بسم الله الرحمن الرحیم

موضوع کلی: فقه رمز ارزها تاریخ: ۱۱ آبان ۱۴۰۱

موضوع جزئی: موضوع شناسی – ماهیت رمز ارزها – منشأ معادله‌ها در شبکه – کیف پول – ابزارهای استخراج – انواع استخراج مصادف با: ۷ ربیع الثانی ۱۴۴۴

جلسه: ۹

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

خلاصه جلسه گذشته

بحث در بیان حقیقت و ماهیت رمز ارزها بود؛ عرض شد که رمز ارز در حقیقت یک جایزه‌ای است که به پاداش حل یک مسأله ریاضی که باید با محاسبات پیچیده این کار انجام شود، به کسی که این عملیات را انجام می‌دهد پرداخت می‌کنند. درباره فرآیند حل این معادله و این مسأله در حدی که فرصت اقتضا می‌کرد توضیحاتی داده شد.

منشأ معادله‌ها و معماها در شبکه

سؤالی که در جلسه گذشته مطرح شد این بود که این معادله و این مسأله یا معما چگونه در این شبکه قرار می‌گیرد و از کجا این معما در درون شبکه گذاشته می‌شود که هزاران نفر به وسیله ابزارهای لازم، در صدد حل آن برمی‌آیند. این معما یا مسأله در واقع از ناحیه متصدیان آن رمز ارز در درون شبکه گذاشته می‌شود. الان هر یک از این رمز ارزها یک سازمان مرکزی دارند که تعداد زیادی نیروهای فنی آنجا مشغول کار هستند؛ طبیعتاً اهدافی را برای این کار در نظر می‌گیرند و مخصوصاً در این زمان، بعد از هفت هشت سال که رغبت مردم به رمز ارزها بیشتر شده، این هدف روشن‌تر است. شاید در آغاز کار که آن فرد که به نامی شهرت پیدا کرده ولی همگان در این نام تردید می‌کنند، چنین چیزی را پیش‌بینی نمی‌کرد؛ در آغاز کار یا یک فرد یا یک گروه وقتی به این شکل وارد عرصه شدند و این معما یا مسأله در شبکه مجازی قرار گرفت، خود طراحان هم گمان نمی‌کردند که چنین روزی فرا برسد. مثلاً آن موقع دو هزار بیت کوین شاید به اندازه یک دلار یا چند دلار ارزش داشت، ولی امروز به جایی رسیده که تا همین چند ماه پیش یک بیت‌کوین قیمتی حدود ۶۹ هزار دلار داشت؛ الان رمز ارزها سقوط کرده‌اند، ولی باز هم در مقایسه با روزهای اول، اساساً قابل مقایسه نیست. آن موقع که این معما و مسأله در این قالب وارد عرصه فضای مجازی شد، شاید ضرورتی حس نمی‌شد یا خیلی هدف روشنی برای این امر نمی‌شد تعریف کرد؛ اما الان کاملاً می‌توانیم تصویر کنیم که یک جمع معتنابه بنشینند و این مسائل و معماها را در فضای مجازی قرار دهند و یک جنب و جوشی برای تولید رمز ارز و استخراج آن ایجاد شود. پس این مسأله و معادله به این ترتیب از ناحیه متصدیان آن رمز ارز در درون شبکه قرار می‌گیرد؛ مثلاً بیت‌کوین الان یک سازمانی دارد با ده‌ها کارمند؛ یا اتریوم یک سازمانی دارد که شاید صدها نیروی فنی در آنجا مشغول کار هستند.

