



تقریرات دروس خارج فقه

حضرت آیت الله سید محمد رضا مدرّسی طباطبائی یزدی (دامت برکاته)

سال تحصیلی ۱۴۰۰-۱۳۹۹

جلسه پنجاهم؛ سه شنبه ۱۳۹۹/۹/۲۵ (فقه معاصر - جلسه هشتم)

توضیح اصطلاح حمله پنجاه و یک درصدی

یک مسئله مهم در بیت کوین وجود دارد که خیلی ها به آن پرداخته اند و به **حمله پنجاه و یک درصدی** مشهور شده است. **توضیح** اینکه: اشاره کردیم که عدد نانس باید توسط یک ماینر استخراج شود و هش آن بلاک گرفته شود و توسط سیستم برای سایر اعضای فعال فرستاده شود تا آنها هم تراکنش را تأیید کنند. متاهی در اینجا گفته اند ممکن است اتفاقی بیفتد و کسی بتواند از سیستم بیت کوین سوء استفاده کند.

فرضاً کسی پنج بیت کوین خرج می کند و با آن کارخانه ای را می خرد. این تراکنش همراه با تراکنش های دیگر باید در یک بلاک قرار گیرد و تأیید شود. و از آنجا که قرار دادن تراکنش ها در بلاک ها اختیاری است، لذا اگر حداقل پنجاه و یک درصد کاربران با هم هماهنگ باشند و یک تراکنشی را در بلاک قرار ندهند و یکی از کاربران آن بلاک را از جای دیگر تکمیل کرده و هش گیری کند و منتشر کند و دیگران هم تأیید کنند، در این صورت آن بلاک بسته شده است بدون اینکه آن تراکنش داخلش باشد و در نتیجه سیستم تشخیص می دهد که این تراکنش واقعی نیست و آن بیت کوین هایی را که خرج شده به همان کیف پولی برمی گرداند که از آن خارج شده است و در حقیقت آن فرد، کالایی را خریده بدون اینکه بیت کوینی از کیف پولش خرج شود. کما اینکه یک نفری هم می توان چنین کاری را انجام داد؛ یعنی اگر کسی آنقدر مهارت داشته باشد که بتواند قبل از دیگران یک بلاک را به ثبت برساند و تراکنش خود را داخل آن بیاورد و آن بلاک و زنجیره بلوکی را منتشر کند و دیگران هم تأیید کنند، حمله پنجاه و یک درصدی اتفاق می افتد. البته زنجیره بلوکی که درست می کند باید بزرگتر از زنجیره های قبلی باشد و الا سیستم آن زنجیره بلوکی را انتخاب نمی کند.

منتها تقریباً احتمال داده نمی‌شود که پنجاه و یک درصد کاربران در سراسر دنیا بتوانند با هم هماهنگ شوند و منافع مشترکی داشته باشند که این کار را انجام دهند و یا اینکه یک نفر آنقدر قدرت پردازش کامپیوترش و مهارت شخصی‌اش بالا باشد که بتواند قبل از اینکه دیگران تراکش او را تأیید کنند، او یک زنجیره‌ای درست کند که بزرگتر از زنجیره‌های قبلی باشد و آن زنجیره را به تأیید دیگران برساند. و این کار آنقدر هزینه بالا و مهارت زیاد نیاز دارد که چندان به صرفه نیست که این انگیزه را در افراد ایجاد کند تا چنین کاری کنند. البته حمله پنجاه و یک درصدی در بعضی از رمزارزها غیر از بیت‌کوین، اتفاق افتاده است، اما تا کنون در بیت‌کوین اتفاق نیفتاده است.

بله، بعضی گفته‌اند اگر سیستم‌های خیلی قوی کامپیوتری پیدا شود که قدرت پردازش آنها قابل قیاس با کامپیوترهای معمولی نباشد و مثلاً میلیون‌ها برابر باشد، با استفاده از آن کامپیوترها می‌توان سیستم بیت‌کوین را مختل کرد، منتها فعلاً احتمالش تقریباً وجود ندارد. بنابراین امنیت بیت‌کوین کمتر از پول‌های اعتباری یا حتی سکه طلا و نقره نیست. بله، اگر کسی بتواند در سیستم رخنه کند، چه بسا آسیبی که پیدا می‌شود خیلی بیشتر از آسیبی باشد که در پول‌های اعتباری ممکن است پیدا شود؛ چون این پول‌ها را اگر کسی بخواهد سرقت کند یا تقلبی آن را چاپ کند، در یک حجم محدودی آسیب وارد می‌شود، اما اگر کسی بتواند سیستم بیت‌کوین را مختل کند به انگیزه اینکه خودش سیستم جدیدی بیاورد و منافعش را کسب کند و یا به انگیزه‌های دیگری اعم از سیاسی، اقتصادی و امنیتی، آسیب بسیار زیاد است، الا اینکه در زمان ما احتمالش تقریباً صفر است و آسیب جزئی هم که احتمالاً وارد می‌شود، بیشتر از آسیب‌هایی که در پول‌های فیزیکی اتفاق می‌افتد نیست، ولی در عین حال باید جانب احتیاط را فراموش نکرد.

