیری بیشتر است؛ یعنی ذخیره اطلاعات با سهولت بیشتری انجام می‌شود. بازایی اطلاعات راحت‌تر انجام می‌شود. همانطور که اشاره شد، در یک پایگاه داده سنتی آن اطلاعات موجود را راحت‌تر می‌تواند حذف کند، تغییر بدهد یا اصلاح کند، برای همین است که انعطاف‌پذیرتر

است. اما در بلاک چین این انعطاف وجود ندارد، لذا گفتیم تغییر و حذف داده‌ها یا اصلاح آنها معنا ندارد؛ آن قبلی‌ها سر جای خودش محفوظ است، فوئش در یک دفتر جدید اطلاعات در یک بلوک جدید افزوده می‌شود؛ دیگر اینجا حذف، تغییر، دستکاری امکان ندارد. در بلاک چین دو عملیات مورد استفاده قرار می‌گیرد برای بازیابی و خواندن اطلاعات یا افزودن اطلاعات؛ البته هر پایگاه داده دو کار عمده و دو عملیات مهم انجام می‌دهد؛ یکی افزودن اطلاعات و داده‌هاست و دیگری خواندن و بازیابی داده‌ها؛ این اطلاعات باید در جایی وارد شود و بعد مورد استفاده قرار گیرد. این دو عملیات در هر دو فناوری انجام می‌شود، اما فناوری بلاک چین در این عرصه انعطاف ناپذیرتر است نسبت به پایگاه‌های داده سنتی؛ هم در بحث افزودن اطلاعات و هم در عرصه خواندن و بازیابی اطلاعات. یعنی اگر در این دو بستر شما می‌بینید پایگاه داده هرگونه دستکاری در آن ممکن است، البته در چهارچوب‌های مربوط به خودش، اما در صنعت بلاک چین چنین چیزی نیست.

تفاوت چهارم

در حقیقت اینها تفاوت‌های ماهوی بین این دو است که طبیعتاً از زاویه‌های مختلف وقتی به آنها نگاه می‌شود، این تفاوت‌ها خودش را نشان می‌دهد. یعنی با توجه به این نکاتی که گفتیم، بالاخره یک آثار و نتایجی بر اینها مترتب می‌شود. یکی دیگر از این تفاوت‌ها، مربوط می‌شود به شفافیت و عریان بودن فعل و انفعالات مربوط به صنعت بلاک چین. ما گفتیم در صنعت بلاک چین تمرکز وجود ندارد و اطلاعات توسط همگان یا اکثریت تأیید می‌شود و لذا کاملاً شفاف است؛ یعنی شفاف‌تر از پایگاه‌های داده سنتی است. پایگاه‌های داده سنتی چون متمرکز هستند، هیچ الزامی برای شفافیت ندارند. در پایگاه‌های داده سنتی اگر مدیریت پایگاه یا آن سیستمی که آن را اداره می‌کند، این مطلب را دنبال نکند، به راحتی می‌تواند این شفافیت از بین برود. اولاً در عرصه افزودن اطلاعات به سلیقه خودش با آن معیارهایی که مدیریت در نظر دارد انجام شود، در بازخوانی و بازیابی اطلاعات هم همین اعمال می‌شود؛ و تازه آنها هم که در معرض دید دیگران قرار می‌گیرد، کاربر نمی‌تواند این اطلاعات را تأیید یا رد کند. ولی در صنعت بلاک چین کاملاً متفاوت است؛ چون در این فناوری تمرکز وجود ندارد و چون امکان حذف و تغییر و اصلاح نیست، بنابراین هرچه اتفاق افتاده همیشه در مرئی و منظر است. یکپارچگی داده‌ها در فناوری بلاک چین کاملاً محفوظ است و هر کسی می‌تواند از نقطه صفر تراکنش‌ها را تا زمان حاضر تعقیب کند و اینها را ببیند. لذا این دو در مقایسه با هم، کاملاً می‌تواند یکی را بسیار شفاف‌تر از دیگری قرار دهد.

