

بیت کوین و مصرف انرژی

علی رئیس پور رجبعلی^۱، غزال سیف^۲

^۱مدرس و عضو هیئت علمی دانشگاه آزاد اسلامی، کرمان

^۲دانشجوی دکتری اقتصاد

نویسنده مسئول :

علی رئیس پور رجبعلی

چکیده :

ارز دیجیتال شکل خاصی از پول دیجیتال است که بر پایه علم رمزنگاری ایجاد شده است. بیشتر ارزهای دیجیتال برای بهره‌مند شدن از ویژگی‌های اساسی مانند غیرمتمرکز بودن، شفافیت و تغییرناپذیر بودن از بلاک چین استفاده می‌کنند. بیت کوین یک پول یا ارز دیجیتالی است که به صورت الکترونیکی توزیع و استفاده می‌شود. شبکه این ارز دیجیتال به صورت غیر متمرکز و کاربر به کاربر است. هیچ شخص یا نهادی این شبکه را کنترل نمی‌کند. ارز دیجیتال بیت کوین نمی‌تواند خارج از برنامه ریزی انجام شده، چاپ یا خلق شود و تعداد آن محدود است. استخراج بیت کوین، ستون فقرات شبکه این ارز دیجیتال است. ماینرها یا استخراج کنندگان برای تامین امنیت و تایید تراکنش‌های بیت کوین، نقش حیاتی ایفا می‌کنند. بدون وجود ماینرها، شبکه مورد حمله قرار می‌گیرد و ناکارآمد خواهد بود. استخراج بیت کوین توسط کامپیوترهای خاصی انجام می‌شود و وظیفه ماینرها این است که شبکه را امن کرده و تراکنش بیت کوین را پردازش نمایند. ماینرها با حل یک مساله محاسباتی به جوابی دست می‌یابند که به آن‌ها اجازه می‌دهد تا بلاک‌های تراکنش‌ها را به هم متصل کنند. روش اجماع با حداقل اعتماد بیت کوین از زمان پیدایش وابسته به الگوریتم اثبات-کار بوده است. ماشین‌هایی که «کار» را انجام می‌دهند برای این مهم میزان عظیمی انرژی مصرف می‌نمایند. شاخص مصرف انرژی بیت کوین برای فهم میزان مصرف و ارتقای آگاهی در مورد ناپایداری الگوریتم اثبات-کار ایجاد شده است. باید در نظر داشت که این شاخص منحصر به بیت کوین و بیت کوین کش بوده و دیگر شاخه‌های بیت کوین را در نظر آورده نمی‌شود. بیت کوین یک پدیده بسیار عجیب و غریب در دنیای امروزی ما است و برداشت آن به روش‌های دیجیتالی و کاملاً کامپیوتری انجام می‌شود. شاید در نگاه نخست به نظر بیاید که بیت کوین با توجه به مصرف الکتریسیته، یک موضوع و ماهیت سبز است ولی در عمل مصرف انرژی مورد نیاز برای برداشت آن به اندازه‌ای زیاد است که این پدیده را به شدت مخرب ساخته است.

واژگان کلیدی :

بیت کوین، ارز دیجیتالی، مصرف انرژی، بلاکچین، ماینینگ

مقدمه

در دنیای امروز مادیات از اهمیت ویژه ای برخوردار بوده و نمی توان پول و مسائل مربوط به آن را نادیده گرفت. به همین دلیل، بیت کوین و ارزهای مجازی دیگر دوباره در صدر خبرها جای گرفته اند. اکثر مردم اطلاعات دقیقی از ارزهای دیجیتال به ویژه بیت کوین ندارند و فقط خبر افزایش یا کاهش قیمت آن را می شنوند و نمی دانند که چرا موضوع بیت کوین آنقدر در جهان و حتی ایران داغ شده است. نقدینگی دیجیتال^۳ یا نقدینگی رمزپایه^۴ در مدت اخیر با توجه به رشد چشم گیر قیمت آن توجه افراد مختلف را در حوزه فعالیت های مالی به خود جلب کرده و صحبت از ارزهای دیجیتال به ویژه مشهورترین آنها یعنی بیت کوین^۵ که نوسانات شدیدی را نیز در این مدت تجربه کرده، بالا گرفته است. (بیلندی، ۱۳۹۶)

در چند سال اخیر ارزهای دیجیتالی رمزنگاری شده بسیاری همچون بیت کوین، مونرو، ریپل و اتریوم از محبوبیت و استقبال بی نظیری برخوردار شده و کاربران بسیاری در جهان به دنبال استخراج و تبدیل پول های خود به ارزهای دیجیتالی هستند؛ چراکه این روزها بسیاری از افراد با خرید و استخراج این ارز توانسته اند به پول زیادی دست پیدا کنند. بسیاری از کشورهای جهان در تلاشند تا این پول بی افسار را کنترل کرده و معاملات با آن را تا حد امکان محدود کنند؛ چراکه آن ها بر این باورند بیت کوین به تجارت های غیرقانونی و غیرمجاز همچون تجارت اسلحه، تجهیزات تروریستی، قاچاق دارو و مواد مخدر دامن زده و به علت آنکه مقامات قضایی و پلیس نمی توانند طرفین معامله را شناسایی و ردگیری کنند، باعث سهولت استفاده از آن می شود. این درحالیست که برخی دیگر از کشورها با وضع قوانین دقیق و درست، استفاده از این ارزهای دیجیتالی رمزنگاری شده را مجاز اعلام کرده اند. براساس گفته های تحلیلگران، زمانی که بیت کوین در سال ۲۰۰۹ برای نخستین بار در بازارهای جهانی ظهور پیدا کرد، ارزش آن حتی از یک دلار هم کمتر بود اما در ماه های گذشته حتی تا مرز ۲۰ هزار دلار هم رسید. درواقع، فناوری بیت کوین که یک پول رمزنگاری شده است، این امکان را به کاربران می دهد که بدون نیاز به هیچ بانکی مبادلات مالی خود را انجام دهند و همچنین هویت طرفین معامله نیز ناشناس باقی می ماند. نکته ای که باید در نظر داشت آن است که بیت کوین تنها یک نوع خاص از یک ارز دیجیتالی رمزنگاری شده و این در حالیست که مردم و کاربران بیشتر با بیت کوین آشنایی دارند و باید بدانند که این ارزها انواع و دسته بندی های متفاوت و گوناگونی دارند. (منصوری، ۱۳۹۷)

مبانی نظری

کارکرد ارز دیجیتال و خصوصیات آنها

هر کشوری واحد رسمی پول و یا ارز خود را دارد، مثلا اکثر کشورهای اروپایی از یورو استفاده می کنند، ارز روسیه روبل و ایالات متحده دلار آمریکا است و در بانک ها یا مبادلات خارجی از ارز مشخصی برای انتقال به حساب افراد و شرکت ها استفاده می شود. اکنون چند سالی است که در مقابل این ارزهای رسمی هر کشوری، ارز دیجیتال که یک فرم از پول الکترونیکی است، مطرح گردیده که از رمزنگاری برای انتقال در اینترنت استفاده می شود. ابتدا رمزنگاری در جنگ جهانی دوم برای انتقال پیام و فرمان های نظامی مورد استفاده قرار گرفت؛ در عصر دیجیتال، ریاضیات و علوم کامپیوتر برای امنیت ارتباطات، اطلاعات و انتقال پول مورد استفاده قرار گرفته اند. اولین ارز دیجیتال بیت کوین است که در سال ۲۰۰۹ ایجاد شد و اکنون پادشاه دنیای ارزهای دیجیتال محسوب می شود. در چند سال گذشته ارزهای دیجیتال زیادی معرفی و عرضه شده اند و در حال حاضر حدود ۹۰۰ ارز دیجیتال در بازارهای جهانی تجارت می شود که به غیر از بیت کوین، ارزهای دیگری به نام اتریوم، ریپل و لایت کوین مشهور هستند. نکته بسیار مهم آن که برخلاف طلا و نقره، نقدینگی های دیجیتال ارزش ذاتی ندارند و تنها دلیل ارزش دادن آن ها اعتقاد مردم به ارزش دادن آن ها است. ارز دیجیتال^۶ شکل خاصی از پول دیجیتال است که بر پایه علم رمزنگاری ایجاد شده است. بیشتر ارزهای دیجیتال برای بهره مند شدن از ویژگی های اساسی مانند غیرمتمرکز بودن، شفافیت و تغییرناپذیر بودن از بلاک چین استفاده می کنند. ماهیت غیرمتمرکز ارزهای دیجیتال به این معنی است که هیچ نهاد، گروه یا سازمانی آن ها را کنترل نمی کند. کریپتوکارنسی ها را می توان به صورت مستقیم و بدون دخالت هرگونه واسطه ای در اینترنت به شخص دیگری ارسال کرد. یعنی برای ارسال ارزهای دیجیتال به یکدیگر نیازی به افتتاح حساب بانکی، استفاده از خدمات بانک ها یا هر سازمان واسطه دیگری نخواهید داشت. ارزهای دیجیتال همانند ریال و دلار پول هایی هستند که با سازوکار مختلفی ایجاد و توزیع می شوند. فرایند خلق برخی از این پول ها مانند بیت کوین با ماینینگ انجام می شود و برای تعدادی دیگر از آن ها، تمامی سکه ها از قبل به صورت استخراج شده در شبکه قرار

