



## درس فارغ فقه استاد حاج سید مجتبی نورمفیدی

موضوع کلی: فقه رمز ارزها

تاریخ: ۴ آبان ۱۴۰۱

موضوع جزئی: موضوع شناسی - کاربردهای بلاک چین (زنجیره بلوکی) و پایگاه داده - انواع بلاک چین

مصادف با: ۲۹ ربیع الاول ۱۴۴۴

چیستی رمز ارز: مقدمه

جلسه: ۷

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

## کاربردهای پایگاه داده و بلاک چین

در بحث از موضوع مورد گفتگو به تفاوت‌های این فناوری و پایگاه داده اشاره کردیم. حدوداً هفت فرق برای این دو روش و نظام اطلاعاتی رایانه‌ای ذکر کردیم. اگر بخواهیم با عنایت به آن تفاوت‌ها به طور خلاصه موارد استفاده این دو روش جمع‌آوری و پردازش اطلاعات را بیان کنیم، می‌توانیم بگوییم پایگاه‌های داده سنتی بهترین موارد استفاده آنها یکی در ذخیره‌سازی اطلاعات محرمانه است و نیز پردازش سریع تراکنش‌های آنلاین و مبادلات اطلاعات و در جاهایی که کار در برنامه یا سیستم نیازی به تأیید داده‌ها و اطلاعات ندارد و عمدتاً مربوط به داده‌ها و اطلاعات ارتباطی است. پایگاه‌های داده الان که بسیار شایع و فراگیر هستند، کاربرپسند هم هستند؛ کاربران با این پایگاه‌های داده با سهولت بیشتری کار می‌کنند و شاهد آن هم مراجعات فراوانی است که در سراسر جهان به وبسایت‌ها و پایگاه‌های اطلاع‌رسانی در موضوعات مختلف می‌شود. تمام وبسایت‌ها بر این پایگاه‌های داده اتکاء دارند. سیستم‌های بانکی و مالی و بورس که نیازمند عملیات سریع می‌باشند، اینها همه برای استفاده بهینه از برنامه و کارهایی که مدنظر آنهاست، از پایگاه داده استفاده می‌کنند. بنابراین مراجعه به فناوری بلاک چین یا زنجیره بلوکی طبیعتاً در شرایط فعلی برای این مواردی که نام برده شد و با توجه به نیازهای مخاطبین، چندان مطلوب نیست.

فناوری بلاک چین بیشتر در مواردی که اشاره می‌کنم مورد استفاده قرار می‌گیرند؛ در ارزش‌های انتقالی، ارزش ذخیره‌سازی، معاملات پولی و همه مواردی که نیازمند تأیید داده هستند و برنامه‌هایی که اصولاً ساختارشان متمرکز نیست، لذا چندان مورد پسند کاربران نیست. اما اگر کسی بیشتر به دنبال شفافیت، اعتماد و تأیید داده‌ها باشد، حتماً به سراغ این فناوری می‌رود و طبیعتاً انتظار می‌رود به مرور در آینده استفاده از این فناوری بیشتر شود.

## انواع بلاک چین

بعد از بیان تفاوت‌ها، خوب است اشاره‌ای به انواع بلاک چین‌ها داشته باشیم. ما تاکنون در معرفی این فناوری، یک نوع را بیشتر تبیین کردیم، ولی باید بدانید که خود بلاک چین سه نوع است که شاید یک نوع از این انواع سه‌گانه بیشتر در ارزش‌های دیجیتال مورد استفاده قرار می‌گیرد و آن تفاوت‌هایی که گفته شد، بیشتر ناظر به یک نوع است؛ بلاک چین عمومی یا بدون مجوز، بلاک چین فدرالی یا کنسرسیومی، بلاک چین خصوصی یا با مجوز.

## نوع اول

در نوع اول که با عنوان عمومی شناخته می‌شود، تمام کاربران بدون هیچ محدودیتی به این شبکه دسترسی دارند، در آن فعالیت می‌کنند و در مدیریت آن حضور دارند؛ یعنی حسابرسی می‌کنند، داده‌ها را تأیید و امضاء می‌کنند. در جلسه قبل توضیح داده شد که چرا به این شکل عمل می‌شود. این کاملاً شفاف است و با اجماع کاربران یا تعبیر فنی‌تر الگوریتم اجماع آن هم به صورت

