بسم الله الرحمن الرحیم

درس خارج فقه استاد حاج سید مجتبی نورمفیدی

موضوع کلی: فقه رمز ارزها | تاریخ: ۱۰ آبان ۱۴۰۱

موضوع جزئی: **موضوع شناسی – ماهیت رمز ارزها – بیان اجمالی – بیان تفصیلی** | **مصادف با: ۶ ربیع الثانی ۱۴۴۴**

جلسه: ۸

«الحمدلله رب العالمین و صلی الله علی محمد و آله الطاهرین و اللعن علی اعدائهم اجمعین»

ماهیت رمز ارزها

در بحث موضوع‌شناسی از رمز ارزها چند مطلب را تا اینجا به عنوان تمهید معرفت و شناخت رمز ارزها بیان کردیم. اکنون باید ببینیم اساساً خود رمز ارز چست و چه ماهیتی دارد؛ رمز ارز چگونه تولید یا استخراج می‌شود، منشأ آن کجاست. بعد آن وقت بررسی کنیم آیا این دارایی که تولید شده یا کالا یا پول، از نظر فقهی کلیه افعال مرتبط با آن چه حکمی دارد، اعم از تولید و استخراج، نگهداری، معامله با آن و همه اموری که به نوعی مرتبط با این موضوع است. من تلاش می‌کنم یک تصویر ساده و روشنی از این پدیده ارائه دهم به نحو اجمال، بعد یک مقداری این را توضیح می‌دهم. چون واقعاً شناخت این پدیده در بیان حکم شرعی آن خیلی تأثیر دارد. گاهی یک پدیده‌ای به درستی تجزیه و تحلیل نمی‌شود، لذا حکمی هم که برای آن بیان می‌شود با واقعیت آن موضوع و پدیده سازگار و منطبق نیست.

بیان اجمالی

اگر بخواهم در چند جمله این پدیده را معرفی کنم، باید بگویم رمز ارز در حقیقت یک جایزه‌ای است که به کسانی که یک مسأله بسیار پیچیده ریاضی را با محاسبات خاص حل می‌کنند و پاسخ آن را پیدا می‌کنند داده می‌شود. حالا چگونه این معادله یا مسأله که مجهولاتی دارد حل می‌شود و پاسخ داده می‌شود، چه فرآیندی طی می‌کند را توضیح خواهیم داد. آنچه که به ازای تلاش برای حل این معادله پیچیده ریاضی آن هم به عنوان جایزه به افراد داده می‌شود، رمز ارز است، حالا یا بیت‌کوین یا رمز ارزهای دیگر. در آن واحد ممکن است ده‌ها هزار نفر در حال حل این معادله باشند، اما آن کسی که توانمندی بیشتری چه از حیث امکانات سخت افزاری و چه از جهت نرم‌افزاری دارد و زودتر این معادله را حل کند، این جایزه را از آن خود کرده است. لذا یک رقابت سنگینی در این جهت شکل گرفته که در عرصه‌های مختلف، زمان حل این مسأله را کوتاه‌تر کنند و البته این باید به تأیید برسد و امضا شود؛ وقتی که تأیید و امضا شد، آن جوایز یا آن رمز ارزها که یک میزان مشخصی هم دارد، به آن شخص تعلق می‌گیرد. این یک بیان بسیار ساده و کوتاه و مجمل از حقیقت رمز ارز است.

البته سؤالات و ابهامات مختلفی در اینجا مطرح است که باید آنها را بیان کنیم. اینکه اساساً از کجا شروع می‌شود، این معادله کجاست هست، چه کارهایی باید انجام شود تا این معادله حل شود، چگونه باید به تأیید دیگران برسد؟ بعد که این پول به او تعلق می‌گیرد، در کجا نگهداری می‌شود و چگونه این را خرج می‌کند؟ اینها همه اموری است که باید در اینجا توضیح دهیم. این توضیح اجمالی را من بیان کردم تا آن را بسط بدهم و خیلی خلاصه با مراحل و فرآیندهای استخراج رمز ارز آشنا شویم.