^۳ Digital currency^۴ Cryptocurrency^۵ Bitcoin^۶ Cryptocurrency

می‌گیرند. ارزشهای دیجیتال بر روی فناوری دفترکل توزیع شده ساخته شده‌اند که یکی از محصولات مهم آن، فناوری بلاک چین است. بلاک چین‌های عمومی که اکثر ارزشهای دیجیتال از آن استفاده می‌کنند، قابلیت مشاهده تمامی تراکنش‌ها را چه برای افرادی که در شبکه حضور دارند و چه برای افراد خارج از شبکه فراهم می‌کند. (احمدی، ۱۳۹۸)

ایده شکل‌گیری ارزشهای دیجیتال از دو مشکل بزرگ «اعتماد به شخص ثالث» و «دوبار خرج کردن» ریشه می‌گیرد. هنگامی که شما از بانک‌ها برای انتقال پول و نگهداری آن استفاده می‌کنید، در واقع به آن بانک اعتماد کرده‌اید. حتی اگر کلی‌تر به ماجرا نگاه کنید، اعتماد برای پیش بردن بسیاری از کارهایتان ضروری است. مشکل دوبار خرج کردن در سیستم‌های مالی که توسط سروهای مرکزی با بررسی موجودی‌ها حل شده بود، جلوی افراد را از خرج کردن دوباره‌ی مقدار مشخصی پول می‌گرفت. این راهکار به صورت غیرمتمرکز در بیت کوین ارائه شد و تمامی افراد با بررسی تاریخچه تراکنش‌ها می‌توانستند از تقلب کردن سایرین جلوگیری کنند.

بیت کوین به عنوان اولین پول الکترونیکی عرضه شد که توانسته بود مسئله اعتماد و دوبار خرج کردن را حل کند. دیگر نیاز نبود افراد برای انتقال و نگهداری پول به شخص، سازمان، گروه و یا بانکی اعتماد کنند. مسئله اعتماد نیز نه تنها در انتقالات پولی، بلکه در بسیاری از امور دیگر برای انسان‌ها به یک دردسر بزرگ تبدیل شده بود. برای همین سیستم عاری از اعتمادی که بیت کوین ارائه داده بود، در سایر فعالیت‌های انسانی نیز به کار گرفته شد. رفته رفته ارزشهای دیجیتال برای حل دغدغه‌های متفاوتی به وجود آمدند. به عنوان نمونه اتریوم خود را بستری برای توسعه برنامه‌های مختلف و اجرای قراردادهای هوشمند معرفی کرد و رپبل با نگاه خوشبینانه نسبت به بانک‌ها، بر روی تجدید ساختار ارتباطات بین بانکی و ارائه سیستم پرداختی پرسرعت و کم‌هزینه متمرکز شد.

امروزه توکن‌های بسیاری بر روی بستر ارزشهای دیجیتالی مانند اتریوم، ایاس و ترون ساخته شده‌اند که از قدرت بلاک چین‌های اصلی برای اجرای تراکنش‌هایشان بهره می‌گیرند. ارزشهای دیجیتال برای اجرای تراکنش‌های خود، مدل‌های مختلفی را به کار می‌گیرند. به عنوان نمونه بیت کوین از مدل اثبات کار استفاده می‌کند که طی آن استخراج‌کنندگان یا ماینرها تراکنش‌ها را تایید می‌کنند. این مدل‌های مختلف در بلاک چین‌ها که با نام «الگوریتم‌های اجماع» یا سازوکارهای توافق جمعی شناخته می‌شود، نحوه به اتفاق نظر رسیدن مشارکت‌کنندگان شبکه را در مورد تایید کردن یا نکردن یک تراکنش در شبکه تعیین می‌کنند. (کاشیان، ۱۳۹۷)

تراکنش ارزشهای دیجیتال به صورت همتا به همتا (P2P) عمل می‌کند. مسئولیت نظارت بر شبکه ارزشهای دیجیتال و تامین امنیت آن توسط نودها تامین می‌شود. نودها در شبکه‌های مختلف به روش‌های مختلفی انتخاب می‌شوند. برای مثال در بیت کوین، استخراج‌کنندگان یا ماینرها هستند که این مسئولیت را بر عهده دارند، در ایاس و ترون درباره انتخاب این نودها رای‌گیری می‌شود و در شبکه‌های اثبات سهام، هر کسی که بخشی از سکه‌هایش را در شبکه به صورت سهام قفل کرده باشد، می‌تواند در مورد تراکنش‌ها تصمیم‌گیری کند. برخی ویژگی‌های منحصر به فرد سبب ایجاد تمایز بین ارزشهای دیجیتال و پول‌های معمولی شده است. البته تمام این ویژگی‌ها در همه ارزشهای دیجیتال وجود ندارد و می‌توان استثنائاتی را نیز مشاهده کرد. اولین ویژگی ارزشهای دیجیتال غیرقابل برگشت بودن تراکنش‌هاست. اگر انتقال ارز دیجیتالی را انجام دهید و تراکنش شما تایید شود، دیگر نمی‌توانید آن را برگردانید و این کار تنها در صورتی امکان‌پذیر خواهد بود که گیرنده مایل به انجام این کار باشد. اما این شیوه در بانک‌ها متفاوت است. اگر شما به اشتباه پولی را به حساب شخصی دیگر انتقال داده باشید، در نهایت با پیگیری قضایی می‌توانید آن را پس بگیرید. اما اگر بیت کوین یا ارز دیجیتال دیگری اشتباهاً به آدرس دیگری فرستاده شود می‌بایست قید آن را زد.

دومین ویژگی منحصر بفرد ارزشهای دیجیتال ناشناس بودن یا نیمه ناشناس بودن آن‌هاست. آدرس کیف پول‌ها که همان نقش شماره کارت یا شماره حساب را در حساب‌های بانکی دارند، شامل اطلاعات هویتی شما نمی‌شوند. این آدرس‌ها که از رشته عبارات حروف و اعداد تشکیل شده‌اند را تنها با بررسی تاریخچه تراکنش‌ها و تحلیل‌های عمیق می‌توان به هویت افراد پیوند زد. البته برخی ارزشهای دیجیتال پیگیرگریز و حریم خصوصی محور مانند مونرو، زی‌کش و گرین طوری طراحی شده‌اند که شناسایی هویت را خیلی سخت و تقریباً غیرممکن می‌کنند.

سومین ویژگی ارزشهای دیجیتال جهانی یا فرامرزی بودن آن‌هاست. ارسال پول به نقاط مختلف دنیا ممکن است با سیستم‌های فعلی تا چندین روز طول بکشد ولی ارزشهای دیجیتال این کار را در عرض چند دقیقه می‌توانند انجام دهند. ارزشهای دیجیتال محدودیت مرزی نمی‌شناسند و آن‌ها را می‌توان از هر نقطه‌ای در دنیا به نقطه دیگر فرستاد. (گودرزی، ۱۳۹۷)

چهارمین ویژگی امنیت ارزهای دیجیتال است. این امنیت در مبادلات درون شبکه‌ای توسط قدرت هش به اشتراک گذاشته شده توسط افراد (در سیستم‌های اثبات کار) تامین می‌شود. از طرفی سیستم رمزنگاری کلید عمومی و کلید خصوصی این امکان را به اشخاص می‌دهد که خودشان کنترل پول‌های دیجیتالشان را بر عهده بگیرند و شخص دیگری نتواند به آن‌ها دسترسی پیدا کند.

پنجمین ویژگی که ارزهای دیجیتال را نسبت به پول‌های معمولی متمایز کرده، انحصاری نبودن آن‌هاست. افراد برای اینکه بتوانند از شبکه‌های ارز دیجیتال مختلفی مانند بیت کوین، اتریوم، لایت کوین و غیره استفاده کنند، نیازی نیست از شخص یا گروه و سازمانی اجازه بگیرند. آن‌ها می‌توانند کل تاریخچه تراکنش‌ها را دانلود کرده و خودشان بدون نیاز به کسب اجازه اقدام به ارسال یا دریافت ارز دیجیتال کنند.