تفاوت پنجم

تفاوت دیگر مربوط به هزینه‌هاست. هزینه‌های پایگاه داده سنتی بسیار کمتر از هزینه‌های بلاک چین است. البته در شرایط فعلی و تا زمانی که فناوری بلاک چین تکامل پیدا نکرده، چون ممکن است این فناوری با تکامل و فراگیر شدن و عمومی‌تر شدن، هزینه‌های کمتری را طلب کند؛ اما در شرایط کنونی هر کسی که الان می‌خواهد یک پایگاه داده درست کند، اعم از یک شخص یا سازمان، برای هر منظوری که باشد، چه قصد فعالیت اقتصادی داشته باشد، چه قصد فعالیت علمی و پژوهشی داشته باشد، چه بخواهد در عرصه اطلاع رسانی و اخبار کار کند، در عرصه فروش یا خرید، می‌تواند با استفاده از همین ساختارهایی که در پایگاه‌های داده معمولی وجود دارد این کار را انجام دهد. الان آنقدر برنامه‌ها وجود دارد که لازم نیست کسی برای کارهایی که می‌خواهد انجام دهد از نقطه صفر شروع کند؛ یک هزینه ناچیزی می‌دهد و این پایگاه داده را که در قالب‌های مختلف و با قابلیت‌های مختلف عرضه می‌شود، این را می‌خرد یا خیلی از آنها رایگان است. الان بسیاری از نرم افزارهایی که با فناوری

دیتابیس عمل می‌کنند، چه در امور حسابداری، کتابداری، خرید و فروش، عرصه‌های مربوط به پژوهش، اینها رایگان هستند. بله، برای همین قبلاً باید کلی هزینه می‌شد، اما الان اینقدر فراگیر شده و مورد استفاده قرار می‌گیرد که واقعاً برای بهره‌برداری از یک پایگاه داده سنتی، لازم نیست هزینه‌های آنچنانی صورت بگیرد. اما در مورد بلاک چین با توجه به نوع ساختار و عملکرد آن، مخصوصاً با توجه به اینکه هنوز داده‌ها و بازخوانی داده‌ها به این شکل عمومیت و شیوع پیدا نکرده، طبیعتاً یک هزینه بسیار بیشتری را تحمیل خواهد کرد.

شما اگر بخواهید از یک پایگاه داده سنتی استفاده کنید، (عرض کردم پایگاه داده آن ساختاری است که سایت از آن استفاده می‌کند، شبکه‌های اجتماعی از آن استفاده می‌کنند، همه اینها از آن استفاده می‌کنند) اینها یک قالب‌های آماده دارد که برخی از برنامه نویسان با تغییرات اندکی این را برای امور مختلف آماده می‌کنند و شما اطلاعات را وارد آن می‌کنید و کار تمام می‌شود. اما اگر بخواهیم فناوری بلاک چین را در همه این زمینه‌هایی که الان دارد مورد استفاده قرار می‌گیرد وارد کنیم، هم زمان طولانی نیاز دارد و هم بسیار هزینه بر است. الان اگر کسی بخواهد سایت بزند، نیاز به پلتفرم دارد، نیاز به یک سری مقدمات دارد اما اینها همه یک مبنا دارند که آن مبنا به راحتی آماده است و این اطلاعات و داده‌ها در آن قرار می‌گیرد و بعد مدیریت می‌شود. اما اگر در این صنعت بخواهد این کار انجام شود، خیلی هزینه دارد، چون فقط این نیست که یک قالبی باشد و شما هم اطلاعات را وارد آن کنید. این چون قرار است هم‌تا به هم‌تا عمل کند، کار پر هزینه‌ای است که از آغاز تا انجام آن حتماً هزینه‌های زیادی دارد.

تفاوت ششم

تفاوت دیگر مربوط به سرعت این دو پایگاه داده است. پایگاه‌های داده سنتی سریع‌تر به نتیجه می‌رسند؛ این پایگاه‌های داده سریع‌تر ساخته می‌شوند، سریع‌تر داده‌ها در آن قرار داده می‌شود و سریع‌تر مورد بهره‌برداری قرار می‌گیرند. یعنی پایگاه‌های داده سنتی میلیون‌ها اطلاعات و داده را در زمان کوتاهی مدیریت می‌کند، اما در بلاک چین اینطور نیست؛ بلاک چین سرعت کندتری دارد برای ایجاد داده‌ها و استفاده کاربران از آن. چون در ساختار بلاک چین سه کار باید انجام شود که زمانبر است؛ این سه کار در پایگاه داده سنتی لازم نیست. این سه کار عبارتند از:

۱. تأیید امضاء؛ یعنی تراکنش‌های بلاک چین یا تبادل اطلاعات زمانی انجام می‌شود که به صورت رمزنگاری و با کمک دستورالعمل‌هایی که وجود دارد، این کار را انجام دهد. هدف از این کار بالا بردن اعتبار تراکنش است؛ یعنی اگر کسی اطلاعاتی را در این زنجیره می‌گذارد، این باید تأیید شود، معتبر باشد؛ یک منبع معتبری باید این را تأیید کند. این یک فرآیندی دارد که زمان می‌برد. بحث در این نیست که برنامه کند است، حتی اگر کل این برنامه هم سریع باشد، خود عملیات تأیید امضا زمان می‌برد. اما در پایگاه داده شما چیزی به نام تأیید امضا ندارید.

