بیت‌کوین؛ انقلابی در سیستم پولی

پادکست دایجست | قسمت ۳
دی ۱۳۹۶
فرشاد محمودی
ویرایش و تنظیم: شادی حسین‌نیا

مقدمه

در این قسمت از پادکست دایجست می‌خواهیم درباره‌ی موضوع داغی که این روزها تقریباً از همه‌جا به گوش می‌رسد، صحبت کنیم و آن چیزی نیست جز بیت‌کوین. می‌توان گفت بیت‌کوین به داغ‌ترین خبر و کلمه‌ی این روزهای تلویزیون، رادیو و مخصوصاً اینترنت تبدیل شده‌است. هرروز خبر تازه‌ای منتشر می‌شود که قیمت بیت‌کوین از فلان هزار دلار گذشت و فردا تیتر روزنامه‌ها این است که بیت‌کوین رکورد قبلی خودش را شکست. می‌خواهیم بررسی کنیم بیت‌کوین چیست، از کجا آمده و چگونه کار می‌کند. در این قسمت از پادکست دایجست باید سعه‌ی صدر داشته باشید، چراکه همه‌ی مفاهیم و کلمات جدید هستند و توضیح دادن این موضوع کمی سخت است.

بیت‌کوین چیست؟

بیت‌کوین در اصل یک «رمز-ارز» یا به بیان معمول، «پول دیجیتال» است. یعنی پولی که فقط در فضای اینترنتی و دیجیتالی وجود دارد و مثل اسکناس یک برگه‌ی چاپ‌شده و قابل مشاهده نیست؛ درنتیجه قابل لمس نیست، زیرا بُعدِ فیزیکی ندارد.

بیت‌کوین پولی است که تحت کنترل هیچ بانک مرکزی و دولت و حتی شخص خاصی نیست. تمام پول‌های رایج دنیا (ریال، دلار، پوند و...) که در دست من و شماست، تحت نظارت دولت و بانک مرکزی یک کشور هستند که تصمیم می‌گیرند چه میزان از آن چاپ و وارد بازار کنند. در مورد بیت‌کوین چنین کنترلی وجود ندارد و کسی کم و زیاد شدن پول در بازار را مدیریت نمی‌کند. می‌دانم سؤالات زیادی ذهنتان را مشغول کرده است. نگران نباشید؛ به بیشتر آن‌ها جواب خواهیم‌داد. تا این‌جا آموختیم که بیت‌کوین یک رمز-ارز دیجیتالی‌ست که تحت کنترل هیچ شخص و دولتی نیست. قبل از اینکه ماهیت این پول را بیشتر توضیح بدهیم، خوب است راجع به روند پیدایش آن بدانیم.

تاریخچه‌ی اجمالی پیدایش پول، بانکداری و انگیزه‌ی خلق بیت‌کوین

بیت‌کوین اولین تجربه‌ی اجرایی شدنِ ایده‌ی رمز-ارز بود. ایده‌ی رمز-ارز را «وای دای» در سال ۱۹۹۸ مطرح کرد. وای دای می‌گفت رمز-ارز یک پول جدید است که با استفاده از علم رمزنگاری می‌تواند مبادلات خودش را کنترل کند و به یک قدرت و محوریت مرکزی مثل دولت یا مالک نیاز ندارد. بر اساس این تعریف، شخصی با هویت ناشناس مقاله‌ای راجع به بیت‌کوین نوشته و سیستم آن را تشریح کرد. او این مقاله را در سال ۲۰۰۸، در بحبوحه‌ی رکود مالی بانک‌ها، به یک لیستِ ایمیلی از افراد علاقه‌مند به رمزنگاری ارسال کرد. اسم مستعار این شخص که تا امروز هم ناشناس مانده‌است، ساتوشی ناکاماتو (Satoshi Nakamoto) است. اولین بیت‌کوین در سال ۲۰۰۹ توسط وی خلق شد.

چرا چنین پولی خلق شد؟ انگیزه‌ی ساتوشی ناکاموتو از خلق بیت‌کوین چه بود؟

هزاران سال قبل مردم برای تجارت از روش «مبادله‌ی کالا به کالا» استفاده می‌کردند. مثلاً فرد ده کیلو سیب‌زمینی می‌داد و در ازایش یک کیلو گوشت می‌گرفت. پس از مدتی، به علت سختی جابه‌جایی کالاها، پول را ایجاد کردند. سکه‌هایی از جنس طلا و نقره و... ساختند و ارزش هرکدام را به‌صورت قراردادی تعیین کردند و پس از آن در هنگام تجارت، این سکه‌ها را به‌کار بردند. اما حمل و نقل همین سکه‌ها هم دشوار بود و با استفاده از آن‌ها امکان پرداخت رقم‌های کمتر وجود نداشت. در نتیجه تصمیم گرفتند که طلا و نقره‌های خود را در گاوصندوق‌های جایی به نام بانک سپرده‌گذاری و معادل مقدار داراییِ خود، برگه‌هایی را دریافت کنند. مثلاً روی برگه نوشته می‌شود «صد عدد سکه‌ی طلا» و این یعنی فردی که برگه را در دست دارد، مالک صد سکه‌ی طلا در بانک است. فرد به هنگام داد و ستد تنها از همین برگه استفاده می‌کرد، چراکه حمل‌ونقلش راحت‌تر بود. بدین‌ترتیب پول کاغذی ما به وجود آمد. ماجرای پول از این‌جا به بعد جالب می‌شود.