تشریح کامل بیت کوین

بیت کوین^۷ یک پول یا ارز دیجیتالی است که به صورت الکترونیکی توزیع و استفاده می‌شود. شبکه این ارز دیجیتال به صورت غیر متمرکز و کاربر به کاربر است. هیچ شخص یا نهادی این شبکه را کنترل نمی‌کند. ارز دیجیتال بیت کوین نمی‌تواند خارج از برنامه ریزی انجام شده، چاپ یا خلق شود و تعداد آن محدود است. فقط ۲۱ میلیون بیت کوین برای همیشه تولید می‌شود. تراکنش‌های شبکه بیت کوین، در یک لاگ عمومی با تکنولوژی بلاک چین^۸ ذخیره می‌شوند. در برخی مطالعات داخلی بیت کوین آینده پولهای دیجیتال نامیده شده است. اکنون به آن آینده در حال نزدیک شدن هستیم ولی باید یک گام فراتر گذاشته و بیت کوین را آینده پول بنامیم. در واقع بیت کوین و تکنولوژی پشت این پول و مزایای این تکنولوژی، شرایطی را به وجود آورده تا به این نتیجه برسیم که سیستم فعلی مالی و پولی دنیا که سالها بر اساس آن تبادلات مالی انجام شده، یک اشتباه و ناشی از ضعف و عدم وجود تکنولوژی‌های دیجیتال بوده است. پول آینده، بیت کوین یا چیزی شبیه به آن خواهد بود. (فتاحی، ۱۳۹۷)

بیت کوین برای اولین بار در سال ۲۰۰۹ به عنوان یک نرم افزار متن باز توسط یک برنامه نویس ناشناس (یا گروهی از برنامه نویسان) تحت نام مستعار ساتوشی ناکاموتو^۹ معرفی شد. شایعات زیادی در مورد هویت واقعی ساتوشی ناکاموتو مطرح شده است، اما اغلب افراد نام برده شده به عنوان خالق بیت کوین، این ادعا را رد کرده اند. ناکاموتو خود را یک مرد ۳۷ ساله که در ژاپن زندگی می‌کند معرفی کرده است. با این حال از آنجا که تسلط وی به انگلیسی بسیار خوب به نظر می‌رسد و هیچ نشانه‌ای از نرم افزار وی در ژاپن وجود ندارد، در مورد این ادعا تردیدهایی وجود دارد. در اواسط سال ۲۰۱۰ ناکاموتو به سراغ موارد دیگری رفت و بیت کوین را در اختیار چند عضو برجسته جامعه بیت کوین قرار داد. ساتوشی نام گاوین اندرسون^{۱۰} را به عنوان برنامه نویس و توسعه دهنده اصلی اعلام کرده است. تخمین زده می‌شود که ناکاموتو دارای یک میلیون بیت کوین است، که ارزش آن با قیمت فعلی، در حدود ۶.۵ میلیارد دلار تخمین زده می‌شود.

به گفته ی گاوین اندرسن، اولین چیزی که او پس از ناکاموتو در این پروژه بر آن تمرکز کرد، تمرکز زدایی بیشتر شبکه بیت کوین بود. او گفته که به گونه ای عمل کرده که حتی اگر با اتوبوس تصادف کند، این ارز دیجیتال به صورت مستقل و خودگردان به وجود خودش ادامه دهد. از نظر بسیاری از مردم، مزیت اصلی بیت کوین، استقلال آن از دولت‌های جهان، بانک‌ها و شرکت‌ها است. هیچ مقام و یا صاحب قدرتی قادر نیست در تراکنش‌های بیت کوین دخالتی داشته باشد، بر آنها مالیات بسته و یا پول مردم را به زور چپاول کند. علاوه بر این، فعالیت‌های بیت کوین کاملاً شفاف است. هر تراکنشی که صورت می‌گیرد در یک دفتر حساب گسترده عمومی به نام بلاک چین ذخیره می‌شود.

اساساً، با این که بیت کوین به عنوان یک شبکه تحت کنترل نیست، این امکان را برای کاربران فراهم می‌سازد تا کنترل کاملی بر تمام امورات مالی خود داشته باشند. یک کاربر در کیف پول خود فقط مقدار بیت کوین و مراحل و نتیجه تراکنش‌ها را می‌تواند مشاهده کند. در پشت فرایندهای شبکه بیت کوین، یک دفتر حساب عمومی به نام بلاک چین قرار دارد. این دفتر حساب شامل تمام تراکنش‌هایی است که تا به حال پردازش شده است. سوابق دیجیتال تراکنش‌ها در به اصطلاح بلاک‌ها قرار دارند. (صیاد، ۱۳۹۴)

⁷ Bitcoin

⁸ blockchain

⁹ nakamoto

¹⁰ anderson

تراکنش ها توسط کاربران یا کیف پول آنها رمزگذاری شده و به شبکه ارسال می شوند. به این دلیل بیت کوین، ارز رمزیایه یا ارز رمزنگاری شده یا رمز ارز^{۱۱} نامیده می شود. این تراکنش های رمزگذاری شده سپس در بلاکها گنجانده می شوند.

اگر شخصی سعی کند فقط یک حرف یا عدد را در یک بلاک تراکنش تغییر دهد، این کار بر تمام بلاک ها تاثیر گذار خواهد بود. از آنجا که این یک دفتر حساب عمومی است، تلاش های اشتباه یا تقلب می تواند به راحتی توسط هر کسی قابل تشخیص و اصلاح باشد. هر کاربر در کیف پول خود می تواند اعتبار و صحت هر مبادله را بررسی کند. صحت هر تراکنش توسط امضای دیجیتال مربوط به آدرس های ارسالی محافظت می شود. به دلیل وجود فرایند تایید، ممکن است تکمیل یک تراکنش در شبکه بیت کوین، چند دقیقه زمان ببرد. پروتکل بیت کوین به گونه ای طراحی شده است که استخراج هر بلوک در حدود ۱۰ دقیقه زمان می برد.

در سال ۲۰۰۹، هنگامی که بیت کوین برای اولین بار معرفی شد، مشخص نبود که چطور و کجا می توان از آن برای پرداخت ها استفاده کرد. در حال حاضر می توان عملاً توسط این ارز همه چیز خرید. به عنوان مثال شرکت های بزرگی مانند مایکروسافت و دل، این ارز رمزیایه را جهت پرداخت برای خریداری بسیاری از محصولات و محتوای دیجیتال خود پذیرفته اند. می توانید بلیط هواپیما از هواپیمایی هایی مانند بالتیک ایر خریداری کنید و یا بلیط تئاتر خود را با بیت کوین بخرید. موارد دیگری مانند پرداخت هزینه هتل، خرید ملک، پرداخت صورت حساب رستوران و یا تهیه کارت هدیه نیز وجود دارند که می توان برای پرداخت و تهیه آن ها از بیت کوین استفاده کرد. در بازارهای بین المللی نیز جهت پرداخت ها می توان از این ارز رمزیایه استفاده کرد. (معروف، ۱۳۹۴)

به هر حال، بیت کوین هنوز هم یک شکل جدید و کاملاً پیچیده پرداخت است و بنابراین طبیعی است که مواردی که بتوان پرداخت ها را با این ارز انجام داد، محدود باشد. اما هر روز بازارها و مشاغل بیشتر و بیشتری انجام پرداخت های خود با این ارز را می پذیرند، از مشاغل و کافی شاپ های کوچک گرفته تا غول های صنایع مختلف. علاوه بر این با توجه به دائمی بودن تغییر نرخ مبادلات بیت کوین، این ارز رمزیایه می تواند فرصت مناسبی برای سرمایه گذاری باشد.

ساده ترین روش برای داشتن بیت کوین خرید آن است. این ارز رمزیایه را می توان از طریق انواع صرافی های موجود و در دسترس خریداری کرد و یا به طور مستقیم از طریق سایر اشخاص آن را خرید. جهت پرداخت می توان از پول نقد یا کارت های اعتباری استفاده کرد و یا حتی از طریق سایر ارزهای رمزنگاری و تبادل با بیت کوین، آن را تهیه کرد. اما برای اولین انتقال و دریافت بیت کوین شما به یک کیف پول نیاز خواهید داشت. برای تهیه کیف پول گزینه های مختلفی وجود دارند، اما از مهم ترین آنها می توان به کیف پول های آنلاین و کیف پول های نرم افزاری که بر روی هارد رایانه شما ذخیره می شوند اشاره کرد. هیچ کیف پولی به طور کامل امن نیست، زیرا هارد رایانه شما می تواند خراب شود و یا کیف پول آنلاین ممکن است مورد حمله هکرها قرار گیرد. کیف پول های موبایل نیز وجود دارند که دارای ظرفیت ذخیره سازی بالایی هستند و هر لحظه همراه شما هستند. کیف پول های سخت افزاری و کیف پول کاغذی با دو کد QR نوع دیگر کیف پول ها هستند که نسبت به حملات سایبری و یا خرابی سخت افزاری ایمن می باشند. یکی از سایتهای ارائه دهنده کیف پول آنلاین، بلاک چین دات کام است که جزو اولین وبسایتها در این زمینه نیز می باشد. (طوفان زاده، ۱۳۹۴)

ویژگی های بیت کوین

- غیرمتمرکز بودن

یکی از اهداف اصلی ساتوشی ناکاموتو هنگام خلق بیت کوین، استقلال شبکه آن از هر گونه قدرت کنترل گر بود. این ارز دیجیتال رمزیایه به گونه ای طراحی شده است که هر شخص و هر کسب کار و همچنین هر دستگاه دخیل در استخراج و تایید اعتبار تراکنش ها، بخشی از یک شبکه وسیع را تشکیل می دهند. همچنین طراحی طوری است که حتی اگر بخشی از شبکه از دسترس خارج شود، پول همچنان در حرکت خواهد بود.