عدم اطلاق پول در شرایط فعلی بر بیت‌کوین و سایر رمزارزها

با توضیحاتی که تا اینجا بیان کردیم، یک تصویر قابل اعتمادی نسبت به رمزارزها خصوصاً بیت‌کوین در ذهن شکل گرفت و اکنون باید ببینیم آیا تعریف پول شامل این رمزارزها یا حداقل بیت‌کوین می‌شود یا نه؟ اگر یادتان باشد در تعریف پول گفتیم: «پول، مالی است که به طور معمول در هر شرایطی می‌تواند عوض هرگونه کالا و خدمت قرار بگیرد». پس اولاً تمام ویژگی‌های مال را دارد و فصلش هم این است که می‌تواند عوض هرگونه کالا یا خدمت قرار بگیرد. و از آنچه گفتیم معلوم می‌شود که در حال حاضر، این رمزارزها پول نیستند؛ نه در کشور ما و نه در سایر کشورهای دیگر تا آنجا که اطلاع داریم. و اگر کسی بازار برود و بخواهد به جای ریال، یورو، دلار، یوان و یا هر پول دیگری بیت‌کوین بپردازد، فروشنده از او

قبول نمی‌کند؛ زیرا آنچه که به عنوان فصل پول است را واجد نمی‌باشد؛ یعنی به طور معمول در هر شرایطی نمی‌تواند عوض هر کالا و خدمتی قرار بگیرد. و حتی بیت‌کوین که قوی‌ترین و معروف‌ترین رمزارز است، در کشورهایی که بیشترین رواج را دارد توسط، عموم بهای کالا و خدمت قرار نمی‌گیرد و اگر کسی آسیبی به دیگری زده باشد و بدهکار او باشد، اگر آن شیء قیمی باشد، باید خسارت را با پول جبران کند و بیت‌کوین از او پذیرفته نمی‌شود.

بنابراین در حال حاضر در هیچ کجای جهان سراغ نداریم که بیت‌کوین و امثال آن، قانوناً یا عقلاً به عنوان پول پذیرفته شوند، بلکه ممکن است طرفین با هم تراضی کنند اما این حرف دیگری است.^۱ و اینکه قید «در حال حاضر» را آوردیم، به این جهت است که در آینده نه چندان دور، ممکن است برخی از این رمزارزها به عنوان پول رایج یک کشوری شناخته شوند و به گونه‌ای باشد که مردم به راحتی بتوانند در مبادلاتشان از آن استفاده کنند، نظیر کارت‌های اعتباری که امروزه شاید اکثریت قاطع مردم با کارت‌های اعتباری مبادلات خود را انجام می‌دهند و چه بسا این رمزارزها در آینده تبدیل به رمزپول شده و در این کارت‌ها باشد و مردم بتوانند به جای پول‌های اعتباری یا در عرض آنها از این رمزپول‌ها استفاده کنند، منتها لازمه‌اش آن است که این رمزپول‌های کارتی در مثل بیت‌کوین در نهایت به شبکه پیوندند.

آیا بیت‌کوین و امثال آن مال هستند؟

حال که بیت‌کوین و سایر رمزارزها فعلاً پول نیستند، این سؤال مطرح می‌شود که آیا مال می‌باشند یا خیر؟ در جواب می‌گوییم: بله، در حال حاضر تعریف مال بر آنها صادق است. قبلاً در تعریف مال گفتیم: «چیزی است که در جامعه‌ای مورد رغبت تعداد قابل توجهی از مردم باشد و به اندازه رغبت به آن در دسترس نباشد و شأنیت و قابلیت انتقال نیز داشته باشد» و امروزه معلوم است که بیت‌کوین و سایر رمزارزهای معتبر، این خصوصیات را دارا بوده و مالیت دارند، منتهی چون مالیت آنها فقط در یک فضای خاصی به نحو پول‌های اعتباری است و هیچ فایده ذاتی و مصرفی ندارند، لذا همانطور که عده‌ای گفته‌اند مناسب است در حال حاضر از این پول‌های دیجیتالی تعبیر به رمزارز یا ارز دیجیتالی کنیم.

۱. بله، می‌توان گفت رمزارزها در محیط غیر جغرافیایی، پول هستند؛ یعنی در محیط کامپیوتری و در محیط کاربرانی که از این ارزهای دیجیتالی استفاده می‌کنند. و این التزام عملی را هم دارند که در آن محیط، هر کالا یا خدمتی را در مقابل این رمزپول‌ها ارائه دهند که در آن محیط خاص یک مفهوم جدیدی خلق می‌شود، و نظیر این است که الان گفته می‌شود پول ایران، پول اروپا، پول انگلیس، پول روسیه، پول چین و هکذا، آن هم می‌گوییم پول محیط اقتصادی کامپیوتری.