بانک‌ها شروع کردند به چاپ کردن پول، بیشتر از طلا و نقره‌ای که در گاوصندوق‌هایشان داشتند. مثلاً اگر شما معادل ۱۰۰ سکه در بانک سپرده داشتید، بانک معادل ۱۰۰۰ سکه پول چاپ می‌کرد و وام می‌داد. به همین دلیل هر چندوقت یک‌بار دست یکی از بانک‌ها رو شده و ورشکست می‌شد و نمی‌توانست پول مشتریانِ اعتمادکرده‌ی خود را بازپرداخت کند.

به همین دلیل «بانک مرکزی» به وجود آمد. وظیفه‌ی بانک مرکزی آن بود که بر عملکرد بانک‌ها نظارت کند و به نحوی جلوی چاپ بی‌پشتوانه‌ی پول را بگیرد. درصورت ورشکستگی هر بانک، بانک مرکزی ضمانت می‌کرد که مردم متضرر نشوند. با این وجود چون هنوز هم در این سیستم بیش از میزان ذخایر بانکی پول چاپ می‌شد، ریسک ورشکستگی کامل بانک‌ها از بین نرفت. در حقیقت تعداد دفعات ورشکستگی‌ها کمتر، ولی شدت و تأثیرشان بیشتر شد. هنوز هم بانک‌ها هر چندوقت یک‌بار ورشکسته می‌شدند. اما این‌بار ورشکستگی یک بانک، سایر بانک‌ها را هم درگیر می‌کرد و دولت باید برای نجات بانک‌ها مداخله می‌کرد. در پی این مشکلات، نیکسون (رئیس‌جمهور وقت آمریکا) در سال ۱۹۷۱ رابطه‌ی پولی که چاپ می‌شد را با دارایی و طلایی که پشتوانه‌ی آن بود، قطع کرد. این باعث شد که دیگر هیچ محدودیتی برای تولید پول کاغذی وجود نداشته‌باشد.

از این‌جا به بعد تمام پولی که خلق می‌شد، تحت عنوان «اعتبار» و «بدهی» بود و دیگر به پشتوانه‌ی دارایی‌ای مثل طلا ارتباط نداشت. یعنی وقتی وام می‌گرفتید، پول برای شما خلق می‌شد و به شما قرض داده می‌شد. شما این پول را با بهره‌ی مشخصی به بانک بازمی‌گرداندید. بانک‌ها هم باید مقداری پول را به عنوان ذخیره نگه می‌داشتند. خود این ذخیره از منبع همان پول اعتباری بود و از مقدار وامی که داده می‌شد، بسیار کمتر بود.

رفته‌رفته تولید و عرضه‌ی پول آن‌قدر افزایش یافت که به‌طور کلی می‌توان گفت این کار یکی از دلایل سقوط سیستم‌های مالی دنیا در سال ۲۰۰۶ بود.

افزایشِ میزان پولی که در حال گردش است، باعث می‌شود که هرسال قیمت‌ها چند درصد افزایش پیدا کنند. البته افزایش قیمت تا حدودی کمتر از میزانِ تولید و عرضه‌ی پول است؛ چراکه بهره‌وری تولید و صنعت هر سال افزایش می‌یابد. درواقع شما در کاری که آن را بیشتر و بیشتر انجام می‌دهید، باتجربه‌تر می‌شوید، علمتان بیشتر می‌شود، تکنولوژی‌های جدید به کمکتان می‌آیند و نتیجتاً هر سال نسبت به سال قبل، آن کار را با هزینه‌ی تمام‌شده‌ی کمتری انجام می‌دهید. پس چرا قیمت‌ها هرسال کمتر از سال قبل نمی‌شوند؟ چون تولید پول کماکان در جریان است و این باعث تورمی می‌شود که هرساله از آن صحبت می‌کنند.

بانک‌ها پس از مدتی که به چم و خم کار مسلط شدند، دریافتند که باید با چه درصدی میزان تولید و رشد پول را محاسبه کنند که هم سیستم‌هایشان رشد کند و هم صدای مردم درنیاید. جدا از مالیات هنگفتی که برای مردم وضع می‌شود، چندسال یک‌بار بانک‌ها هم با این روش‌ها مردم را به اسارت می‌برند. با آغاز هر بحران اقتصادی جدید، دولت‌ها باید به کمک بانک‌ها بشتابند، وگرنه سیستم مالی از هم می‌پاشد.

علاوه بر این‌ها، بانک‌ها شرایطی را به‌وجود آورده‌اند که تقریباً هیچ مبادله‌ی تجاری و مالی‌ای بدون حضور واسطه‌ای «بانک» قابل انجام نیست. اگر شما هم از آن دسته افرادی هستید که فکر می‌کنید تجارت کردن حق لاینفک شماست، ممکن است این فکر حتی کمی ترسناک باشد! در حقیقت نبودِ یک پول درست، ریشه‌ی همه‌ی این مشکلات بوده‌است. پول کاغذی به وجود آمد و ماندگار شد، چون جایگزین بهتری نداشته‌است. طلا و نقره هم که مشکلات خاص خود را دارند.