- ناشناس بودن

این روزها بانک ها تقریباً همه چیز را درباره ی مشتریان خود شامل تاریخچه اعتبار، آدرس ها، شماره تلفن ها، روند دخل و خرج و نیز غیره را می دانند. با توجه به این که نیازی نیست کیف پول به هیچ گونه اطلاعات شناسایی شخصی مرتبط شود، این داستان در بیت کوین بسیار متفاوت است. در حالی که برخی از مردم نمی خواهند اموال آن ها به وسیله ی هیچ یک از مقامات کنترل و ردیابی شود، گروهی دیگر ممکن

¹¹ cryptocurrency

است استدلال کنند تجارت مواد مخدر، تروریسم، و سایر فعالیت های غیر قانونی و خطرناک با توجه به ویژگی ناشناس بودن بیت کوین، رشد و رونق پیدا می کند. (مژدهی، ۱۳۹۴)

- شفاف بودن

ناشناس بودن هویت دارندگان بیت کوین نسبی است، زیرا تراکنش های این ارز رمزپایه تنها زمانی انجام می گیرند که در پلت فرم بلاک چین ذخیره شده باشند. در تئوری، اگر آدرس کیف پول شما به طور عمومی مورد استفاده قرار گیرد، هر شخصی به وسیله ی مطالعه دفتر حساب بلاک چین، قادر است بگوید چه مقدار پول در آن قرار دارد. هر چند، ردیابی از آدرس بیت کوین به اشخاص هنوز هم تقریباً غیر ممکن است. کسانی که تمایل دارند تراکنش هایشان ناشناس بماند، می توانند اقدامات لازم را برای گریز از رادار انجام دهند. کیف پول های متعددی وجود دارند که ابهام در تراکنش ها و امنیت شما را در اولویت قرار می دهند، اما ساده ترین کار، استفاده از چندین آدرس و عدم انتقال مقادیر عظیم پول تنها به یک آدرس بیت کوین می باشد.

- سریع

شبکه بیت کوین پرداخت ها و انتقالات را تقریباً بلافاصله انجام می دهد و به طور معمول فقط چند دقیقه طول می کشد که در آن سوی دنیا شخص دیگری ارز را دریافت کند، در حالی که انجام چنین انتقالی در بانک ها می تواند چندین روز طول بکشد.

- غیر قابل لغو

زمانی که بیت کوین را برای کسی انتقال می دهید، هیچ راهی برای لغو یا بازگرداندن آن وجود ندارد، مگر این که شخص دریافت کنند بخواهد بیت کوین را به شما بازگرداند. این یک تضمین برای دریافت و انتقال پرداخت است، به این معنی که شخصی که شما ارز را برای وی انتقال داده اید هرگز نمی تواند ادعا کند که انتقال برای وی انجام نشده است. (رشیدی، ۱۳۹۴)

نقاط ضعف بیت کوین

❖ مسائل قانونی

موقعیت قانونی بیت کوین از کشوری تا کشور دیگر به شدت متفاوت است. در برخی کشورها، استفاده و معامله از طریق بیت کوین ترغیب می شود در حالی که در دیگر کشورها غیرقانونی و ممنوع اعلام شده است. نگرانی های زیادی در رابطه با نیاز جنایتکاران به بیت کوین وجود دارد، برخی خبرگزاری ها حتی اعلام کرده اند شهرت بیت کوین تنها به دلیل توانایی آن برای مبادله کالاهای غیرقانونی می باشد. در حقیقت، هنگامی که بازار سیاه اینترنتی به نام Silk Road متلاشی شد، ارزش بیت کوین فوراً کاهش یافت. (wired.com)

❖ درجه ی به رسمیت شناختن

اگر چه بعضی از دولت های جهان هنوز هیچ قوانینی را در رابطه با بیت کوین وضع نکرده اند و حتی بعضی به طور کامل آن را ممنوع کرده اند، این ارز رمزپایه در کشورهای بسیاری به رسمیت شناخته شده و کاملاً قانونی است. اکثر تجارت ها اعم از بزرگ و کوچک همچنان به آن بی توجه هستند. تقریباً می توان گفت این که بخواهیم دیگر ارزها را رها کرده و منحصر از بیت کوین استفاده کنیم، تقریباً غیرممکن است.

❖ مفقودی کلیدها (رمزها)

کلید یک رمز عبور منحصر به فرد و الفبایی است که برای دسترسی به کیف پول بیت کوین ضروری است. گم کردن این کلید به معنای از دست دادن کیف پول می باشد. با این حال، اکثر کیف پول های فعلی مکانیسم هایی برای پشتیبان گیری اطلاعات و بازگردانی رمز عبور دارند. اما بدیهی است قبل از اینکه کاربران بتوانند از آن ها استفاده کنند باید اقدامات لازم جهت تنظیم آن ها را انجام بدهند.

❖ نوسانات

قیمت این ارز رمزپایه دارای فراز و نشیب هایی بوده و می باشد و از میان چرخه های گوناگون صعودی و نزولی گذر کرده است که از بعضی از آن ها به عنوان حباب و یا انفجار قیمتی یاد می شود. بیت کوین در تاریخ پیدایش خود با افزایش های جدیدی تنها به منظور این که

بتواند با افت های بزرگی که پس از آنها بوجود می آیند مواجهه کند، همراه بوده است. ارزش این ارز دیجیتال غیرقابل پیش بینی است زیرا معمولاً به سرعت و به شدت در حال تغییر است که می تواند باعث خسارت مالی قابل توجهی به یک سرمایه گذار بی احتیاط شود.

❖ توسعه مداوم

آینده ی بیت کوین نسبتاً مشخص نیست. در حال حاضر، دولت ها و بانک ها قادر به کنترل این ارز نیستند. اما هرچه این ارز بزرگتر و مشهور تر می شود، دولت های بیشتری سعی می کنند آن را تحت کنترل خود قرار دهند. یک بیت کوین که تحت کنترل قرار گرفته و قانون گذاری شده است، یک نوع ارز کاملاً متفاوت خواهد بود. (پاکروان، ۱۳۹۸)

معاملات بیت کوین در ایران

در ایران معاملات بیت کوین با کشورهای دیگر کمی تفاوت دارد؛ میثاق (۱۳۹۷) در پژوهشی بیان دارد که بعضی صرافی ها معاملات بیت کوین را انجام می دهند اما در حال حاضر وضعیت تفاوت کرده و صرافی های کمی به این کار مشغول هستند بنابراین شرایط معاملات در ایران کاملاً چهره به چهره است؛ افراد در گروه های تلگرامی مربوط به بیت کوین عضو هستند و آنجا درباره معاملات صحبت می شود و معمولاً تا کاربران یکدیگر را نبینند، معامله ای انجام نمی شود. شیوه کار هم به این صورت است که طرفین معامله مقابل بانک قرار می گذارند، همدیگر را می بینند، همان لحظه از طریق کیف پول معامله بیت کوین انجام می شود و پول به صورت کارت به کارت رد و بدل می شود بنابراین اصلاً مشخص نیست پولی که جابجا شده، بابت چه کاری بوده است؛ البته این موضوع درباره سایر معاملات در ایران نیز صدق می کند و مشخص معامله بیت کوین نیست. (میثاق، ۱۳۹۷)

در ایران وضعیت این معاملات هنوز مشخص نشده است؛ برخی آن را به خاطر مصرف زیاد برق نادرست می دانند و برخی دیگر به خاطر فقدان قانون مختص به آن، معاملات بیت کوین غیر قانونی شناخته شده است. با این حال هنوز تصمیم متمرکزی درباره آن گرفته نشده است. وزارت صنعت آن را قانونی اعلام کرده اما رییس مرکز ملی فضای مجازی گفته آنچه هم اکنون توسط عده ای از مردم انجام می شود، خلاف قانون است، چون قانونی وجود ندارد که با آن مغایرت داشته باشد.

بیت کوین به عنوان راهی برای دور زدن تحریم ها مطرح شد و البته هیچگاه به مرحله اجرا نرسید اما آهسته آهسته میان مردم عادی استفاده شد. تعداد افرادی که از این طریق در ایران معامله می کنند، مشخص نیست و از سوی دیگر مواجهه مقامات بانک مرکزی با این پدیده هم چندان روشن نیست.

افرادی که در این حوزه فعالیت دارند، معتقدند تا سال های آینده جمعیت افرادی که به معاملات بیت کوین علاقمند خواهند شد، به شدت افزایش خواهد یافت، با این حال به علت وضعیت فنی مبهم شیوه تولید پول که برای بسیاری از کاربران ناشناخته است، این احتمال وجود دارد که افراد زیادی نخواهند دارایی خود را برای خرید و فروش پدیده ای مصرف کنند که از طریق نهادهای رسمی نظارت ناپذیر است، با این حال افرادی که به طور حرفه ای در کار معامله بیت کوین هستند، معتقدند ارزهای دیجیتال به منظور امنیت و ناشناس بودن ساخته شده اند بنابراین تقلب در تراکنش های آن جایگاهی ندارد؛ کسی مالک آن ها نیست و کسی نمی تواند آن ها را متوقف یا هک کند. (مهرانی راد، ۱۳۹۸)

ماینینگ یا استخراج

استخراج بیت کوین، ستون فقرات شبکه این ارز دیجیتال است. ماینرها یا استخراج کنندگان برای تامین امنیت و تایید تراکنش های بیت کوین، نقش حیاتی ایفا می کنند. بدون وجود ماینرها، شبکه مورد حمله قرار می گیرد و ناکارآمد خواهد بود. استخراج بیت کوین توسط کامپیوترهای خاصی انجام می شود و وظیفه ماینرها این است که شبکه را امن کرده و تراکنش بیت کوین را پردازش نمایند. ماینرها با حل یک مساله محاسباتی به جوابی دست می یابند که به آن ها اجازه می دهد تا بلاک های تراکنش ها را به هم متصل کنند (بلاک های متصل تشکیل یک بلاکچین می دهند). ماینرها به ازای این سرویس که به شبکه می دهند، کارمزد تراکنش و بیت کوین جدید جایزه می گیرند. در حقیقت با این کار بیت کوین تولید کرده اند و به همین دلیل هم به کار آنها استخراج می گویند.

