

بہ نام خدا



سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

مدیریت فروش، توسعه و مطالعات

سیت کوین، نخستین پول مجازی

میراثم سید حسینی، مراثم دعائی

کد گزارش: ۹۳-۶-۲۰۱۴

تاریخ: تیر ۹۳

چکیده

بیت‌کوین نوعی پول مجازی است که در سال ۲۰۰۹ راه‌اندازی شد. این پول، ارزی جدید با هزینه معاملاتی کمتر نسبت به بازارهای ارز سنتی است و به‌صورت غیرمتمرکز و بدون وجود نهاد واسط و نهاد ناظر (دولت، بانک و مؤسسات مالی) برخلاف ارزهای سنتی صادرشده توسط دولت‌ها فعالیت می‌کند. بیت‌کوین به‌صورت فیزیکی وجود ندارد و تنها حساب‌هایی شامل رمزهای عمومی و خصوصی وجود دارند. اطلاعات حساب‌ها به همراه تراکنش‌های صورت گرفته بین حساب‌ها در یک دفتر کل ثبت می‌شود که نیازمند حجم وسیعی از توان محاسباتی کامپیوتری برای تأیید و ثبت این اطلاعات در سرتاسر کامپیوترهای عضو شبکه در جهان می‌باشد. در ابتدا ارزش بیت‌کوین نسبت به ارزهای دیگر ناچیز بود، ولی در حال حاضر استفاده و ارزش آن به‌صورت چشمگیری افزایش پیدا کرده است. از طرف دیگر ابهامات بسیاری در مورد پشتیبانی و افراد تأمین‌کننده این سیستم وجود دارد. در این راستا در این نگارش سعی بر آن است تا خواننده تا حد امکان با این سیستم آشنایی پیدا کند و ابعاد مختلف اقتصادی، اجتماعی، سیاسی و قانونی آن بررسی شود.

کلمات کلیدی: بیت‌کوین، ارز مجازی، پول رمزگذاری شده، بلوک، زنجیره بلوکی، استخراج بیت‌کوین، کیف پول بیت‌کوین، سیستم نظیر به نظیر

فهرست مطالب

- ۱- مقدمه ۱
- ۲- معرفی و تاریخچه پول مجازی ۱
- ۳- مبانی اصلی سیستم بیت کوین ۶
- ۳-۱- بلوک بیت کوین ۶
- ۳-۲- زنجیره بلوکی ۷
- ۳-۳- استخراج بیت کوین ۷
- ۳-۴- کیف پول بیت کوین ۸
- ۴- بحث بر سر بیت کوین ۸
- ۵- تنظیم و نظارت بیت کوین و قوانین مربوطه ۱۰
- ۶- بحث فقهی بیت کوین ۱۱
- ۷- نتیجه گیری ۱۲
- ۸- منابع ۱۳

۱- مقدمه

پس از ورود پول به مبادلات روزمره مردم، بانک‌ها با حمایت دولت‌ها، هر از چند گاهی با انتشار یا جمع‌آوری پول سعی در اجرای سیاست‌های اقتصادی خود داشته‌اند. همچنین سیاست‌های پولی گاهی موجب می‌شد که آن‌ها با سرازیر کردن مقدار زیادی پول به بازار، ارزش آن را تحت تأثیر قرار دهند. از طرف دیگر در مبادلات کنونی جهانی، بانک‌ها و مؤسسات مالی به عنوان نهادهای واسطه مالی، مبالغ قابل توجهی را به عنوان هزینه‌های انتقال وجه و هزینه مبادلات پول دریافت می‌کنند.

برای تسهیل انجام امور مالی و ایجاد پولی بدون حضور واسطه‌ها (بانک‌ها و مؤسسات مالی)، مفهوم پول مجازی^۱ به معنای پول رمزگذاری شده^۲، اولین بار در سال ۱۹۹۸ توسط وی‌دای^۳ مطرح شد. وی پیشنهاد نوع جدیدی از پول را ارائه داد که از روش رمزگذاری کامپیوتری برای کنترل تولید پول و انجام معاملات بدون واسطه و مرجع مرکزی استفاده شود؛ اما این ایده تا سال ۲۰۰۹ فقط در حد یک نظریه بود. در این سال همزمان با رکود اقتصادی، فردی (شاید هم‌گروهی رموز) با نام ساتوشی ناکاماتو^۴، یک واحد پول مجازی به نام بیت‌کوین^۵ را به صورت کاربردی، همراه با الگوریتم ریاضی تولید آن در جهان مطرح کرد و مقاله‌ای ارائه داد و آن را متعاقباً به صورت اجرایی درآورد. پول مجازی هیچ سرویس‌دهنده مرکزی یا مؤسسه مالی برای کنترل نقل و انتقال ندارد؛ چون همه چیز بر ارتباطات نظیر به نظیر^۶ بنا شده است. این پدیده‌ای است که دولت‌ها نمی‌توانستند آن را دست‌کاری کنند و بانک‌ها نمی‌توانستند ارزش آن را کم‌وزیاد نمایند.

در ادامه ابتدا به معرفی و تاریخچه پول مجازی پرداخته و سپس مفاهیم تخصصی این سیستم و نحوه عملکرد آن مورد بررسی قرار خواهیم داد. سپس نقاط مثبت و منفی این سیستم را مورد بررسی قرار داده و در نهایت به ابعاد قانونی و شرعی چنین سیستمی از دیدگاه دول مختلف پرداخته‌ایم.

۲- معرفی و تاریخچه پول مجازی

بیت‌کوین یک سیستم اینترنتی عمومی است که یک شبکه پرداخت وجوه و تولید پول به صورت کاملاً الکترونیکی معرفی کرده است. بیت‌کوین اولین شبکه پرداخت غیرمتمرکز و نظیر به نظیر است که قدرت خود را از کاربران می‌گیرد و هیچ واسطه یا مرجع مرکزی برای مدیریت که در آن دخل و تصرف کند، وجود ندارد. از منظر کاربران، بیت‌کوین درواقع پول اینترنتی است.

