



## درس فارغ فقه استاد حاج سید مجتبی نورمفیدی

موضوع کلی: فقه رمز ارزها

تاریخ: ۲۷ مهر ۱۴۰۱

مصادف با: ۲۲ ربیع الاول ۱۴۴۴

موضوع جزئی: موضوع شناسی - فناوری مورد استفاده در رمز ارزها - بلاک چین یا زنجیره بلوکی -

برخی عرصه‌های مورد استفاده فناوری بلاک چین

جلسه: ۵

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

### خلاصه جلسه گذشته

عرض شد اگر بخواهیم آن بستری را که در آن ارزهای دیجیتال یا رمز ارزها تولید و منتشر می‌شوند را معرفی کنیم، باید از فناوری بلاک چین یا زنجیره بلوکی نام ببریم که در نظام‌های رایانه‌ای به عنوان یکی از سیستم‌های اطلاعاتی شناخته می‌شود؛ یعنی در دسته‌بندی نظام‌های رایانه‌ای، فناوری بلاک چین در واقع یک نظام و سیستم جمع‌آوری و پردازش داده‌ها و اطلاعات است، منتهی با یک شکل جدید. در جلسه گذشته درباره پایگاه‌های اطلاعات یا داده‌ها در شکل متعارف آن مطالبی را عرض کردیم.

### بلاک چین یا زنجیره بلوکی

حالا باید ببینیم بلاک چین چیست و چه تفاوت‌هایی با پایگاه‌های داده سنتی و متعارف دارد؛ چون رمز ارز فرآورده یک چنین فناوری است. لذا برای بهتر شناختن رمز ارزها باید این فناوری تا حدودی بیان شود، چون بالاخره واقعاً یک تکنولوژی پیچیده‌ای است که به این سادگی‌ها نمی‌شود آن را توضیح داد و فهمید. اجمالاً برای اینکه با این فناوری و کارکرد آن که البته مختص به رمز ارزها هم نیست آشنا شویم، یک توضیح اجمالی و کلی ذکر می‌کنیم و البته چه‌بسا با این توضیحات همه ابهامات مربوط به آن هم برطرف نشود و همه پرسش‌ها پاسخ داده نمی‌شود.

به این فناوری از این جهت اطلاق زنجیره بلوکی می‌شود که تعدادی از بلوک‌ها و بخش‌هایی که حاوی اطلاعات و داده‌ها هستند، وقتی در کنار هم قرار می‌گیرند یک زنجیره‌ای تشکیل می‌دهند که به همین جهت به آنها زنجیره بلوکی گفته می‌شود. این زنجیره‌ها همانند دفاتری است که به هم پیوستگی پیدا می‌کنند و زنجیره را تشکیل می‌دهند، دفتر کل که تمام داده‌ها و اطلاعات، اسناد و تراکنش‌های مالی و غیرمالی در آن ثبت و ضبط می‌شود؛ شما فرض کنید یک دفتری که در مرئی و منظر همه هست حالا در امور مالی، چون این در سایر رشته‌ها هم مورد استفاده قرار می‌گیرد؛ در خصوص امور مالی و حسابداری یک دفتری را در نظر بگیرید که این دفتر یک وقت در اختیار یک شخص است و او متصدی ثبت و ضبط داده‌ها و اطلاعات است، کسی دیگری به این دسترسی ندارد؛ او می‌تواند اطلاعات داده شده یا ثبت شده در این دفتر را حذف کند و اصلاح کند، تغییر بدهد و نهایتاً یک دفتری به شما ارائه دهد که سوابق این تغییرات در آن نباشد. با اینکه این تغییرات و تراکنش‌ها را منعکس می‌کند، ولی چون خودش متصدی این کار است، می‌تواند ضمن اینکه آن سوابق را ثبت و ضبط کرده، تغییراتی هم در آن اعمال کند؛ چیزی را حذف کند و عددی را اصلاح کند و آن وقتی که دفتر را به شما ارائه می‌دهد، این دفتر دیگر سوابق این تراکنش‌ها به معنای نمایانگر بودن حذف‌ها، تغییرات و اصلاحات، در آن وجود ندارد. اما اگر فرض کنید یک دفتری را بگذارند، به جای اینکه یک