کیف پول

یک مسأله مهمی که در اینجا باید مورد توجه قرار گیرد و در جلسه گذشته به آن اشاره داشتیم، این است که بالاخره این رمز ارزهای تولید شده یا استخراج شده، کجا قرار می‌گیرند؟ کسی که به عنوان پاداش و کارمزد یک مقداری بیت‌کوین یا اتریوم یا انواع دیگر رمز ارز را بدست می‌آورد، کجا آن را نگهداری می‌کند؟ یک اصطلاحی دارند به نام کیف پول؛ کیف پول در حقیقت

یک نرم افزاری است که خود آنها در درون این پلتفرم طراحی کرده‌اند که آنچه که به عنوان پاداش به معدن‌کاوان داده می‌شود، آن را در این نرم افزار حفظ می‌کنند؛ مثل یک گاوصندوق که در فضای واقعی کسی اشیاء قیمتی را در آن نگهداری می‌کند یا صندوقچه‌ای که ممکن است پول را مثلاً در آن قرار دهد، این حکم همان محفظه را دارد، این کیف پول رمزهایی دارد (مثل رمز کارت‌های اعتباری ولی با این تفاوت که رمز کیف پول غالباً از دوازده یا بیست‌وچهار کلمه لاتین تشکیل شده که باید براساس ترتیبی که در همان ابتدا کیف پول ارائه می‌کند، وارد شود) که با آن می‌تواند وارد شود و هر تصرفی می‌خواهد انجام دهد، آن را انجام دهد. آن آدرس عمومی یا خصوصی یا به تعبیر دیگر کلید عمومی و کلید خصوصی، برای استفاده از این کیف پول بسیار تعیین کننده است؛ این آدرس عمومی به دیگران داده می‌شود تا دیگران بتوانند به این کیف واریز داشته باشند. رمز برای این است که خودش بتواند در این دارایی که در کیف پول وجود دارد تصرف کند و اگر این رمز فراموش شود، هیچ کسی توان بازگرداندن آن را ندارد. آدرس عمومی و کلید عمومی می‌تواند در اختیار همگان قرار گیرد، اما این کلید یا آدرس خصوصی فقط در اختیار خود این شخص است؛ اگر این شخص این رمز را به کسی نگفته باشد، جایی مکتوب نکرده باشد و آن را فراموش کند، دیگر امکان بازیابی نیست و تمام آنچه که اندوخته، همه از بین می‌رود. گرچه سطح ایمنی فناوری به کار رفته در مورد رمز ارزها بسیار بالاست، اما اگر به هر دلیلی ولو در یک احتمال بسیار ضعیف کسی این رمز را بدست بیاورد، به راحتی می‌تواند همه آنچه که او اندوخته، برداشت کند و وارد کیف پول خود کند. به هر حال این کیف پول سند مالکیت کسی است که این دارایی به او داده شده است.

اگر بخواهیم برای تقریب بیشتر به ذهن، مسأله رمز ارزها و کیفیت استخراج آنها را بیان کنیم، این کار را به معدن کاوی تشبیه می‌کنند، لذا به کسانی که به دنبال استخراج رمز ارز هستند، معدن‌کاو می‌گویند. شما یک معدن طلا را در نظر بگیرید، فرض کنید این معدن واجد طلاهایی است؛ مالک معدن به اشخاص و کارگران اعلام می‌کند که شما به هر میزان که از این طلاها استخراج کنید، من به شما کارمزد می‌دهم. این البته از یک جهت این فرآیند را در ذهن روشن می‌کند ولی در عین حال یک تفاوت‌های اساسی با مسأله معدن دارد؛ چون آنجا یک چیزی موجود است و آنها این را استخراج می‌کنند و ارائه می‌دهند؛ اینجا متناسب با فضای مجازی، کاربران وارد می‌شوند و این را در حقیقت تولید می‌کنند و در درون شبکه همه می‌فهمند که این مقدار رمز ارز تولید شده است.