¹ Virtual Currency or Digital Currency

² Cryptocurrency

³ Wei Dai

⁴ Satoshi Nakamoto

⁵ Bitcoin

^۶ Peer to Peer: فناوری نظیر به نظیر به کاربران این اجازه را می‌دهد که اسناد کامپیوتری را به صورت مستقیم، بدون دخالت یک سرویس‌دهنده یا پایگاه اینترنتی مرکزی، به یکدیگر انتقال دهند که منجر به امن‌تر و سریع‌تر شدن سیستم شده و امکان دست بردن در اسناد و تغییر آن‌ها تقریباً صفر می‌شود.

در اوت سال ۲۰۰۸ دامنه پایگاه Bitcoin.org در اینترنت ثبت شد و تا به امروز نیز مشخص نیست که چه کسی این دامنه را به ثبت رسانده است. اکتبر سال ۲۰۰۸ فردی به نام ساتوشی ناکاماتو در خبرنامه رمزگذاری شده‌ای به نام metzdowd.com اعلام کرد: «من در حال کار بر روی سیستم پول الکترونیکی جدیدی هستم که کاملاً نظیر به نظیر و بدون دخالت شخص ثالث می‌باشد». مقاله علمی مذکور سرمنشأ این پول مجازی یعنی بیت‌کوین بوده و معروف به مقاله سفید با عنوان «بیت‌کوین: سیستم پولی الکترونیک نظیر به نظیر» می‌باشد. در ژانویه ۲۰۰۹ بلوک صفر بیت‌کوین در دنیای اینترنت استخراج^۱ شد که تنها شامل پیغامی مبنی بر شروع به کار سیستم بوده و جایزه آن ۵۰ بیت‌کوین برای ساتوشی بود. چند روز بعد اولین نسخه از نرم‌افزار بیت‌کوین به‌صورت متن‌باز^۲ ارائه شد و فردای آن روز بلوک یک بیت‌کوین استخراج گردید و تراکنش بیت‌کوین بین کاربران اولیه صورت گرفت. در بخش‌های بعدی این مفاهیم به‌صورت گسترده‌تر توضیح داده خواهد شد.

ارزش اولیه بیت‌کوین توسط کاربران مختلف در تالارهای گفتگو و بیشتر بر اساس هزینه‌هایی ازجمله هزینه برق فعالیت کاربران سیستم تعیین می‌شد تا جایی که در فوریه ۲۰۱۰ اولین صرافی اینترنتی برای تبدیل بیت‌کوین به ارزهای دیگر برای کاربران راه‌اندازی شد. یکی از جالب‌ترین خریدهای اولیه توسط بیت‌کوین در می ۲۰۱۰، خرید دو عدد پیتزا از یک پیتزافروشی مطرح در آمریکا به قیمت ۱۰,۰۰۰ بیت‌کوین بوده است که این امر نشان‌دهنده ارزش بسیار پایین بیت‌کوین در آغاز می‌باشد.

یکی از بزرگ‌ترین مشکلات سیستم بیت‌کوین، شکاف‌های امنیتی است که تا به حال کشف شده است؛ اوت ۲۰۱۰ در سیستم بیت‌کوین یک شکاف امنیتی کشف شد که منجر به تولید بی‌رویه ۱۸۴ میلیارد بیت‌کوین و مصرف چندباره^۳ آن‌ها شده بود که به‌سرعت شناسایی و جلوی این تولید بی‌رویه گرفته شد. در طی سال‌های اخیر موارد بسیاری از دزدی و هک شدن دستگاه‌های کاربران گزارش شده که منجر به از دست رفتن رمزهای خصوصی و در نتیجه از دست رفتن سرمایه کاربران شده است.

با رشد بیت‌کوین و افزایش کاربران، ابزارهای مالی جدید در مورد بیت‌کوین به کار گرفته شد. در اکتبر ۲۰۱۰ قرارداد فروش استقرایی بین کاربران بیت‌کوین شکل گرفت. در همان سال قراردادهای اختیار خرید و فروش روی بیت‌کوین شکل گرفت.

بیت‌کوین به‌مرور در حال شناخته شدن بود و موارد مهمی ازجمله شرکت ویکی‌لیکس^۴ در افزایش ارزش آن تأثیر داشته‌اند. در سال ۲۰۱۱ پایگاه اینترنتی ویکی‌لیکس اقدام به افشای اطلاعات محرمانه دولت‌های مختلف بخصوص دولت آمریکا کرد و بسیاری از افراد عادی در راستای حمایت از این سایت اقدام به اهدای پول به این سایت نمودند ولی بسیاری از

^۱ Mined

^۲ Open Source

^۳ Double Spending

^۴ WikiLeaks: ویکی‌لیکس یک سازمان خبرنگاری غیرانتفاعی جهانی به‌صورت اینترنتی است که اطلاعات و اخبار محرمانه و لو رفته و سری و طبقه‌بندی شده را از منابع ناشناس افشا می‌کند.

سرویس‌دهندگان شخص ثالث (مانند پی‌پال^۱ و مسترکارت^۲) وجه‌اهدایی را به دلیل فشار دولت آمریکا به ویکی‌لیکس انتقال ندادند. پی‌پال حساب‌های این سازمان را نیز مسدود کرد تا اجازه دسترسی به منابع مالی خود را نیز نداشته باشند.

بسیاری از کاربران و اهداکنندگان اعتراض کردند که سرویس‌دهندگان شخص ثالث حق چنین کاری را ندارند. باوجود اینکه این سرویس‌دهندگان حق تصمیم در مورد نحوه مصرف پول توسط کاربران را ندارند؛ در بسیاری از موارد در این امر دخالت می‌کنند. کاربران برای انجام تراکنش‌های اینترنتی از این سرویس‌ها استفاده می‌کنند و زمانی که دولت بخواهد این انتقال وجوه را کنترل و محدود نماید، این سرویس‌دهندگان را ملزم به چنین کاری می‌کند. برای انجام تراکنش اینترنتی باید یک حساب نزد یکی از سرویس‌دهندگان وجود داشته باشد که تراکنش‌های درخواستی کاربر را انجام دهند. تا قبل از به وجود آمدن بیت‌کوین، پولی وجود نداشت که بین دو کاربر بدون دخالت و نظارت طرف ثالث ردوبدل شود.