نفر اطلاعات در آن وارد کند، همه کسانی که درگیر کار هستند، در این دفتر اطلاعات وارد کنند و به گونه‌ای باشد که هیچ کسی نتواند تغییری را بدون دیدن دیگران انجام دهد؛ اگر یک نفر در این دفتر دست ببرد و تغییری ایجاد کند، حذف یا اصلاح کند، دیگران می‌فهمند؛ چون همه می‌توانند داده‌ها را در این دفتر ثبت کنند؛ یک دفتر کل که همه این داده‌ها در آن جمع می‌شود، منتهی یک وقت یک نفر این کار را انجام می‌دهد و یک وقت این دفتری است که همه کسانی که با آن موضوع مرتبط هستند، این داده‌ها را می‌توانند وارد آن دفتر کنند و هر کسی اگر کوچکترین تغییری در سوابق اطلاعات ثبت شده بخواهد ایجاد کند، همگان آن را می‌فهمند و کشف می‌کنند. زنجیره بلوکی یا بلاک چین در واقع یک دفتر کل یا زنجیره‌ای از دفاتر منعکس کننده تراکنش‌ها و رد و بدل شدن داده‌ها و اطلاعات است؛ به گونه‌ای که هر نوع تغییر، حذف یا اصلاح، به سرعت برای همگان آشکار می‌شود و البته تأیید این اطلاعات و داده‌ها، راستی آزمایی اطلاعات ثبت شده، تابع یک قاعده و الگوریتمی است به نام اجماع؛ یعنی همگان با هم کأن تأیید می‌کنند اطلاعات موجود در این سیستم را و تا این اجماع و اتفاق حاصل نشود، کأن صحت و درستی آن مورد تأیید قرار نمی‌گیرد. این مثالی که من زدم، البته از یک جهت مقرب است، مسأله دفتر و حضور یک نفر یا همگان در ثبت و ضبط داده‌ها و اطلاعات، این از یک جهت می‌تواند مقرب به ذهن باشد برای معرفی این زنجیره. لکن از جهاتی هم چه بسا به خاطر تفاوت‌هایی که دارد، مبعده باشد. آن مقداری که اینجا می‌توانیم در این رابطه توضیح دهیم، این است که این سیستم اطلاعاتی یا زنجیره بلوکی یا بلاک چین، در حقیقت یک تکنولوژی رمزنگاری شده است؛ این سیستم اطلاعات مالی یا غیرمالی جمع آوری شده را در یک چیزی که به صورت عمومی و در مرئی و منظر همگان است ارائه می‌کند و تمام جزئیات و سابقه همه تراکنش‌های انجام شده را در درون خود ذخیره می‌کند و این را در مرئی و منظر دیگران قرار می‌دهد. کاربران و همه کسانی که به نوعی با این سیستم اطلاعاتی، در آن حوزه مرتبط با خودشان اصطلاحاً به آنها گره گفته می‌شود و هر اطلاعاتی که در این بانک و در این سیستم گنجانده می‌شود، باید به این تأیید این کاربران برسد و چون این بلوک‌های رمزنگاری شده به هم پیوسته و در هم تنیده هستند، هر داده و اطلاعاتی که در این بلوک‌ها ذخیره می‌شود، به کل زنجیره منتقل می‌شود و همگان از آن اطلاع پیدا می‌کنند. لذا یکی از مزایای این بانک اطلاعاتی و سیستم اطلاعاتی یا این فناوری این است که امکان تقلب و فریبکاری در آن ضعیف است. چون اساساً یک تمرکز و نظارت متمرکز - البته در برخی اقسام آن - چندان وجود ندارد که اراده اشخاص یا سازمان‌ها در آن دخیل باشد و بتوانند این را تغییر بدهند.

اگر بخواهیم توضیح بیشتری برای این فناوری ارائه دهیم، باید تفاوت‌هایی که بین این فناوری و پایگاه‌های داده سنتی وجود دارد را تا حدودی بیان کنیم؛ ببینیم چه اشتراکاتی بین این دو سیستم و نظام اطلاعاتی رایانه‌ای وجود دارد. اما اجمالاً برای اینکه یک شناخت کلی از این فناوری ارائه دهیم، عرض کردم کأن یک مجموعه‌ای از بلوک‌ها که شبیه دفاتر هستند را در نظر بگیرید که اینها بهم پیوسته‌اند و همه کاربران می‌توانند وارد این دفاتر و بلوک‌ها شوند و اطلاعات را در آن ثبت و ضبط کنند. این توضیحات من فارغ از این است که چگونه رمز ارز در این سیستم تولید و منتشر می‌شود؛ چون عرض کردم شاید اولین و مشهورترین استفاده‌ای که از این فناوری به عمل آمد، در دفتر کل تراکنش‌های بیت‌کوین بود. اولین رمز ارز که مورد استفاده قرار گرفت و مبنایی شد برای ده‌ها و بلکه صدها رمز ارز دیگر، بیت‌کوین بود. این فناوری و اینکه چگونه بیت‌کوین یا رمز

ارزها محصول آن به حساب می‌آیند، آن را بعداً یک اشاره اجمالی می‌کنیم. الان این فناوری را به عنوان یک نظام اطلاعاتی رایانه‌ای که در عرصه‌های گوناگون مورد استفاده قرار می‌گیرد داریم معرفی می‌کنیم، با قطع نظر از آن جهت.