«ارز» یعنی آنچه که فقط حامل ارزش می‌باشد و در عین حال به عنوان کالا نیست و در محیطی که با آن مبادله می‌شود به عنوان پول شناخته نمی‌شود، ولی در خارج از آن محیط کار پول را انجام می‌دهد و با تراضی طرفین می‌توان آن را جایگزین پول کرد. خاصیت این ارزهای دیجیتالی، فرقی با ارزهای مربوط به کشورهای دیگر نمی‌کند، منتهی همانطور که ارزهای مربوط به کشورهای متعدد «اعتبار، قدرت خرید و تبادل، عرضه و تقاضای» آنها فرق دارد، ارزهای دیجیتالی نیز از این جهت هم با ارزهای فیزیکی فرق دارند و هم در میان خودشان متفاوت است و بعضی از رمزارزهای معمول، دارای اعتبار و مورد رغبت بیشتری هستند؛ نظیر اینکه امروزه ارزهایی مانند یورو، دلار، یوان چین، ین ژاپن و امثال اینها دارای اعتماد و مطلوبیت بیشتری هستند و مردم رغبت بیشتری به نگهداری و استفاده از آنها دارند. درمقابل ارزهایی هستند که به آن اندازه دارای اهمیت نیستند، فرضاً مانند روبل روسیه یا ارز بعضی از کشورهای آفریقایی. منتها تمام این ارزها روزانه نرخ برابری‌شان اعلام می‌شود و برای بعضی از مردم مهم است؛ چراکه می‌خواهند به آن منطقه مثلاً مسافرت کنند یا تجارتی با آنها انجام دهند و یا به هر دلیلی احتیاج به آن دارند.

استخراج و استفاده از رمزارزها، یکی از بهترین راهکارها برای دور زدن تحریم‌ها

این نکته را هم در اینجا تذکر دهیم که چون در حال حاضر هیچ مرکز کنترلی نسبت به بیت‌کوین و بعضی رمزارزها وجود ندارد و دولت‌های قلدر و ستمگر نمی‌توانند خواسته‌های خود را علی‌الطلاق بر این سیستم تحمیل کنند و تراکنش‌های آن معمولاً قابل پیگیری نیست خصوصاً برای کشوری نسبت به کشور دیگری، لذا در شرایط حاضر یکی از بهترین راه‌ها برای شکستن و دور زدن تحریم‌ها، استفاده از این رمزارزها است و می‌توان بسیاری از کالاها یا خدمات را از کشورهایی مثل چین و بعضی کشورهای دیگری که حتی بیت‌کوین را به عنوان یک کالا شناخته‌اند - نه به عنوان پول - وارد کرد و پولش را از طریق کامپیوتر با بیت‌کوین پرداخت کرد یا نفت و سایر کالاها را صادر کرد و پولش را با بیت‌کوین تحویل گرفت.

البته باید با آن کشورها و افراد طرف معامله توافق کرد و یک نوع تضمینی وجود داشته باشد که جنس را تحویل می‌دهند و یا ابتدا جنس را تحویل بگیریم و بعد از طریق بیت‌کوین پرداخت کنیم و این یک روش کاملاً عقلایی است و عدم استفاده از این روش در حال حاضر غبن است. به هر حال فعلاً احتیاط در این است که در رابطه با دشمن، به قدر توان از این رمزارزها استفاده کنیم و بعضی از غموض‌هایی که ممکن است باشد را در اولویت بعدی قرار دهیم. دولت و بانک مرکزی نیز باید از روش ماینینگ برای

استخراج این ارز استفاده کنند؛ چراکه با توجه به تولید برقی که به برکت نفت و گاز داخلی داریم، در مجموع فعلاً روش ماینینگ در ایران به صرفه است.

بنابراین می‌توان با استخراج بیت‌کوین، نیازهای ارزی کشور را تأمین کرد و نیز نفت و سایر کالاهای صادراتی را با بیت‌کوین فروخت و هزینه کالاهای وارداتی را از طریق بیت‌کوین پرداخت کرد. بله، اشاره کردیم که این کار نیاز به برنامه‌ریزی و عقد قرارداد با طرف مقابل دارد و می‌توان راه‌کارهای مناسبی برای مبادله پیدا کرد؛ خصوصاً اگر این مبادلات از طریق افراد باشد و آنها به طور جزئی با یکدیگر مبادله کنند. البته طرف مقابل هم باید مورد اعتماد باشد، و آلاً ممکن است بیت‌کوین را بگیرد و آن کالا را نفرستد و فعلاً هم راهی حقوقی که بتوانیم او را محکوم کنیم نداریم. برخلاف مبادلات رسمی بانک‌ها که از طریق ال‌سی انجام می‌شود که راهکاری برای پیگیری دارد. و با همه اینها بعضی ملاحظات را که قبلاً مورد اشاره قرار دادیم فراموش نکنیم.

والحمد لله رب العالمین

تقریر و تنظیم: جواد احمدی