بیان تفصیلی

همانطور که قبلاً گفتم، رمز ارزها همگی از یک فناوری به نام زنجیره بلوکی یا بلاک چین استفاده می‌کنند؛ البته خود بلاک

چین‌ها هم انواعی دارند، ولی اصول و رئوس این فناوری در همه اینها مشترک است؛ تفاوت آن را هم با پایگاه داده سنتی ذکر کردیم. اولین گام برای استخراج رمز ارز، پیوستن به این زنجیره است؛ یعنی یک بلوکی برای کسی که می‌خواهد وارد این فعالیت شود باید ایجاد شود یا اضافه شود، چون طبق فناوری بلاک چین یک دفتر کل وجود دارد که همه تراکنش‌ها و مبادلات اطلاعاتی در آن ثبت می‌شود. شما از کلمه تراکنش ذهنتان به سمت تراکنش مالی نرود، چون عمدتاً این اصطلاح را در تبادل اطلاعات مالی به کار می‌برند؛ اینکه مثلاً این صد تومان را او به حساب واریز کرد، آن دویست تومان به حساب او واریز کرد، ممکن است یک نفر در حساب بانکی خودش از صبح تا شب دو تا تراکنش داشته باشد، یعنی دو تا مبادله داشته باشد، یا ممکن است بیست تا یا صدتا باشد. این تراکنش و مبادله فقط در مسائل مالی نیست؛ اگر دو نفر برای هم پیام بفرستند، سلام کنند و دیگری جواب بدهد و بعد درباره یک موضوعی گفتگو کنند، این هم یک تراکنش است. هر نوع مبادله اطلاعات در این فضا یک تراکنش است. لذا همانطور که قبلاً گفتم تراکنش‌های بلاک چین می‌تواند در امور مختلف باشد؛ فقط در حوزه رمز ارز و مسائل مالی نیست. در خدمات به مشتری، زنجیره تأمین نیازهای مشتریان، در حوزه سلامت و پزشکی، در خیلی از امور این فناوری مورد استفاده قرار می‌گیرند، هر چند یک امر جدیدی است؛ یعنی اینقدر مهم است که این را یکی از انقلاب‌ها در این حوزه دانسته‌اند. یعنی اگر مثلاً ما بخواهیم تمام فعل و انفعالات مهم که نقطه عطف در حوزه فناوری دیجیتال است را به پنج یا شش نقطه و مرحله تقسیم کنیم، قطعاً آخرین آن همین است؛ لذا از آن به عنوان یک انقلاب نام می‌برند. همانطور که اینترنت یک انقلاب بود؛ همانطور که ایجاد و اختراع رایانه‌های شخصی یک انقلاب بود. اولین گام این بود که این رایانه را اختراع کردند، آن موقع شخصی بودن معنا نداشت؛ اما به سرعت آن دستگاه تبدیل شد به یک دستگاه قابل استفاده برای هر شخص. بعد اینترنت وارد این عرصه شد، بعد شبکه‌های اجتماعی؛ خود شبکه‌های اجتماعی یک انقلاب در این عرصه بود. اما به طور حتم آخرین انقلاب یا نقطه عطف در عرصه فضای دیجیتال، این فناوری است که تازه چند سالی است دارد مورد استفاده قرار می‌گیرند.

اولین کار برای پیوستن به آن زنجیره، ایجاد یک بلوک یا اضافه کردن یک بلوکی است که حکم یک ورقی است که به آن دفتر کل اضافه می‌شود؛ یک صفحه کأن به دفتر کل اضافه می‌شود. کسی که یک بلاک را ایجاد می‌کنند یا مجموعه‌ای از تراکنش‌ها را در یک بسته یا فایلی قرار می‌دهد و به آن مجموعه اضافه می‌کند اولین گام است. یک بلوکی را باید ایجاد کند؛ اینکه این بلاک یا به تعبیر ساده این صفحه چطور اضافه می‌شود و چه فرآیندی طی می‌کند، این خودش یک روند پیچیده‌ای دارد.