شبکه بلاک چین طوری طراحی شده است که ماینرها با هدف تامین امنیت شبکه و تایید تراکنش های بیت کوین فعالیت می کنند و برای خدماتی که ارائه می دهند هر ده دقیقه یکبار یک بلاک تولید می کنند که به ازای آن بیت کوین دریافت می کنند. اما سوال مهمی که شاید از

خودتان پیروید این است که چرا باید چیزی به اسم استخراج وجود داشته باشد. این سوال از جنبه‌های زیادی قابل بررسی است اما اساسی‌ترین دلایل وجود ماینر موارد زیر است که به شرح هر کدام پرداخته شده است: (باغبان، ۱۳۹۸)

۱. موضوع تولید و ایجاد بیت کوین جدید

ارزهای سنتی -مانند دلار یا یورو- توسط بانک‌های مرکزی صادر می‌شوند. این بانک مرکزی است که به صورت انحصاری می‌تواند واحدهای جدیدی از پول را در هر زمانی براساس سیاست‌های خود (بهبود وضعیت اقتصاد یا حتی گاهی اوقات تضعیف آن) صادر کند. موضوع چاپ پول و پشتوانه طلایی آن همیشه مساله‌ای رمزآلود برای عموم مردم باقی خواهد ماند. اما بیت کوین متفاوت است و این مشکل متمرکز سازی را تا حد زیادی حل کرده است. ماینرها به صورت غیرمتمرکز در سرتاسر دنیا در حال فعالیت هستند و تمام خدمات و کارهایشان در شبکه قابل مشاهده و پیگیری است و تمام مردم می‌توانند بدون واسطه شاهد انجام امور مالی خود باشند. ماینرها نیز هر ده دقیقه مقدار مشخصی بیت کوین پاداش می‌گیرند. نرخ پاداش و کارمزد تراکنش‌ها در کد نوشته شده برای شبکه تنظیم شده است، بنابراین ماینرها نمی‌توانند سیستم را فریب دهند یا بیت کوین از جایی دیگری تولید یا وارد شبکه کنند. ماینرها مجبورند از توان محاسباتی خود برای استخراج پول استفاده کنند. (فتاحی، ۱۳۹۷)

۲. تایید تراکنش‌ها بدون وجود نهاد مرکزی و به صورت غیرمتمرکز

یک تراکنش می‌تواند تنها زمانی امن و کامل در نظر گرفته شود که در یک بلاک قرار داشته باشد. چون فقط با قرار گرفتن در یک بلاک است که به طور رسمی در بلاکچین بیت کوین قرار خواهد گرفت. بلاکچین زنجیره‌ای از بلاک‌هاست که به یکدیگر متصل هستند. برای تغییر یک بلاک در ساختار بلاکچین، باید تمامی بلاک‌های قبل و بعد آن تغییر کند که با توجه به تعریف بلاکچین چنین چیزی تقریباً غیرممکن است. پس اگر تراکنشی را در شبکه فرستاده شد همیشه باید منتظر تایید ماینرها و ایجاد بلاک های بعدی آن شد. پیشنهاد شده است تا ۶ بلاک بعدی برای تایید نهایی تراکنش خود منتظر ماند چرا که:

صفر بلاک: این تراکنش ممکن است برگشت بخورد! پس حتما حداقل یک بلاک منتظر بمانید.

یک بلاک: تراکنش‌های کوچک. اگر تراکنشی با ارزش کمتر از ۱۰۰۰ دلار ارسال یا دریافت کرده‌اید، ایجاد یک بلاک برای شما کافی است.

سه بلاک: برای تراکنش‌هایی بین ۱۰۰۰ تا ۱۰,۰۰۰ دلار سه بلاک کافی خواهد بود، معمولاً اکسچنج‌ها هم سه بلاک برای تراکنش‌های برداشت منتظر خواهند ماند.

شش بلاک: تراکنش‌های بزرگ. این مقدار انتظار برای تراکنش‌های بین ۱۰,۰۰۰ تا ۱,۰۰۰,۰۰۰ دلار کافی خواهد بود. ایجاد شش بلاک به طور کلی، مطمئن‌ترین زمان برای قطعی دانستن یک تراکنش در شبکه است. (فتاحی، ۱۳۹۷)

۳. امنیت سیستم

ماینرها با دشوار کردن حمله یا متوقف کردن آن، شبکه را امن می‌کنند. به دلیل خاصیت غیرمتمرکز بودن شبکه، ماینرها و نودهای شبکه در سرتاسر دنیا و بدون وجود نهاد مرکزی با یکدیگر شبکه را مدیریت می‌کنند. این یعنی قدرت انحصاراً دست فرد یا گروه خاصی نیست و بین همه تقسیم شده است. پس می‌توان گفت هرچه تعداد ماینرها و نودها بیشتر باشد، امنیت شبکه بالاتر خواهد رفت. در این حالت، تنها راه حمله به شبکه، داشتن بیش از ۵۱ درصد از قدرت هش شبکه است که با توجه به سختی شبکه امری تقریباً غیرممکن است و از سال ۲۰۰۸ که بیت کوین وارد دنیا شده است تا کنون، چنین اتفاقی نیفتاده است. در حقیقت این توزیع قدرت است که باعث امنیت شبکه بیت کوین شده است.

پیشینه مطالعاتی

✓ بیلندی (۱۳۹۶) در پژوهشی با عنوان «بیتکوین، ارزی مجازی» بیان دارد که تا سال ۲۰۲۷، حدود ۱۰ درصد از تولید ناخالص داخلی جهان بر پایه ارزهای مجازی خواهد بود و دولتها به دلیل از دست دادن قدرت پولی خود، به فکر راهکارهای جایگزینی در

برابر توسعه ارزهای مجازی خواهند افتاد. از اینرو، از قدرت دلار در سطح جهان کاسته خواهد شد. در بین ارزهای مجازی، بیتکوین توانسته است بیشتر مورد توجه و اقبال عمومی قرار بگیرد و حتی اگر خود بیتکوین هم، با فرض محال، نتواند ادامه حیات دهد، بدون شک کمک شایسته ای به رونق ارزهای مجازی خواهد کرد. شالوده ارزهای مجازی و به ویژه بیتکوین، بر نظام رمزگذاری استوار است. پرداخت از کیف پول، برگشت پذیر نیست و با توجه به اینکه تمامی مبادلات بدون وجود هویت واقعی شما صورت می گیرد، کوچکترین اشتباه در درج نشانی ممکن است موجب از دست دادن پول، بدون امکان برگشت آن باشد. در چنین فضایی هم مبادله های نقدی و هم کشف و پیشگیری از تقلبها، بسیار متفاوت خواهد بود.

✓ رشیدی و صیاد معروف (۱۳۹۴) در مقاله واحد پول دیجیتالی بیت کوین و نقش آن در تجارت الکترونیک بیان دارند که بیت کوین پول مجازی است که تولید آن حاصل فعالیت محاسباتی زمانبری است که به آن کاوش گفته میشود، این پول بین المللی تحت مدیریت هیچ بانکی نبوده و میتواند برای خرید کالا از هرجایی در جهان مورد استفاده قرار بگیرد، همچنین میتواند آنرا مانند سهام یا پول فلزی داد و ستد کرد. هدف اصلی این مقاله پرداختن به بیت کوین به عنوان یک پول مجازی از دید یک کاربر میباشد که در کنار آن به اهدافی مانند آشنایی با بیت کوین برای ناشناختگان آن، جذب افراد مستعد و به رخ کشیدن قابلیت های بیت کوین در دنیای مجازی و تجارت الکترونیک نیز پرداخته شده است. در این مقاله نگاهی دوباره و دیدی جدید نسبت به رایجترین پول دیجیتالی شناخته شده پرداخته شده است و با پیشبرد اهداف خود از منظر حقوقی و اقتصادی بیت کوین، باتوجه به تجارت الکترونیک پرداخته شده است. این پول، ارزی جدید با هزینه معاملاتی کمتر نسبت به بازارهای ارز سنتی است و به صورت غیر متمرکز و بدون وجود نهاد واسطه و نهاد ناظری همچون دولت، بانک و مؤسسات مالی بر خلاف ارزهای سنتی صادر شده توسط دولت ها فعالیت میکند.

✓ پاکروانی و مهرانی راد (۱۳۹۸) در مقاله تکنولوژی بانک چین و تاثیرات آن بر حرفه حسابرسی بیان دارند که فناوری بانک چین برای اولین بار به عنوان فناوری مرکزی و هسته اصلی و پشتیبان بیت کوین تعریف گردیده و دارای دو مبنای اصلی شامل: (۱) این موضوع به عنوان سرچشمه سیستم اکوسیستم دیجیتال غیرمتمرکز و (۲) بمنظور اجرایی نمودن بعد از سال ۲۰۰۸ به عنوانی مبنایی اصلی این فناوری تعریف گردیده است که بر اساس آن این تکنولوژی با استفاده از تکنولوژی شبکه همکار مورد استفاده قرار می گیرد و سیستم آن همراه با رمزنگاری عمل می نماید، بطوریکه ترکیب این عوامل یک مجموعه تشکیل داده که آنها را قادر می سازد که بدون هرگونه تحویل و تحول داده به یکدیگر و بدون نیاز به یک واسطه اعتبار بخشی سنتی همانند یک بانک یا شبکه پردازش پرداخت با حذف واسطه ها با استفاده از قدرت شبکه های درون مجموعه اقدام نماید. در این سیستم زنجیره فناوری ذیربط ممکن است فرصت های جدیدی را برای کاهش قابل ملاحظه هزینه های انجام معاملات را فراهم می آورد و همچنین زمان انجام معاملات را کاهش می دهد. بدین ترتیب بانک چین بصورت بالقوه برای تبدیل داده ها و حذف اختلالات سیستمی در بسیاری از صنایع از جمله حوزه خدمات مالی، بخش عمومی و اطمینان بخشی گردیده است و سرمایه گذاری های قابل انجام و همچنین حوزه مدیریت سرمایه گذاری در تعداد زیادی از شرکت های بزرگ با تکنولوژی بانک چین در هم تنیده شده اند.