ساتوشی ناکاماتو در پاسخ به تمام مشکلات سیستم‌های بانکی، یک سیستم پولی الکترونیک فرد-به-فرد به نام بیت‌کوین را خلق کرد و اولین جمله‌ای که در اولین بلاگش نوشت، تیتری از روزنامه‌ی تایمز لندن بود: «صدراعظم در شرف دومین کمک به بانک‌ها است.» و در ادامه، تاریخِ «۳ ژانویه ۲۰۰۹». این خبر از قصد دوباره‌ی دولت برای تزریق میلیاردها پول به سیستم، حکایت می‌کرد.

پس هدف ساتوشی از خلق بیت‌کوین، انقلابی در سیستم پولی بود که دیگر بانک در آن کنترلی نخواهدداشت.

ساختار و ویژگی‌های بیت‌کوین

به‌خاطر دارید که گفتیم یکی از مشکلات سیستم بانکی و پولی این بود که بانک‌ها هروقت بخواهند، پول چاپ می‌کنند. بیت‌کوین این‌گونه نیست. اول از همه اینکه هیچ بانکی پشت آن نیست و دوم اینکه بی نهایت بیت‌کوین وجود ندارد. بیت‌کوین انتها دارد و یک روز دیگر بیت‌کوینی روی کره‌ی زمین تولید نخواهدشد. در حقیقت همه‌ی بیت‌کوینی که وجود خواهدداشت، ۲۱ میلیون عدد است که تخمین زده‌شده در سال ۲۱۴۰، آخرین بیت‌کوین تولید یا استخراج می‌شود. تا به امروز، چیزی حدود ۱۶ میلیون و ۷۵۰ هزار بیت‌کوین استخراج شده‌است.

به این دلیل کلمه‌ی «استخراج» را به کار می‌برم که بیت‌کوین بیشتر شبیه یک معدن طلاست. اولاً مثل طلا یک روز تمام می‌شود و دیگر پیدا نخواهدشد و دوم اینکه شما برای تولید بیت‌کوین جدید، باید آن را از معادن رمزنگاری‌شده استخراج کنید. به افرادی که این کار را انجام می‌دهند، معدنچی (Miner) می‌گویند. راجع به نحوه‌ی تولید یا استخراج بیت‌کوین در ادامه توضیح می‌دهم.

اما قبل از آن باید به این سؤال پاسخ دهیم که بیت‌کوین چگونه ارزش یافت و چگونه گسترش پیدا کرد؟ اگر من و شما هم نابغه‌ی ریاضی و کامپیوتر و اقتصاد باشیم و پول خودمان را اختراع کنیم، ارزش پیدا می‌کند؟ آیا کسی از آن استفاده می‌کند؟

نکته‌ای وجود دارد که باید بدانیم: لازمه‌ی ارزش یافتن هر پولی که به وجود می‌آید این است که مجموعه‌ای از افراد توافق کنند آن را بین هم مبادله و برای آن ارزش تعیین کنند. مثلاً اولین معامله‌ای که با بیت‌کوین در دنیای حقیقی شکل گرفت این بود که برای خرید دو عدد پیتزا، ۱۰,۰۰۰ بیت‌کوین دادند. اگر آن فرد هنوز آن ۱۰,۰۰۰ بیت‌کوین را نگه داشته‌باشد، الان صاحب ۷۲۰ میلیارد تومان پول است؛ آن هم در ازای تنها دو پیتزا!

به صورت کلی چند دسته از مردم، از اولین کسانی بودند که این پول را به ارزش امروزی‌اش رساندند. این آدم‌ها جذب ۳ مشخصه در بیت‌کوین شدند:

۱. بیت‌کوین کاملاً غیرمتمرکز است و دست شخص خاص یا بانک یا هیچ دولتی نیست.
۲. هویت شما در هنگام استفاده از بیت‌کوین محرمانه باقی می‌ماند؛ یعنی کسی نمی‌تواند شما را ردیابی کند.
۳. شما برای نقل و انتقالات پول بیت‌کوینی، کمیسیونی در حد صفر پرداخت می‌کنید. انگار اصلاً چیزی نمی‌پردازید.

بسیاری از اشخاصی که اولین استفاده‌کنندگانِ بیت‌کوین بودند، کسانی بودند که گرایشات سیاسی داشتند و نمی‌خواستند که دولت‌ها از کارهایشان باخبر باشند. یا کسانی که با ایده‌ی چاپِ وقت و بی‌وقتِ پول توسط دولت، مشکل داشتند. در حقیقت این تفکر ایدئولوژیک اولیه، چیزی بود که باعث شد این افراد به سمت بیت‌کوینَ گرایش پیدا کَرده و از آن استفاده کنند.

دسته‌ی دیگری که به استفاده از بیت‌کوین علاقه‌مند شدند، کسانی بودند که دوست نداشتند ردیابی شوند. بیت‌کوین در بازی‌های شرط‌بندی آنلاین طرفدار داشت. در این میان خلافکارانی هم بودند که مواد مخدر و اسلحه معامله می‌کردند. مثلاً از بیت‌کوین در سایت سیلک‌رود (Silk Road) استفاده‌ی زیادی می‌شد.