البته لازم است به این نکته هم اشاره کنم که برنامه رمز ارزها به گونه‌ای تنظیم شده که یک سقفی برای آنها در نظر گرفته‌اند؛ لذا پاداش‌هایی که برای حل آن معادله داده می‌شود، اینطور نیست که همینطور به صورت فزاینده زیاد شود. مثلاً در مورد بیت‌کوین به ازای ثبت یک بلاک و اضافه کردن بلاک، یک مقداری به مجموع بیت‌کوین‌ها اضافه می‌شود؛ اما وقتی چهار سال شد، این نصف می‌شود. این مقدار پاداش و آن چیزی که به این سبب اختراع می‌شود نصف می‌شود. ممکن است بگویید این چطور انگیزه برای کاوش و استخراج ایجاد می‌کند؟ به هرحال چون ارزش و اعتبار این رمز ارزها روز به روز در حال بالاتر رفتن است، قهراً پاداش و کارمزدی که به معدن‌کاوان داده می‌شود، اگرچه کمتر می‌شود اما ارزش آن از آنچه که در گذشته دریافت می‌کرد، بیشتر است. مثلاً می‌گویند آن اوایل کسی که این معادله را حل می‌کرد، به ازای اضافه کردن یک بلاک، پنجاه بیت‌کوین تولید می‌شد و به مجموع بیت‌کوین‌ها اضافه می‌شد. بعد از مدتی به ۲۵ رسید و بعد شد ۱۲,۵ و الان هم نصف شده و حدود شش و خرده‌ای بیت‌کوین برای اضافه کردن یک بلاک و حل آن مسأله و معادله داده می‌شود. هم کارمزد پایین آمده و هم برای مجموع آن رمز

ارزی که تولید می‌شود، یک سقف گذاشته‌اند. الان مثلاً در بازار پولی دنیا اختیار انتشار پول بدست نهادها یا بانک‌های مرکزی که در کنترل دولت‌ها هستند صورت می‌گیرد. گاهی پول بی‌پشتوانه نشر می‌دهند، حالا ما درباره پول و ماهیت آن بعداً صحبت می‌کنیم تا ببینیم آن تعریفی که برای پول ارائه کردند، بر این رمز ارزها قابل انطباق هست یا نیست. اما سقفی برای آن وجود ندارد و برای نشر آن هم محدودیتی نیست. اما در رمز ارزها سقف پولی که تولید می‌شود یک حدی دارد. شاید برای این است که تولید بیش از حد، اختصاص بیش از حد پاداش به مستخرجان و کاربران، در نهایت باعث کاهش ارزش و اعتبار بیت‌کوین نشود.

ابزارهای استخراج

مطلب دیگری که اینجا لازم است به آن اشاره کنیم، این است که استخراج رمز ارز توسط سخت‌افزار و نرم افزار صورت می‌گیرد. یعنی اینطور نیست که یک شخص پای دستگاه بنشیند و مثل سایر مواردی که یک مسأله و معمایی را حل می‌کند، خودش به این کار مبادرت کند؛ این چنین نیست که قائم به یک شخص و هوش و نبوغ او باشد. البته تجربه و نوع نرم افزار یا سخت‌افزار خیلی می‌تواند مؤثر باشد. من برای اینکه تشبیه کنم مثل ابزارهایی است که برای قمار امروز در دنیا وجود دارد و عده‌ای می‌روند پول خرج می‌کنند و از این ابزارها گاهی سودهای کلانی نصیب آنها می‌شود. در قمار مسأله شانس و تصادف واقعاً بسیار مهم است؛ اما تجربه افراد هم به آنها کمک می‌کند، اما اساس آن بر مسأله تصادف استوار است. در اینجا هم کشف آن راه‌حل و پیدا کردن جواب آن مسأله و معما، عمدتاً به کمک تجهیزات انجام می‌شود. ما وقتی می‌گوییم تجهیزات، یک بخشی از آن نرم افزار است. اوایل به کمک نرم‌افزارها در کامپیوترهای شخصی می‌توانستند این کار را انجام دهند، اما الان به جایی رسیده که خود متصدیان امر رمز ارزها ماینرهایی را اختراع کرده‌اند که کارشان فقط استخراج رمز ارز است. یعنی دستگاه‌های مخصوصی است، دستگاه که می‌گوییم یعنی یک مجموعه و زنجیره‌ای از دستگاه‌های پردازش با قدرت فوق العاده و سرعت بسیار، یعنی کسی یک جایی ممکن است تعداد زیادی از اینها را قرار دهد و این دستگاه‌ها خودشان شروع می‌کنند به انجام عملیات. اینها مثلاً یک عددی را باید کشف کنند، در میان هزاران و صدها هزار عدد و مسأله کسی ممکن است تصادفاً به آن عدد برسد؛ یک کسی زودتر یا کسی دیرتر برسد. اما این دستگاه‌ها را اختراع کرده‌اند، و هر چه زمان می‌گذرد این دستگاه‌ها پیشرفته‌تر می‌شود و مورد استفاده قرار می‌گیرد.