✓ احمدی علیانی (۱۳۹۸) در پژوهشی با عنوان ارز دیجیتال ۳۸۱ اینطور بیان داشتند که امروزه در دنیای تجارت، روش های پرداخت نوآورانه ای به وجود آمده است. چنین روش هایی بر مبنای پلت فرم هایی مانند تلفن های موبایل، اینترنت و کارت های ذخیره سازی دیجیتالی بنا شده اند. این سیستم های پرداخت جایگزین روز به روز در حال گسترش و پیشرفت هستند. سیستم های پرداختی که بر پایه واحد های پول بدون پشتوانه به وجود آمده اند، به خودی خود باعث می شوند که استفاده از ارزهای دیجیتالی راحت تر شود. در نتیجه پرداخت ها سریع تر، انعطاف پذیرتر و روش های آن خالقانه تر خواهند شد.

✓ باغبان (۱۳۹۸) در پژوهشی با عنوان مقاله چالش های حقوقی فعالیت بیت کوین در ایران بیان داشت که بیت کوین از جمله نوآوری ها در حوزه تجارت الکترونیکی و مالی محسوب می شود که طی پنج سال گذشته گسترش یافته است. بیت کوین نوعی نوآوری اینترنتی با کارکردی مشابه پول است که طی سال هایی که رواج یافته، ارزش آن در بازارهای جهانی از چند صدم دلار به هزاران دلار افزایش یافته است. اگر چه تعداد زیادی خواستار رونق بیتکوین اند، افراد زیادی هم خواستار ممنوع شدن آن هستند و

بدین ترتیب بیت کوین با چالش های جدی مواجه می باشد که سبب می شود آینده مبهمی داشته باشد و سرمایه گذاران را با نگرانی جدی مواجه سازد.

✓ فتاحی (۱۳۹۷) در مقاله تاثیر فناوری اطلاعات بر ابزارهای مبادلاتی (پول) مطالعه موردی بیت کوین اینگونه بیان دارد که تاثیر فناوری اطلاعات بر ابزارهای مبادلاتی ، باعث ظهور انواع پول مجازی گردیده است . در این مقاله ، به طور ویژه ، بیت کوین مورد بررسی قرار گرفته است . توضیحاتی در خصوص نحوه تولید ، ابزارهای مورد نیاز برای تهیه یا خرید و فروش با آن ، تفاوت بیت کوین با سایر انواع پول و نحوه کار شبکه بیت کوین ارائه شده است.

مصرف انرژی و بیت کوین

روش اجماع با حداقل اعتماد بیت کوین^{۱۲} از زمان پیدایش وابسته به الگوریتم اثبات-کار^{۱۳} بوده است. ماشین هایی که «کار» را انجام می دهند برای این مهم میزان عظیمی انرژی مصرف می نمایند. شاخص مصرف انرژی بیت کوین برای فهم میزان مصرف و ارتقای آگاهی در مورد ناپایداری^{۱۴} الگوریتم اثبات-کار ایجاد شده است.

در نظر داشته باشید که این شاخص منحصر به بیت کوین و بیت کوین کش^{۱۵} بوده و دیگر شاخه های بیت کوین را در نظر نیاورده است. هر بلوک مجموعه ای جدید از تراکنش ها است که تقریباً هر ده دقیقه یکبار توسط ماینرها به بلاکچین بیت کوین اضافه می شود. برای کار روی بلاکچین نیازی به وجود اعتماد بین ماینرها نیست. تنها چیزی که ماینرها باید به آن اعتماد کنند کدی است که بیت کوین را اجرا می کند. این کد شامل چندین قانون برای تأیید تراکنش های جدید است. برای مثال یک تراکنش تنها زمانی می تواند صحیح باشد که فرستنده میزان درج شده در تراکنش را دارا بوده باشد. تک تک ماینرها به صورت انفرادی التزام تراکنش به این قوانین را تأیید کرده و لزوم اعتماد بین ماینرها را مرتفع می سازند. (علیائی، ۱۳۹۸)

مسئله اصلی اقتناع ماینرها به توافق روی تاریخچه یکتایی از تراکنش ها است. هر ماینر در شبکه به طور مداوم وظیفه آماده سازی دسته تراکنش های بعدی بلاکچین را بر عهده دارد. تنها یک بلوک به صورت تصادفی^{۱۶} از میان این همه انتخاب شده و تبدیل به آخرین بلوک زنجیره خواهد گردید. انتخاب تصادفی در یک شبکه توزیع یافته کار ساده ای نیست و اینجاست که اثبات-کار به میان می آید. در اثبات-کار بلوک بعدی متعلق به اولین ماینری است که بتواند یک بلوک معتبر تولید کند. البته این امر در مقام عمل به این سادگی نیست. پروتکل بیت کوین انجام این کار را برای ماینرها دشوار می سازد. درواقع این دشواری به طور منظم توسط پروتکل چنان تغییر می کند که تضمین کند تمام ماینرها در شبکه هر ده دقیقه (تقریب) تنها یک بلوک معتبر تولید کنند. زمانی که یکی از ماینرها موفق به تولید یک بلوک معتبر شود به بقیه شبکه هم اطلاع می دهد. دیگر ماینرها پس از تأیید مطابقت بلوک با تمام قوانین آن را قبول کرده و بلوکی که خود در حال ساختنش بودند را دور می ریزند. ماینر خوش شانس علاوه بر کارمزد تراکنش های پردازش شده در بلوک به میزان ثابتی کوین (coin) پاداش می یابد. این چرخه بار دیگر از اول آغاز می شود. فرایند تأیید یک بلوک معتبر به شدت وابسته به سعی و خطا است. ماینرها چندین بار در ثانیه به دنبال مقدار صحیح یک مؤلفه بلوک به نام نانس^{۱۷} هستند و امیدوارند بلوک کامل شده مطابق با الزامات باشد (راهی برای پیش بینی نتیجه نیست). به این دلیل است که گاهی ماینرینگ (استخراج) را به انتخاب ارقام بلیت در مسابقه بخت آزمایی^{۱۸} تشبیه می کنند. تعداد تلاش ها در هر ثانیه برای یافتن نانس را هَش (hash) می نامند و میزان آن وابسته به قدرت پردازشی دستگاه ماینرینگ است که معمولاً با گیگا-هش در ثانیه (یک میلیارد هش در ثانیه) نمایش داده می شود. (کاشیان، ۱۳۹۷)

سیکل مداوم استخراج بلوک به مردم در سرتاسر جهان برای استخراج بلوک پاداش می دهد. با توجه به این که ماینرینگ می تواند یک جریان ثابت درآمدی به وجود بیاورد، مردم حاضر به اجرا کردن ماشین های پرمصرف برای به دست آوردن گوشه ای از درآمد ماینرینگ هستند. این

¹² Bitcoin

¹³ proof-of-workproof-of-work

¹⁴ unsustainability

¹⁵ Bitcoin CashBitcoin Cash

¹⁶ Random

¹⁷ nonce

¹⁸ lottery

امر و بالا رفتن قیمت بیت‌کوین در طول سال‌های اخیر باعث افزایش انرژی مصرفی شبکه بیت‌کوین و رسیدن به مقادیر خیره‌کننده‌ای گشته‌اند. بر اساس گزارش منتشرشده توسط آژانس بین‌المللی انرژی^{۱۹} مصرف شبکه کلی بیت‌کوین بیشتر از برخی کشورها است. مصرف انرژی بیت‌کوین را می‌توان به‌عنوان درصدی از مصرف انرژی کشورهای بزرگ هم بیان نمود. بزرگ‌ترین مشکل بیت‌کوین مصرف میزان عظیمی انرژی نیست، مسئله اینجا است که انرژی شبکه غالباً توسط الکتریسیته تولیدشده از نیروگاه‌های با سوخت زغال‌سنگ در چین تأمین می‌شود. در این کشور الکتریسیته بر پایه زغال‌سنگ باقیمت اندکی تولید می‌گردد. حتی با فاکتورهای محافظه‌کارانه انتشار دی‌اکسید کربن، تأثیر کربن هر تراکنش بیت‌کوین رقم خیره‌کننده‌ای است. در مقایسه با یک تراکنش معمول بدون وجه نقد در یک سامانه مالی معمول، بیت‌کوین هزاران بار بیشتر انرژی مصرف می‌کند. ممکن است این میزان انرژی به نظر عده‌ای قیمتی مناسب برای عدم نیاز به وجود شخص ثالث معتمد باشد، اما نشان خواهیم داد که لزومی به پرداخت چنین هزینه بالایی نیست.