در همین راستا ویکی‌لیکس از همان زمان بیت‌کوین را به‌عنوان منبع کمک مالی قبول کرد که هیچ طرف ثالث و دولتی امکان مداخله در آن را نداشت. به‌مرور بسیاری از پایگاه‌ها و فروشگاه‌های اینترنتی، مؤسسات خیریه و حتی گروه‌های تروریستی نیز بیت‌کوین را برای پرداخت وجوه قبول می‌کردند که تعدادی از این شرکت‌ها و سایت‌ها توسط دولت آمریکا توقیف و بسته شدند؛ ازجمله سایت مطرح فروش داروهای مختلف به نام جاده ابریشم^۳ که متهم به فروش داروهای غیرقانونی بود. همین امر منجر شد که در سال ۲۰۱۲ اف‌بی‌آی گزارشی در مورد خطرهای حال حاضر بیت‌کوین و استفاده‌های غیرقانونی آن توسط گروهک‌های تروریستی و قاچاق مواد، اسلحه و دارو هشدار دهد؛ بااین‌وجود اولین دستگاه خودپرداز برای مبادله بیت‌کوین با سایر ارزها در می ۲۰۱۳ در سان‌دیگو، کالیفرنیا راه‌اندازی شد.

در همان سال ۲۰۱۲ تحقیقاتی توسط دادگاه ایالات‌متحده صورت گرفت که ادعا می‌کرد که بیت‌کوین شبیه طرح پونزی^۴ عمل می‌کند. به‌طوری‌که از پول خود افراد به آن‌ها سود می‌دهد؛ چیزی شبیه شرکت‌هایی که آن‌ها را هرمی می‌خوانند^۵. درواقع طرح پونزی یک نوع طرح کلاهبرداری سرمایه‌گذاری است که وعده نرخ سود بالا با ریسک کم را به سرمایه‌گذاران می‌دهد. در این طرح به سرمایه‌گذاران قدیمی از طریق پول سرمایه‌گذاران جدید سود داده می‌شود. وقتی که سرمایه‌گذاران جدید وارد این سیستم نشوند به‌طور خودکار پرداخت سود قطع شده و سیستم از هم می‌پاشد. شرکت بانی مقدار پول زیادی را به دست آورده و متواری می‌شود. این فرضیه همچنان پابرجا است و همچنان بسیاری به این مبحث مشکوک هستند.

ارزش بیت‌کوین هیچ پشتوانه‌ای نداشته و کاملاً بستگی به میزان عرضه و تقاضا دارد. لازم به ذکر است که طبق آخرین آمار در تاریخ ۲۴ ژوئن سال ۲۰۱۴ (۹۳/۴/۳) بیش از ۱۲,۹ میلیون بیت‌کوین باارزشی بالغ بر ۷,۸ میلیارد دلار موجود و نرخ استخراج

¹ PayPal

² Master Card

³ Silk Road

⁴ Ponzi Scheme

⁵ Pyramid Scheme

بیت‌کوین، ۲۵ عدد در هر ۱۰ دقیقه بوده است. نمودار شماره ۱ روند تغییرات قیمت بیت‌کوین را بین سال‌های ۲۰۰۹ تا ژوئن ۲۰۱۴ نشان می‌دهد.



نمودار شماره ۱- روند تغییرات قیمت بیت‌کوین بین ۲۰۰۹ تا ۲۰۱۴ (منبع: bitcoincharts.com)

درواقع می‌توان بیان کرد که در عالم واقعیت چیزی به‌عنوان بیت‌کوین وجود ندارد و فقط حساب‌های مجازی شامل رمزهای عمومی و خصوصی متشکل از رشته طولانی از اعداد و حروف هستند که از طریق یک الگوریتم کدگذاری ریاضی ایجاد شده‌اند. رمز عمومی (شبیه شماره حساب بانکی) به‌عنوان آدرسی برای کاربر در دنیای مجازی است که دیگران می‌توانند به آن بیت‌کوین ارسال کنند. رمز خصوصی (شبیه رمز کارت عابر بانک) باید مخفی نگه داشته شود و به‌منظور اجازه و تأیید انجام تراکنش‌های بیت‌کوین استفاده می‌شود.

از زمان راه‌اندازی شبکه بیت‌کوین بحث بسیاری در مورد ماهیت بیت‌کوین وجود داشته است؛ آیا واقعاً بیت‌کوین را می‌توان به‌عنوان یک نوع ارز، سرمایه یا کالا در نظر گرفت یا بیت‌کوین دارای هیچ ارزش خاصی نیست. در مارس سال ۲۰۱۴ سرویس درآمد داخلی (IRS)^۱ ایالات متحده اعلام کرد که تمامی ارزهای مجازی از جمله بیت‌کوین، شامل مالیات بر دارایی می‌شوند و ارز به‌حساب نمی‌آیند. سود یا ضرر ناشی از بیت‌کوین اگر به‌عنوان سرمایه نگهداری شود، تحت عنوان سود و زیان سرمایه تلقی می‌شود؛ درحالی‌که اگر به‌عنوان موجودی نگهداری شود، شامل سود و زیاد عادی خواهد شد.

افراد یا شرکت‌های مجزایی تحت عنوان «استخراج‌گر»^۲ که قدرت و تجهیزات محاسباتی لازم را دارا هستند، در شبکه بیت‌کوین به فعالیت مشغول می‌شوند و انگیزه آن‌ها دستیابی به جایزه استخراج (انتشار بیت‌کوین جدید در شبکه) و کارمزد معاملاتی است که برحسب بیت‌کوین پرداخت می‌شود. این استخراج‌گرها را می‌توان به‌عنوان مرجع غیرمتمرکز در نظر گرفت که انجام معاملات و اعتبار شبکه بیت‌کوین را فراهم می‌کنند. بیت‌کوین جدید با یک نرخ ثابت به استخراج‌گرها جایزه داده می‌شود؛ البته این نرخ به‌صورت بازه‌ای نصف می‌شود؛ به‌نحوی که درنهایت تعداد کل بیت‌کوین در شبکه به سمت ۲۱ میلیون

¹ Internal Revenue Service

² Miner

عدد میل می‌کند و بیشتر از آن نخواهد شد. هر بیت‌کوین تا هشت رقم قابلیت ریز شدن دارد که به ریزترین واحد، ساتوشی اطلاق می‌شود. البته بر اساس نیاز و توافق استخراج‌گرها، این واحد می‌تواند ریزتر بشود.

