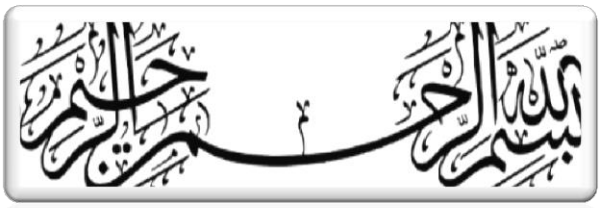

تقریرات دروس خارج فقه

حضرت آیت الله سیّد محمّد رضا مدرّسی طباطبایی یزدی (دامت برکاته)

سال تحصیلی ۱۴۰۰-۱۳۹۹

جلسهٔ چهل و دوم و چهل و ششم؛ سه‌شنبه ۱۱و۱۳۹۹/۹/۱۸ (فقه معاصر ششم و هفتم)

بیت‌کوین، شبکه‌ای «همتا به همتا»

همان‌طور که اشاره کردیم، شخص یا اشخاصی که اوّلین بار پیشنهاد بیت‌کوین را مطرح کردند، آن را چنین نام‌گذاری کردند: «بیت کوین، پول الکترونیک همتا به همتا». گفتیم «بیت» کوچکترین واحدی است که در برنامه‌نویسی کامپیوتری مورد استفاده قرار می‌گیرد که همان صفر و یک است و از مجموع چند بیت، یک بایت پدید می‌آید و «کوین» هم یعنی سکه. و این سکه‌ای که از بیت‌ها تشکل شده «الکترونیکی» است، به این معنا که در غیر از فضای الکترونیک اصلاً موضوع ندارد و اگر در جایی رایانه و برنامه‌های رایانه‌ای نباشد، اصلاً این پول نمی‌تواند معنا پیدا کند، آن هم فقط در فضای شبکه‌ای، و الا اگر کسی آفلاین باشد، هرچقدر هم که بیت‌کوین داشته باشد نمی‌تواند از آن استفاده کند، مگر از طریق کیف پول آفلاین که آن هم در نهایت با اتّصال به شبکه مفید است. و این شبکه هم به صورت «همتا به همتا» می‌باشد؛ یعنی تمام کسانی که داخل شبکه هستند به طور یکسان به تمام خدمات و اطلاعات دسترسی دارند. **توضیح اینکه**:

شبکه‌های کامپیوتری انواعی دارد؛ رایج‌ترین شبکه آن است که یک کامپیوتر اصل بوده و تعدادی کامپیوتر هم فرع هستند. کامپیوتر اصلی که به آن سرور می‌گویند، خدمات را ارائه می‌دهد و کامپیوترهای فرع، آن خدمات را دریافت می‌کنند ـ چه در مقابل پرداخت مقداری هزینه و چه به صورت رایگان ـ و سرویسی که به دستگاه‌های فرعی ارائه می‌شود، در اختیار آن سِرْوِر است و به هیچ وجه غیر سِرْوِر نمی‌تواند در برنامه‌های کامپیوتری تصرّف کند مگر در محدودهٔ خاصّی که کاملاً مشخص است. ارتباطاتی هم که برقرار می‌شود معمولاً

از طریق همان سِرْوِر است و محدودیت آن مرکز بر همهٔ دستگاه‌های تابعه تحمیل می‌شود.

امّا شبکهٔ دیگری وجود دارد به نام «**همتا به همتا**» که تمام کسانی که وارد این شبکه می‌شوند در عرض یکدیگر هستند و از امتیازات یکسان برخوردار می‌باشند و هیچ کدام امتیاز مضاعفی نسبت به دیگری ندارد و هر عملیاتی که یک فرد داخل شبکه انجام می‌دهد، دیگری هم می‌تواند انجام بدهد. و بالجمله تمام اعضاء می‌توانند در سطح یکدیگر خدمت ارائه دهند و از خدمات دیگران استفاده کنند. و هنری که سازندگان بیت‌کوین و بسیاری از رمزارزها به کار برده‌اند ـ هرچند بعض از رمزارزها هم هستند که با سرور مرکزی اداره می‌شوند ـ این است که با استفاده از شبکهٔ همتا به همتا، خواسته‌اند تمرکززدایی کنند تا یکی از مهم‌ترین ویژگی‌های پول‌های اعتباری فیزیکی «یعنی تمرکز مدیریّت پول در یک نهاد» را برطرف کنند.