اگرچه اثبات-کار اولین الگوریتم اجماع بود که توانست خود را اثبات کند ولی تنها الگوریتم اجماع نیست. در طی سال‌های اخیر الگوریتم‌های با مصرف انرژی بهینه‌تری مانند اثبات-سهام^{۲۰} در حال توسعه بوده‌اند. در اثبات-سهام، به‌جای ماینرها این صاحبان کوین هستند که بلوک را می‌سازند و در نتیجه دیگر نیاز به ماشین‌های پرمصرف برای تولید حداکثر میزان هش در ثانیه نیست. به همین دلیل مصرف انرژی اثبات-سهام در مقایسه با اثبات-کار ناچیز است. اتخاذ چنین الگوریتم اجماعی توسط بیت‌کوین می‌تواند باعث افزایش قابل‌توجه پایداری سیستم گردد. تنها عیب این امر وجود نسخه‌های متعددی از اثبات-سهام است که هیچ‌کدام هنوز نتوانسته‌اند خود را کاملاً اثبات کنند. با این وجود کارهای انجام‌گرفته بر روی این الگوریتم‌ها نوید حل این مسئله در آینده را می‌دهد. (گودرزی، ۱۳۹۷)

تمام کامپیوترهایی که سعی دارند در رقابت محاسباتی تولید توکن برنده باشند، تلاش می‌کنند تا یک پاسخ خاص و تقریباً تصادفی در الگوریتم ریاضی پیدا کنند. اما الگوریتم بسیار پیچیده است و تنها راه یافتن پاسخ دلخواه این است که حدس‌های فراوانی زده شوند. هرچه یک کامپیوتر بتواند حدس‌های بیشتری بزند، احتمال یافتن توکن در این کامپیوتر افزایش می‌یابد. اما در مقابل هر بار که یک رایانه حدس می‌زند، از برق برای محاسبات خود استفاده می‌کند. این روند عمدتاً مردم را تشویق می‌کند تا از رایانه‌های سریع‌تر و میزان مصرف برق بیشتری استفاده کنند تا جواب درست را پیدا نمایند و بیت‌کوین‌های جدید را که هر ۱۰ دقیقه یکبار یا بیشتر توزیع می‌شوند را استخراج کنند. این فرایند با استفاده از نرم‌افزار اصلی بیت‌کوین، که در سال ۲۰۰۹ (۱۳۸۸) منتشر شد، تعریف شده است. در آن سال هدف این بود که سکه‌های جدید را برای افرادی که در شبکه بیت‌کوین حضور دارند، بدون دخالت یک موسسه مرکزی که پول را تحویل دهد، توزیع کنند. اوایل، رقابت فقط بین کامپیوترهای لپ‌تاپ بود. اما قوانینی در شبکه ایجاد شدند که بر اساس آنها هرچه تعداد رایانه‌های موجود در شبکه بیشتر شوند، الگوریتم به صورت خودکار تنظیم می‌شود تا سخت‌تر گردد، و هر کسی که بخواهد رقابت کند، باید از رایانه‌های قوی‌تر و برق بیشتری استفاده کند. (فتاحی، ۱۳۹۷)

این روزها، در حدود ۱۲.۵ بیت‌کوین در هر ۱۰ دقیقه یا بیشتر عرضه می‌شوند، که حدود ۱۲۰ هزار دلار (۵۵۰ میلیون تومان) ارزش دارند. به طوری که مردم مایل به سرمایه‌گذاری‌های نجومی برای شرکت در این رقابت هستند. این امر باعث شد که رقابت سخت‌تر و سخت‌تر شود و به همین دلیل است که در حال حاضر سرورهای بزرگی در سراسر جهان به استخراج بیت‌کوین اختصاص داده شده‌اند. این فرایند برای موجودیت بیت‌کوین مهم است زیرا در فرایند استخراج بیت‌کوین، تمام کامپیوترها به عنوان حسابداران شبکه بیت‌کوین خدمت می‌کنند. کامپیوترها الگوریتمی را حل می‌کنند که نیازمند آنها است تا تمامی معاملات جدید را که در شبکه وجود دارند، پیگیری کند و آنها را حل نماید.

رقابت استخراج بیت‌کوین از آن جهت سخت است که هیچ کس نمی‌تواند بر نحوه حسابداری غلبه کند و سوابق را نادیده بگیرد. در مقاله ۲۰۰۸ که برای اولین بار بیت‌کوین را توصیف می‌کرد، خالق مرموز پول مجازی، ساتوشی ناکاموتو، نوشت که سیستم به گونه‌ای طراحی شده است تا حمله مهاجم حریص^{۲۱} را که ممکن است بخواهد سوابق را عوض کند و یا مردم را با سرقت پرداخت‌ها همراه کند، به دلیل قوانین ماینینگ و حسابداری، خنثی شود. در دسامبر ۲۰۱۷، چند تحلیلگر با انتقاد از مصرف زیاد برق توسط مراکز استخراج بیت‌کوین و ارزهای دیجیتال روند استخراج را «فاجعه‌ی زیست‌محیطی» نامیدند. پیش از این، نشریه‌ی کوین‌تلگراف گزارش داده بود که استخراج ارزهای دیجیتال احتمالاً مصرف برق بیشتری نسبت به خانوارها در سال ۲۰۱۸ خواهند داشت. (پاکروان، ۱۳۹۸)

¹⁹ International Energy Agency International Energy Agency

²⁰ proof-of-stake

²¹ greedy attacker

اسماری مک‌کارتی (سیاستمدار و عضو حزب^{۲۲} ایسلند و یکی از فعالان حوزه‌ی نوآوری و اطلاعات) اظهار داشت مصرف بیش‌ازحد منابع برای بیت‌کوین چیزی جز ضرر نیست؛ چرا که کاربرد اصلی بیت‌کوین «سفته‌بازی» است و فقط به منظور انجام معاملات ریسک‌دار تولید می‌شود. اگر دوست‌داران محیط‌زیست و تحلیلگران کاربرد اصلی بیت‌کوین و ارزهای دیجیتال دیگر را فقط سفته‌بازی می‌دانند، مصرف این مقدار برق ممکن است غیرقابل قبول باشد. اما کاربرد اصلی بیت‌کوین واقعاً سفته‌باز نیست. بیت‌کوین در کشورهایی که تعداد بانک‌ها برای دسترسی مردم به خدمات مالی ناکافی است، عملکرد مطلوبی دارد. به عنوان نمونه، در ونزوئلا ساکنان محلی برای تهیه‌ی غذا، کالاهای مورد نیاز و دارو از خارج از کشور از بیت‌کوین استفاده می‌کنند. زیرا پول ملی این کشور (بولیوار ونزوئلا) تقریباً تمام ارزش خود را از دست داده است. (صیادمعرف، ۱۳۹۴)

الگوریتم اجماع مبتنی بر اثبات کار بیت‌کوین، از توان محاسباتی جهانی برای تأیید تراکنش‌ها و تولید ارزهای دیجیتال جدید از طریق یک سیستم ریاضی استفاده می‌کند. سیستم اثبات کار بیت‌کوین اجازه نمی‌دهد که هرکس به پروتکل غیرمتمرکز آن دسترسی پیدا کند و به این شکل سیستم بیت‌کوین بلاکچین می‌تواند تراکنش‌ها را بدون واسطه و به صورت هم‌تا به هم‌تا انجام دهد. بنابراین، بهانه کردن مصرف برق به منظور زیر سؤال بردن ارزهای غیرمتمرکز که تأثیر شگرفی بر اقتصاد جهانی دارند غیرمنطقی است و این نوعی ادعای بیمارگونه است که می‌گویند کاربرد ارزهای دیجیتال و فناوری بلاکچین فقط سفته‌بازی است.

سفته‌بازی در هر حوزه‌ای که در مراحل اولیه‌ی رشد و پیشرفت است وجود دارد. در ابتدا، سرمایه‌گذارها قصد دارند روی ارزش و قیمت ارزهای دیجیتال و دارایی‌های دیجیتال سفته‌بازی‌هایی انجام دهند. اما این سرمایه‌گذارها با رشد صنعت و بازار مجبور می‌شوند از توکن‌ها برای کاربردهای سودمندتر و قابلیت تعویض‌پذیری استفاده کنند. (مهرانی راد، ۱۳۹۸)

مدل مصرف انرژی و مفروضات اصلی

اگرچه به‌سادگی می‌توان قدرت هش کل شبکه را محاسبه نمود، به علت نبود سوابق و اطلاعات درباره تمام ماشین‌های فعال، محاسبه مصرف انرژی شبکه غیرممکن است. در گذشته گمانه‌زنی‌های صورت گرفته در مورد مصرف انرژی برای رسیدن به عدد مشخصی از وات مصرفی در ثانیه بر پایه مفروضاتی در باب نوع ماشین‌های فعال و نحوه توزیع آن‌ها بود. یک بررسی دقیقاً یک معدن^{۲۳} واقعی بیت‌کوین نشان می‌دهد چگونه چنین رویکردی با صرف‌نظر از اطمینان به ماشین^{۲۴} و محیط و هزینه‌های سرمایه‌ش باعث حاصل شدن عدد کوچک‌تری می‌گردد. این رویکرد غیردقیق منجر به مشاهده تخمین‌های متفاوت و با انحراف قابل‌توجه از یکدیگر و در مواردی بی‌توجهی به عواقب اقتصادی این پارامترها شده است. شاخص مصرف انرژی بیت‌کوین قصد دارد با تغییر دیدگاه مسئله را از دید اقتصادی موردتوجه قرار دهد. در ساخت این شاخص فرض بر این بوده که هزینه‌ها و درآمد یک ماینر با یکدیگر ارتباط دارند. با توجه به این که هزینه الکتریسیته یک مؤلفه اصلی در هزینه‌ها به شمار می‌رود، به این نتیجه می‌رسیم که مصرف انرژی بیت‌کوین در کل شبکه هم باید با درآمد ماینرها ارتباط داشته باشد. به بیان ساده‌تر، هرچه درآمد ماینرها بیشتر باشد، تعداد بیشتری ماشین پرمصرف می‌توانند پشتیبانی شوند. (باغبان، ۱۳۹۸)

چگونگی محاسبه شاخص مصرف انرژی بیت‌کوین

• اول: محاسبه کل درآمد از استخراج بیت‌کوین (دلار)

• دوم: تخمین درصد هزینه برای الکتریسیته

در این شاخص فرض شده است که در موازنه به‌طور متوسط ۶۰٪ درآمد ماینرها صرف هزینه‌های عملیاتی می‌شود.