از چهار طریق می‌تواند بیت‌کوین به دست آورد:

- فروش کالا و خدمات بر اساس بیت‌کوین؛
- خرید بیت‌کوین از صرافی‌های بیت‌کوین؛
- خرید بیت‌کوین از افرادی که بیت‌کوین دارند؛
- جایزه گرفتن بیت‌کوین از طریق فرایند رقابتی استخراج (تولید بیت‌کوین).

فرد با در اختیار داشتن بیت‌کوین، به راحتی و آسان‌تر از خرید با کارت اعتباری، خریدهای خود را انجام می‌دهد. پرداخت‌ها به سادگی از طریق برنامه موبایل یا کامپیوتر با وارد کردن آدرس دریافت‌کننده، مقدار پرداخت و فشردن گزینه ارسال قابل انجام است. حتی برای ساده‌تر شدن کار از بارکد مشخص نیز می‌توان استفاده کرد. افزایش روز افزون این نرم‌افزارها و امکانات مختلفی که در اختیار کاربران برای انجام تراکنش‌ها می‌دهند، مشکلاتی نیز به همراه دارد، از جمله عدم امنیت بالای تمام این نرم‌افزارها و امکان هک و دزدیده شدن بیت‌کوین کاربران. در شکل شماره ۱ نمونه‌ای از برنامه موبایل انتقال بیت‌کوین نشان داده شده است.

The image shows two side-by-side screenshots of the Bitcoin.org mobile application interface. The left screenshot is titled 'Send Bitcoins' and features a 'Pay to' field with a placeholder 'type address or name', an 'Amount to pay' field set to 'BTC 0.00', and a 'Fee' field set to 'BTC 0.0005'. At the bottom are 'Cancel' and 'Send' buttons. The right screenshot is titled 'Request Bitcoins' and features a 'Requested amount (optional)' field set to 'BTC 1.66', an 'Address to request to' field containing a long alphanumeric string, and a checkbox labeled 'include label with address'. At the bottom right, there is a QR code with the text 'Have this QR-code scanned by the sender:' above it.

شکل شماره ۱- نمایی از ارسال و دریافت بیت‌کوین با استفاده از یک برنامه مخصوص موبایل (منبع: Bitcoin.org)

۳- مبانی اصلی سیستم بیت کوین

در این بخش، تعریف واژگان مرتبط و اصلی با این سیستم ارائه شده است. این واژگان عبارتند از بلوک بیت کوین، زنجیره بیت کوین، استخراج بیت کوین و کیف پول بیت کوین.

۳-۱- بلوک بیت کوین

بلوک‌ها اسناد کامپیوتری هستند که داده‌های متعلق به شبکه بیت کوین را به صورت دائمی در خود ثبت می‌کنند. یک بلوک، تعدادی یا کل سوابق تراکنش‌های شبکه بیت کوین در یک بازه زمانی که در بلوک‌های قبلی وارد نشده است را ثبت می‌کند؛ بنابراین یک بلوک مانند صفحه‌ای از یک دفتر کل یا دفتر ثبت اسناد است. هر بار که یک بلوک کامل می‌شود، ساخت بلوک بعدی در زنجیره بلوکی آغاز می‌شود. هر بلوک ذره‌ای از بلوک‌های قبلی و آدرس بلوک بعدی را در خود قرار می‌دهد تا امکان دست‌کاری بلوک‌ها یا حذف یک بلوک وجود نداشته باشد. بنابراین یک بلوک، مخزن دائمی اسنادی است که یک‌بار ثبت شده‌اند و دیگر قابل تغییر یا حذف شدن نیست. شبکه بیت کوین شاهد حجم زیادی از تراکنش‌ها است. نگهداری سابقه این تراکنش‌ها به کاربران کمک می‌کند تا مقدار بیت کوین موجود در هر آدرس را مورد محاسبه قرار داده و جابجایی بیت کوین‌ها بین آدرس‌های مختلف را مشاهده کنند.

برای فهم بهتر بیت کوین، بهتر است این پول را با تراکنش‌های بانکی مقایسه کنیم. زنجیره بلوکی مانند دفتر ثبت بانک است و یک بلوک ممکن است تنها یک تأیید تراکنش باشد که دستگاه خودپرداز بانک بعد از بهره‌برداری آن را چاپ می‌کند. درواقع یک بلوک جزء کوچکی از زنجیره بلوکی است.

یک مسئله ریاضی به هریک از بلوک‌ها پیوند زده شده است. استخراج‌گرانی وجود دارند که به طور مداوم در حال رقابت بر سر پردازش و ثبت تراکنش‌های شبکه بیت کوین هستند. آن‌ها تلاش می‌کنند که سریع‌تر از بقیه، بلوک حال حاضر را تکمیل کنند تا به ازای آن، هم کارمزد معاملات را دریافت کنند و هم بیت کوین از شبکه پاداش بگیرند. زمانی که استخراج‌گر، بلوکی را تکمیل کند، برنده به حساب می‌آید و اقدام به حل مسئله می‌کند؛ جواب مسئله بین گروه‌های استخراج به اشتراک گذاشته می‌شود و سپس تأیید اعتبار می‌شود. هر بار که یک استخراج‌گر یک مسئله را حل کند، ۲۵ بیت کوین جایزه دریافت می‌کند و می‌تواند آن را در چرخه شبکه بیت کوین خرج کند. اولین مدرک ثبت‌شده در بلوک بعدی تراکنش مربوط به جایزه‌ای است که استخراج‌گر برنده بلوک قبلی دریافت کرده است. مسئله ریاضی به نحوی است که درجه سختی آن نسبت به زمان تعیین می‌شود؛ یعنی درنهایت مسئله حل می‌شود ولی میزان محاسبات آن به صورتی تنظیم می‌شود که با توجه به توان محاسباتی متوسط سخت‌افزار کامپیوترهای مورد استفاده توسط استخراج‌گرها کمتر از مثلاً ۱۰ دقیقه طول نکشد. درواقع سطح دشواری مسئله ریاضی که باید توسط استخراج‌گر برنده در پایان تکمیل هر بلوک حل شود، نرخ تولید بیت کوین جدید در شبکه را تنظیم می‌کند؛ زیرا تا زمانی که مسئله حل نشده است، ساخت بلوک جدید در شبکه آغاز نمی‌شود. در حال حاضر حدود ۱۰ دقیقه طول می‌کشد تا یک مسئله در شبکه حل شود؛ پس در هر ۱۰ دقیقه ۲۵ بیت کوین تولید می‌شود.

