

هر آن چه که لازم است درباره‌ی بیت کوین بدانید!



هر آن چه که لازم است درباره‌ی بیت کوین بدانید!



نویسنده: مهران منصوری فر

تدوین

در این مقاله پاسخ پرسش‌هایی از این قبیل را بررسی می‌کنیم: با توجه به رشد فزاینده‌ی ارزش ارزهای رمزنگاری شده یا دیجیتال، آیا می‌توان آن‌ها را پایدار دانست؟ ارزهای رمزپایه چگونه عمل می‌کنند؟ و..... بسیاری پرسش‌های دیگر از این قبیل.....

در دنیای امروز، مادیات از اهمیت ویژه‌ای برخوردار بوده و نمی‌توان پول و مسائل مربوط به آن را نادیده گرفت. به همین دلیل، بیت کوین و ارزهای مجازی دیگر دوباره در صدر خبرها جای گرفته‌اند.



اتریوم
ethereum

اگر بیت کوین را پادشاه بدانیم، بدون شک
اتریوم ملکه این قلمرو خواهد بود.

اتریوم چیست؟

حتماً اتریوم را می‌شناسید و در مورد آن شنیده‌اید. اتریوم یک ارز رمزپایه است که ارزش آن تنها در طول سال ۲۰۱۷ میلادی به میزان ۲۵۰۰ درصد رشد کرده است! ممکن است درباره‌ی ارزهای مجازی کوچک‌تر هم چیزهایی شنیده باشید. قیمت این ارزها در نخستین روزهای فروش به صدها میلیون دلار رسید! شاید هم فقط روی بیت کوین تمرکز داشته‌اید. در سال ۲۰۱۳ میلادی، ارزش این ارز به ۲۰۰ دلار افزایش یافت و تتر خبرها را به خود اختصاص داد، اما امروز، ارزش آن به چندین هزار دلار رسیده و افراد زیادی را ثروتمند نموده است!

حال، سؤال این است که آیا این قیمت‌ها تنها به صورت حبابی افزایش یافته‌اند یا این که واقعاً سیستم مالی جهان را دچار تحول عمیقی خواهند کرد؟ برای بررسی این موارد در ابتدا لازم است به چند پرسش کلی و معمول درباره‌ی این فناوری و ثروت نوین پاسخ دهیم تا بفهمیم که آیا افرادی که حاصل یک عمر تلاش خود را در این زمینه سرمایه گذاری نموده‌اند، اشتباه بزرگی مرتکب شده‌اند؟ یا نه!



بیت کوین چیست؟

بیت کوین، نخستین ارز مجازی است که هنوز هم در نوع خود جایگاه ویژه‌ای دارد. در اصل، این نوع جدیدی از دارایی بوده و ترکیبی از رمزنگاری و هم‌گرایی شبکه است. در صورتی که یک بیت کوین داشته باشید، در واقع، تنها کنترل یک کلید دیجیتال را در دست دارید که توسط آن، می‌توانید ثابت کنید، بیت کوین مزبور به شما تعلق دارد. در صورتی که قصد خرج کردن آن بیت کوین را داشته باشید، باید در کل شبکه اعلام کنید که مالکیت آن را انتقال داده‌اید. برای این کار، لازم است برای اثبات هویت خود از همان کلید مجازی استفاده نمائید. با توجه به این موارد، کلید شما شباهت زیادی به یک رمز عبور دارد که دستیابی به پول‌تان را امکان پذیر نموده و در صورت گم کردن آن، به هیچ وجه امکان بازنشانی مجدد آن وجود ندارد. هر شخصی که به کلید شما دسترسی پیدا کند، می‌تواند کنترل کامل و بی‌قید و شرط دارایی شما را در دست بگیرد. گزارش کلیدی نقل و انتقالات به صورت اسنادی در اختیار مالک بیت کوین قرار می‌گیرد. این گزارش را در اصطلاح، Blockchain یا زنجیره‌ی بلوکی یا زنجیره‌ی بستک می‌نامند.



این سیستم چه مزیتی بر سیستم بانکی دارد؟

طرفداران بیت کوین، مزایای گوناگونی را به این سیستم نسبت می‌دهند. از آن جمله می‌توان به قابلیت استفاده از زنجیره‌ی بلوکی برای پیگیری امور مالی مربوط به تراکنش‌های هوشمند و اجرای خودکار آن در شرایط ویژه، اشاره کرد.