• سوم: یافتن قیمت پرداختی ماینرها برای هر کیلو-وات ساعت (kW/h)

به ازای هر ۵ سنت هزینه عملیاتی، فرض شده که ۱ کیلو-وات ساعت انرژی مصرف‌شده است.

• چهارم: تبدیل هزینه‌ها به مصرف انرژی

تولید زمان می‌برد. تغییر قیمت‌ها می‌تواند زیاد یا کم باشد ولی ماشین‌های پرمصرف جدید یک‌شبه ظاهر نخواهند شد. رفتار واقع‌بینانه در مورد تغییرات قیمت، لحاظ کردن زمان کافی برای تولیدکنندگان جهت پاسخ به تغییر در شرایط خواهد بود.

²² Pirate

²³ mine

²⁴ reliability

شاخص بر این فرض استوار است که ماشین‌های جدید منوط به این که سودآور باشند تولید خواهند شد تا زمانی که رسیدن به سود غیرممکن باشد و بازار به تعادل برسد.

پیش‌بینی مصرف انرژی بیت‌کوین در آینده

شاخص مصرف انرژی بیت‌کوین، برخلاف تخمین‌های وابسته به میزان هَش، یک مدل پیش‌بینی برای مصرف آینده بیت‌کوین هم هست. این مدل پیش‌بینی می‌کند که در آخر ۶۰٪ درآمد ماینرها صرف هزینه‌های الکتریسیته خواهد شد. در حال حاضر (ژانویه ۲۰۱۸) این میزان به مراتب کم‌تر است. در اواخر ژانویه ۲۰۱۸ شاخص انرژی بیت‌کوین میزان مخارج الکتریسیته را حدود ۲۲٪ درآمد تخمین زده است. بر این اساس شاخص مصرف انرژی بیت‌کوین، با فرض درآمد ثابت، میزان تقریبی ۱۳۰ تراوات ساعت در سال را برای مصرف انرژی بیت‌کوین در آینده تخمین می‌زند. مورگان استنلی هم مصرف انرژی بیت‌کوین در آینده را چیزی بین ۱۲۰ تا ۱۴۰ تراوات در ساعت محاسبه کرده است. می‌توان نتیجه گرفت که شاخص نسبتاً ساده تخمین مصرف انرژی بیت‌کوین همان چیزی را نشان می‌دهد که شواهد غیرقابل‌انکار در مورد واقعیت استخراج بیت‌کوین در شرایط واقعی و همچنین پیش‌بینی‌های تولید چیپ‌های استخراج به آن اشاره می‌کنند. (باغبان، ۱۳۹۸)

بیت‌کوین قاتل انرژی

دانشمندان معتقدند که مصرف انرژی مورد نیاز برای برداشت بیت‌کوین به شدت بالا است و این امر در حال بدتر شدن است و عواقب خطرناکی برای زمین در بر خواهد داشت. بیت‌کوین یک پدیده بسیار عجیب و غریب در دنیای امروزی ما است و برداشت آن به روش‌های دیجیتالی و کاملاً کامپیوتری انجام می‌شود. شاید در نگاه نخست به نظر بیاید که بیت‌کوین با توجه به مصرف الکتریسیته، یک موضوع و ماهیت سبز است ولی در عمل مصرف انرژی مورد نیاز برای برداشت آن به اندازه‌ای زیاد است که این پدیده را به شدت مخرب ساخته است.

تحقیقات جدید دانشمندان نشان داده است که برداشت بیت‌کوین از محیط‌های ابری در طول سال گذشته میلادی مسبب مصرف رقم نجومی ۷.۷ گیگاوات انرژی الکتریکی بوده است. این انرژی بسیار زیاد است و برای درک دقیق‌تر حجم آن کافی است بدانید که می‌توان با چنین انرژی الکتریکی‌ای، کل کشور استرالیا را برای یک سال تامین توان کرد. با این حال موضوع نگران‌کننده اصلی این است که این موضوع در حال بدتر شدن و حجم انرژی مصرفی بیت‌کوین، روزبه‌روز در حال افزایش یافتن است. پیش‌بینی شده که بیت‌کوین در پایان سال جاری میلادی، نیم درصد از انرژی الکتریکی کل جهان را به خود اختصاص می‌دهد. این تحقیقات به تازگی در ژورنال بین‌المللی Joule منتشر شده‌اند. بنابر تحقیقات مذکور ارزهای دیجیتال تا چه اندازه برای محیط‌زیست مخرب هستند. انرژی الکتریکی در بسیاری از مناطق جهان از طریق راهکارهای غیر سبز تهیه می‌شود و همین امر نیز موجب شده است که مصرف بالاتر الکتریسیته توسط بیت‌کوین، آلودگی بیشتری را نیز ایجاد کند.

بیت‌کوین در دنیای امروزی ما به هیچ‌عنوان یک پدیده بهینه نبوده و یک فاجعه زیست‌محیطی به حساب می‌آید. با این حال پیش‌بینی می‌شود که به زودی قوانینی اعمال شود که جلوی این تخریب و روند نامناسب را خواهد گرفت و آینده بیت‌کوین و تمامی ارزهای دیجیتال ممکن است دستخوش تغییراتی بزرگ شوند. آکس دوریس به عنوان یک متخصص بلاک چین درباره این موضوع می‌گوید که هر بیت‌کوین در جهان نیاز به انرژی ۲.۵۵ گیگاواتی برای یک تراکنش دارد. این امر موجب می‌شود که یک تراکنش بیت‌کوینی مصرف انرژی بیشتری از کل مصرف یک خانوار در طول یک ماه داشته باشد. او نیز معتقد است که بیت‌کوین مشکلی بزرگ دارد که در حال بزرگ‌تر شدن هم هست. (فتاحی، ۱۳۹۷)

منابع

۱. بیلندی، علی فرزین، ۱۳۹۶، بیتکوبین ارزی مجازی، مقاله علمی پژوهشی حسابرسی، شماره ۹۲، دی ماه ۱۳۹۶
۲. منصوری فر، مهران، ۱۳۹۷، ملزومات بیت کوین، مقاله پژوهشی حسابداری، www.modireweb.com
۳. احمدی علیائی، ریحانه، ۱۳۹۸، ارز دیجیتال ۳۸۱، دومین کنفرانس ملی پدافند سایبری
۴. احمدی علیائی، ریحانه، ۱۳۹۸، ارز دیجیتال ۳۸۱، دومین کنفرانس ملی پدافند سایبری، مراغه، دانشگاه آزاد اسلامی واحد مراغه.
۵. کاشیان، عبدالمحمد و گودرزی، فهیمه (۱۳۹۷)، نگاهی نو به ماهیت اقتصادی و فقهی پول های رمز پایه، همایش بین المللی مدیریت، حسابداری و اقتصاد دانش بنیان
۶. محمدی، محمد، ۱۳۹۷، تاثیر ابزار فناوری بر ارکان مبادلاتی (پول) مطالعه موردی بیت کوین، دومین همایش ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران
۷. صیادمعروف، محمدرسلول؛ علی طوفان زاده مژدهی و حسن رشیدی، ۱۳۹۴، واحد پول دیجیتالی بیت کوین و نقش آن در تجارت الکترونیک، دومین کنفرانس بین المللی پژوهش در علوم و تکنولوژی، ترکیه - استانبول، موسسه سرآمد همایش کارین.
۸. پاکروان، لقمان و قاسم مهرانی راد، ۱۳۹۸، تکنولوژی بلک چین و تاثیرات آن بر حرفه حسابرسی، دومین کنفرانس بین المللی مدیریت، مهندسی صنایع، اقتصاد و حسابداری، تفلیس-گرجستان، دبیرخانه دائمی با همکاری دانشگاه امام صادق(ع)
۹. باغبان، اسماعیل، ۱۳۹۸، چالش های حقوقی فعالیت بیت کوین در ایران، دومین کنفرانس ملی پدافند سایبری، مراغه، دانشگاه آزاد اسلامی واحد مراغه.
۱۰. فتاحی، عصمت، ۱۳۹۷، تاثیر فناوری اطلاعات بر ابزارهای مبادلاتی (پول) مطالعه موردی بیت کوین، دومین همایش ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران، تهران، موسسه برگزار کننده همایش های توسعه محور دانش و فناوری سام ایرانیان