غیر متمرکز، داده‌ها و اطلاعات را تأیید می‌کنند و امکان تغییر و حذف و اصلاح در آنها وجود ندارد. یکی از دوستان سؤال کردند الگوریتم اجماع یعنی چه. اگر بخواهیم خیلی ساده معنا کنیم، الگوریتم عبارت است از یک روش و برنامه گام‌به‌گام و مرحله به مرحله برای رسیدن به مقصود؛ به یک معنا همه ما در زندگی روزمره یک الگوریتمی داریم مثلاً صبح که می‌خواهیم از منزل خارج شویم، از زمانی که از خواب برمی‌خیزیم تا زمانی که از منزل خارج شویم، مرحله به مرحله یک کارهایی را انجام می‌دهیم؛ گام به گام پیش می‌رویم تا آماده شویم از منزل بیرون بیاییم. این در حقیقت یک روش گام به گام و مرحله به مرحله برای رسیدن به مقصود و انجام کار است. این یک معنای خیلی ساده و کلی آن است؛ الگوریتم اجماع در علوم رایانه‌ای یک پیچیدگی خاصی دارد ولی بالاخره یک روشی است که در طی آن مرحله به مرحله و گام به گام، این کارها انجام می‌شود و اجماع نسبت به آن داده‌ها محقق می‌شود.

ارزهای دیجیتال بیشتر از این نوع از بلاک چین‌ها استفاده می‌کنند، لذا ما در توضیح این فناوری بیشتر ناظر به این نوع از فناوری بودیم.

### نوع دوم

نوع دوم که با عنوان بلاک چین فدرالی یا کنسرسیومی شناخته می‌شود، در حقیقت نظارت گروهی و رهبری جمعی دارد. یک جمع و گروهی نسبت به این عملکردها و تراکنش‌ها نظارت دارند و مدیریت می‌کنند. اینها هستند که باید اطلاعات و داده‌ها را تأیید کنند و اجازه نمی‌دهند به دیگران که این تراکنش‌ها را تأیید کنند. ممکن است به ذهن شما بیاید این نوع از فناوری اساساً ماهیتاً با آنچه که درباره بلاک چین گفته شد متفاوت است؛ آن مختصاتی که ما برای بلاک چین گفتیم، با این نوع سازگار نیست. تفاوتی که بین بلاک چین و پایگاه‌های داده سنتی ذکر کردیم، یک بخشی از آن نسبت به این نوع وجود ندارد. به‌رحال این نوع هر چند با نوع اول تفاوت دارد و یک مقداری از آن ماهیت بلاک چین و زنجیره بلوکی فاصله گرفته، اما باز با پایگاه داده سنتی متفاوت است. اینجا نکته‌ای که مهم است، این است که یک تعداد مشخصی کآن از کاربران این قدرت و اختیار را دارند که این اطلاعات و داده‌ها را تأیید کنند. دیگر اجماع و نقش همه کاربران منتفی می‌شود.

### نوع سوم

بلاک چین با مجوز یا به تعبیر دیگر خصوصی است. این قسم از بلاک چین کاملاً از نوع اول فاصله دارد و شاید برای شرکت‌ها - چه شرکت‌های مالی و اقتصادی و چه غیر آن - به خاطر اینکه نیازمند مجوز است و نظارت بیشتری روی آن اعمال می‌شود و دولت‌ها و نهادها بیشتر می‌توانند بر این فناوری و برنامه‌های مبتنی بر این فناوری نظارت کنند، مطلوب‌تر است. این شاید بگوییم یک چیزی بینابین است؛ یعنی به نوعی مثل پایگاه‌های داده سنتی است ولی در عین حال با آنها متفاوت است. من این را اشاره کردم که اگر در مواردی مشاهده کردید که این فناوری وجود دارد ولی بعضی از این مشخصه‌هایی که اشاره کردیم نیست، این منشأ سؤال و شبهه و ابهام نشود. آن چیزی که بیشتر مدنظر است و در رمز ارزها از آن استفاده می‌شود، همان نظام اطلاعاتی نوع اول است، بلاک چین نوع اول که با عنوان عمومی شناخته می‌شود.

### دو بستر رمز ارزها

مطالبی که در این باره لازم بود، اجمالاً گفتیم. البته این فناوری یک جزئیاتی دارد که شاید در بحث از چگونگی کاربرد این فناوری در تولید و استخراج رمز ارز بیشتر به آن اشاره کنیم. اصطلاحاتی وجود دارد که در ادامه بیشتر به آن خواهیم پرداخت. تا اینجا دو بستر که در آن رمز ارز تولید می‌شود را شرح دادیم؛ یک بستر فناوری و نظام اطلاعاتی بلاک چین یا زنجیره بلوکی