همان‌طور که گذشت یکی از مهم‌ترین نواقص اسکناس‌های کاغذی اعتباری این است که مؤسسهٔ ناشر اسکناس به راحتی می‌تواند حجم پول را در بازار به صورت مستقیم با نشر اسکناس و یا غیر مستقیم با به کار گرفتن سیاست‌های خاصّ پولی، زیاد کند و نهایت اینکه باید قانونی بگذراند تا اجازهٔ انتشار اسکناس جدید داشته باشد. غرض از شبکهٔ همتا به همتا در بیت‌کوین، رهایی از آن مرکزِ کنترل کننده است تا دولت‌ها نتوانند به خاطر مصالح یا منافع خود، به حجم این پول اضافه کنند. در بیت‌کوین همه اختیار مساوی دارند و همه به گونه‌ای این توانایی را دارند که حجمش را بالا ببرند بدون آنکه این حق از دیگران سلب شود. و در عین حال بدون حساب و کتاب نمی‌توانند حجمش را بالا ببرند بلکه طبق فرمول خاصّی است تا حجم بیت‌کوینِ در دسترس بیش از اندازه نشود و مانع از سقوط ارزش با انتشار بی‌رویه شود. بنابراین با یک فرمول خاصّی هر کسی که شرایط لازم را کسب کند و وارد این زمینه شود، این توانایی را دارد که به حجم بیت‌کوین اضافه کند. البتّه در مثل بیت‌کوین یک سقف نهایی هم وجود دارد، که توضیح آن خواهد آمد إن شاء الله.

علاوه برنامهٔ بیت‌کوین دارای ضریب امنیتی بسیار بالایی است. هم کیف پولی که به اصطلاح برای کاربر تولید می‌شود و هم تراکنش‌هایی که اتفاق می‌افتد، هر دو دارای ضریب امنیتی بالایی هستند. وقتی کسی برنامهٔ بیت‌کوین را نصب می‌کند، کیف پولی در اختیار او قرار می‌گیرد و بیت‌کوین‌هایی که به مبادله یا از طریق دیگری تحصیل می‌کند، در این کیف پول قرار می‌گیرد و اگر هم خواسته باشد بیت‌کوین‌هایی را هزینه کند، از این کیف پول خارج می‌شود.

این کیف پول از لحاظ امنیتی شبیه ایمیل است. وقتی کسی ایمیل درست می‌کند، یک اسم عمومی دارد که دیگران می‌توانند آن را ببینند و هر کسی می‌تواند اسمی حقیقی یا مستعار برای ایمیل خود انتخاب کند تا اگر دیگران خواستند برای او ایمیلی ارسال کنند، از این اسم عمومی استفاده کنند. و در کنار آن یک رمز یا به اصطلاح پسورد دارد که مخصوص صاحب ایمیل می‌باشد و دیگران [در شرایط عادی] به آن دسترسی ندارند. منتها در ایمیل، معمولاً پسوردها توسط یک سرور مرکزی نگه‌داری می‌شود و اگر بخواهند می‌توانند از آن استفاده کنند و آن امنیت بالا را ندارد و اگر کسی هم پسورد خود را فراموش کند قابل بازیابی است. برخلاف بیت‌کوین که هیچ کس به‌جز خود فرد به پسوردی که انتخاب می‌کند دسترسی ندارد و هیچ سرور مرکزی وجود ندارد که آن را ذخیره و بازیابی کند و لذا اگر احیاناً کسی آن پسورد را فراموش کند، به هیچ عنوان دسترسی به بیت‌کوین‌های خود ندارد و نمی‌تواند از آنها استفاده کند و از راه دیگری هم نمی‌تواند آن پسورد را به دست آورد. و در عین حال اگر کسی به آن پسورد دسترسی داشته باشد، می‌تواند به تمام بیت‌کوین‌های آن فرد دسترسی داشته باشد. لذا فرد باید مراقب باشد پسورد خود را در جایی نگه‌داری نکند که در اختیار دیگران یا در معرض حملهٔ هکرهای کامپیوتری باشد.

بنابراین بیت‌کوین اصطلاحاً یک **کلید عمومی** و یک **کلید خصوصی** دارد. کلید عمومی برای این است که اگر کسی خواست بیت‌کوین را برای آن فرد بفرستد، از طریق آن آدرس بفرستد وکلید خصوصی فقط در اختیار خود شخص است تا بتواند بیت‌کوین‌های خود را نگه‌داری و هزینه کند. و برای این مقصود همان‌طور که گفته‌اند هم از روش رمزگذاری استفاده شده و هم از روش «تابع هش»[1] که توضیحش خواهم آمد.