اگر کسی بخواهد یک بلاک اضافه کند در درجه اول باید یک آدرسی را برای خودش داشته باشد؛ خود آدرس هم باید ساخته شود. ساختن آدرس کار سختی نیست و خیلی هم نیاز به زمان ندارد؛ اما برای اینکه به آن شبکه متصل شود، این آدرس باید ایجاد شود. این آدرس هم دو قسم است؛ یک آدرس عمومی دارد و یک آدرس خصوصی. این آدرس عمومی و خصوصی را تشبیه می‌کنند به شماره و رمز کارت‌های اعتباری که همگان برای مبادلات پولی استفاده می‌کنند. کارت‌ها یک شماره‌ای دارند که ما این شماره را در اختیار همه قرار می‌دهیم؛ آن شماره یک آدرس عمومی است که در اختیار دیگران قرار می‌گیرد تا بتوانند پول به آن واریز کنند. اما یک آدرس و نشانه خصوصی دارد که همان رمزی است که در اختیار شماست. هر بلاکی یک آدرس عمومی باید داشته باشد و یک آدرس خصوصی؛ این باید در درجه اول ایجاد شود. این بلاک در حقیقت یک صفحه (به اعتبار اینکه زنجیره بلوکی را به یک دفتر کل تشبیه کردیم) یا فضای محدودی است که ایجاد شده و همه تراکنش‌ها از صفر تا صد در آن منعکس می‌شود. اگر این مبادلات و تراکنش‌ها در حوزه رمز ارز باشد، طبیعتاً در این عرصه این اتصال برقرار می‌شود؛ ممکن

است این در عرصه‌های دیگر اتفاق بیفتد. این درخواست با امضاء شخص در شبکه ارسال می‌شود و صحت درخواست مورد تأیید قرار می‌گیرد؛ اینکه درخواست می‌شود، این ممکن است انتقال پول یا ارز باشد یا یک متن. فرض کنید شما می‌خواهید به شخصی سلام کنید، این توسط شما ارسال می‌شود، منتهی ارسال این درخواست به صورت یک متن قابل مشاهده برای همگان نیست. شما وقتی می‌خواهید برای کسی ایمیل بفرستید، این ایمیل ممکن است متضمن یک پیام یا یک جمله یا یک سؤال باشد؛ وقتی این را شما ارسال می‌کنید با آن آدرسی که دارید، طرف مقابل این را می‌بیند بدون اینکه بخواهد عملیات خاصی روی آن انجام دهد. اما در این سیستم آن چیزی که شما درخواست می‌دهید یا اطلاعاتی که در آن فضا ارسال می‌کنید، تماماً به صورت رمز و عدد است. اگر بخواهم تشبیه کنم، کسانی که جاسوس هستند و در محیطی جاسوسی می‌کنند، اطلاعاتی که می‌خواهند به مرکز خودشان ارسال کنند، نمی‌آیند عیان و آشکار همه آن مطالب را به مرکز ارسال کنند؛ چون بالاخره در معرض دید دیگران یا نفوذ دیگران می‌تواند قرار گیرد. لذا با یک سری اعداد و رمزها که صرفاً توسط خود آنها قابل خوانش است، ارسال می‌شود. اینجا در سیستم بلاک چین اطلاعات و آن چیزهایی که می‌خواهد مبادله شود، تماماً به صورت رمز و عدد است؛ یعنی من و شما ممکن است این رمزها و اعداد را ببینیم، کاملاً یک چیز بی‌معنا به نظر برسد.