بود. در کنار این، ما توضیح دادیم که جنس فناوری بلاک چین از جنس نظام‌های اطلاعاتی رایانه‌ای است، یعنی یک شکل تحول یافته و متکاملی از پایگاه‌های داده سنتی است؛ به عبارت دیگر یک پایگاه داده و یک نظام اطلاعاتی و نظام جمع و پردازش اطلاعات، منتهی بسیار پیچیده؛ این خیلی مهم است که این فناوری اجماًلاً به عنوان ابزار تولید رمز ارز شناخته شود. در کنار این، ما اشاره‌ای به پلتفرم‌ها داشتیم. چون آن هم یکی از بسترهایی است که در تولید رمز ارز نیاز به آن وجود دارد. پس هر رمز ارزی که می‌خواهد تولید شود، اولاً نیازمند فناوری زنجیره بلوکی یا بلاک چین است؛ این فناوری در تمام رمز ارزها وجود دارد به عنوان شرط لازم حضور در این عرصه و در همه جا هم یکسان است. این فناوری، یک فناوری است که هر کسی که بالاخره می‌خواهد در این عرصه فعالیت کند، آن را باید به کار بگیرد. و نیز تمام رمز ارزها احتیاج به یک پلتفرم دارند، منتهی پلتفرم‌ها متفاوت‌اند. یعنی انواع سکوها و بن‌سازه‌ها برای تولید و استخراج رمز ارز هم اکنون مورد استفاده قرار می‌گیرند. شما شرکت‌های تولید خودرو را در دنیا نگاه کنید، همه اینها خودرو تولید می‌کنند؛ اما پلتفرم خودروها در شرکت‌های خودروسازی با هم متفاوت است. البته شرکت‌های خودروسازی بزرگ و نه شرکت‌های رده دوم که اینها هزینه‌های سنگینی برای ایجاد پلتفرم انجام نمی‌دهند؛ اینها از شرکت‌های بزرگتر و مهم‌تر این پلتفرم‌ها را می‌خرند ولی آنها یک تغییراتی اعمال می‌کنند؛ آن ساختار و سازه و بن سازه تولید خودرو که شامل تولید نیروی محرکه و ارتباط اجزاء اصلی یک ماشین است، اینها هم پلتفرم‌های متفاوتی دارند؛ سکوها و بن‌سازه‌های مختلفی دارند. نوع تولید نیروی محرکه خودرو در اینها متفاوت است. خودروها به ظاهر خیلی متفاوت هستند و مختصات آنها کاملاً فرق می‌کند، ولی اینها از پلتفرم بهره می‌گیرند. در مسأله رمز ارزها هم همینطور است؛ الان ده‌ها پلتفرم برای استخراج و تولید رمز ارز وجود دارد که عملکردهای اینها متفاوت است. پس رمز ارز نیازمند دو بستر مهم است: ۱. فناوری بلاک چین که در تمام رمز ارزها یکسان است. ۲. پلتفرم‌هایی که با استفاده از آن فناوری کار جمع داده و پردازش را انجام بدهند. قبلاً هم عرض کردم شما اگر به سایت‌ها و پایگاه‌های اطلاع‌رسانی که مرتبط با این موضوع هستند مراجعه کنید، آنجا می‌بینید ده‌ها پلتفرم نام می‌برند و مقایسه می‌کنند که برای اینکه به کار رمز ارز مشغول شوید، کدام پلتفرم‌ها ترجیح دارد. کسانی که در این عرصه فعالیت می‌کنند، برای جذب مشتری توصیه‌هایی به کاربران دارند؛ هم پلتفرم‌ها را معرفی می‌کنند و هم مقایسه می‌کنند که کدام یک از این پلتفرم‌ها بهتر است. ممکن است پلتفرم یک خودرو مثلاً طوری طراحی شده که استفاده بهتر و هزینه کمتر و آسیب کمتر در شرایط خاص متوجه بهره‌بردار می‌کند. در رمز ارز هم این تفاوت‌ها وجود دارد، ممکن است یک پلتفرمی نسبت به بقیه از سرعت بیشتری برخوردار باشد، چون مهم این است که آن فناوری را در یک قالب بریزند؛ آن قالبی که آن فناوری در آن استفاده می‌شود و آن سکو یا سازه‌ای که فناوری را می‌آورند آنجا و مبادرت به تولید رمز ارز می‌کنند، این خودش خیلی مهم است.

### چیستی رمز ارز

گفته شد برای رمز ارز ابتداءً نیازمند به این دو مؤلفه و دو عنصر هستیم: ۱. فناوری بلاک چین یا زنجیره بلوکی؛ ۲. پلتفرم. اکنون باید ببینیم رمز ارز چیست و ماهیت آن کدام است.