امنیت مبادلات بیت‌کوین و روش تأیید تراکنش‌ها

مسئلهٔ دیگر، امنیت خود این پول‌ها هنگام مبادله است و اینکه فرد هنگام مبادله بتواند بیت‌کوین‌های خود را به کیف دیگری منتقل کند، و طرف مقابل باید این اطمینان را داشته باشد که بیت‌کوینی که برای او فرستاده شده تقلبی نیست و یا اینکه کسی یک بیت‌کوین را برای دو نفر نفرستد و آن را دو بار هزینه نکند. این جهت در پول‌های کاغذی فیزیکی تضمین شده است و مؤسسهٔ ناشر اسکناس با امتیاز انحصاری‌ای که دارد و با روش‌هایی که به کار می‌گیرد، اسکناس‌هایی چاپ می‌کند که در حالت معمول قابل چاپ کردن برای دیگران

---

۱. Hash function

نیست. علاوه آنکه حکومت‌ها نیز مراقبت می‌کنند و با تعقیب متقلّبین، [تا حدّ امکان] مانع از انتشار اسکناس تقلّبی می‌شوند. از طرف دیگر پول، یک امر فیزیکی است و وقتی دارندهٔ اسکناس آن را تحویل دیگری می‌دهد و آن فرد مطمئن می‌شود که این واقعاً پول است، تبادل محقق می‌شود و امنیت جامعه هم مانع از دستبرد به آن می‌شود و یا اگر انتقال از درون بانک به صورت حضوری انجام شود، مأمور بانک کنترل می‌کند که انتقال دهنده چقدر پول در حسابش دارد و چه مقدار از حساب او کسر می‌شود و وارد حساب طرف مقابل می‌شود، البته ممکن است این کارها را با یک برنامه کامپیوتری انجام دهد، امّا به هر حال آن سیستم مرکزی که یک انسان یا یک برنامهٔ کامپیوتری است، این تراکنش‌ها را کنترل می‌کند. امّا در مورد مثل بیت‌کوین، سیستم کنترل‌کنندهٔ مرکزی وجود ندارد و هیچ کس مسئول نیست، لذا این سؤال مطرح می‌شود وقتی مرتبطین شبکه ـ که به اصطلاح به آنها **نود**[۲] می‌گویند ـ می‌خواهند این رمزارزها را تبادل کنند و مثلاً کالا یا خدمات خریداری کنند، فروشندگان کالا و خدمت چگونه می‌توانند مطمئن شوند که طرف مقابل واقعاً بیت‌کوین دارد و یا آن بیت‌کوین را دو بار هزینه نکرده و امنیت این انتقال چگونه تأمین می‌شود؟

استفاده از فن‌آوری زنجیرهٔ بلوکی و تابع هش، برای تأیید و تأمین امنیت تراکنش‌ها

در **جواب** می‌گوییم: برای اینکه امنیت تراکنش‌ها حفظ شود، طراحان بیت‌کوین از یک فن‌آوری به نام **زنجیرهٔ بلوکی** یا «**بلاک چین**»[۳] استفاده کرده‌اند. این برنامه که زیرمجموعهٔ برنامهٔ بیت‌کوین است، هر تراکنشی را که در بیت‌کوین اتفاق می‌افتد کنترل می‌کند؛ به این معنا که تمام تراکنش‌ها و نقل و انتقالاتی که در بیت‌کوین اتفاق می‌افتد، در این زنجیره قرار می‌گیرد و این زنجیره برای تمام کسانی که در شبکه حضور دارند قابل رؤیت است و به آن دسترسی دارند و حتّی با صرف وقت می‌توانند جزئیات آن را مشاهده کنند که این بیت‌کوین مثلاً از چه کیف پولی و در چه زمانی و با چه خصوصیاتی منتقل به کیف پول دیگری شده است. البتّه بیان کردیم افراد می‌توانند برای خود اسامی مستعار انتخاب کنند و به طور معمول نمی‌توان فهمید که طرفین مبادله چه کسانی هستند، مگر اینکه کسی رصد کرده باشد که این داده از کدام کامپیوتر و در چه زمانی و با چه خصوصیاتی خارج شده و از بیرون بداند که صاحب این کامپیوتر کیست، منتها این کار سختی است و به

---

۲. node

۳. Blockchain

سادگی برای معمول مردم میسور نیست و تقریباً نیاز به یک کار اطلاعاتی دارد.