وقتی این رمزها یا اعداد و حروف به آن مجموعه ارسال می‌شود، باید کاری انجام شود که رمزگشایی شود؛ یعنی رسیدن از این اعداد و رمزها به محتوای آن پیام و اطلاعات کار بسیار سختی است. شما مثلاً ممکن است در این بلاکی که ایجاد کردید، یک جمله‌ای را نوشته باشید، مثل سلام و احوالپرسی؛ اما وقتی این در شبکه قرار می‌گیرند، برای اینکه دیگران بفهمند که شما چه نوشته‌اید، یعنی آن اعداد و حروف را تبدیل کنند به سلام و احوالپرسی، این بسیار کار سختی است. مهم‌ترین قسمت کار اینجاست، یعنی تبدیل رمزها و اعداد و حروف به محتوای قابل فهم برای شما. این نیاز به محاسبات بسیار فراوان دارد؛ نیاز به پردازش‌های سخت و مشکل دارد که این به وسیله دستگاه‌هایی که یک مجموعه‌ای از کامپیوترهای به هم متصل شده است انجام می‌شود؛ به دستگاه‌هایی که این رمزگشایی را انجام می‌دهند، «ماینر» می‌گویند. ماینینگ یعنی همین عملیات رمزگشایی؛ ماینر هم به کسی که این کار را انجام می‌دهد گفته می‌شود و هم به دستگاه‌هایی که در صدد حل این معما هستند. این معما چیست؟ تبدیل آن اعداد و رمزها به چیزهایی که قابل فهم باشد. این رمزگشایی مهم‌ترین قسمت این کار است.

پس در درجه اول یک بلاکی باید تأسیس شود، یک ورقی به آن دفتر کل اضافه شود و یک سری پیام‌ها و اطلاعات در آن قرار بگیرد، تراکنش‌هایی در آن ثبت شود؛ آنگاه وقتی تمام آن شبکه، آنهایی که در این زنجیره فعالیت دارند، این بلاک را ببینند و اطلاعات آن را تأیید کنند، اینجاست که آن جایزه‌ای که گفتیم اختصاص داده می‌شود. بنابراین در درجه اول باید این بلاک و این فضا و بسته، به آن زنجیره اضافه شود و آن معادله حل شود. حالا آن معادله از کجا در اختیار قرار می‌گیرد؟ از ناحیه خود شبکه این معادله کأن در معرض دید همگان قرار می‌گیرد و یکباره همه تلاش می‌کنند به کشف این رموز برای حل این معادله و برای اینکه این مسأله پیچیده ریاضی را حل کنند، بعد از اینکه این معادله حل شد و این رمزنگاری‌ها کشف شد، اولین مجموعه‌ای که رمزگشایی می‌کند، به او جایزه تعلق می‌گیرد.

حال این رمزگشایی چگونه صورت می‌گیرد؟ این با استفاده از یک نرم افزار که اصطلاحاً به آن هش می‌گویند؛ هش در حقیقت تأیید حل مسأله و کشف آن رموز است؛ هش در واقع مثل اثر انگشتی است که در فضای دیجیتال اتفاق می‌افتد. به طور طبیعی برای تطبیق اینکه یک نامه و درخواست مربوط به یک شخص است، در فضای غیر دیجیتال و در فضای واقعی با اثر انگشت

این انطباق صورت می‌گیرد. یعنی معلوم می‌شود این نوشته و این درخواست یا متن متعلق به این شخص است. اینها را برای تقریب ذهن عرض می‌کنم. چنین کاری در فضای دیجیتال صورت می‌گیرد که تأیید می‌کند که این مربوط به این شخص و درست است. هش نقش اساسی و مهمی در ماجرای استخراج ارزها دارد. اگر این صفحه و این بلاک که به آن زنجیره اضافه می‌شود معتبر نباشد، و مورد تأیید قرار نگیرد، تمام زنجیره‌های بعدی را هم خراب می‌کند؛ مثل این است که یک بنایی را بسازند، پایه‌هایی را برای آن قرار بدهند و بعد هر کجای این پایه اشکال داشته باشد، باید دوباره همه آنچه که روی آن قرار داده‌اند خراب کنند و از نو بسازند. لذا یک دقت و وسواس بر همه حکم‌فرماست که آن بلاکی که اضافه شده، این صفحه‌ای که اضافه شده، معتبر باشد و به تأیید همگان برسد. اشاره کردم یک برنامه و الگوریتمی به نام الگوریتم اثبات کار یا الگوریتم اجماع وجود دارد که به صورت مرحله به مرحله و گام به گام این را به تأیید همگان می‌رساند. یک تلاش جدی وجود دارد برای اعتبار این بلاک و اطلاعات و تراکنش‌هایی که در آن وجود دارد.