### **برخی عرصه‌های مورد استفاده فناوری بلاک چین**

الان در عرصه‌های مختلف، مثلاً در خدمات مربوط به سلامت از این فناوری استفاده می‌شود؛ در حوزه درمان کاربردهای متفاوتی برای این فناوری وجود دارد.

#### **۱. عرصه پزشکی و سلامت**

اطلاعات بیماران که مورد نیاز مراکز درمانی و پزشکان است و برای رد و بدل کردن آن همیشه با یک مشکلاتی مواجه هستند، الان از این فناوری استفاده می‌شود. در پایگاه‌های داده سنتی که به صورت متمرکز این اطلاعات ذخیره می‌شود و انتقال پیدا می‌کند. الان شما همین نسخه‌هایی که دکترها و اطباء می‌نویسند، الان مثل گذشته روی دفترچه و کاغذ نمی‌نویسند، داخل سیستم وارد می‌کنند و شما کد رهگیری را می‌گیرید و همان کد را به داروخانه می‌دهد و به شما آن دارو را می‌دهند. بالاخره این یک نقل و انتقال اطلاعات مربوط به بیماران است. پرونده‌های پزشکی که یک طبیب بخواهد برای بیمارستان بفرستد یا بالعکس، اینها الان به صورت متمرکز در یک مجموعه‌ای ذخیره می‌شود، حالا یک فرد این کار را برای خودش می‌کند یا یک نهاد و سازمان، این انتقال داده‌ها و اطلاعات انجام می‌شود؛ ولی همیشه یک خطری متوجه این سنخ ثبت و ضبط و نگهداری و انتقال داده‌ها وجود دارد و آن اینکه اینها از بین برود؛ چون به صورت متمرکز است، امکان از بین رفتن این داده‌ها وجود دارد؛ این ممکن است به خاطر مشکلات سخت افزاری باشد یا به خاطر نرم افزارهای دارای ویروس یا بدافزار این اتفاق بیفتد. الان گروه‌های بزرگی در سراسر دنیا به عنوان هکرها شناخته می‌شوند که کارشان نفوذ به همین سیستم‌ها و داده‌های اطلاعاتی است و آسیب‌های فراوانی از این جهت متوجه سازمان‌ها و نهادها می‌کنند. یک باره تمام ذخایر و داده‌های یک سازمان و نهاد را از بین می‌برند؛ اگر هم از اینها کپی گرفته باشند، استفاده و بارگذاری مجدد اینها زمان‌بر و هزینه‌بر و با مشکلاتی مواجه است. اما زنجیره بلوکی خطر از بین رفتن و نابودی این داده‌ها را کم می‌کند.

یک دارویی از مرحله‌ای که تولید می‌شود تا وقتی که به دست مصرف کننده می‌رسد، با این فناوری قابل ردیابی است؛ مرحله به مرحله این دارو کجا قرار گرفته است. حتی در دوران کرونا یکی از اموری که توسط این فناوری می‌توانست مورد استفاده قرار گرفت و بعضی هم استفاده کردند، ثبت اطلاعات کسانی که تست داده بودند و کسانی که تست نداده بودند، کسانی که واکسن زده بودند و کسانی که نزده‌اند، و اینکه مثلاً این شخص آیا می‌تواند از وسایل حمل و نقل عمومی استفاده کند یا نه؛ گرچه این کار به وسیله سیستم‌های اطلاعاتی متعارف هم انجام می‌شد، اما انجام این کار و پیگیری و ردیابی بیماران در یک بیماری فراگیری مثل کرونا، با این نظام اطلاعاتی بسیار سریع‌تر و دقیق‌تر ممکن بوده و هست. من اینها را توضیح می‌دهم تا ذهن شما در مورد این فناوری صرفاً معطوف به بخش رمز ارز نشود؛ اگرچه الان بیشترین استفاده از این فناوری در حوزه رمز ارزهاست.