استخراج از طریق سخت‌افزار، آن هم سخت‌افزارهای مخصوص در شرایط فعلی بیشتر به خاطر رشدی است که فناوری بلاک چین پیدا کرده است؛ یعنی این فناوری نسبت به هشت سال قبل خیلی متفاوت و کامل شده است. امروز کسی نمی‌تواند با کامپیوترهای شخصی مبادرت به عملیات استخراج کنند، در حالی که هفت سال پیش این امکان وجود داشت؛ سرعت پیشرفت این فناوری و برنامه‌های مرتبط با آن به حدی زیاد شده که کسی با کامپیوتر شخصی نمی‌تواند این کار را انجام دهد؛ یک مجموعه‌ای با یک توان محاسباتی بسیار قوی لازم است تا آن معادله هش را حل کنند؛ هش یک عددی است که باعث ایجاد یک بلاک جدید و ثبت تراکنش در شبکه می‌شود. براساس حساب احتمالات ممکن است میلیون‌ها احتمال برای کشف آن عدد باشد، این عددها به صورت احتمال ارائه می‌گردند تا با آن عددی که پاسخ آن معادله محسوب می‌شود، منطبق شود.

انواع استخراج

الان چیزی که برای استخراج این ارزها بیشتر مورد استفاده قرار می‌گیرد، استخرهای استخراج هستند؛ منظور از استخر ماینینگ

تعدادی از ماینرها هستند که با ترکیب توان محاسباتی خودشان، یک توان قوی‌تری را ایجاد می‌کنند تا هش مورد نظر را کشف کنند و پاداش بگیرند. این ماینرها یا این سخت‌افزارها می‌توانند یک جا مجتمع شوند و می‌توانند در نقاط مختلف با هم اتصال و ارتباط برقرار کنند. اگر این کار به صورت گروهی انجام شود، از ارتباط و اتصال چند ماینر این محاسبه صورت بگیرد، طبیعتاً آن پاداشی که به افراد داده می‌شود، به نسبت تقسیم می‌شود. چون همه اینها با توجه به سرمایه‌گذاری که کردند، در کشف این معادله سهیم هستند و لذا باید پاداش به نسبت بین اینها تقسیم شود.

اینجا یک مقایسه‌هایی هم صورت می‌گیرد که کدام یک از این روش‌ها بهتر است؛ گاهی ممکن است کسی شخصاً به یک استخر متصل شود، خودش را انفرادی ببرد داخل یک مجموعه، یک کسی ممکن است خودش توان این را داشته باشد یک استخر استخراج درست کند. استخر استخراج در واقع آن مجموعه‌ای از این دستگاه‌ها هستند که با هم ترکیب شده‌اند و به دنبال کشف این معادله هستند. البته مزرعه استخراج هم داریم که در واقع آن مرکز عملیاتی استخراج رمز ارز است. یعنی آن مکانی که برای استخراج رمز ارزها آماده و مجهز شده باشد، به آن مکان مزرعه می‌گویند. این طبیعتاً با استخر متفاوت است؛ مزرعه‌های استخراج در حقیقت سالن‌هایی هستند که این دستگاه‌ها را در آن قرار می‌دهند. وقتی می‌گویند مزرعه استخراج، مثلاً یک سالن بزرگ را پر کرده‌اند از تعداد زیادی سخت‌افزار و سرورهایی که این وظیفه را به عهده دارند. شما همین اواخر شاید در اخبار شنیده‌اید که یک مزرعه استخراج کشف شد یا چینی‌ها در ایران مزارع استخراج رمز ارز ایجاد کرده‌اند، یعنی مکان‌هایی را با امکانات و ابزارهای لازم و پر از ماینرهایی که آنها به کار استخراج و محاسبه برای کشف مجهول در معادله مبادرت می‌کنند. استخراج به صورت استخری آن هم با کمک سخت‌افزارهای پیشرفته، امری است که الان متداول شده است.