می‌توان گفت سیلک‌رود تقریباً اولین سایت خرید آنلاین مواد مخدر در دنیا و پول رایج آن بیت‌کوین بود. طبیعتاً مشتریان این سایت نمی‌توانستند با سیستم بانکداری و پولی معمول و سنتی خرید کنند؛ زیرا در این‌صورت مالک سیلک‌رود باید یک حساب بانکی باز می‌کرد و بدین‌ترتیب پلیس بدون فوت وقت هم صاحب سایت را دستگیر می‌کرد و هم شخص خریدار و واریزکننده‌ی پول را. در نتیجه تنها چاره‌ی سیلک‌رودی‌ها، بیت‌کوین بود. پادکستِ خوبِ کانال بی (ChannelB) در چند اپیزود به ماجرای سیلک‌رود پرداخته است. اگر علاقه‌مند هستید، پیشنهاد می‌کنم این چند اپیزود را گوش کنید.

البته فقط سایت‌های خلافکاری نبودند که نمی‌توانستند با سیستم پولی و بانکی کار کنند، بلکه سایتی مثل ویکی لیکس (wikileaks) هم که اسناد سیاسی لورفته را منتشر می‌کرد، بیت‌کوین را به کار می‌گرفت؛ چراکه توسط دولت‌ها تحریم شده بود.

مسئله‌ی مهم این است که این دو گروه (خلاف‌کاران و سیاسیون) آن‌قدر پرشمار نبودند که بتوانند بیت‌کوین را در این حد رایج کنند. ویژگی سوم بیت‌کوین، یعنی حق کمیسیون بسیار ناچیز و سرعت بالای انتقالاتش بود که باعث می‌شد قشر عامی جامعه را جذب خود کند. مثلاً اگر شما بخواهید ده هزار دلار به حساب کسی در یک جای دیگر دنیا واریز کنید، اولاً بسیار زمان‌بر است، دوماً باید (مثلاً) صد دلار هم بابت کمیسیون به بانک بدهید. این همان چیزی است که برای عضویت افراد بیشتر در بیت‌کوین لازم بود. پرداخت با کارت‌های اعتباری مثل ویزا یا مستر یا حساب پی‌پال، به‌طور میانگین چیزی حدود ۲٫۵ درصد هزینه‌ی مبادله دارد، درحالی‌که هزینه‌ی جابه‌جایی پول بیت‌کوین نزدیک به صفراست.

مسئله دیگر مایکرو-ترنزکشن‌ها یا همان مبادلات خرد هستند. مثلاً اگر شما بخواهید با کارت اعتباری ۱۰ سنت به حسابی دیگر واریز کنید، کارت اعتباری حداقل ۳۰ سنت از شما پول می‌گیرد، به علاوه‌ی ۲٫۵ درصد هزینه‌ی مبادله. یا اگر بخواهید به خیریه‌ای یک دلار پرداخت کنید، حدود یک سوم آن را باید بابت هزینه مبادله بپردازید. با بیت‌کوین هزینه‌ی مبادله‌ی شما در هر میزان مبادله‌ی پول، تقریباً صفر است.

نهایتاً این دسته افراد کسانی بودند که خواسته یا ناخواسته دست به دست هم دادند و اسم این پول را به گوش مردم عادی رساندند. تا جایی که امروزه روی هر دیواری تبلیغ بیت‌کوین به چشم می‌خورد. اکنون زمان آن رسیده که بدانیم بیت‌کوین چگونه کار می‌کند.

مکانیزم‌های کاری بیت‌کوین

به بیان خیلی ساده، در این سیستم هر کسی یک کیف پول بیت‌کوین دیجیتالی دارد که از طریق آن می‌تواند پول بفرستد و دریافت کند. پس اول از همه یک کیف پول بیت‌کوینی لازم دارید. گفتیم که بیت‌کوین تحت نظارت هیچ سیستم مرکزی‌ای نیست. پس چگونه کار می‌کند؟ اگر بانکی وجود ندارد، سیستم از کجا می‌فهمد که من به کسی پول داده‌ام یا کسی برای من پول واریز کرده‌است؟ چه کسی حساب‌ها را نگه می‌دارد؟ برای فهمیدن جواب این سؤال باید با یکی از تکنولوژی‌هایی که بیت‌کوین از آن استفاده می‌کند آشنا شویم. این تکنولوژی بلاک‌چین نام دارد.

بلاک‌چین (Block Chain) چیست و چگونه کار می‌کند؟

بلاک‌چین تکنولوژی‌ای است که نقش آن در همه‌ی ابعاد زندگی ما -از خرید کردن تا هر چیز دیگری- در حال افزایش است. بلاک‌چین در واقع یک دیتابیس غیرمتمرکز است که به جای اینکه در دست یک نفر باشد، دست همه است. این همان تکنولوژی‌ای است که بیت‌کوین از آن استفاده می‌کند. برای بهتر توضیح دادن این تکنولوژی من باید از یک مثال استعاری استفاده کنم.

فرض کنید شما و دوستانتان به شمال رفته‌اید و قرار است بازی کنید. کارت‌ها را جلو می‌گذارید. حالا باید پول‌هایتان را وسط بگذارید که آخر هر دست هر کسی پول‌هایش را جمع کند، اما متوجه می‌شوید که هیچ‌کس پول نقد ندارد. قرار می‌گذارید که روی یک برگه‌کاغذ بنویسید که هرکسی چه قدر برده و چه قدر باخته‌است.