#### **۲. عرصه مالیات**

در مورد اخذ مالیات؛ مالیات انواع و اقسامی دارد، معمولاً سازمان‌هایی که متصدی این کار هستند، از مشاغل و صنوف مختلف مالیات می‌گیرند؛ این مالیات‌ها در گذشته به صورت دستی و ثبت در دفتر بود و بعد هم با نرم‌افزارهایی داده‌ها و اطلاعات را ثبت می‌کنند و برای هر شغل یا صنفی، میزان مالیات را مشخص می‌کنند. یکی از مشکلاتی که در اخذ مالیات‌ها وجود دارد و

دولت‌ها با آن مواجه هستند، مسأله فرار مالیاتی است یا کلاهبرداری‌هایی که در این حوزه اتفاق می‌افتد. این ولو با پایگاه‌های داده سنتی و به صورت رایانه‌ای انجام می‌شود، اما راه برای این فرار باز است. برای اینکه یک مرکزیتی وجود دارد که می‌تواند این اطلاعات را حذف کند، تغییر دهد و اصلاح کند. اما در فناوری زنجیره بلوکی یا بلاک چین این امکان به حداقل می‌رسد؛ به دلیل اینکه متمرکز نیست و یک نفر در آن وارد نمی‌شود تا بخواهد هر طور مثل آن شخصی که دفتر در اختیار اوست، اطلاعات را تغییر بدهد، جابجا کند، حذف کند؛ این زنجیره، آن هم به صورت شفاف طوری است که امکان هر گونه تغییر را از افراد سلب می‌کند. نقطه به نقطه معاملات، خرید و فروش‌ها، فعالیت‌ها، به گونه‌ای است که نمی‌توانند در آن مداخله کنند و آن را تغییر دهند. مخصوصاً برای مالیات بر ارزش افزوده که طبیعتاً هرکسی یک جنسی را می‌فروشد، بالاخره یک چیزی به عنوان مالیات بر ارزش افزوده برای او مقرر شده و طبیعتاً با وجود این فناوری، امکان اینکه فرار مالیاتی صورت بگیرد به حداقل می‌رسد؛ شفافیتی که اینجا هست، عدم تمرکزی که اینجا وجود دارد و اینکه واسطه‌ای در کار نیست، مستقیماً این معاملات و خرید و فروش‌ها در مرئی و منظر قرار می‌گیرد و دیگر اینطور نیست که کسی بخواهد اظهار کند؛ کسانی که می‌خواهند مالیات بدهند باید اظهارنامه پر کنند، مثلاً بنویسند که فلان کار را کردیم و اینقدر هزینه شد و فلان مقدر سود داشت. طبیعتاً این اظهارنامه‌ها باید مورد بررسی قرار گیرد و مطابقت شود با دفاتر مالی آنها که آیا این اظهارنامه مطابق با دفاتری که منعکس کننده فعالیت‌های مالی هستند، می‌باشد یا نه. شما حساب کنید چقدر نیرو می‌خواهد، چقدر هزینه و زمان می‌خواهد تا این بررسی صورت بگیرد که آیا مطابقت دارد یا نه. این در فناوری بلاک چین به طور خودکار انجام می‌شود؛ هزینه‌ها کاسته می‌شود و نیازی به این بررسی‌های هزینه‌بر نیست، نه هزینه انسانی و نه هزینه مالی. در لحظه این امکان وجود دارد که شما سود و زیان اشخاص را کشف کنید؛ لازم نیست که یک زمانی بگذرد تا این مسأله معلوم شود. این سیستم اطلاعاتی آنقدر قوی است که بتواند با اطلاعاتی که از همه اطراف و توسط همگان در آن قرار می‌گیرد، پردازش کند و به نوعی خروجی داشته باشد و این خروجی مورد استفاده آن سازمان یا نهاد مربوطه قرار گیرد. چون کأن فرآیند پرداخت و انتقال و همه اینها به صورت خودکار انجام می‌شود و دیگر نیازی نیست که یک دستگاه عریض و طویل محاسبه کنند که مالیات این شخص چقدر می‌شود.

می‌خواهم با این مثال‌ها ذهن شما را نزدیک کنم به کارآیی و کاربرد این فناوری. شاید این فناوری خیلی هنوز در بحث‌های مالیاتی مورد استفاده قرار نگرفته است؛ ولی در آینده مطمئناً این اتفاق خواهد افتاد.