به هر حال بیت‌کوین به اصطلاح یک **دفتر کلّ** دارد که تمام تراکنش‌هایی که در سراسر دنیا واقع می‌شود، در این دفتر کلّ نوشته می‌شود و علاوه بر آنکه این تراکنش‌ها نوشته می‌شوند، باید تعداد معتنابهی از دارندگان بیت‌کوین، این تراکنش‌ها را تایید کنند و تأیید یک نفر کافی نیست. البته تأیید تراکنش‌ها کار آسانی نیست و مثلاً به آسانی نمی‌توان زیر آن نوشت که صحیح است، بلکه یک تأیید ریاضی پیچیده‌ای است که از طریق **تابع هش** اتفاق می‌افتد. «**هش**» در اصل لغت به معنای خرد کردن و تا اندازه‌ای درهم ریختن و شاید در بعضی از ترکیباتش مثل «hash out» به معنای «به نتیجه و توافق نهایی رسیدن» باشد. و اصطلاحاً یک فناوری بسیار جالبی است که با کمک آن می‌توان یک داده را به هر شکل و مقداری که باشد ـ عدد باشد یا حرف و یا مخلوط از هر دو، کوتاه باشد یا بلند و... ـ تبدیل به دادهٔ ثابتی کرد که ظاهراً حجم آن در برنامهٔ بیت‌کوین ۲۵۶ بیت می‌شود، هرچند حجم اصل یک ترابایت یا بیشتر و یا کمتر باشد. و این تابع هش، یک علامت ثابت است، به این معنا که در هر وقت و هر شرایطی آن داده را به این الگوریتم بدهند، همان نتیجه را می‌دهد و دادهٔ یکتاست، بدون اینکه اندک تغییری کند. و اگر این داده‌ها حتّی به اندازهٔ یک بیت که کوچکترین واحد کامپیوتر است تغییر کند، حتماً نتیجهٔ این الگوریتم هم تغییر خواهد کرد. برای **تقریب** مطلب به ذهن، **مثالی** می‌زنیم که از جهتی مقرّب و از جهاتی مبعّد است و آن اینکه:

اگر یک داده‌ای از یک طرف داشته باشیم که «دو به اضافهٔ دو» و طرف دیگر یعنی نتیجه «چهار» باشد، این معادله در هر زمان، مکان و شرایطی که باشد، همین نتیجه را می‌دهد که دو به اضافه دو مساوی با چهار است و اگر این داده‌ها کم یا زیاد شود، نتیجه هم متفاوت می‌شود؛ مثلاً پنج یا سه می‌شود و هکذا. تابع هش نیز چنین است که اگر آن داده در هر شرایطی به او داده شود، همان نتیجه را می‌دهد با این تفاوت که حجمش همیشه ثابت است برخلاف مثال مذکور که دو به اضافهٔ دو می‌شود چهار ولی اگر به اضافهٔ هشت شود، نتیجه دوازده می‌شود که یک عدد دو رقمی است. امّا تابع هش این خصوصیت را دارد که هرچه یک طرفش بزرگتر شود، طرف دیگر از لحاظ حجم ثابت بوده و همان ۲۵۶ بیت است. فرق دیگری نیز موجود است که اگر داده مثلاً سه به علاوهٔ یک بود نیز طرف دیگر معادله دقیقاً چهار است، به خلاف تابع هش که با هر تغییر به هر شکل، تغییر خواهد کرد.

البته حجم خروجی در تابع هش در جاهای دیگر می‌تواند متفاوت باشد و شاید تا پانصد بیت هم برسد، منتها این تابع را در سیستم بیت‌کوین براساس ۲۵۶ بیت درست کرده‌اند. و جالب اینکه عکسش درست نیست، به این معنا که از طریق نتیجه نمی‌توان به آن داده‌ها رسید، برخلاف بسیاری از معادلات دیگر که از طریق نتیجه نیز می‌توان به اصل رسید، البتّه در مثال دو به اضافهٔ دو نیز این خاصیت وجود دارد؛ یعنی از طریق نتیجه که چهار باشد، نمی‌توان به طور دقیق به همان داده رسید که دو به اضافهٔ دو است، بلکه شاید یک به اضافهٔ یک به اضافهٔ یک به اضافهٔ یک بوده یا سه به اضافهٔ یک بوده باشد. بنابراین در تابع هش به حسب ابزارهای امروزی، قطعاً امکان برگشت وجود ندارد و از طریق نتیجه نمی‌توان به دادهٔ اولیه رسید.[٤]