۲. در پایگاه‌های داده گفتیم مسأله تمرکز وجود دارد؛ اما در بلاک چین مکانیزم اجماع باید تحقق پیدا کند تا یک مطلبی در آن زنجیره قرار گیرد. اعتبارسنجی تراکنش‌ها با مکانیزم اجماع صورت می‌گیرد. طبیعتاً مکانیزم اجماع یک امر زمانبر است. ما در پایگاه داده این کار را نیاز نداریم چون این مکانیزم وجود ندارد. یک پایگاه داده سنتی می‌تواند تراکنش‌ها را به صورت خودکار کنترل و تأیید کند؛ از یک جا این تأیید صورت می‌گیرد، در حالی که در بلاک چین کأن همگان باید این را تأیید کند.

۳. در صنعت بلاک چین اعضا همه مشارکت دارند در مدیریت؛ یعنی مثل این است که کآن باید همه اعضا نظر بدهند، یعنی هر کاربر ایفاء نقش می‌کند در تأیید و اعتبار آن اطلاعات و داده‌ها. طبیعتاً این خیلی زمان بیشتری نیاز دارد تا اینکه یک نفر بخواهد این کار را انجام دهد یا از یک مرکز این کار صورت بگیرد.

لذا به این جهت اصولاً زمانی که برای فناوری بلاک چین نیاز است، یک زمان طولانی‌تری است و به عبارت دیگر کارش نسبت به پایگاه داده کندتر است.

تفاوت هفتم

جهت دیگری که می‌توانیم برای تفاوت بین این دو ذکر کنیم، امنیت بالاتر بلاک چین است؛ یعنی ضریب خطا در بلاک چین بسیار کمتر است تا پایگاه داده سنتی. در پایگاه داده سنتی حتماً باید آن مدیریت متمرکز باشد تا کنترل شود و اگر این مدیریت از دسترس خارج شود، مثلاً آن سروری که این مدیریت را انجام می‌دهد از دسترس خارج شود، به راحتی می‌تواند در این عملیات اختلال ایجاد شود، مثلاً یک شبکه مهم اجتماعی مثل اینستاگرام یک دفعه در سراسر جهان دچار اختلال می‌شود، برای اینکه آن سروری که از این برنامه پشتیبانی می‌کند برای مدتی گرفتار برخی مشکلات شده است و به سرعت همه چیز بهم می‌ریزد. یا هکرها خیلی راحت می‌توانند به پایگاه داده سنتی نفوذ کنند و اطلاعات را پاک کنند یا دستکاری کنند، اختلال در امور ایجاد کنند. الان بسیاری از مشکلاتی که در صنایع نفت و پتروشیمی یا نیروگاه‌ها ایجاد می‌شود از همین طریق است. چند وقت قبل در کشور ونزوئلا برق بسیاری از شهرها قطع شد، همه هم به خاطر این بود که اختلال در برنامه‌های نیروگاه‌های تولید برق آنجا ایجاد کردند. اما در فناوری بلاک چین این خطاپذیری بسیار پایین‌تر است، یعنی ضریب خطا پایین‌تر است؛ چون یک سرور مرکزی ندارد. مثل این است که این اطلاعات پیش‌ده‌ها نفر وجود دارد که اگر نصف آن هم از بین برود، عیناً نزد نصف دیگر هست. هزاران کاربر یا هزاران گره در سراسر دنیا وجود دارند که اگر دو سوم اینها هم کارشان مشکل پیدا کند، اما بقیه هستند و آنها می‌توانند به راحتی این تراکنش و تبادل را انجام دهد.

این چند موضوع برای مقایسه پایگاه‌های داده و بلاک چین وجود دارد. من این تفاوت‌ها را ذکر کردم تا به فهم بهتر این موضوع کمک کند. البته این موضوع هنوز برای شما به صورت کامل روشن و شفاف تجزیه و تحلیل نشده؛ شما الان پیش متخصصین این امور هم بروید و بخواهید این فناوری را برای شما شرح بدهند، مخصوصاً چون جدید است، یک مقداری با مشکلات همراه است. تلاش ما این است که یک تصویر اجمالی از این فناوری ارائه بدهیم تا اجمالاً معلوم شود بلاک چین چیست، چون رمز ارز در این بستر کار می‌کند.

«والحمد لله رب العالمین»