۳-۲- زنجیره بلوکی

همان‌طور که بیان شد، زنجیره بلوکی یک دفتر ثبت عمومی است که تمامی تراکنش‌های بیت‌کوین که تا به حال اجرا شده است را در خود دارد و همواره با اضافه شدن بلوک‌های جدید در حال رشد است. بلوک‌های جدید به صورت زنجیروار و بر اساس تاریخ به زنجیره بلوکی اضافه می‌شوند. هر یک از گره‌ها (کامپیوترهای استخراج‌گران که به شبکه بیت‌کوین متصل هستند و از برنامه کامپیوتری متن‌باز^۱ برای تأیید اعتبار و جریان انداختن تراکنش‌ها استفاده می‌کند) یک کپی از زنجیره بلوکی را به صورت خودکار بعد از پیوستن به شبکه بیت‌کوین دریافت می‌کند. زنجیره بلوکی شامل اطلاعات کامل آدرس حساب‌ها و محتویات آن‌ها از زمان شروع تا حال حاضر است؛ یعنی در واقع می‌توان فهمید که هر آدرس در شبکه بیت‌کوین دارای چه مقدار بیت‌کوین بوده و هست. همین مسئله باعث می‌شود که بسیاری از طرفداران بیت‌کوین اذعان کنند که استفاده از بیت‌کوین برای کارهای غیرقانونی مثل پول‌شویی یا قاچاق اسلحه بسیار دشوارتر از پول سنتی است، مگر اینکه گردانندگان اصلی بیت‌کوین، روش‌های خاصی برای این کار بکار گیرند. البته درست است که شفافیت تا حدی وجود دارد ولی بیت‌کوین نیز مانند هر ابزار مال‌دیگری می‌تواند برای مقاصد مجرمانه به کار گرفته شود. تعداد بلوک در حال اضافه شدن به زنجیره بلوکی ممکن است این نگرانی را ایجاد کند که حجم داده‌ها برای ذخیره‌سازی بر روی هر کامپیوتر بسیار زیاد خواهد شد ولی با فناوری استفاده شده در شبکه بیت‌کوین حجم زنجیره بلوکی بسیار پایین است و با توجه به قانون مور^۲ در مورد کامپیوترها که اذعان دارد سرعت محاسباتی پردازنده‌ها هر دو سال دو برابر می‌شود، مشکلی برای انتقال سریع این زنجیره در شبکه وجود ندارد.

۳-۳- استخراج بیت‌کوین

همان‌طور که مطرح شده است، استخراج بیت‌کوین فرایندی است که در آن تراکنش‌های تأیید شده و به دفتر ثبت عمومی به نام زنجیره بلوکی اضافه می‌شوند و همچنین به واسطه این فرایند، بیت‌کوین جدید در شبکه منتشر می‌شود. هر فردی با دسترسی به اینترنت و داشتن سخت‌افزار مناسب می‌توان به عنوان استخراج‌گر در فرایند استخراج سهیم شود. مقدار بیت‌کوین جدیدی که در ازای استخراج هر بلوک منتشر می‌شود را جایزه بلوک می‌خوانند. جایزه بلوک طبق تعریف سیستم بعد از کامل شدن ۲۱۰,۰۰۰ بلوک که تقریباً ۴ سال طول می‌کشد، نصف می‌شود. جایزه بلوک سال ۲۰۰۹ با مقدار ۵۰ بیت‌کوین شروع شد و در حال حاضر نصف شده و ۲۵ بیت‌کوین است. این روند نصف شدن جایزه منجر می‌شود که در نهایت مقدار بیت‌کوین به سمت ۲۱ میلیون میل کند و بیشتر از آن نشود.

سؤالی که در اینجا مطرح می‌شود این است که مسئله ریاضی که برای دستیابی به جایزه استخراج بلوک باید حل شود تا چه اندازه دشوار است؟ جواب این سؤال به تلاشی که برای استخراج در شبکه صورت می‌گیرد بستگی دارد؛ یعنی میزان قدرت محاسباتی سخت‌افزار بکار گرفته شده توسط استخراج‌گران. دشواری استخراج بر اساس سیستم شبکه بیت‌کوین بعد از تکمیل هر ۲۰۱۶ بلوک؛ یعنی تقریباً هر دو هفته یک‌بار، تنظیم می‌شود. سختی مسئله به نحوی تنظیم می‌شود تا نرخ تکمیل بلوک‌ها

¹ Open Source

² Moore's Law

ثابت بماند. پس اگر قدرت محاسباتی بیشتری (کامپیوترهای قوی‌تر) برای استخراج به کار گرفته شود، سختی مسئله نیز افزایش می‌یابد و بلعکس.

در روزهای اولیه بیت‌کوین، استخراج با استفاده از واحد محاسباتی مرکزی^۱ (CPU) کامپیوترهای معمولی انجام می‌شد. بعد به دلیل کارآمدتر بودن واحد محاسباتی گرافیکی^۲ (GPU)، محبوبیت بیشتری پیدا کرد. در سال ۲۰۱۳ اولین سخت‌افزارهای مخصوص استخراج، برای شبکه بیت‌کوین به نام ASIC تولید شدند که قدرت محاسباتی بالاتر و مصرف انرژی کمتری داشتند و در حال حاضر نیز در حال پیشرفت و قدرتمندتر شدن هستند. نکته مهم اینجاست که در صورتی که از سخت‌افزاری استفاده شود که مصرف انرژی آن بهینه نباشد، ممکن است هزینه مصرف انرژی بیشتر از درآمد حاصل از استخراج شود.