برای اینکه اهمیت تابع هش را بدانید، در قالب مثال می‌گوییم: فرض کنید کسی مقالهٔ حساسی می‌نویسد و مطالب زیادی در آن می‌گذارد و یا سخنرانی مهمّی انجام می‌دهد و می‌خواهد این مقاله یا سخنرانی را از طریق نقل و انتقالات رایانه‌ای ارسال کند، امّا احتمال می‌دهد در این میان هکرها و یا سرویس‌های امنیتی به اغراضی که دارند، سخنرانی یا مقالهٔ او را دستکاری کنند و یا به صورت ناقص بفرستند و یا حتّی احتمال می‌دهد که حین ارسال، رایانهٔ او خراب شود و بخشی از آن مطلب یا سخنرانی ارسال نشود. در اینجا فرد می‌تواند از فایل ارسالی خود، تابع هش بگیرد و هش آن را با ۲۵۶ بیت تعیین کند. سپس به طرف مقابل بگوید او هم از فایل دریافتی هش بگیرد، اگر هر دو هش یکسان بود، معلوم می‌شود فایل کامل منتقل شده و دست نخورده است؛ چراکه گفتیم حتّی اگر آن فایل تغییر کوچکی کند و مثلاً به اندازهٔ یک بیت کم یا زیاد شود، هش آن متفاوت خواهد بود.

کسانی که از طریق تابع هش می‌خواهند تراکنش‌های اتّفاق افتاده در برنامهٔ بیت‌کوین را تأیید کنند، اصطلاحاً به آنها «**ماینر**»[٥] می‌گویند و این کار هم برای آنها اجباری نیست بلکه اختیاری است و طراحان بیت‌کوین برای اینکه این انگیزه را برای افراد ایجاد کنند تا حاضر باشند هزینه کنند و تراکنش‌ها را تأیید کنند، برای این کار جایزه‌ای قرار داده‌اند که اگر کسی بتواند از طریق تابع هش این کار را انجام بدهد و یک بلاک را درست و تأیید کند، از سیتم بیت‌کوین یک مقدار کوین به عنوان پاداش به او داده می‌شود.

بیت‌کوین را در ابتدا به گونه‌ای تنظیم کرده‌اند که هرچه اقبال به آن بیشتر می‌شود، سکه‌های کمتری جایزه

---

٤. البته گفته شده و قاعدتاً نیز باید چنین باشد که اگر کامپیوترهای فوق‌العاده‌ای پیدا شود و سال‌های زیادی ـ که بعضی‌ها تعبیر بـه میلیون‌هـا سـال کرده‌اند ـ کار بکند، می‌تواند به اصل برسد، ولی با ابزارهای امروزی امکان آن به هیچ وجه وجود دارد.

٥. Node

می‌دهد ولی چون استقبالِ بیشترِ مردم موجب می‌شود ارزشِ بیت کوین هم بالا برود، لذا همچنان برای افراد به صرفه است. در اوائل اگر کسی تعدادی از این تراکنش‌ها را در یک بلاک می‌گذاشت و آن بلاک را به روش هش تأیید می‌کرد، پنجاه بیت‌کوین به او جایزه می‌دادند که ظاهراً هر چهار سال یک بار نصف می‌شود و بعداً جایزه به بیست و پنج رسید و بعد دوازده و نیم و الان گویا شش و بیست و پنج صدم است.

به هر حال هر تراکنشی که اتفاق می‌افتد، در یک **بلاک** (مجموعهٔ زنجیره‌ای) قرار داده می‌شود و هر بلاک بیت‌کوین طبق آنچه که گزارش شده، ظرفیت ذخیره‌اش یک مگابایت است و به طور میانگین ۲۵۰۰ تراکنش در هر بلاک قرار می‌گیرد ـ البته نمی‌دانیم این گزارش چقدر دقیق باشد ـ و هر بلاکی که ظرفیتش تکمیل شد، باید توسط نودها تأیید شود.

ماینرها برای تأیید هر تراکنش، باید ببینند آیا سابقه‌ای از این تراکنش در آن سلسله تراکنش‌هایی که قبلاً ضبط شده و مهر و موم شده و هش‌گیری شده، موجود بوده است یا خیر؟ سپس آن تراکنش در کنار تراکنش‌های دیگر قرار داده می‌شود و وقتی ظرفیت آن بلاک تکمیل می‌شود، از مجموع این تراکنش‌ها هش‌گیری می‌شود و به **ضمیمهٔ** سایر خصوصیات از جمله **هش بلاک قبلی**، هش جدیدی ساخته می‌شود. در نتیجه **هش** هر بلاک علاوه آنکه خصوصیات خودش را به طور فردی داراست، خصوصیات بلاک و بلکه بلاک‌های قبلی را هم داراست. و بالجمله در هر **هدر بلاک** که باید هش‌گیری شود، شش خصوصیت وجود دارد:

خصوصیّات شش‌گانهٔ هدر بلاک

خصوصیّت اوّل: یکی از مهمترین مزایای بیت‌کوین این است که «**اپن سورس**»[۶] است، به این معنا که پشت برنامه و منابعش باز است. در بخش عمده‌ای از برنامه‌های کامپیوتری، کاربر دسترسی به پشت برنامه و آنچه که کدها را سازمان‌دهی کرده ندارد، و این منابع نزد برنامه‌نویس است و اگر کسی بخواهد چیزی اضافه کند که در خود برنامه پیش‌بینی نشده باشد، فقط از طریق آن برنامه‌نویس می‌تواند انجام بدهد. امّا بیت‌کوین مانند سیستم **عامل لینوکس** ـ برخلاف ویندوز ـ منبع باز است؛ یعنی تمام آنچه را از طریق آن به این برنامه رسیدند، همراه

۶. Open Source

برنامه وجود دارد و اگر کاربری تسلّط بر برنامه‌نویسی داشته باشد، می‌تواند جزئیات برنامه را کنترل کند و در آن تصرّف کرده و ارتقائش دهد، منتهی اگر این تصرّفات به گونه‌ای باشد که برنامه کارایی‌اش را از دست بدهد، سایر کاربران آن را قبول نمی‌کنند، امّا اگر کسی بتواند ورژن برنامه را ارتقاء دهد و اکثریت اعضاء هم آن را قبول کنند، می‌توان از آن ورژن جدید استفاده کرد و همان‌طور که گفتیم در هدر بلاک باید ورژنی که از آن استفاده شده ثبت شود.

به هر حال تقریباً تمام کسانی که در زمینهٔ بیت‌کوین مطلب نوشته‌اند، در این مسئله اتفاق نظر دارند که اصل برنامهٔ بیت‌کوین، منابع و عملکرد برنامه و هر چیز دیگری که وجود دارد، به اصطلاح در یک ویترینی گذاشته شده و تمام کاربران به آن دسترسی دارند و هیچ برنامهٔ مخفی‌ای در آن وجود ندارد که کسی فکر کند ممکن است یک وقتی فعال شود و سیستم را از کار بیندازد.[۷]

خصوصیت دوم: باید هش هدر بلاک قبلی در هش هدر بلاک جدید ثبت شود.

خصوصیت سوم: هر هدر بلاک باید مشتمل بر هش ریشهٔ درخت مرکل تراکنش‌های آن بلاک باشد. هش ریشه مرکل نقش مهمی در سازماندهی و امنیت تراکنش‌ها دارد و به نحو پیچیده‌ای است و می‌تواند سطح بالایی از اطمینان را ایجاد کند که هیچ تصرف و مداخله‌ای در این تراکنش‌ها نشده است و خلاصه‌اش این است که مجموع تراکنش‌های موجود در بلاک را هش‌گیری می‌کنند و این هش خلاصه‌ای از اطلاعات تراکنش‌ها را نشان می‌دهد، و این غیر از هش کلّی بلاک‌ها است.

خصوصیت چهارمی که در هدر بلاک وجود دارد، «**زمان**» است که نشان می‌دهد ماینر چه زمانی شروع به پیدا کردن هش بلاک کرده است که معمولاً پیدا کردن آن زمان زیادی می‌برد.

خصوصیت پنجم که نوعاً ذکر نمی‌شود ولی خیلی مهم است، «**تارگت**» یا هدفی است که توسط شبکه مشخص شده است. وقتی تراکنش‌هایی انجام می‌شود و ماینر می‌خواهد یک بلاک جدید را تأیید کند، شبکه

---

۷. بله، فقط یک نقطهٔ ابهامی وجود دارد که بیت‌کوین‌های جدید، با تأیید تراکنش‌های قبلی استخراج می‌شود تا به بیست و یک میلیون برسد، امّا این سؤال مطرح می‌شود که حداقل اوّلین بیت‌کوین‌ها را چگونه درست کردند؟ و جواب این سوال را در کتاب‌هایی که در این‌باره نوشته شده ندیدم، به‌جز یک کتاب که این سؤال را مطرح کرده و گفته لامحاله باید از طریق یک بدافزاری این را به دست آورده باشد. امّا وجه این کلام معلوم نیست. البته حدس زده می‌شود که برنامه را طوری نوشته باشند که ابتدا چند بیت‌کوین وجود داشته باشد، منتها منبعی ندیدم که این را دقیق و منطقی توضیح داده باشد.

یک عددی به ماینر می‌دهد و هشی که ماینر پیدا می‌کند باید مساوی یا کمتر از این عدد باشد. پس شبکه به طور خودکار یک محدودیتی قرار می‌دهد و اگر هشی که ماینر پیدا کرده مساوی یا کمتر از آن عدد باشد، آن بلاک استخراج شده تلقی می‌شود و آن ماینر پیروز بوده و استحقاق جایزه دارید. و مقصود از تساوی یا کمتر بودن در اینجا، از حیث تعداد صفرهایی است که در ابتدای هش قرار می‌گیرد.