روال بازی به این صورت است که هر کس در زمان دادن پول به دیگری، باید در جمع اعلام کند. قبل از شروع بازی تعیین می‌کنید که چه کسی مسئول نوشتن حساب‌ها شود. فرشاد را برای این کار انتخاب می‌کنید. سارا می‌گوید «من به فرشاد اعتماد ندارم، چون او همیشه تقلب می‌کند و چیزی خلاف واقعیت می‌نویسد.» وقتی می‌خواهید فرد دیگری را برای یادداشت حساب‌ها انتخاب کنید، سارا دوباره می‌گوید «من به هیچ‌کس اعتماد ندارم و بهتر است هرکس برای خودش گردش پول را بنویسد.» همه این ایده را می پذیرند و تصویب می‌کنید که هرکس کاغذی جلوی خود بگذارد و روی آن بنویسد چه کسی چه مقدار پول به چه کسی داده‌است. بدین‌ترتیب هم تا حدی جلوی تقلب گرفته می‌شود، هم همه روی گردش پول کنترل دارند.

چون من از این مثال برای توضیح تکنولوژی بلاک‌چین استفاده می‌کنم، بیایید توافق کنیم که از این‌جا به بعد من آن برگه‌های کاغذ که در مثال مورد استفاده قرار گرفتند را «بلاک» نام‌گذاری کنم. پس در ادامه‌ی مثال، هرجا که از واژه‌ی «بلاک» استفاده کردم، منظورم همان برگه‌های کاغذی صورت‌حساب‌هاست.

بازی شروع می‌شود. در بازی دست مدام در حال چرخیدن است و بازیکنان مبادلاتشان را انجام می‌دهند. گفتیم که هرکسی باید این

مبادلات را در جمع اعلام کند. مثلاً من می‌گویم «من ۱۰۰ تومان به علی دادم.» و همه در بلاک‌هایشان می‌نویسند «فرشاد ۱۰۰ تومان به علی داد.» سالار می‌گوید «من ۲۵۰ تومان به مونا دادم.» همه دوباره در بلاک‌هایشان می‌نویسند «سالار ۲۵۰ تومان به مونا داد.»

بازی تا صبح ادامه پیدا می‌کند. خسته می‌شوید و می‌خواهید که بازی را تمام کنید و بخوابید. حالا وقت آن شده که حساب کنید هرکسی باید چه‌قدر پول به دیگری بدهد. چون بازی طولانی بوده، هر کدام از بازیکنان ده بلاک (برگه) را پر کرده‌اند. همه بلاک‌هایشان را حساب می‌کنند. فرشاد می‌گوید مطابق بلاکی که من نوشته‌ام، باید ۱۰۰۰ تومان پول داشته باشم. شخص دیگری می‌گوید به حساب من تو باید ۵۰۰ تومان داشته باشی. دیگری می‌گوید باید ۷۰۰ تومان داشته باشی و... همه بلاک‌هایشان را بررسی می‌کنند و هرکسی عددی متفاوت از دیگران دارد! این یعنی در حین بازی و نوشتنِ بلاک‌ها، یا عده‌ای تقلب کرده و پول بیشتری برای خود نوشته‌اند، یا اشتباه شنیده و اشتباه نوشته‌اند.

حساب و کتاب بازی به هم می‌ریزد. قرار می‌گذارید که فردا شب با پر شدنِ هر بلاک، عدد و رقم‌ها را با هم چک کنید که حساب بازی تا آخر اشتباه نشود. در بازیِ فردا، هر بلاکی که پر می‌شود، همه بلاک‌ها را وسط می‌گذارند تا با هم مقایسه کنند و مطمئن شوند که مغایرتی وجود ندارد. یک راه چک کردن این است که بلاک‌ها را خط به خط از بالا تا پایین بخوانید. فرض کنید که نفرات حاضر در بازی، جمع دوستانه‌ی شما نیستند، بلکه یک میلیون نفر مشغول بازی بوده‌اند و باید بلاک‌های همه‌ی این افراد را چک کنید! (با افزایش نفرات و تغییر شرایط، در حال بسط مثال هستم تا به درک موضوع اصلی -تکنولوژی بلاک‌چین- برسیم.) این‌جاست که به‌جای بررسی خط‌به‌خط بلاک‌ها، به راه‌حل دیگری نیاز دارید. یک نفر یک راه‌حل ریاضی پیشنهاد می‌کند. او می‌گوید این مسئله با استفاده از تابع ریاضی هش (Hash) حل می‌شود.

تابع هش یک داده‌ی ورودی با هر سایزی را به یک داده‌ی خروجی با سایز مشخص تبدیل می‌کند. مثلاً اعداد ۱، ۲، ۳، ۴ را به عنوان داده‌ی ورودی در نظر بگیرید. تابع هش می‌گوید «همه‌ی این‌ها را با هم جمع کن.» و حاصل جمع این اعداد، می‌شود ۱۰. خروجی‌ای که به جای چهار سایز متفاوت، یک سایز واحد دارد.

درواقع اگر داده‌های ورودی را داشته باشید، به‌راحتی می‌توانید خروجی را حساب کنید؛ ولی اگر خروجی را داشته باشید، تشخیص ورودی‌ها ساده نیست.

مثلاً در همین مثالِ حاصل جمع اعدادِ ۱ تا ۴، هزاران عدد وجود دارند که می‌توانند به بی‌نهایت صورت مختلف با هم جمع شده و حاصل آن‌ها ۱۰ باشد. برای نمونه «۵+۵»، «۳+۳+۳+۱»، «۶+۴» و... تنها راه تشخیص داده‌های ورودی «حدس زدن» است! نکته‌ی مهم این است که با کوچک‌ترین تغییر در ورودی‌ها، نتیجه‌ی خروجی به کل تغییر می‌کند.