۳-۴- کیف پول بیت‌کوین

کیف بیت‌کوین نرم‌افزاری است که بیت‌کوین‌ها در آن نگهداری می‌شوند. از لحاظ فنی، بیت‌کوین در هیچ کجا نگهداری نمی‌شود، بلکه رمزهای خصوصی هستند که برای آدرس هریک از بیت‌کوین‌ها وجود دارند و در کیف بیت‌کوین فردی که صاحب حساب است، نگهداری می‌شود. کیف بیت‌کوین ارسال و دریافت بیت‌کوین را تسهیل بخشیده و مالکیت حساب بیت‌کوین را برای کاربر نگه می‌دارد. کیف بیت‌کوین به چهار صورت نرم‌افزار کامپیوتری، موبایل، تحت وب و به صورت سخت‌افزاری برای کاربران موجود است.

مراقبت از کیف بیت‌کوین بسیار حیاتی است زیرا در صورت گم‌شدن یا دزدیده شدن امکان بازیابی اطلاعات وجود ندارد. بهتر است رمز ورود بسیار قوی برای کیف استفاده شود یا رمزهای خصوصی مربوط به بیت‌کوین‌ها در مکانی امن به صورت دستی یادداشت شود.

۴- بحث بر سر بیت‌کوین

حال که مفهوم بیت‌کوین و نحوه عملکرد آن بیان شد، به مقایسه این سیستم با پول سنتی پرداخته می‌شود تا ضمن درک بیشتر، مزایا و معایب آن نیز بر خواننده آشکار شود.

بیت‌کوین از فناوری نظیر به نظیر و بدون یک واسطه مرکزی استفاده می‌کند؛ بیت‌کوین یک ارز غیرمتمرکز است که با فناوری نظیر به نظیر مدیریت می‌شود. تمامی فعالیت‌ها مانند انتشار بیت‌کوین، پردازش و اعتبارسنجی معاملات توسط شبکه انجام می‌شود و هیچ واسطه یا مرجع مرکزی برای سرکشی و دخالت در فرایند وجود ندارد. برعکس پول سنتی که توسط بانک مرکزی یک کشور در راستای تعهد این نهاد برای کنترل سیاست‌های پولی منتشر می‌شود.

¹ Central Processing Unit

² Graphical Processing Unit

بیت کوین اصولاً به صورت الکترونیکی وجود دارد: بیت کوین به منظور پول الکترونیکی بودن طراحی شده است، درحالی که پول سنتی اصولاً به صورت فیزیکی است و حساب‌هایی که در بانک‌ها وجود دارد را می‌توان در صورت تمایل به سرعت به وجه نقد تبدیل کرد.

بیت کوین سقف حداکثری ۲۱ میلیون عدد را دارد/است: حداکثر تعداد بیت کوینی که ممکن است تولید شود ۲۱ میلیون است. فرایند استخراج بیت کوین در حال حاضر هر ۱۰ دقیقه ۲۵ بیت کوین تولید می‌کند (نرخ تولید هر ۴ سال نصف می‌شود)؛ بنابراین این مقدار تا سال ۲۱۴۰ تقریباً به حد بالا خواهد رسید. درحالی که منتقدان بیت کوین معتقد هستند که این حد بالا کافی نیست، حامیان بیت کوین بیان دارند، از آنجایی که هر بیت کوین قابل تقسیم تا ۱۰ رقم است، مقدار تقسیم‌های کوچک به اندازه کافی وجود دارد. در مقابل پول سنتی به هر اندازه که نیاز باشد قابل انتشار است که این امر منجر به دست‌کاری ارزش آن توسط دولت‌ها می‌شود.

بیت کوین محصول پیچیده‌ای است: مفهوم ارز مجازی در کل پیچیده و انتزاعی است و فهم اینکه چطور و چرا بیت کوین فعالیت می‌کند، نیازمند سطح قابل قبولی از دانش فناوری اطلاعات دارد. درحالی که پول سنتی برای تمام بشر قابل درک است.

بیت کوین مورد پذیرش عامه نیست: در حال حاضر بیت کوین در میان عامه مردم مورد قبول نیست و در اکثر صنایع کاربرد ندارد؛ اگرچه ممکن است به مرور مقبولیت به دست آورد. برعکس، برای مثال دلار آمریکا به عنوان پول سنتی مقبولیت جهانی پیدا کرده است.

معاملات بیت کوین دارای محدودیت‌هایی است: معامله بیت کوین ممکن است تا ۱۰ دقیقه طول بکشد؛ زیرا زمانی که یک تراکنش انجام می‌شود و وارد شبکه می‌شود باید توسط حداقل شش گره تأیید شود و بعد در بلوک قرار گیرد و زمانی که بلوک کامل شد و مسئله ریاضی حل شد و در نتیجه اجازه قرارگیری بلوک در زنجیره بلوکی از طرف سیستم صادر شد، تراکنش کامل شده است. همچنین معاملات برگشت‌ناپذیر است زیرا بلوکی که در زنجیره قرار گیرد، دیگر امکان تغییر ندارد. چنین محدودیت‌هایی برای پول سنتی وجود ندارد زیرا معاملات کارت‌های اعتباری در کمتر از چند ثانیه تأیید می‌شود و بسیاری از تراکنش‌ها امکان استرداد دارد.

محتوای حساب بیت کوین یک کاربر تضمین شده نیست: یعنی اگر یک کاربر بیت کوین خود را به هر دلیلی گم کند (برای مثال دیسک سخت کامپیوتر نابود شود یا کیف الکترونیکی هک شود و بیت کوین‌ها دزدیده شوند) امکان بازیابی وجود ندارد. درحالی که حساب‌های بانکی در برابر بسیاری از اتفاقات تضمین شده هستند.