اما بزرگ‌ترین مزیتی که همه در مورد آن توافق دارند این است که بیت کوین یک ارز غیر متمرکز است که به هیچ نهاد مالی یا سیستم بانکی وابسته نبوده و به شدت در مقابل سانسور مقاومت دارد. گرچه، روند پرداخت و تراکنش بیت کوین قابل رویت است، اما نمی‌توان آن را متوقف نمود. این امر با روش‌های معمول بانکداری کاملاً متفاوت است. سیستم بانکداری معمول، این توانایی را دارد که در روند انتقال مالی مداخله نموده و به دلیل اجرای مقررات و دریافت مالیات و ممانعت از انجام پول‌شویی، حساب‌ها را مسدود نماید. بنابراین، سیستم مذکور، مکانی امن برای انجام جرائم اینترنتی و تجارت مواد مخدر بوده و امکان پرداخت در سیستم‌های اقتصادی بسته را فراهم کرده و از عدم وابستگی حمایت می‌کند.



هنگام خرید از یک فروشگاه قابل

استفاده نیست.

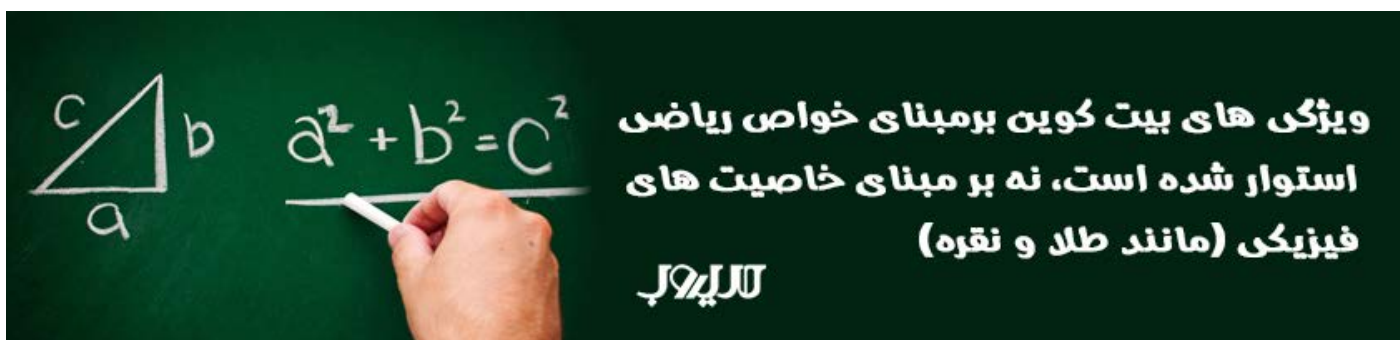
تلاش

در خریدهای روزانه نیز می‌توان از بیت کوین استفاده کرد؟!

متأسفانه بعید است که بتوان این کار را انجام داد! یکی از موانع عمده‌ای که بر سر راه کاربرد فیزیکی بیت کوین وجود دارد این است که در بهترین حالت، پرداخت‌ها تنها هر ۱۰ دقیقه یک بار تأیید می‌گردند. البته گاهی این امر، روزها به طول می‌انجامد. این، به آن معنا است که ممکن است جایی بیت کوین را خرج کنید و سپس به محل دیگری رفته و مجدداً همان بیت کوین را بپردازید. نهایتاً تنها یکی از این تراکنش‌ها تأیید شده و دیگری بی‌محل خواهد بود!

کلاً، نقل و انتقال بیت کوین در بین شرکت‌های بزرگ و مصرف‌کنندگان عادی دارای مزایای محدودی است. انتقال بیت کوین ساده و سریع نبوده و ارزش آن دائماً در نوسان است. علاوه بر این‌ها، انطباق آن با سیستم بانکی رایج، کاری دشوار است.

البته این موارد، مانع از این نشدند که برخی شرکت‌های بزرگ این تبادلات را به محک آزمایش بگذارند. برای مثال، شرکت میکروسافت در فروشگاه آنلاین خود، بیت کوین را می‌پذیرد و شرکت PayPal نیز سیستم یک پارچه‌ای را برای بازرگانان در نظر گرفته که در آن می‌توانند ارزشهای مجازی را پرداخت نمایند.



آیا بیت کوین حقیقتاً با طلا قابل قیاس است؟!

احتمالاً پاسخ این پرسش منفی است. این، به هیچ عنوان مقایسه‌ی جامعی نیست. یکی از خصائص جالب بیت کوین این است که تعداد آن محدود بوده و تنها ۲۱ میلیون قطعه‌ی مجازی بیت کوین موجود است! این رقم، کمیته‌ی است که در کد مبداء نگاشته شده و عملکردی است که طی آن، به افرادی که قابلیت انجام محاسبات را ایجاد کرده و شبکه را فعال نگه می‌دارند، پاداش داده می‌شود. به دلیل مقایسه‌ی بیت کوین با طلا، این افراد معدن‌چی نامیده می‌گردند.