پس ما یک استخراجی داریم که به وسیله نرم افزار صورت می‌گیرد که البته این دیگر تقریباً شاید منسوخ شده باشد؛ یک استخر استخراج داریم که توضیح دادم کیفیت استخراج در استخر چگونه است. یک استخراج ابری هم داریم که یک نوع برون سپاری کار محاسبه به دنیای استخراج رمز ارز است. یعنی کسی به جای اینکه خودش بیاید دستگاه‌های گران قیمت را بخرد و یک استخری را ایجاد کند، می‌رود با کسانی که این امکانات را دارند صحبت می‌کند و قدرت محاسباتی مورد نیاز خودش را از آن شرکت‌ها اجاره می‌کند. خودش این امکانات را ندارد، ولی از امکاناتی که آنها برای این منظور فراهم کرده‌اند، از طریق اجاره استفاده می‌کند. این طبیعتاً از یک جهت مؤونه‌های استخراج را کم می‌کند، هزینه‌ای برای خرید این دستگاه‌ها لازم نیست بدهد، هزینه‌ای برای برق لازم نیست بدهد، چون برق یکی از گران‌ترین اموری است که برای استخراج ارز لازم است. برقی که این دستگاه‌ها مصرف می‌کنند وقتی که با هم ترکیب می‌شوند، فوق العاده زیاد است. در قطعی برق تابستان گذشته، یکی از ادله‌ای که می‌آوردند که حالا البته اینقدر نبود که باعث خاموشی شود، ولی یکی از چیزهایی که بیان می‌شد از ناحیه برخی، کثرت فعالیت مزارع استخراج رمز ارز بود؛ چون فوق العاده برق مصرف می‌کنند و طبیعتاً کسی که با اجاره این توان محاسباتی وارد این فضا می‌شود، هزینه‌های کمتری می‌کند اما از آن طرف سود و پاداش او کمتر است. درست است که هزینه برق نمی‌خواهد بدهد، هزینه این دستگاه‌ها را نمی‌دهد، اما از آن طرف سود کمتری هم نصیب او می‌شود و البته زمینه کلاهبرداری هم زیاد است؛ بسیاری از شرکت‌ها در دنیا هستند که به عنوان اینکه از این دستگاه‌ها دارند، با افراد قرارداد می‌بندند اما بعداً معلوم می‌شود که چیزی نیست و کلاهبرداری است و پول‌های مردم را از بین می‌برند.

هر کدام از این روش‌ها مزایا و خطراتی دارد، اما اجمالاً این کار به این شکل انجام می‌شود؛ اگر بخواهیم یک به یک این

دستگاه‌هایی که با آنها مبادرت به استخراج می‌کنند توضیح دهیم، هم زمان می‌برد و هم ضرورتی ندارد؛ ما کار نداریم که این دستگاه‌ها چگونه محاسبه می‌کنند و پاسخ را بدست می‌آورند، اینها بحث‌های تخصصی است. اجمالاً شما اینجا با چیستی رمز ارز و ماهیت آن یک آشنایی اجمالی پیدا کردید؛ حالا با ملاحظه این امر، باید وارد بحث شویم.

سؤال:

استاد: منفعت و منافع فراوانی اینها دارند؛ .... اینجا باید از چند منظر این را بررسی کنیم؛ آنها عناوین ثانوی است، باید ببینیم از نظر عناوین اولی اصلاً این پول است، اصلاً مالیت دارد، آیا قمار است؛ حرام است به خاطر اینکه قمار است. .... کفر و استکبار و جاسوسی اینها بحث‌هایی که تحت عنوان ثانوی مطرح می‌شود؛ ما در درجه اول باید به عنوان اولی ببینیم چه حکمی دارد. اصلاً فرض کنیم که سازنده و همه چیز آن مسلمان است، دست استکبار هم نیست، در ایران بانک مرکزی رمز ریال، یعنی رمز ارز ریالی می‌خواهند درست کنند، حالا من نمی‌دانم در چه مرحله‌ای است ولی گفته‌اند این دارد راه‌اندازی می‌شود در داخل کشور. فرض کنیم اینجا دارد درست می‌شود؛ پس اینکه این تولید استکبار جهانی است را فعلاً مطرح نکنیم.

«والحمد لله رب العالمین»