### مقدمه

در جلسات ابتدایی این بحث یک اشاره خیلی اجمالی کردم که اساساً اختلاف است؛ آیا رمز ارز پول است یا دارایی است؟ یا نه پول است و نه دارایی، هر سه احتمال قائل دارد. بعضی‌ها می‌گویند یک کالا است، برخی می‌گویند یک نوع خاصی از پول است؛ بعضی‌ها می‌گویند این نه پول است، نه کالا و نه دارایی. برای اینکه این مسأله روشن شود، توجه کنید که در فضای مجازی و در

رایانه‌ها، بازی‌های آنلاین که الان متأسفانه خیلی شایع شده و کودکان و نوجوانان و بلکه جوانان و بزرگسالان به آن آلوده شده‌اند و اوقات بسیاری را صرف این می‌کنند، گاهی یک چیزهایی را به عنوان جایزه برنده می‌شوند؛ سکه و پول در بازی مثلاً به عنوان اینکه از یک جایی عبور کرده یا کسی را از بین برده، بالاخره به هر دلیلی این سکه‌ها و پول‌ها را از آن خود می‌کنند. اما این پول یا سکه فقط در همان محدوده قابل استفاده است و با آن نه کسی می‌تواند در فضای مجازی چیزی بخرد و نه بفروشد و نه آن را مبدل به یک دارایی دیگر کند، هیچ ارزشی ندارد. ارزش این پولی که در بازی‌های رایانه‌ای بدست می‌آید، این فقط در همان بازی‌ها وجود دارد؛ در آن محدوده می‌تواند مثلاً با این پول یک چیزی را در بازی بدست بیاورد یا بفروشد یا بخرد. مثلاً در این بازی‌ها خانه و زمین می‌خرند، این غیر از متاورس است، این هیچ چیزی ندارد. رمز ارز کاملاً با این متفاوت است؛ اینطور نیست که فقط یک خیال محض باشد، اعتبار محض و بدون هیچ پشتوانه‌ای باشد؛ هر چند برخی معتقدند که این هم پشتوانه ندارد. بالاخره در مورد رمز ارز اختلاف است که این را باید در آینده معلوم کنیم که آیا پول است، کالا است یا یک دارایی است یا هیچ کدام از اینها نیست.

این را هم باید بحث کنیم که آیا ملاک‌های مالیت در فقه بر این کالا و این شیء یا دارایی یا پول منطبق می‌شود یا نه. معیارهای مالیت باید مطرح شود و بعد ارزیابی کنیم که این مالیت دارد یا نه. پول را باید ببینیم حقیقت آن چیست و بعد ببینیم آن مختصاتی که برای پول ذکر کرده‌اند، بر این شیء منطبق می‌شود یا نه. این شیء، مال، پول، کالا یا دارایی، اسمش حالا هر چه که باشد، این بالاخره یک جایی ایجاد می‌شود، در عالم واقع که نیست، این یک جایی خلق می‌شود؛ ایجاد این مال یا پول یا دارایی یا کالا، در رایانه‌ها به کمک فناوری بلاک چین و در بستر یک نوعی از پلتفرم‌ها انجام می‌شود. این چگونه است؟ یعنی مثلاً فرض کنیم کسی این پلتفرم را فراهم کرده و با این فناوری هم که بسیار فناوری پیچیده‌ای است و ابزارهای فراوانی نیاز دارد، یک مجموعه‌ای از دستگاه‌ها و کامپیوترهای فوق‌العاده قوی نیاز دارد، حالا یا به صورت عمومی و به صورت مزرعه استخراج یا استخراج، یا اینکه خیلی محدودتر، این کار انجام شود. چه اتفاقی می‌افتد و اینها چه کار می‌کنند و چه تولید می‌کنند، این مطلبی است که باید در ادامه توضیح بدهیم. چگونگی تولید یا استخراج آن باید بیان شود. البته استخراج همان تولید است و اینها با هم فرق نمی‌کنند؛ اینطور نیست که مثلاً یک جایی تولید شود و بعد عده‌ای استخراج کنند؛ لذا اصطلاح معدن را هم اینجا به کار می‌برند که یک عده کارشان معدن‌کاوی است؛ یعنی کأن یک معدنی وجود دارد و از این معدن این رمز ارزها را استخراج می‌کنند. مثل معدن طلا که طلا استخراج می‌کنند، آنجا یک چیزی مثل معدن وجود دارد که اینها را استخراج می‌کنند. این احتیاج به توضیح و بررسی بیشتر دارد که در جلسات آینده این بحث را دنبال خواهیم کرد.

«والحمد لله رب العالمین»