خصوصیت ششم عدد **نانس**[۸] است و حدس زدن این عدد همان کاری است که معدن‌کاوها و ماینرها باید انجام دهند. ماینر علاوه بر اطلاعاتی که در اختیار دارد و توسط سیستم داده می‌شود ـ یعنی تعداد تراکنش‌ها، هش ریشه درخت مرکل، ورژن، هش هدر بلاک قبلی، زمان، تارگت یا هدف ـ باید عددی را حدس بزند که اگر آن عدد را به این اطلاعات اضافه کند و هش بگیرد، آن هش [مساوی یا] کمتر از تارگت و هدف مورد نظر بشود. و حدس زدن این عدد کار ساده‌ای نیست و نظیر حلّ معادله‌ای است که در آن مجهول وجود دارد ولی حدودش معلوم است. ماینر باید عدد نانس را حدس بزند و به همراه اطلاعات دیگر به سیستم بدهد و سیستم از مجموع آن‌ها هشی می‌دهد که اگر [مساوی یا] کمتر از تارگت یا هدف تعیین شده توسط شبکه باشد، آن بلاک استخراج می‌شود. ولی اگر بزرگتر از آن عددی باشد که شبکه می‌دهد فایده ندارد و ماینر باید دوباره عدد دیگری را حدس بزند. و اینکه معدن‌کاوی و ماینینگ مشکل می‌شود، به خاطر همین است و الا هش‌گیری آسان است و حجم داده‌ها هر مقدار هم باشد به راحتی می‌توان هش آن را استخراج کرد.

به هر حال سیستم بیت‌کوین این محدودیت را ایجاد کرده که عدد نانس باید [مساوی یا] کوچکتر از تارگت و هدف تعیین شده توسط شبکه باشد و گاهی حدس زدن این عدد ممکن است دو یا سه سال برای یک فرد زمان ببرد؛ یعنی اینکه یک ماینر قبل از دیگران موفق به حدس زدن مناسب عدد نانس و تأیید یک بلاک شود، این مقدار زمان طول می‌کشد و الّا گفته‌اند در مجموع برای تأیید یک تراکنش ده دقیقه وقت لازم است تا توسط یک ماینری در سراسر جهان تأیید شود، البته اگر سیستم و خطوط درست کار بکنند. و تمام ماینینگ‌ها در سراسر جهان مرتّب در تلاش هستند تا با این داده‌ها و با نانسی که حدس می‌زنند، بتوانند هش مورد نظر را زودتر از دیگران به دست بیاورند.

---

۸. **Nonce**

تأیید تراکنش‌ها احتیاج به کامپیوترهای قوی و مصرف زیاد برق[۹] و در عین حال تلاش فرد دارد و به این کار «mining»؛ یعنی معدن کاوی می‌گویند و کسانی هم که این کار را می‌کنند ماینر یعنی معدن کاو هستند. «معدن کاوی» یک نوع کاسبی است و فرد ممکن است بیت‌کوین نداشته باشد و با تأیید یک بلوک از طریق تابع هش، حداقل شش و نیم بیت‌کوین درآمد به دست آورد.[۱۰] بعضی از افراد و چه بسا دولت‌ها، کامپیوترهای مخصوص این کار را در جایی نصب می‌کنند و به آن مزرعهٔ بیت‌کوین می‌گویند و شروع به تأیید تراکنش‌های در شبکه می‌کنند و یک نوع رقابتی در سراسر دنیا برای تأیید تراکنش‌ها در جریان است و ماینرها تلاش می‌کنند آن تابع هشی که باید از طریق آن تراکنش‌ها تأیید شود را زودتر از بقیه پیدا می‌کنند.[۱۱] اوّلین کسی که این هش را به دست آورد، برندهٔ آن جایزه می‌شود و بعد از اینکه تابع هش درست شد، خود به خود در شبکه پخش می‌شود و بقیه هم باید آن را تأیید کنند؛ یعنی آن داده‌ها را به سیستم بدهند و ببینند آیا همان هش از آن بیرون می آید یا نه؟ و اگر آن هش را به دست آوردند، روی گزینهٔ صحیح بودن کلیک می‌کنند و آنها هم مقدار کم‌تری مزد نصیب‌شان می‌شود، امّا انگیزه اصلی برای آن معدن‌کاو است.