در بلاک‌ها آدرس یا هدر بلاک مهم‌ترین رکن است؛ باید آدرس و نشانی از این بلاک ارائه دهند قبل از اینکه تراکنشی در آن ثبت شود. هر هدر بلاک یا آدرسی که در ابتدای امر قبل از ثبت هر تراکنش ایجاد می‌شود، چند جزء و رکن دارد. چند کار باید در این مرحله انجام شود.

۱. یکی اینکه آن نسخه پروتکلی که می‌خواهد از آن استفاده کند، آنجا بگذارد و این نسخه را همه ببینند؛ ببینند از چه نسخه‌ای برای این کار دارد استفاده می‌کند. این حتماً باید انجام شود؛ اصل آن برنامه و نسخه باید آنجا گذاشته شود که دیگران ببینند.

۲. هشی که در بلاک قبلی بوده، در این بلاک هم ثبت شود؛ آن تأییدیه‌ای که در بلاک قبل بوده، اینجا هم ثبت شود.

۳. مجموع تراکنش‌های موجود در آن بلاک را بتواند هش‌گیری کند؛ هش در واقع عبارت است از خلاصه کردن و جمع کردن. عرض کردم که مثلاً می‌خواهید اطلاعاتی را برای شخصی بفرستید، این اطلاعات به صورت آشکار و عیان فرستاده نمی‌شود. این را باید داخل یک قالبی تبدیل به هش کنید، امضا و تأیید کنید، این هش همان رمزهاست که وقتی به دست دیگری می‌رسد، او هم باید اینها را باز کند.

۴. ثبت زمان؛ یعنی باید در آنجا ثبت شود که این هش بلاک در چه زمانی ثبت شده است.

۵. تارگت یا هدف؛ وقتی که یک بلاک جدید را می‌خواهد تأیید کند، یک عددی را شبکه به این ماینر می‌دهد و این ماینر یک هش پیدا می‌کند که با استفاده از آن هش که باید مساوی یا کمتر از آن عدد باشد، آن بلاک استخراج شده تلقی می‌شود.

۶. آخرین جزئی که اینجا لازم است، یک عددی است که به آن عدد نانس می‌گویند. این عدد باید توسط فعالان این حوزه، معدن‌کارها و ماینرها حدس زده شود؛ یعنی اطلاعات که می‌آید، تراکنش‌ها، آن هش‌ها، وقتی اینها با هم منتقل می‌شود، باید یک عددی حدس زده شود که اگر آن عدد به این اطلاعات اضافه شود، یک هش و عددی از آن بدست می‌آید که این آخرین مرحله است و بعد از آن است که این جایزه در اختیار این شخص قرار می‌گیرد و این بسیار کار مشکل و سختی است.

گفتیم رمزگشایی مهم‌ترین کاری است که در این عرصه باید انجام شود؛ منتهی این رمزگشایی در کدام مرحله و در چه مقطعی است؟ این طبیعتاً نیاز به تحلیل دارد.

البته من خیلی خلاصه و تا حدی مبهم و مجمل این مسأله را بیان کردم؛ در حد نیم ساعت و آن هم با این اصطلاحات و پیچیدگی‌هایی که این مسأله دارد و لذا کار ساده‌ای نیست. من سعی کردم خیلی خلاصه یک توضیح اجمالی بدهم. آنچه که لازم

است از این مسأله در ذهن شما نقش ببندد این است که حقیقت رمز ارز و تولید و استخراج آن عبارت است از جایزه‌ای که به خاطر تلاش برای حل یک مسأله و معادله بسیار پیچیده ریاضی به شما می‌دهند. جایزه‌ای که به جهت حل یک معادله پیچیده ریاضی و گشودن رمزها داده می‌شود. همیشه این کار استخراجی نیست؛ ممکن است کسی پول بدهد و بیت‌کوین و رمز ارز بخرد، کالا بدهد و رمز ارز بگیرد. پس ما یک استخراج و تولید رمز ارز داریم که من اجمالاً توضیح دادم؛ یک رمز ارزی هم هست که به این شکل تهیه می‌شود، یک کسی خودش این دارایی را استخراج می‌کند و یک کسی هم چیزی را می‌دهد و این را از دیگری می‌گیرد.

«والحمد لله رب العالمین»