در هر ۱۰ دقیقه، یکی از این معدن‌چیان مقداری بیت کوین پاداش می‌گیرند. این پاداش جنبه‌ی فیزیکی نداشته و از طرف هیچ کس نیست، بلکه کاملاً مجازی بوده و به کیف پول معدن‌چیان افزوده می‌گردد. در ابتدا، این پاداش معادل ۵۰ بیت کوین بود. اما هر ۴ سال یک بار، مقدار آن نصف می‌شود. تا زمانی که آخرین بیت کوین تولید گردد. تخمین زده می‌شود که این زمان، نیمه‌ی قرن بیست و دوم خواهد بود.

از نظر گروه خاصی از اقتصاددانان این محدودیت جنبه‌ی کاملاً مثبتی دارد. در صورتی که اعتقاد شما

بر این باشد که مشکل اصلی سیستم مالی در طول ۱۰۰ سال گذشته به چاپ پول توسط بانک‌ها و ایجاد تورم در طول این روند مربوط بوده است، پس بیت کوین عاملی است برای ایجاد اکوسیستم جایگزینی که تورم را برای همیشه مهار می‌کند.



بیت کوین چه ارتباطی با دی اکسید کربن دارد؟

بر اساس تخمین‌های سیتی بانک، برق مصرفی شبکه‌ی بیت کوین تا پایان کار آن، معادل میزان برق مصرفی کشور ژاپن است. مشکل این جا است که روند استخراج بیت کوین به طرز شگفت‌آوری با اتلاف انرژی همراه بوده و این موضوع تا حدودی عمدی است.

معدن‌چپانی که با یکدیگر رقابت می‌کنند تا نخستین کسی باشند که مسائل محاسباتی را حل می‌کنند، برای کسب موفقیت باید چرخه‌های زیادی را پشت سر بگذارند. با این حال، موفقیت آنان، اغلب به شانس بستگی دارد.

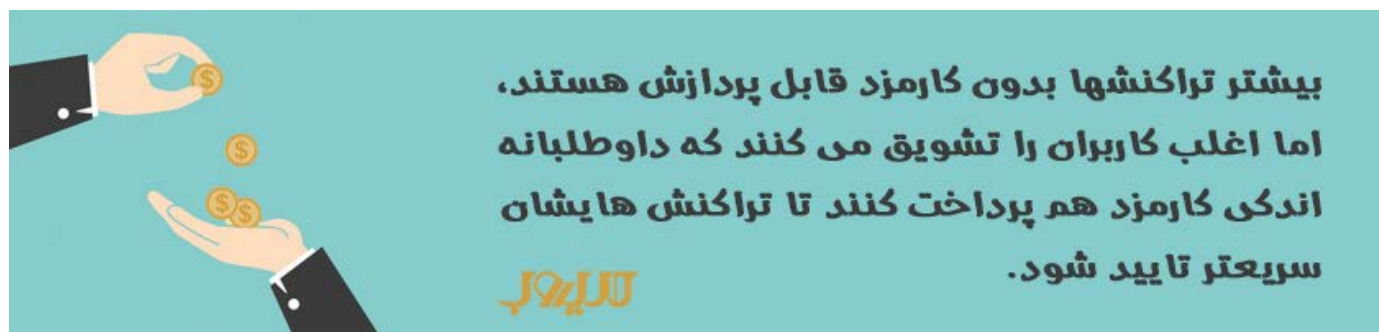
هر ۱۰ دقیقه یک بار، اولین کامپیوتری که محاسبه را انجام می‌دهد و به نتیجه می‌رسد، پاداش قابل توجهی دریافت می‌کند. اما کامپیوترهای دیگری که برنده نشده‌اند نیز همین روند را طی کرده و زمان مشابهی را برای انجام محاسبات ریاضی صرف می‌کنند.

وجود محاسبات پیچیده و مبتنی بر شانس، موجب می‌گردد که هیچ کس نتواند کنترل رویدادهای شبکه را در دست گرفته یا آن‌ها را پیش بینی نماید. دریافت پاداش توسط یک معدن‌چی، اثبات این موضوع است که کامپیوتر او مسئله را حل نموده است. اما، در عین حال، این پاداش تا لحظه‌ی تأیید نهایی تراکنش‌های آخرین ۱۰ دقیقه، مخفی باقی می‌ماند.

از آن لحظه به بعد، دستگاه‌های موجود در شبکه به حل مسئله‌ی تازه‌ای می‌پردازند که توسط آخرین معدن‌چی تنظیم شده است. اما، نکته‌ی مهم این است که آنان تنها در صورت موافقت با

فهرست تراکنش‌های معدن‌چی مزبور، این کار را انجام می‌دهند. یعنی، برنده شدن در این رقابت کافی نیست تا از دیگران بخواهید که پول‌شان را به حساب شما واریز کنند. چرا که افراد به سادگی می‌توانند شما را نادیده گرفته و به حرف معدن‌چی دیگری در زنجیره گوش کنند. این پاداش به خودی خود برای بیت کوین ضروری نیست. اما، وجود آن برای اطمینان از این موضوع است که معدن‌چیان شبکه به اندازه‌ی کافی برق مصرف کنند. امید بر این است که در طولانی مدت، هزینه‌های مربوط به تأیید سریع تراکنش‌های داوطلبانه بتوانند جای این مورد را بگیرند.