از تابع هش در رمزنگاری استفاده‌ی زیادی می‌شود. تابع هش مورداستفاده در بیت‌کوین، bit ۲۵۶ Secure Hash algorithm SHA۲۵۶ (الگوریتم امن هش ۲۵۶ بایتی) نام دارد که توسط سازمان امنیت ملی آمریکا درست شده‌است.

برگردیم به مثال بازی و ببینیم عملکرد این تابع در بازی ما چگونه است. فرض کنید که هر بلاک، یک داده‌ی ورودی‌ست. در حقیقت هر بلاک (برگه) حاوی مبادلات مالی ثبت‌شده‌ای است که نشان می‌دهد هر کسی چه‌قدر پول به دیگری داده‌است. قاعدتاً اگر همه مبادلات (داده‌های ورودی) را صحیح و بدون اشتباه نوشته باشند، باید همه‌ی بلاک‌ها شبیه به هم باشند. پس اگر این مقدار را به تابع هش وارد کنید، باید خروجی یکسانی داشته باشد. مثلاً اگر عدد حاصل از هر بلاک را به یک عدد شانسی اضافه کنیم، خروجیِ هش آن عددی کوچک‌تر از ۱۰۰ باشد. پس داده‌های تابع بدین شکلند:

ورودی هش = اطلاعات هر بلاک + یک عدد نامعلوم

خروجی هش = عددی کوچک‌تر از ۱۰۰

سؤال این‌جاست: آن عدد نامعلوم چه عددی‌ست که خروجی دل‌خواه را از تابع هش می‌گیرد؟ عده‌ای برای پیدا کردن آن عدد شانسی داوطلب می‌شوند. کامپیوترهایشان را آماده می‌کنند. عددهای شانسی مختلفی را با ورودی آن بلاک جمع می‌کنند تا ببینند خروجی هش زیر ۱۰۰ می‌شود یا نه. مثلاً یک بار عدد ۱ را وارد می‌کنند و می‌بینند که حاصل هش ۱۵۴۷ می‌شود. عدد ۲ را وارد می‌کنند و حاصل هش ۴۳۷ می‌شود. به حدس زدن و آزمودن اعداد مختلف ادامه می‌دهند تا وقتی که خروجی هش، عددی کمتر از ۱۰۰ باشد. (فراموش نکنید که تمام این اعداد مثالند و تنها برای درک مکانیزم تابع استفاده می‌شوند و مبنای منطقی ندارند.) بعد از مدتی یکی از داوطلب‌ها می‌گوید که با عدد ۱۲۰ در تابع به جواب ۹۵ رسیده‌است. یعنی اگر این عدد را با اطلاعات بلاک جمع کنند، خروجی تابع هش، ۹۵ می‌شود که عددی کوچک‌تر از ۱۰۰ است.

همه بلاک‌هایشان را با ۱۲۰ جمع کرده و از آن هش می‌گیرند. قاعدتاً اگر همه‌ی بلاک‌ها شبیه هم باشند، باید همگی به عدد ۹۵ برسند. در این صورت صحت هر بلاک تأیید می‌شود و بازی در بلاک بعدی ادامه می‌یابد. در هش‌گیری از بلاک‌های بعدی، حاصل بلاک‌های قبلی هم وارد می‌شود تا مطمئن شوند کسی داده‌های قبلی خود را دست‌کاری نکرده‌باشد. در نتیجه تمام بلاک‌ها زنجیره‌وار به هم وصل می‌شوند و امکان تقلب برای کسی وجود نخواهد داشت. در حقیقت وجه تسمیه‌ی تکنولوژی بلاک‌چین همین است؛ chain یا زنجیره‌ای از بلاک‌ها. اگر در این بین کسی شیطنت کرده و اعداد اشتباهی در بلاک خود نوشته باشد، وقتی بلاکش را با ۱۲۰ جمع کند و از آن هش بگیرد، عدد ۹۵ به دست نمی‌آید و مثلاً ۷۸۹ می‌شود. سیستم بلاک‌چین سریعاً بلاک او را برمی‌دارد و یک کپی از بلاک درست را برای او جایگزین می‌کند. در نتیجه تقلب ناممکن خواهدبود. افراد داوطلب در دنیای واقعی باید آن اعداد شانسی را با زحمت زیاد پیدا کنند. کامپیوترهای آن‌ها باید برق زیادی مصرف کنند و تجهیزات کامپیوتری وسیعی خریداری شود.

چه انگیزه‌ای باعث می‌شود که افراد داوطلبانه این کار پرزحمت را انجام دهند؟ داوطلبانی که بلاک‌ها را تأیید کرده و حساب‌ها را آپدیت نگه‌می‌دارند، بیت‌کوین جایزه می‌گیرند. به همین دلیل است که به این داوطلبان «معدنچی» می‌گویند و درحقیقت به این علت است

که می‌گوییم بیت‌کوین چاپ نمی‌شود، بلکه استخراج می‌شود. هر بار که معدنچی بلاکی را تأیید کند، بیت‌کوین‌های جدیدی برای خودش استخراج می‌کند. تعداد بیت‌کوین‌های استخراجی تقریباً هر ۴ سال یک‌بار نصف می‌شود و در نهایت به جمع ۲۱ میلیون عدد بیت‌کوین می‌رسیم. در ابتدا (یعنی از سال ۲۰۰۹ تا ۲۰۱۲) جایزه‌ی هر استخراج ۵۰ بیت‌کوین بود. در چهار سال بعد (یعنی تا ۲۰۱۶) به ۲۵ رسید. این جایزه در حال حاضر و تا سال ۲۰۲۰، ۱۲٫۵ بیت‌کوین است و پس از آن به ۶٫۲۵ می‌رسد و به همین ترتیب نصف می‌شود و ادامه پیدا می‌کند. هرچه جلوتر می‌رویم، تأیید بلاک‌ها بیشتر شده و استخراج بیت‌کوین سخت‌تر می‌شود.