در کل با توجه به موارد ذکر شده می‌توان نقاط قوت و ضعفی که باعث روی آوردن بسیاری به بیت کوین و مخالفت عده‌ای دیگر با این سیستم شده است را به شرح زیر ذکر کرد:

- بیت کوین به عنوان اولین نوع پول مجازی توجه عموم را جلب کرده است؛

- بیشترین حجم انتشار بیت کوین ۲۱ میلیون خواهد بود و به همین دلیل منجر به بی‌ارزش شدن به علت عرضه بیش از حد نخواهد شد؛
- بیت کوین به عنوان یک ارز غیرمتمرکز، مستقل از تأثیر و دست کاری دولت است؛
- هزینه های معاملاتی بسیار کمتر از ارزهای سنتی است.

از طرف دیگر معایب ذیل به بیت کوین وارد است:

- از آنجایی که بیت کوین پشتوانه ای ندارد، قیمت بیت کوین شدیداً دارای نوسان است که این امر ارزیابی ارزش واقعی آن را دشوار کرده و ریسک ضرر سرمایه گذاری در ارز مجازی را بالا می برد؛
- گمنامی کاربران بیت کوین ممکن است منجر به استفاده بیت کوین در فعالیت های غیرقانونی و نامشروع مثل فرار مالیاتی، صادرات اسلحه، قمار و دور زدن سیاست های کنترلی ارز شود؛ البته بیان شد که این سیستم دارای شفافیت بیشتری نسبت به پول سنتی است ولی با این حال در سال های اخیر موارد بسیاری از استفاده غیرقانونی گزارش شده است؛
- این حقیقت که بیت کوین فقط به صورت الکترونیکی وجود دارد، منجر به گم شدن و دزدیده شدن آسان آن می شود؛
- بیت کوین برای دولت ها مطلوبیت ندارد زیرا در بسیاری از موارد باعث خارج شدن ارز می شود،

۵- تنظیم و نظارت بیت کوین و قوانین مربوطه

از آنجایی که پول مجازی موضوع به نسبت جدیدی است بحث قانونی و تنظیم و نظارت آن بسیار جای بحث دارد. در کل تلاش بسیاری از دولت ها برای تنظیم قوانین و نظارت بر این سیستم با ماهیت وجودی بیت کوین که به منظور حذف واسطه و مرجع مرکزی است در تناقض می باشد.

به هر حال کشورها و دولت های مختلف، برخوردهای متفاوتی با بیت کوین به عنوان پول مجازی جدید دارند. در کل می توان کشورهای مختلف را بر اساس رویکرد قانونی نسبت به بیت کوین به چهار دسته تقسیم کرد. نخست کشورهایی که نسبت به بیت کوین در حال حاضر منع قانونی ندارند و فعالیت با پول مجازی و خرید و فروش بر اساس بیت کوین ممنوع نیست؛ البته بسیاری از این کشورها در حال تدوین مقررات مختلفی از جمله مقررات مالیاتی برای این سیستم هستند. دسته دیگر کشورهایی هستند که نسبت به بیت کوین بدبین بوده و سعی در نهی مردم، بانک و بورس ها در استفاده از بیت کوین داشته و به دنبال وضع قوانینی هستند که بتوانند تا جای ممکن مانع از گسترش این سیستم شوند، البته فعالیت و معامله با بیت کوین در این کشورها اکیداً غیرقانونی نیست. دسته دیگر کشورهایی هستند که شدیداً نسبت به بیت کوین خصمانه هستند و آن را غیرقانونی اعلام کرده اند که در حال حاضر فقط دو کشور ویتنام و ایسلند چنین شرایطی دارند. دسته چهارم نیز کشورهایی هستند که موضع خاصی نسبت به بیت کوین نداشته یا هیچ اطلاعاتی مبنی بر رویکرد دولت در مورد این سیستم جدید موجود نیست.

تمامی بخش‌های قاره آمریکا جزء دسته اول هستند؛ به جز مکزیک که جز دسته دوم و چند کشور آمریکای جنوبی که جزء دسته چهارم هستند، از جمله ونزوئلا و بولیوی. تمامی بخش‌های قاره آفریقا نیز جزء دسته چهارم هستند، به جز آفریقای جنوبی که جزء دسته اول است. به جز چند کشور غیر پیشرفته اروپایی که جزء دسته چهارم هستند، مابقی اروپا جزء دسته اول هستند. کشورهای همسایه ایران نیز جزء دسته چهارم هستند. کشور چین، روسیه و هند که از لحاظ مساحت و جمعیت در جهان حرف اول را می‌زنند، جزء دسته دوم هستند و به نظر می‌آید که نسبت به بیت‌کوین و استفاده از آن خوش‌بین نیستند و سعی بر جلوگیری از آن دارند. مابقی کشورهای آسیای شرقی اکثراً جزء دسته اول هستند. برای اطلاع از رویکرد دقیق هر یک از کشورها به پایگاه اینترنتی bitlegal.io مراجعه شود.

در آمریکا نیز خزانه‌داری در کل بیت‌کوین را به عنوان یک نوع ارز قابل تبادل با دلار قبول کرده است. به درخواست کمیسیون بورس و اوراق بهادار (SEC)، یک قاضی دادگاه فدرال رأی بر پول بودن بیت‌کوین داده و بیت‌کوین در تعریف اوراق بهادار در قانون بورس و اوراق بهادار ایالات متحده می‌گنجد. شبکه انتظاماتی جرائم مالی آمریکا¹ بیت‌کوین را در دسته پول‌های مجازی قابل تبادل با دلار رده‌بندی کرده است ولی امکان ارز مرجع شدن برای پرداخت‌ها در هیچ حوضه قضایی را ندارد. سرویس درآمد داخلی آمریکا بیت‌کوین را به عنوان دارایی در نظر گرفته است و عایدی ناشی از آن، مانند کسب سرمایه یا درآمد معمولی مردم شامل مالیات می‌شود. البته هریک از ۵۰ ایالت آمریکا تا حدی قوانین و تنظیم و نظارت مختص به خود را دارند و نمی‌توان در مورد تمام ایالات به صورت جامع سخن گفت.