### ۳. عرصه خرید

الان تهیه و تأمین کالاها و نیازهای مصرفی مردم نسبت به ۲۰ سال قبل خیلی متفاوت شده است. ۲۰ سال قبل اگر یک کالایی را می‌خواستید که مثلاً در شهر شما و در مغازه سرکوجه نبود، باید از این طرف شهر به آن طرف شهر می‌رفتید و این کالا را تهیه می‌کردید. یا اگر این کالا در شهر شما نبود، باید به شهرهای دیگر مراجعه می‌کردید؛ یا اگر در تهران وجود داشت، باید آنجا می‌رفتید و بگردید این جنس را کجا دارند. ولی الان تأمین کالاهای مورد نیاز بسیار متفاوت شده است؛ زنجیره‌ای برای تأمین فراهم شده در فضای دیجیتال که کار اینها این است که محصولات را معرفی کنند و در کمترین زمان ممکن اینها را برای شما ارسال کنند. مثلاً دیجی‌کالا که همگان برای اینکه چیزی را پیدا کنند، به همین پلتفرم مراجعه می‌کنند. الان زنجیره‌های تأمین در شکل فعلی به وسیله پایگاه‌های داده و اطلاعات به صورت سنتی انجام می‌شود، یعنی این که جدید است و با ۲۰ سال پیش

خیلی فرق کرده، این خودش در مقایسه با فناوری بلاک چین، به عنوان روش سنتی محسوب می‌شود. در این فناوری کار تأمین و زنجیره تأمین نیازهای مردم، بسیار دقیق‌تر، سریع‌تر و کم هزینه‌تر انجام می‌شود؛ یعنی اگر از این فناوری در مسأله تأمین کالاهای مورد نیاز مردم استفاده شود، از آنجا که این بسیار شفاف و قابل ردیابی است و تمرکز در آن نیست، دیگر امکان اختفاء، کلاهبرداری و فریبکاری، وجود ندارد. این فناوری با اینکه هنوز در این بخش چندان مورد استفاده قرار نگرفته، اما در جاهایی که از آن استفاده می‌کنند، مزایای فوق‌العاده‌ای برای آن ذکر می‌کنند که چقدر هزینه‌ها پایین می‌آید و چقدر دسترسی به کالای مورد نیاز سریع‌تر و دقیق‌تر است؛ چون در تمام مراحل این کالا ردیابی می‌شود و این ردیابی هم توسط متقاضیان و مشتریان به گونه‌ای است که دیگری نمی‌تواند در آن اعمال نظر کند، مثلاً این کالا را بگذارد و فردا ببیند گران شد بردارد؛ تأثیرگذاری مسائل اقتصادی بر ارزانی و گرانی، این بحث دیگری است و در همه جا اتفاق می‌افتد؛ اینکه کالایی را برای عرضه گذاشته شده، امروز مدیر این مجموعه این کالا را می‌گذارد و می‌بیند که مثلاً اتفاقاتی دارد می‌افتد و این را برمی‌دارد و دیگر در معرض قرار نمی‌دهد؛ در این زنجیره این امکان خیلی کم می‌شود، چون آن تمرکز و مدیریت واحد وجود ندارد؛ آن دخالتی که در تبادل اطلاعات و تراکنش‌ها از یک ناحیه ممکن است صورت بگیرد، دیگر اینجا وجود ندارد. مثل یک اتاق شیشه‌ای که همه داخل آن را می‌بینند. چون این چنین است، امکان این دخالت‌ها را به حداقل می‌رساند و طبیعتاً این شفافیت خیلی کمک می‌کند. این مخصوصاً در مورد کالاهایی که تقلب در آنها زیاد است، اصل و بدل دارد، آنجا بیشتر خودش را نشان می‌دهد که اساساً زمینه تقلب را بسیار کاهش می‌دهد. اینها برای محصولات تولید شده است؛ شما حساب کنید مواد اولیه‌ای که یک کارخانه برای تولید یک محصول نیاز دارد، برای یک شرکت نسبت به این مواد اولیه این نظارت و ردیابی را شما می‌توانید داشته باشید. یعنی یک مشتری نه تنها از مبدأ کارخانه که این محصول را تولید می‌کند، حتی پیش از آن، مواد اولیه‌ای که این را تولید کرده برای او قابل ردیابی است. نمی‌گوییم به صفر می‌رسد ولی این را به حداقل می‌رساند.

من مثال‌هایی را ذکر کردم و هنوز این بحث باقی مانده است. اگر اشتراکات و تفاوت‌هایی که بین این دو نظام اطلاعاتی وجود دارد تبیین شود، بیشتر به فهم مسأله کمک می‌کند.

«والحمد لله رب العالمین»