نکته‌ی جالب اینکه این کار به یک صنعت تبدیل شده و Mining نامیده می‌شود. افراد به‌صورت گروهی شرکتی تأسیس می‌کنند و شبانه‌روزی به استخراج بیت‌کوین مشغولند. در اوایل پیدایش بیت‌کوین، استخراج آن پس از دو-سه روز کار مداوم و روشن ماندن کامپیوتر، شدنی بود و شما می‌توانستید این کار را با یک لپ‌تاپ هم انجام دهید. ولی امروزه حتماً باید دستگاه‌های مخصوص این کار را خریداری کنید که برق بسیار زیادی مصرف می‌کنند و هرروز هم که می‌گذرد به پردازش‌گر قوی‌تری نیاز دارید. در مثالمان گفتیم، هر بلاک یک صفحه است. حالا فرض کنید که هر بلاک «ده دقیقه مبادله» است؛ یعنی به‌جای اینکه صفحه باشد، وابسته به زمان است. با افزایش تعداد معدنچی‌های داوطلب، این احتمال وجود دارد که معدنچیان به جای ده دقیقه، مثلاً ۵ دقیقه‌ای به جواب برسند. این‌جاست که بیت‌کوین درجه‌ی سختیِ یافتنِ عدد شانسی را بالا می‌برد. مثلاً می‌گوید «عددی پیدا کنید که وقتی از آن هش بگیرید، جواب کمتر از ۲۵ باشد.» در نتیجه احتمال دست‌یابی به پاسخ در زمانِ کم، کمتر می‌شود. این‌جاست که بیت‌کوین می‌بیند سؤال سخت بوده و پیدا کردن جواب ۱۵ دقیقه طول کشیده‌است. مسئله را تغیر می‌دهد و از داوطلبان می‌خواهد عددی پیدا کنند که حاصلِ هشِ آن از ۵۰ کمتر شود. درواقع درجه‌ی سختی سؤال آن‌قدر بالا و پایین می‌شود که معدنچی‌ها دقیقاً در مدت ده دقیقه به جواب دست یابند.

موضوع مهم دیگری درباره‌ی بیت‌کوین وجود دارد: می‌پذیریم که تکنولوژی بلاک‌چین از تقلبات پیشگیری می‌کند و حساب کل را هم نگه می‌دارد؛ اما اگر کسی به‌جای من اعلام کرد که مبلغی را به شخص دیگه منتقل کرده‌است، تکلیف چیست؟

شما برای اینکه از حساب خود برای کسی بیت‌کوین بفرستید، به سه چیز احتیاج دارید: شماره حساب خودتان، شماره حساب مقصد و مقدار بیت‌کوینی که می‌خواهید بفرستید. علاوه بر این، هر کیف پول دو کلید دارد. یک کلید عمومی و یک کلید شخصی و محرمانه. کلید عمومی شما برای همه قابل رؤیت است، اما افرادِ دیگر تنها در صورتی می‌توانند از حساب شما به حساب‌های دیگر پول انتقال دهند که کلید شخصی شما را داشته باشند. این کلید شخصی نوعی امضای دیجیتال است و هویت شما را تأیید می‌کند و سیستم متوجه می‌شود که خود شما ارسال‌کننده‌ی آن مبلغ هستید.

پادکستی رادیو گیک در یکی از قسمت‌های خود به‌طور اختصاصی به موضوع بلاک‌چین پرداخته‌است. اگر علاقه‌مند هستید، شنیدن آن خالی از لطف نیست. بیت‌کوین جزئیات زیادی دارد. آنچه که ما به آن پرداختیم، اطلاعات اولیه‌ای‌ست تا بتوانیم چگونگی کار کردن این پول را درک کنیم. در ادامه برخی از فواید و معایب بیت‌کوین را برمی‌شماریم.

فواید و معایب بیت‌کوین

فواید اصلی بیت‌کوین را پیش‌تر ذکر کردیم:

۱. هزینه‌ی مبادلاتی پایین
۲. حفظ و در امان نگاه داشتنِ هویت شما
۳. مصون بودن از تقلب

از جمله عیب‌های اصلی بیت‌کوین می‌توان به موارد زیر اشاره کرد:

شما مجبورید کیف پول بیت‌کوینی خود را در کامپیوتر یا یک هارد-درایو خارجی نگه دارید. ریسک این کار بالاست؛ زیرا ممکن است کسی کامپیوتر شما را هک کند، به حساب بیت‌کوینتان وارد شود و کیف پولتان را به سرقت ببرد. یا ممکن است خود شما هارد را گم کنید. مشکل اصلی این است که در صورت بروز هر یک از این اتفاقات، مرجعی برای پیگیری وجود ندارد. در سیستم پولی فعلی جهان، اگر کارت اعتباریتان را گم کنید، بانک به شما کمک خواهدکرد. برای مثال حسابتان را قطع می‌کند، یا تراکنش‌های مالی و حساب‌های مقصد را بررسی کرده و پلیس ماجرا را پیگیری می‌کند. اما اگر کیف پول بیت‌کوینی خود را گم کنید، بهتر است به کل فراموشش کنید!