بنابراین هر تراکنشی که اتفاق می‌افتد، به اندازه‌ای که سیستم بیت‌کوین به آن معدن‌کاو جایزه می‌دهد، به حجم پول بیت‌کوین در شبکه افزوده می‌شود، امّا اینطور نیست که مقدار قابل تولید بیت‌کوین بی‌نهایت باشد بلکه سقفی برای آن تعریف کرده‌اند که حداکثر **بیست و یک میلیون** است و بیشتر نمی‌شود و بعد از آن دیگر نمی‌توان بیت‌کوین جدیدی را استخراج کرد و دیگر چنین پاداشی به ماینرها داده نمی‌شود، منتها برای اینکه بعد از رسیدن به این سقف، ماینرها هنوز انگیزه داشته باشند که تراکنش‌ها را تأیید کنند، سیستم بیت‌کوین برای آنها کارمزدی را تعریف کرده است که کارمزد اصلی باز برای کسی است که بتواند زودتر از بقیه یک بلاک را تأیید کند، و به ماینرهای بعدی کارمزد کمتری داده می‌شود؛ چراکه کار آنها آسان‌تر است چون آن هش لازم که باید کوچک‌تر از تارگت و هدف سیستم باشد، پیدا شده و در شبکه پخش شده است و سایر ماینرها فقط باید آن داده‌ها را هش‌گیری کنند و ببینند آیا همان هش را به دست می‌آورند و یا نه. و وقتی یک بلاک استخراج شد و توسط تعدادی از ماینرها تأیید شد، این بلاک که تمام خصوصیات بلاک‌های قبلی را دارد، روی زنجیره قبلی سوار می‌شود و

۹. بعضی ماینرها برای اینکه هزینهٔ برق‌شان بالا نرود، ژنراتور اختصاصی برق نصب می‌کنند.

۱۰. قیمت فعلی یک بیت‌کوین در بازار، حدود ششصد میلیون تومان است. و هر بیت‌کوین تا یک صد میلیونیوم قابل خورد کردن است.

۱۱. طبق گزارشی ـ که البته صحّت وسقم آن را نمی‌دانیم ـ حدود یک سوم استخراج بیت‌کوین‌های جدید در چین اتفاق می‌افتد.

همینطور تا آخر.

نقش واسطه‌ها یا صرّاف‌ها، در مبادلات با بیت‌کوین

با توجه به مراحلی که ذکر شد، معلوم شد امکان تقلّب و دستبرد در سیستم بیت‌کوین به حسب عادی وجود ندارد و کاملاً مطمئن است و می‌توان هر نقل و انتقالی را رهگیری کرد که در چه زمانی و از چه کیف پولی و چه تعداد بیت‌کوین منتقل به کیف پول دیگری شده است. [منتها در مقام عمل برای استفاده از بیت‌کوین در مبادلات،] مشکلی وجود دارد و این‌چنین نیست که همه از سیستم اصلی استفاده کنند، بلکه از طریق **وسائطی** هست که ما اسم آنها را **صرّافی** می‌گذاریم.

وقتی کسی می‌خواهد با بیت‌کوین مثلاً برای خود اتومبیلی بخرد، اگر آن بیت‌کوین را مستقیم به حساب فروشنده واریز کند و تراکنش هم تأیید شود، چه اطمینانی وجود دارد که فروشنده ماشین را تحویل خریدار بدهد؟ و معمولاً هم مراجعهٔ به دادگاه و شکایت فایده‌ای ندارد چون معلوم نیست آن شخص چه کسی است و نشانی از او وجود ندارد و حتّی شاید اسمش هم مستعار باشد و این نقصان بزرگ ذات برنامه بیت‌کوین است. از این جهت واسط‌هایی درست کردند که نقش آنها نظیر نقش گشایش «ال سی»[۱۲] است. این واسطه باید برای طرفین معامله قابل اعتماد باشد و خریدار بیت‌کوین خود را به حساب واسطه واریز می‌کند و واسطه هم آن را نگه می‌دارد و هر وقت فروشنده ماشین را تحویل خریدار داد و خریدار تأیید کرد که اتومبیل به دستش رسیده، واسطه بیت‌کوین را به حساب فروشنده واریز می‌کند و حتّی دربارهٔ کیفیت رسیدن اتومبیل هم ممکن است یک فرایند مطمئنی تعریف کنند. و در این فرایند مبادله توسط واسطه‌ها، معمولاً طرفین مبادله شناسایی می‌شوند و باید حساب بانکی داشته باشند و در خیلی از موارد کارت شناسایی ارائه بدهند و هکذا.

والحمد لله رب العالمین

تقریر و تنظیم: جواد احمدی

۱۲. Letter credit