در کل درحالی‌که به نظر می‌رسد که سیستم بیت‌کوین برای ایالات متحده نیز سیستم عجیب و تازه‌ای است و در حال کنترل و وضع قوانین در مورد این سیستم است، لذا با قطعیت نمی‌توان گفت که آیا خود ایالات متحده از رواج این سیستم منتفع است یا خیر!

۶- بحث فقهی بیت‌کوین

«کالا» در فقه و حقوق همان «عین» است. عین نیز مالی است که دارای وجود مادی بوده و با حواس ظاهر، قابل درک باشد و خود به طور مستقل مورد دادوستد قرار گیرد. این مال در مبادلات اقتصادی، خود دارای دو قسم است:

الف- «وجود شخصی»: که دارای وجود عینی و فیزیکی است و در خارج ذهن، وجود خارجی دارد مانند کالایی که در مبادلات نقدی دادوستد می‌شود مانند ماشین، فرش و رادیو.

ب- «وجود کلی»: یعنی کالایی که در روابط مبادلاتی، آن را اعتبار می‌کنند و یک طرف، نسبت به آن متعهد می‌گردد و بر اساس همین تعهد، مبادله انجام می‌شود. مثل اینکه در معاملات «سلف» که تحویل کالا، مدت‌دار و پرداخت پول به صورت نقد، انجام می‌گیرد کالایی که هنوز حتی ممکن است تولید نشده باشد خریداری می‌گردد. به این صورت که بهای آن پرداخت می‌شود و فروشنده تعهد می‌نماید در زمان مشخصی، کالا را تحویل دهد. مانند تحویل گندم به هنگام درو و یا تحویل اتومبیل

¹ Financial Crimes Enforcement Network

پس از تولید. در اینجا آنچه خریداری و مبادله می‌شود در عین حال که جنبه فیزیکی و مادی دارد و دارای ابعاد سه‌گانه می‌باشد، اما تعین خارجی آن مورد توجه نیست بلکه به صورت کلی در «ذمه و عهده» اعتبار شده و موضوع مبادله می‌باشد که در اصطلاح به آن «کلی فی الذمه» می‌گویند.

«سرمایه» هر آن چیزی است که دارای مالیت باشد، هر چند به صورت عین در خارج وجود خارجی نداشته باشد. لذا هر کالایی که مالیت داشته باشد، سرمایه است اما هر سرمایه‌ای، لزوماً کالا نیست (مانند حق تقدم که سرمایه است نه کالا). مالیت، از نگاه فقها با دو شرط محقق می‌شود؛ یکی این که قابل انتفاع بوده و نزد عقلا دارای منفعت قابل توجهی باشد. دیگر این که شارع آن منفعت را حلال شمرده باشد. شرط دیگری که در کلام برخی از فقیهان به آن اشاره شده، این است که شیء از فراوانی برخوردار نباشد به این معنا که به راحتی قابل دسترسی نبوده و به دست آوردن آن نیاز به انجام کاری یا ایجاد معامله‌ای باشد. به گونه‌ای که عقلا برای به دست آوردن آن از یکدیگر سبقت گرفته و باهم رقابت داشته باشند.

«پول» که از دیدگاه فقهی نوعی ابزار سنجش ارزش است، در اصطلاح فقه و حقوق، به واحد ارزش و هر وجه نقدی - اعم از مسکوک یا اسکناس - که به عنوان ثمن در معاملات مورد استفاده قرار می‌گیرد، تعریف شده است. به عبارت دیگر پول به عنوان ارزش مبادلاتی خالص شناخته می‌شود.

بنابراین با توجه به ماهیت دادوستدی پول مجازی، می‌توان آن را جزء پول برشمرد.

۷- نتیجه‌گیری

در این گزارش سعی بر آن شد تا خواننده با ابعاد مختلف بیت‌کوین آشنا شده و مبانی آن بررسی شود. همان طور که بیان شد پول مجازی و مخصوصاً بیت‌کوین، چند سالی است که وارد عرصه کسب و کار در جهان شده، اما هنوز به صورت فراگیر مورد استقبال مردم قرار نگرفته است. مزایا و معایب این پول باعث شده تا دولت‌ها به فکر فرو روند تا این نوع پول را به عنوان ارز رایج بپذیرند یا رد کنند. همچنین آینده این پول نیز نامشخص است و به نظر می‌رسد در سال‌های اخیر با به وجود آمدن پول‌های مجازی دیگر، رقابت بین آن‌ها شدیدتر شده و دولت‌ها به دنبال این هستند که قوانین مربوطه را به روز کنند. در انتها می‌توان گفت که در حال حاضر ورود به عرصه تجارت با پول مجازی و یا سفته‌بازی با آن بسیار پر ریسک است و دولت باید ابعاد مختلف آن را برای عموم مردم شفاف‌تر کند و همزمان قوانین و مقررات مرتبط با آن را ارائه دهد.

۸- منابع

{۱} حکیم، سید محسن طباطبایی، **نهج الفقاهة**، انتشارات ۲۲ بهمن، قم، بی تا.

{۲} خویی، ابوالقاسم موسوی، **مصباح الفقاهة**، بی تا.

{۳} حسنی، هاشم معروف، **نظریة العقد فی الفقه الجعفری**، منشورات مکتبہ هاشم، بیروت، بی تا.

{۴} سید عباس موسویان، **فرهنگ اصطلاحات فقهی و حقوقی معاملات**، پژوهشکده پولی و بانکی، ۱۳۸۶.

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Consulted* 1.2012 (2008): 28.

[6] Jerry Brito, "Online Cash Bitcoin Could Challenge Governments, Banks" *Times Magazine*, 16-Apr-2011.

[7] FRAN BERKMAN, "A Complete, Interactive History of Bitcoin," *Mashable.com*, 11-Feb-2014.

[8] Bitcoin Organization, "BitCoin for Individuals." [Online]. Available: BitCoin.org.

[9] Wikipedia, the free encyclopedia, "Bitcoin." [Online]. Available: <http://en.wikipedia.org/wiki/Bitcoin>.

[10] Investopedia Staff, "How Bitcoin Works," Jul. 2013.

[11] John Kelleher, "What is Bitcoin Mining?" Investopedia, Apr. 2014.