مشکل این جا است که برق مصرفی و توان محاسباتی این پردازش قوی و پاداش تصادفی آن، گران قیمت‌تر از آن است که بتوان آن را جعل کرد.



آیا بیت کوین تنها ارز مجازی موجود است؟!

به هیچ وجه! البته بیت کوین از تمام ارزهای مشابه خود ارزشمندتر است. در سال ۲۰۰۹ میلادی و پس از به وجود آمدن بیت کوین و به تبع موفقیت آن، ارزهای مجازی دیگری پدید آمدند. این ارزها با بهره بردن از کد عمومی و رایگان بیت کوین، اهداف دیگری را در پیش گرفتند.

برخی از آن‌ها اهداف کاملاً مشخصی را دنبال می‌کردند. مثلاً فایل کوین (Filecoin) قصد دارد تا نوعی دراپ باکس (Dropbox) غیر متمرکز را ایجاد نماید. به علاوه، می‌توانید به شبکه بگوئید مقداری فایل کوین دارید و به این ترتیب می‌توانید برخی اطلاعات رمزنگاری شده را ذخیره کرده و در ازای آن، به افرادی که این اطلاعات را بر روی کامپیوترهای‌شان ذخیره می‌کنند، فایل کوین بپردازید. سؤال این است که چرا باید چنین کاری را انجام دهید؟ خب، دوباره موضوع سانسور مطرح می‌گردد! اگر چیزی را در دراپ باکس خود ذخیره نمائید که باب طبع شرکت نیست، آن‌ها می‌توانند اطلاعات شما را از سیستم حذف کرده و مانع ورود شما گردند. اما با وجود فایل کوین، دسترسی به

اطلاعات ذخیره شده و آگاهی از محتوای آن، غیر ممکن است. به علاوه، امکان ندارد که بتوانند شبکه را مجبور کنند تا کاربری را بلاک کند. اهداف ارزهای دیگر، اندکی مبهم‌تر است. برای مثال، اتریوم (Ethereum) دومین نام بزرگی است که پس از بیت کوین قرار می‌گیرد و یک ارز مجازی است که برای ایجاد ارزهای مجازی تولید شده است! کاربران با نوشتن «تراکنش‌های هوشمند» می‌توانند به طور موثری برنامه ریزی کرده و این برنامه را بر روی کامپیوتر هر کاربری که اتریوم کافی پردازد، فعال نمایند. این ارزهای مجازی در واقع، نوعی اپلیکیشن‌های غیر متمرکز هستند که به اختصار آنان را (dapps) می‌نامند که تنها بر عملکرد سیستم تمرکز نداشته و یک هدف کلی را دنبال می‌کنند.



هارد فورک (hardfork) چیست؟!

شبکه‌ی بیت کوین همراه با توسعه‌ی خویش با مشکلات جدیدی مواجه می‌شود. این شبکه که در ابتدا برای ترافیک خاصی طراحی شده بود، امروزه با موج ترافیک وسیع‌تری مواجه است که همین امر موجب اختلال در عملکرد فنی و تأخیر در تأیید تراکنش‌ها می‌گردد. این مسئله در یک کسب و کار و تجارت متمرکز، موضوع مهمی نیست. چرا که به سادگی می‌توان نرم افزارها را به روز رسانی کرده و مشکل را برطرف نمود. اما، به روز رسانی شبکه‌ی بیت کوین، مستلزم آن است که تک تک معدن‌چیان را متقاعد کنید تا این نرم افزار جدید را بپذیرند. از طرف دیگر، افرادی که همچنان از نرم افزارهای قدیمی استفاده می‌کنند نسبت به کسانی که از نرم افزار جدید بهره می‌برند، پروتکل رمزنگاری شده‌ی متفاوتی را اجرا می‌کنند. این، وظیفه‌ی هارد فورک است. در ۶ سال ابتدایی به وجود آمدن بیت کوین، هارد فورک به کابوس توسعه دهندگان بدل شد و آنان تا جایی که می‌توانستند از آن اجتناب می‌کردند. اما اخیراً، تقسیماتی

که در جامعه‌ی بیت کوین پدید آمده موجب شده که فورک‌های متعددی به وجود آمده و همگی در جهت مقابله با کاهش ترافیک عمل کنند.