شرکت GOX تا اوایل سال ۲۰۱۴، هفتاد درصد کل مبادلات بیت‌کوینی دنیا را انجام می‌داد و در واقع یک صرافی بیت‌کوینی بود. یعنی اشخاص برای تبدیل بیت‌کوین به پول نقد، به این شرکت مراجعه می‌کردند. اما ناگهان در ۲۰۱۴ اعلام ورشکستگی کرد. این شرکت اعلام کرد که حدود ۸۵۰ هزار بیت‌کوین از او دزدیده شده‌است. این مقدار بیت‌کوین در آن زمان چیزی حدود ۴۵۰ میلیون دلار ارزش داشت.

از دیگر مشکلات بیت‌کوین این است که (حداقل الان) قیمت پایداری ندارد و مثل سهام بورس مدام در حال افزایش و کاهش است. در دوره‌ای هر بیت‌کوین نیم دلار ارزش داشت و الان قیمت هر یک بیت‌کوین به حدود ۱۸ تا ۱۹ هزار دلار رسیده و هرروز هم تغییر می‌کند. در نتیجه ریسک سرمایه‌گذاری در آن بالاست. با این حال این روزها قیمت بیت‌کوین مدام در حال افزایش است. بسیاری معتقدند که این وضعیت حباب است و دلیل آن افزایش تقاضاست که متعاقباً به افزایش قیمت منجر می‌شود. البته طرفداران بیت‌کوین می‌گویند قیمت هر بیت‌کوین به چندصدهزار دلار خواهدرسید؛ چراکه هم تعداد آن محدود است و هم با گذشت زمان، عرضه‌ی آن محدود می‌شود. در نتیجه به‌تدریج ارزش آن بالا می‌رود. اما به صورت کلی می‌توان گفت که ریسک سرمایه‌گذاری در بیت‌کوین بالاست.

سرمایه گذاری در بیت‌کوین

برای سرمایه‌گذاری در بیت‌کوین چند راه وجود دارد:

۱. معدنچی شوید و به روشی که گفتیم، بیت‌کوین استخراج کنید.
۲. کالا یا خدماتی بفروشید و در ازای آن بیت‌کوین بگیرید. مثلاً پیتزا بفروشید و بیت‌کوین هم قبول کنید. شاید بپرسید با یک بیت‌کوین که ۶۰ تا ۷۰ میلیون تومان ارزش دارد، چگونه می‌شود خریدهای خرد انجام داد؟ باید بدانید که هر بیت‌کوین می‌تواند تا ۸ رقم اعشار خرد شود. کمترین مقدارِ بیت‌کوین، به افتخار خالقش «یک ساتوشی» نامیده می‌شود -مثل یک شاهی -.
۳. پول بدهید و بیت‌کوین بخرید. برای خرید بیت‌کوین چند راه وجود دارد. صرافی‌های آنلاینی وجود دارند که مخصوص این کار هستند؛ مثل coinbase. با جست‌وجوی فارسی در گوگل هم می‌توانید به لینک ده‌ها شرکت ایرانی برسید که بیت‌کوین می‌فروشند. همچنین می‌توانید به سایت‌هایی مثل local bitcoins رفته و بدون واسطه از خود فروشنده بیت‌کوین بخرید. تعداد محدودی ATM هم در دنیا (از جمله در دوبی) وجود دارد که بیت‌کوین می‌فروشند.

آینده‌ی بیت‌کوین

بیت‌کوین توجه دولت‌ها را به خود جلب کرده‌است، اما دولت‌ها هنوز نمی‌دانند که باید چه واکنشی در مقابلش داشته باشند. مثلاً چین به‌طور کلی استفاده از بیت‌کوین را ممنوع کرده است. در ایران، دولت و مجلس در حال بررسی بیت‌کوین هستند و در حال حاضر استفاده از آن را نه تأیید و نه ممنوع کرده‌اند. بسیاری از دولت‌ها هنوز موضعی در این زمینه اتخاذ نکرده‌اند. موضع دولت‌ها در قبال بیت‌کوین، یکی از عوامل افزایش قیمت بیت‌کوین یا ترکیدن حباب آن خواهدبود.
در ضمن، حدوداً هزار و دویست تا هزار و سیصد مدل رمز-ارز در دنیا وجود دارد و بیت‌کوین فقط یکی از آن‌هاست. مثلاً رمز-ارزهایی وجود دارند به نام‌های لایت‌کوین، دش‌کوین، نیم‌کوین، اتریوم و... که هر کدام تفاوت‌هایی باهم دارند.
نکته‌ی آخر اینکه گفته می‌شود نزدیک به یک تا یک و نیم میلیون از بیت‌کوین‌های موجود در دنیا متعلق به خود ساتوشی ناکاماتو -خالق بیت‌کوین- است. یعنی اگر روزی بیت‌کوین به ارزشِ پیش‌بینی‌شده‌اش برسد، این شخص می‌تواند ثروتمندترین فرد جهان شود.